XXII

22nd International Symposium

In Memory of Dr. Sam Mannan

In Association with IChemE

2019

PROCEEDINGS

MARY KAY O'CONNOR
PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

Table of Contents

Life After A Risk-Based Inspection Implementation
Justin Daarud

Are you struggling with your Asset Integrity program?
Katherine Anderson and Neil Prophet

Choosing Functional Safety Field Instrumentation - Certified Vs Prior Use. Justification of VDI 2180 simplified equations
Gene Cammack and Luis Manuel Fernando Garcia Garcia

Leveraging the Power of Industry 4.0: ORM Digital Twin for Process Industry
Abhilash Menon

On Model-Based Systems Engineering for Design, Management, and Governance of Protective Systems
Antonio Arreola-Risa, Dr. Diana Gallart Hamilton, M. Sam Mannan, Paul Nelson, and Martin A. Wortman

Analysis of Reliability Mapping in Refining Industry: Identification of Critical Regions and Interventions in Complex Production Systems
Cassio Brunoro Ahumada, Érica Cayres, and Salvador Ávila Filho

Practical Considerations for Overfilling Scenario Applicability
Houston Haile and Robert (Bob) Siml

Refrigerated Tanks Base Plate-Heating Hazards – A Case Study of Ethylene Tanks
Mahmoud Mohamad Hassan, Dr. Mahesh Murthy, Pulak Pal, and Gys Van Zyl

Day 1 Track 2

A Practical Approach to Preventing Systematic Error in the Maintenance of Instrumented Safeguards
Eloise Roche and Angela Summers

Managing an Instrumented Protective Systems Program for a Petrochemical Facility
J. Gregory Hall

PPE - Can you have too much of a good thing?
Brenton L. Cox, Sean J. Dee, Russell A. Ogle, and Matthew S. Walters

Behaviour-Based Safety
Dr. Ramesh V.M.

Effective Remedies for Enhancing Safe Operations Through Analysis of Organizational Safety Climate
Shawn Bayouth, Matthew E. Harvey, and Nir Keren

Engaging Your Safety Culture Appreciatively
Dana Cooper

Crude Oil by Rail Accidents: Cross-industry Learning for High Hazard Sectors
Gabor Posta

Are biases towards the recent past causing us to unintentionally expose personnel to increased levels of risk?
Alexander I. Fergusson and Karen Vilas

The Importance of Misalignment to Reduce Risk and Prevent Disasters
Mark Galley

Day 1 Track 3

Reverend Bayes, Meet Process Safety: Use Bayes' Theorem to establish site specific confidence in your LOPA calculation
Keith Brumbaugh and Dave Grattan

Confidence Level Assessment in Enterprise Risk Management: Case Study with Focus on Oil & Gas Production Incidents
Henrique Martini Paula and Magdalena Soto-Ogaz

A New Look at Release Event Frequencies
Benjamin R. Ishii and Jeff Marx

Fault Tree Uncertainty Analysis
Raymond "Randy" Freeman

Assessment of Hazard Analysis and Implementation of STPA in Process Industry
Parveen Chahal, Javeed I Mohammed, and Christina Ngo

Quantitative Review of Storage Tank Performance in Extreme Weather Events (Hurricanes, Flooding, Rainfall)
Philip E. Myers and George Woodworth

Analysis Oxygen Piping Layout to Eliminate High Consequences Risk
Suprayudi Kadir and Dr. Mahesh Murthy

Quantitative Assessment and Consequence Modeling of Deliberately Induced Domino Effects in Process Facilities
Priscilla George and V. R. Renjith

Develop a Hazard Index Using Machine Learning Approach for the Hazard Identification of Chemical Logistic Warehouses
Qingsheng Wang, Mengxi Yu, Shuai Yuan, and Zhuoran Zhang

Day 1 Track 4

Dust Explosions and Collapsed Ductwork
Brenton L. Cox, David C. Hietala, and Russell Ogle

The Nature of Flammable Cloud Volumes in Semi-confined Environment under the Influence of Flow of Air
Karen Silgado Correa, Tatiele Dalfior Ferreira, and Savio Vianna

Image processing techniques for the characterization of explosively driven dispersions
J.M. Buchlin, S. Courtiaud, Charline Fouchier, D. Laboureur, and E. Lapébie

Storage vessels in the proximity of wild fires
V. Casson Moreno, V. Cozzani, M. Papadaki, and G.E. Scarponi

SafeOCS Industry Safety Data - The Value Proposition for the Oil & Gas Industry
Demetra V. Collia and Roland Moreau

Modelling Ice and Wax Formation in a Pipeline in the Arctic Environment
Ben Bbosa., Zhengdong Cheng, Dali Huang, M. Sam Mannan, Michael Volk, and Hongfei Xu

External Fire Impacts on the Interior Temperature of a Building
Benjamin Ishii and Cristian Jimenez

Experimental Study of an Iron-Based Metal-Organic Framework as Flame Retardant for Poly (methyl methacrylate) (PMMA)
Elizabeth Joseph, Ruiqing Shen, Qingsheng Wang, and Hongcai Zhou

Development of a Blast-Resistant Roller Shutter Door
Darrell Barker, Jerry Collinsworth, and John Puryear

Day 2 Track 1

Lessons from Risk Assessment of 6th Generation Drill-ships and Sem-Submersibles
Wael Abouamin

Study of FSRU-LNGC System Based on a Quantitative Multi-cluster Risk Informed Model
Mahmoud M. El-Halwagi, Chenxi Ji, Zeren Jiao, M. Sam Mannan, Hans J. Pasman, James Pettigrew, and Shuai Yuan

How to Improve the Trust in Safety Related Sensors
Wolter Last

Biocompatible Herder for Rapid Oil Spill Treatment over a Wide Temperature Range
Mingfeng Chen, Zhengdong Cheng, Dali Huang, Shijun Lei, Rong Ma, M. Sam Mannan, Roshan Sebastian, Abhijeet Shinde, Hongfei Xu, and Lecheng Zhang

Hurricanes Versus Tropical Storms Impacts – Shut-down? Recovery?
Kumar (Chris) Israni and Yaneira Saud

Exposure of Fabrics Used in Personal Protective Equipment to Combustible Dust Flash Fires
Claudio V.B. Favero, Sean C. O'Hern, Alfonso Ibarreta, Timothy J. Myers, Michael C. Stern, and James Vickery

Integration of Process Safety into Engineering Design during Offshore Project Execution
Jeff Bryant, Charlie Gerschefski, Edward Liu, and Steven Zhang

A Case Study From a Fire Incident in Naphtha Heater Caused by Sulfidation
Kevin Chao Pin Wen

How to Treat Expert Judgement? With certainty it contains uncertainty!
Hans Pasman and William J. Rogers

Lessons Learned - How to Make Them Stick
Jack Chosnek

Day 2 Track 2

Analyzing Procedure Performance using Abstraction Hierarchy: Implications of Designing Procedures for High-risk Process Operations
Nilesh Ade, S. Camille Peres, Farzan Sasangohar, and Changwon Son

Relationship Between Human-Managerial and Social-Organizational Factors: For Industry Safeguards Project: Dynamic Bayesian Networks
Cassio Ahumada, Jade Ávila, Salvador Ávila, and Beata Mrugalska

Exploration of relationships between safety performance and unsafe behavior in coal mining processes
Trent Parker, Ruipeng Tong, Qingsheng Wang, Xiaoyi Yang, and Boling Zhang

Reduce Human Error: Mistake-Proof Procedures and Create an Effective PPE Grid
Nicole Loontjens

Beyond Participation—A Case Study for Driving Employee Engagement in Your Process Safety Program
Tony Bocek

Options for teaching Operational Process Safety
Trish Kerin

Operator Error or Management Failure? Management's Role in Maintaining Operator Discipline
Marc Rothschild

The Future of the United States Chemical Investigation Board: Opportunities and Challenges
Rick Engler

Unravelling Reactive Chemicals Mysteries: Experiences in Reactive Chemicals Incident Investigations
Robert Bellair

We Don't Learn Enough from Incidents: the Roots of Human Errors
Monica Philippart

Day 2 Track 3

Managing Tanks as a Portfolio of Assets
Phil Beccue, Dan Brooks, and Philip Myers

Day 2 Track 4

Finding Health & Safety Buried Treasure with AI
Tom Garvin and Scott Kimbleton

Smart machine learning analytic tools for alarm rationalization
Tongwen Chen, Wenkai Hu, and Sirish Shah

Opportunities and challenges of high-level visualization technology in process operations and safety
Shawn Bayouth, Matthew E. Harvey, and Nir Keren

Unified Hazard Assessment - Bringing Together HAZOP, LOPA, Hazard Registers, and Bowtie in a Unified Structure
Edward Marszal

Measurement for decomposition of lithium ion battery electrolytes with STA-MS and risk assessment of toxic gases
Ji Yun Han, Seungho Jung, and Jeongwook Seo

Quantitative Structure-Property Relationships Methods to expedite Reactive Chemicals Hazards Assessment Processes
Harold U. Escobar-Hernandez, M. Sam Mannan, Maria I. Papadaki, Qingsheng Wang, and Hong-Cai Zhou

Mitigation of a Reactive Relief Case by Instrumentation in Lieu of a Relief Device: A Case Study
Aristides Morillo

Comparison of Explosion Methods for Large-Scale Unconfined Elongated Explosions with Propane and Methane mixtures
Cassio Brunoro Ahumada, Pratik Krishnan, Frank-Ioannis Papadakis-Wood, Noor Quddus, Qingsheng Wang, and Shuai Yuan

Modeling of Vented Deflagration Fireball Hazard
Francesco Colella, Alfonso Ibarreta, Timothy J. Myers, Sean C. O'Hern, Malima Wolf, and May Yen

Heavy gas concentration prediction on complex terrain using CFD with Monin-Obukhov similarity theory
Charles Glover, Delphine Laboureur, and Jiayong Zhu

Day 3 Track 1

PSM Alarm Management – "It's Alarming"
Dana Cooper

Safeguards Verification
Abdullah AlMulla

Data-Driven Prescriptive Maintenance Scheduling and Process Optimization
Baris Burnak, Christopher Kwadwo Gordon, Melis Onel, and Efstratios N. Pistikopoulos

More effective use of Leading Indicators
Gregg Kiihne

Day 3 Track 2

Procedural Systems as Independent Layers of Protection: Are We Giving More Credit Than is Due?
S Camille Peres

Analysis of the Low Perception of Risk: Causes, Consequences and Barriers
Cassio Brunoro Ahumada, Salvador Ávila Filho, and Lucas Menezes Pereira

Enhancing Safety Through strengthening Human Barrier
Abdulla Al-Azmi, Abdulrahman Al-Hajri, Bala Siva Srikanth Adivi, Sridhar Ketavarapu, and Vishal Sawlikar

Crosswalk of Human Reliability Methods of Offshore Oil Incidents
Ronald L. Boring, Dr. Tina Miyake, Jooyoung Park, and Thomas A. Ulrich

Day 3 Track 3

How Dynamic Simulation Helped Mitigate Vapor Disposal System
Kartik Maniar and Omi Soni

Fire and Gas Hazard Mapping Continues to Require Engineering Judgment
James McNay and William Pittman

Inherent Safety as a driver for business success in the Oil & Gas Industry
Hari Attal and Noma Ogbeifun

Studying the Inherent Safety of Flare Utilization Alternatives during Abnormal Operations
Fadwa Eljack, Vasiliki Kazantzi, Nikolaos K. Kazantzis, and Monzure-Khoda Kazi

Day 3 Track 4

Impact of particle density on dust cloud characteristics in the minimum ignition energy testing apparatus using high-speed digital in-line holography
Pranav Bagaria, Purvali Chaudhari, Waruna Kulatilaka, Chad Mashuga, Ankit Saini, and Christian Schweizer

Modelling of the plume rise phenomenon due to warehouse fires considering penetration of the mixing layer
Hans Boot and Sonia Ruiz-Perez

Collision of Convex Objects for Calculation of Porous Mesh in Gas Explosion Simulation
Tatiele Dalfior Ferreira and Savio Vianna

Effects of non-uniform blockage ratio and obstacle spacing on flame propagation in premixed H2/O2 mixtures
Cassio Brunoro Ahumada, Eric L. Petersen, and Qinsheng Wang

Additional Manuscript

Determination of Corrosion Velocity in Industrial Equipment Working under Dual Environments, Combustion and Steam. Case Study: ASTM A335 P91 Steel
Anibal Alviz-Meza, Dario Y Peña-Ballesteros, Adam Duong, and Viatcheslav Kafarov

Poster Presentations

Speaker Biographies

WELCOME TO THE 2019 ANNUAL INTERNATIONAL SYMPOSIUM PROCEEDINGS

I am delighted to welcome you to the 2019 Annual Symposium of the Mary Kay O'Connor Process Safety Center Proceedings. The 2019 Symposium is the 22th in the series, and it honors the memories of our namesake, Mary Kay O'Connor, and our founding director, Professor M. Sam Mannan. The symposium is an important annual event that focuses on research, education, training and service issues that impact safety. Your participation is essential to make the symposium a success, and ultimately to advance process safety technologies and concepts that will make industry safer. We believe that proactive safety programs are good business and have a positive impact on the bottom line.

The objectives for holding this annual symposium are three-fold. First, this annual event provides stakeholders with research reports and updates on the activities and programs of the center. Second, we strongly believe that the center can help solve the complex and intriguing problems faced by the industry. Having identified these problems in discussions at the symposium, the extensive expertise and resources available at the center can be brought to bear through research and educational programs to solve the problems. Finally, we believe this symposium provides an independent and unbiased forum for exchange of ideas and discussion among academia, industry, regulators and the general public.

These proceedings contain the symposium program, the papers presented at the symposium and submitted before the deadline, and other informative items from the center.

We wish you maximum benefit from this symposium and strongly encourage you to participate in the discussions. Please feel free to contact me or other center personnel with your ideas and input regarding the symposium and other activities of the center. We encourage all stakeholders to participate in all the other activities of the center. We also extend to you a warm welcome to Texas A&M University, and to the Bryan/College Station area. We hope your stay here is fruitful and enjoyable.

James C. Holste, Ph.D., P.E.
Interim Director, Mary Kay O'Connor Process Safety Center
Senior Professor, Artie McFerrin Department of Chemical Engineering – TAMU

2019 Symposium Sponsors

THANK YOU!

Your support is integral to the success of this important event.

Symposium Banquet Sponsor

台塑關係企業
FORMOSA PLASTICS GROUP

Mobile App Sponsor

GEXCON

Exhibit Sponsor

Thornton Tomasetti

Media Sponsors

WWW.CHEMICALPROCESSING.COM
CHEMICAL PROCESSING
LEADERSHIP | EXPERTISE | INNOVATION

CHEMICAL ENGINEERING
ESSENTIALS FOR THE CPI PROFESSIONAL

Process Safety in the 21st Century

As an industry, our inability to learn from past incidents and demonstrate that process safety is improving has led to the project Process Safety in the 21st Century and Beyond. The aim of this project is to envision better process safety by outlining efforts that each stakeholder can take.
How was the project undertaken?

Gaining a global perspective of the key challenges in process safety is the first important step. The challenges were considered across four stakeholders: industry, academia, regulators, and society. To determine the challenges, a series of workshops at international symposia were undertaken, including in the UK (with input from other European countries), North America, Asia, Australia/New Zealand, and the Middle East. Various methods of consultation were used, but the key questions remained consistent. In process safety:

- What are the key industry challenges?
- What are the key academic challenges?
- What are the key regulatory challenges?
- What are the key societal challenges?

These questions were answered by professionals from various levels in industry, academia, and regulatory bodies. Once the challenges were identified, a top five list was drawn up for each stakeholder group.

Our goal with this document is to lay out a series of actions to be undertaken at various levels and across all stakeholders to improve process safety because people have a right to not get hurt. To enable this vision, this roadmap is a call to action to all stakeholders and not just process safety professionals.
We invite you to look at the opportunities and think about how you can influence them and positively impact process safety. Every professional is obliged to improve process safety because engineering and science are essential to us all and it must be sustainable in all senses of the word, including process safety. If we, as engineers, do not develop new strategies for continuous improvement, the engineering profession will become irrelevant to society and the need for process safety will become extinct, thus increasing process safety incidents. A question that needs to be answered is where this roadmap is intended to take us. The simple answer is that the roadmap and the associated journey are focused towards improvements in process safety performance, which will ultimately lead us to our vision of zero incidents.

In Association with **IChemE**

The Institution of Chemical Engineers (IChemE) is the global professional membership organization for chemical, biological and process engineers and other professionals involved in the chemical, process and bioprocess industries. With a membership exceeding 44,000 members in over 120 countries, and offices in Australia, New Zealand, Singapore, Malaysia and the UK; IChemE aims to be the organization of choice for chemical engineers.

We promote competence and a commitment to the best practice, advance the discipline for the benefit of society and support the professional development of our member. We are the only organization licensed to award Chartered Chemical Engineer and Professional Process Safety Engineer status.

IChemE exists because chemical engineering matters.

OUR MISSION

IChemE's four key aims are:

- To build and sustain an active international professional community, united by a commitment to qualifications and standards that foster excellence and the delivery of benefits to society.

- To engage with others to promote development, understanding of chemical engineering and an appreciation of its importance.

- To provide support and services to individuals, employers and others who contribute to improving the practice and application of chemical engineering.

- To enable chemical engineers to communicate effectively with each other and with other disciplines.

To support these aims, we operate as an effective, efficient and responsive organization, providing leadership and demonstrating good practice as well as complying with our obligations as a charitable organization.

IChemE is a registered charity in England & Whales (214379) and a charity registered in Scotland (SC 039661).

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Awards and Scholarships

Trevor Kletz Merit Award

The Merit Award recognizes an individual who has made significant contributions to the advancement of education, research, or service activities related to process safety concepts and/or technologies. The contributions or accomplishments leading to the annual Merit Award need not be associated with the Center but must fit within the central theme of the Center, i.e., Making Safety Second Nature. In establishing the Merit Award, the Steering Committee underscores the importance of promoting and recognizing significant contributions and accomplishments of practitioners and researchers worldwide.

The Harry H. West Memorial Service Award

The Service Award was established by the Steering Committee to honor and recognize individuals who have contributed directly to the success of the Center and have played a significant role in advancing the mission of the Center.

Lamiya Zahn Memorial Safety Scholarship

On July 31, 2004, an explosion and fire occurred in a university apartment on the Texas A&M University campus. Four members of the family of Saquib Ejaz, a chemical engineering graduate student - were critically injured and hospitalized. Saquib's mother and his four-year old daughter, Lamiya Zahin subsequently died from injuries sustained in the fire.

In fond and living memory of Lamiya, the Department of Chemical Engineering and the Mary Kay O'Connor Process Safety Center have established the Lamiya Zahin Memorial Safety Scholarship. Graduate students are encouraged to apply for the $1,000 scholarship by writing a 1000-word essay on "Safety Innovations in Research Projects".

Dr. Mannan Endowed Scholarship

Dr. M. Sam Mannan, executive director of the Mary Kay O'Connor Process Safety Center (MKOPSC), passed away on Tuesday, Sept. 11, 2018. Dr. Mannan's work at the MKOPSC has influenced the entire chemical engineering industry in the U.S. and worldwide. Process safety, which was once seen as little more than wearing safety goggles or a lab coat, has become one of the most important areas of chemical engineering. Throughout Dr, Mannan's more than 20 years with the center, the MKOPSC has been a driving force in industry's adoption of more rigorous safety standards.

To honor the legacy of Dr. Mannan, the Artie McFerrin Department of Chemical Engineering has established an endowed scholarship in his name. The Dr. Sam Mannan Endowed Scholarship is designed to prepare chemical engineers for leadership roles in in the process safety field, and will be awarded to a student pursuing an undergraduate degree in Chemical Engineering with a minor in Safety Engineering from Texas A&M University.

Trevor Kletz Merit Award Recipient

Kathy Shell, PE

Executive Vice President, Process Safety & Lifecycle Solutions (aeSolutions)

Kathy has over 35 years of experience in the areas of business and project management, process and detailed design, installation and commissioning. She specializes in the strategic development, rollout, implementation, training and auditing of global and site level process safety risk managements systems.

A senior member of AIChE, Kathy is Chair of the 2018 Global Congress on Process Safety (GCPS). In the past she has held leadership positions at the Global Congress, including chairing and co-chairing the Process Plant Safety Symposium (PPSS) and serving as PPSS Session Chair and Co-Chair. She is a member of the Center for Chemical Process Safety (CCPS) Technical Steering Committee and the Health and Safety Division.

In addition, Kathy is a current member of the steering team and past member of the technical advisory committee for the Mary Kay O'Connor Process Safety Center at Texas A&M University. Kathy is a licensed Professional Engineer and has a B.S. degree in Chemical Engineering from the University of Akron in Ohio. Kathy enjoys bicycling, hiking, and going to classic rock concerts whenever possible.

The Mary Kay O'Connor Process Safety Center would like to recognize and thank the 2019 International Symposium award recipients who have worked tirelessly to assist the center in continuing the theme of Making Safety Second Nature both through their time dedicated to the center as well as through their work worldwide.

Harry West Service Award Recipients

Henry Goyette, PE

Research Fellow and Volunteer Mentor, Mary Kay O'Connor Process Safety Center

Henry Goyette is a volunteer Research Fellow at the Mary Kay O'Connor Process Safety Center at Texas A&M. He currently mentors students with regard to research topics, presentation skills, and career paths. He obtained a bachelor's degree in Environmental Studies from Rutgers University and a master's degree in Environmental Health Engineering from the University of Texas at Austin. He began his career at IBM as a staff environmental engineer at an Austin printed circuit board plant.

He then joined Environmental Resources Management (ERM) where he spent 25 years as a consultant assisting petroleum refinery and chemical plant clients with environmental compliance issues. He is a registered professional engineer in Texas, Louisiana, and Illinois, and resides in Houston.

Stewart Behie, PhD

Manager, Safety and Process Risk Occidental Oil and Gas Corporation (Oxy)

Stewart Behie is Manager, Safety and Process Risk in the corporate HES Risk Management group in Occidental Oil and Gas Corporation's (Oxy) Houston office. In this role, Dr. Behie provides technical risk engineering support and guidance to domestic and international business units.

Dr. Behie has been involved in the Center for over 7 years since moving to Houston. Oxy rep on the Steering Committee Member of the Risk Communication subcommittee of the SC that worked with a number of student volunteers to develop communication pieces for different age groups to explain the differences between Hazard and Risk (team was awarded the Harry West Service Award in 2015). Member of the Vision 25 team that work over the past few years to develop a Strategic Plan for the Center for the next 25 years. The final draft of this plan was rolled out to the Steering Committee a few weeks ago. Stewart holds Bachelor, Masters and doctoral degrees in Chemical Engineering.

Lamiya Zahin Memorial Safety Scholarship Recipient

Ahmed Harhara

PhD Chemical Engineering Student, Texas A&M University

Ahmed is a fourth year chemical engineering PhD student at the Mary Kay O'Connor Process Safety Center. His research focuses on integrating process safety and optimization. A native of Michigan, Ahmed completed his bachelor's degree from Wayne State University. His experience includes working in the automotive and oil & gas industry. At Texas A&M, he has served as the president of two student organizations and one year representing the College of Engineering as a student senator. In his spare time, Ahmed enjoys traveling, cooking, and reading.

Dr. Mannan Endowed Scholarship Recipient

Shantanu Sonthalia

Chemical Engineering Undergraduate Student, Texas A&M University

Shantanu Sonthalia is a senior from Houston at Texas A&M, where he is majoring in chemical engineering with a safety engineering certificate. His interest in safety started after the Deepwater Horizon Oil Spill. Inspired by this incident, he pursued learning about safety and preventing future incidents. On campus, he has helped put on "Aggies Invent- Energy Solutions" and promoted diversity through Student Government. He has also interned with Air Liquide and aspires a career that can make a significant contribution to the energy industry. When he is not busy studying for exams, he enjoys playing tennis and volunteering.

2019 MKOPSC **Consortium Members**

PARTNERS

- Albemarle
- Bayer
- BHP Billiton
- BP America, Inc.
- Cheniere Energy
- Chevron
- ConocoPhillips
- Dow Chemical Company
- Eastman Chemical
- Evonik
- ExxonMobil
- Formosa Plastics
- Huntsman Corporation
- Occidental Petroleum Corporation
- Pemex
- P66
- Reliance
- Reliance Industries
- Saudi Aramco
- Shell
- Total Petrochemicals & Refining

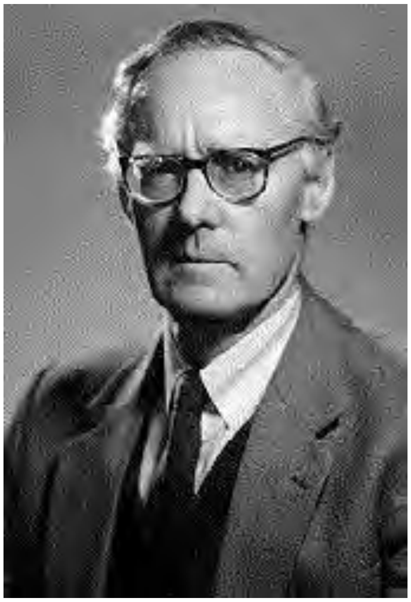
SPONSORS

- ABS Consulting
- AcuTech Consulting
- aeSolutions
- Atkins Global
- DNV GL
- FM Global
- Gexcon
- HIMA Americas
- Honeywell
- INEOS
- KBR
- Lloyd’s Register
- MMI Engineering
- Siemens

ASSOCIATES

- Environmental Intellect
- Kestrel Management Services

Frank P. Lees Memorial Lecture



Frank P. Lees
1931-1999
Emeritus Professor of
Chemical Engineering
Loughborough University,
United Kingdom

Frank P. Lees is noted for his monumental three-volume work, Loss Prevention in the Process Industries (2nd edition, 1996), an extraordinary accomplishment for one man and an outstanding compendium of our present knowledge of process safety. It is not, however, a scissors and paste job, a mere collection of other people's thoughts; he thoroughly surveyed and evaluated present knowledge and provided his own comments on it. Lees also produced an immense amount of original work, particularly on QRA, HAZOP, consequence analysis and computer applications, and trained a generation of students to follow in his footsteps.

The Mary Kay O'Connor Process Safety Center recognizes the contributions made by Frank Lees to the field of process safety and loss prevention. His teachings and findings will be the guiding light and inspiration for many in this generation and future.

Mr. Wascom delivered the 2019 Frank P. Lees Memorial Lecture.

Day 1 Keynote Speaker

Mr. D. G. (Jerry) Wascom

Safety, Security, Health & Environment, Exxon Mobil Corporation

Mr. D. G. (Jerry) Wascom is Vice President, Operational Excellence – Safety, Security, Health & Environment, Exxon Mobil Corporation. Mr. Wascom graduated with a Bachelor's Degree in Mechanical Engineering from Louisiana State University in 1978. He joined Exxon Company, U.S.A. as an employee at the Baton Rouge Refinery in 1979 and progressed through various engineering and supervisory positions.

In 2006, Mr. Wascom moved to Tokyo where he was appointed President and CEO of ExxonMobil Japanese companies and Refining Director of Asia Pacific with responsibility for managing refining operations in Asia Pacific. In April 2009, he returned to Fairfax as Director, Refining Americas, ExxonMobil Refining & Supply, overseeing refining operations in North and Central/South America.

In July 2013, he was appointed Director, Refining North America, ExxonMobil Refining & Supply, overseeing a total of 10 refineries in the USA and Canada. In August 2014, he was appointed President, Refining and Supply. In January of 2018, Mr. Wascom became the Vice President of Operational Excellence - Safety, Security, Health & Environment, Exxon Mobil Corporation.

Dr. Jim Holste presented the 2019 International Symposium Keynote Award to Mr. Jerry Wascom.

Day 2 Keynote Speaker

Dr. Elaine Oran

Department of Aerospace Engineering Texas A&M University

Elaine S. Oran is TEES Eminent Professor in the Department of Aerospace Engineering at Texas A&M University. She also is a Visiting Professor at the University of Maryland, where she is affiliated with Aerospace Engineering, Mechanical Engineering, the Institute for Physical Sciences and Technology, and the Department of Fire Protection Engineering. Dr. Oran is also emerita Senior Scientist for Reactive Flow Physics at the Naval Research Laboratory (NRL). She is currently an adjunct professor of Aerospace Engineering at the University of Michigan and a visiting scientist at the Institute for Advanced Study at Hong Kong University of Science and Technology and Tsinghua University in Beijing.

Dr. Oran received an A.B. in chemistry and physics from Bryn Mawr College and both a M.Ph. in Physics and a Ph.D. in Engineering and Applied Science from Yale University. She is a member of the National Academy of Engineering, an Honorary Fellow of the AIAA, and Fellow of the American Academy of Arts and Sciences, the AIAA, APS, SIAM, ASME, and the Combustion Institute. She has received honorary doctorates from Leeds University, Ecole Central de Lyon, and the Institut National des Sciences Appliques Rouen.

Dr. Jim Holste presented the 2019 International Symposium Keynote Award to Dr. Elaine Oran.

Day 3 Keynote Speaker

Dr. Andrew Hopkins

College of Arts and Social Science, Australian National University

Andrew Hopkins is Emeritus Professor of Sociology at the Australian National University in Canberra. He was an expert witness at the Royal Commission into the 1998 Exxon gas plant explosion near Melbourne.

He was a consultant to the US Chemical Safety Board in its investigation of the BP Texas City Refinery disaster of 2005, and also for its investigation into the BP Gulf of Mexico oil spill of 2010.

He has a BS and an MA from the Australian National University, a PhD from the University of Connecticut and is a Fellow of the Safety Institute of Australia. He was the winner of the 2008 European Process Safety Centre safety award, the first in time it was awarded to someone outside Europe. He is an honorary fellow of the Institution of Chemical Engineers in recognition of his "outstanding contributions to process safety and to the analysis of process safety related incidents". He is an Officer of the Order of Australia (AO) in recognition of his "distinguished service to industrial safety and accident analysis".

Dr. Jim Holste presented the 2019 International Symposium Keynote Award to Dr. Andrew Hopkins.

Symposium Coordinators, MKOPSC

Sheera Helms
sheera@tamu.edu

Paola Camposeco
paolacamposeco@tamu.edu

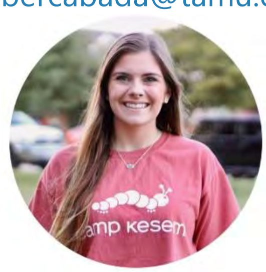
Symposium Student Assistants

Jesus Alvarez
jcarbajal9725@tamu.edu

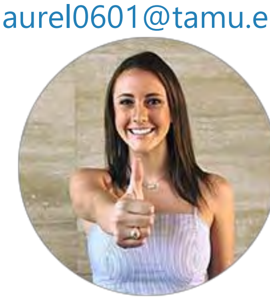
Amber Cabada
ambercabada@tamu.edu

Laurel Patterson
laurel0601@tamu.edu

Pedro Alvarez
p.alvarez10@tamu.edu



Lauren Jodry
lauren.jodry@tamu.edu



Lunden Patterson
lunden12@tamu.edu

Program Technical Committee

The Mary Kay O'Connor Process Safety Center would like to recognize and thank the **Track Leads and Track Chairs** who have volunteered their time to assist with the abstract review, selection process, and session coordination. Their input, expertise, and leadership have been essential to the Symposium's success.

Committee Lead

Stewart Behie, Oxy
Stewart_Behie@oxy.com

Track I Lead: Management, Operational, and Offshore

Trish Kerin, IChemE
TKerin@icheme.org

Track III Lead: Design and Analysis

Robert Bellair, Dow
RJBellair@dow.com

Track II Lead: Human Factors – People in Action

Jeff Thomas
jjt1234@aol.com

Track IV Lead: Research and Next Generation

Nick Gonzales, Shell
nick.gonzales@shell.com

Symposium Track Chairs

Track I Chairs: Management, Operational, and Offshore

Elise Diaz, Chevron
EDiaz@chevron.com

Yuan Lu, Oxy
yuan_lu@oxy.com

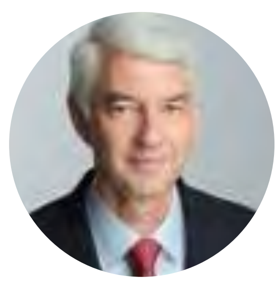
Murtaza Ghandi, BakerRisk
mgandhi@BakerRisk.com

Mike Marshall, USDOL-OSHA
marshall.mike@dol.gov

Track II Chairs: Human Factors – People in Action

Marc Saenz, aeSolutions
Marc.Saenz@aesolns.com

Sara Saxena, BP
Sara.Saxena@bp.com



Mark Slezak, Oxy
Mark_E_Slezak@oxy.com

Track III Chairs: Design and Analysis

Robert Bellair, **Dow**
RJBellair@dow.com

Jim Pettigrew, **OESI**
jim.pettigrew@tamu.edu

Jiaojun Jiang, **Oxy**
Jiaojun_Jiang@oxy.com

Jeremiah Sturgeon, **Oxy**
Jeremiah_Sturgeon@oxy.com

Track IV Chairs: Research and Next Generation

Hari Attal, **Chevron**
Hari.Attal@Chevron.com

Katie Mulligan, **Dow**
KAMulligan@dow.com

Nick Gonzales, **Shell**
nick.gonzales@shell.com

Brenton Drake, **Dow**
bdrake1@dow.com

Saandi Laskar, **Oxy**
Sandipan_Laskar@oxy.com

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Advancing Assets Integrity Management to Meet Safe, Reliable, and Sustainable Operations

Abdul Aldeeb*
Siemens Energy, Inc.
Houston, Texas
*Presenter E-mail: abdul.aldeeb@siemens.com

Abstract

Mechanical Integrity experts can articulate the many benefits of being able to effectively manage a process assets mechanical integrity. However, the significance of assets mechanical integrity means many things to different stakeholders; management, operations, maintenance, projects, and HSE, but all can agree on some common benefits that must be achieved. These include the benefits of maintaining safe operation, contained hazardous components, increased profitability, operation sustainability, earning the license to operate, and grow the business.

The goal of any successful assets mechanical integrity management program is to safely extend the assets life and maximize the operation efficiency and productivity.

Although many operators spend significant effort to establish such programs; however, most recent regulatory and expert audits reveal common mistakes, challenges, and failures. Many of the findings are contributed to limited visibility of the operational risk and inadequate resources.

In this presentation, an overview of how process industry can benefit from recent data analytics and digitalized technology advancements to drive effective assets integrity management programs will be discussed. Technology advancements, if effectively utilized, will lead to better identification of leading and lagging performance indicators and more robust continuous program improvement.

Keywords: Assets Integrity Management, operational risk, performance indicators, analytics

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Life After a Risk-Based Inspection Implementation

Justin Daarud*
Cognascents Consulting Group, LLC
1519 Vander Wilt Lane, Building 4
Katy, TX 77449
*Presenter E-mail: justin.daarud@cognascents.com

Abstract

Many chemical and oil and gas organizations have Risk-Based Inspection (RBI) programs in the form of the American Petroleum Institute (API) API Recommended Practice (RP) 580 Risk-Based Inspection program. Numerous organizations have software databases or software tools that enable the RBI program to function. These same organizations also struggle to ensure that the RBI program performs to expectations following the initial implementation project. Organizations purchase a software expecting this tool to produce the results claimed about a RBI program once it is populated with their data, but then fail to identify that their RBI program requires a systematic approach, combined with personnel expertise and knowledge of the processes to achieve a fully functional and effective RBI program. "Life After a Risk-Based Inspection Implementation" gives simple examples through case studies to identify what to do after a RBI Implementation to produce the kind of results that can be achieved through an effective and sustainable RBI program. These case studies reveal that when a RBI program is managed appropriately, it becomes sustained and valuable, thus leading to the prevention of failures, the added effectiveness and value creation of the inspection, reliability, and maintenance program, and an increase in knowledge to help aid the decision makers produce high yield results.

Keywords: Risk-Based Inspection, RBI, API RP 580, Implementation, RBI Software, RBI Database, Inspection Plans

Introduction

Risk-Based Inspection (RBI) Programs have been implemented and executed within the chemicals manufacturing and oil and gas industries for decades now, but these same organizations are learning how to extract more value from these programs. Initially, the conversation revolving around RBI was about the software tools used to run the program. This software would collect, collate, and analyze the data to produce when and where you would inspect to prevent failures. As programs matured, organizations learned after they purchased a software tool and implemented a RBI program, that the software was just a tool and not the RBI program itself. Initially, when a mechanical integrity (MI) program was audited, stating that the organization has a known RBI software tool would create credibility with the auditor that the organization had an established RBI program, and it was perceived that the organization was proficient enough to run and maintain this program. Given time and experience, these initial assumptions have been shown to be inaccurate for many organizations within this scenario. The software tool may be implemented, accessible with data, and have personnel with logins, but it does not imply that the organization is utilizing a RBI methodology. This article attempts to show how a mechanical integrity program intending to use a RBI methodology following an RBI implementation to start extracting value and continuously improve the results of the RBI program for the operator/facility.

This article focuses on the RBI program after the initial implementation. It is assumed that the RBI Implementation was completed, accurate, and followed a best practice methodology of documenting, executing, and establishing the initial results for an RBI program, inclusive of a damage mechanism review (also known as a “corrosion study”) and Integrity Operating Windows (IOWs). This assumption would also include that the history of the facility, and the experience of the teams involved in the implementation were experienced and competent with RBI implementations. Thus, after the completion of the implementation, the operator would have RBI results within a software program, established deliverables and organization of their equipment, and documented damage mechanisms of their processing impact on the facility’s equipment. After the implementation, how does an RBI program progress? It is often thought that the path is straight forward. As a result of the new RBI program, the facility has equipment risk rankings with corresponding inspection plans for each item, therefore it would be normal to think that the next steps are to execute the recommended inspections. Unfortunately, this is where organizations can misstep. The RBI program shouldn’t be considered a “wait until you inspect” type of program, RBI is and should be embedded into the daily methodology of a mechanical integrity program. Then, following the implementation, how does an organization progress forward with their new RBI results?

For life after an RBI implementation, instead of accepting the results of an RBI study and moving forward with the inspection schedules, the organization may want to consider the below approach to enhance the RBI program to ensure effectiveness and value returned to the operator. These items should be addressed by the operating organization:

- Management and execution of the RBI program
- Actions from the RBI implementation
- Review and confirmation of assumptions and update data gaps
- Verify risk rankings
- Overdue inspections and optimize inspection planning
- Sustaining an RBI program

A summary of each topic is addressed within this article.

Management and execution of the RBI program:

A key to having an effective RBI program, post implementation, is to establish the management system, complete with goals and an established framework to achieve the desired results through management and execution of the RBI program. Establishing an effective management system is ideal for the sustainment of an RBI program. That management system should identify how the program is managed, for example, by defining expectations regarding decision making, information management, and how RBI enhances the mechanical integrity program and other related programs within that organization through integration with operations. Data extracted from the RBI program can feed into other areas to ensure feedback and effectiveness of programs affecting production or asset life. A good example of this feedback is to incorporate RBI into the Management of Change (MOC) process. Within the MOC process, RBI may identify an issue as a result of increased production rates that will increase the degradation of certain equipment. This finding being addressed in the MOC process may then influence the decision to increase or decrease production based on a cost benefit analysis or perhaps influence how the RBI program manages the risk and resulting actions from the decision to increase production. The management system will also define a management decision process. If RBI identifies an asset with high risk with an overdue inspection, how is this addressed by the mechanical integrity program and by the facility's management? The equipment may be shut down and inspected, but the facility must also produce products; having an effective management system provides a framework to address these difficult decisions. For most programs, this management system may already be established with the MI program, but with the changes in philosophy from a traditional time-based inspection approach to managing integrity through equipment risk, the existing management system may need to address these changes when the goals of the MI program shift. This shift may realign mechanical integrity's role in the organization's decision making.

Actions from the RBI implementation:

Following a recommended methodology for an RBI Implementation, the resulting study will identify actions for the facility to execute upon handover of the RBI results. Identifying and executing these actions should be completed immediately following the conclusion of the implementation. This timing is convenient because the data is available, the results are still relevant, and the organization is encouraged by the incorporation of the RBI program. The RBI results at this point should be considered preliminary as completion of these actions may modify the results of the RBI study. As an example, if the RBI study did not incorporate the business impact, also known as production loss, but these results were included as an action following the implementation, this will have a significant impact on the risk results which has an effect on the inspection schedules and planning.

Review and confirmation of assumptions and update data gaps:

Every RBI implementation must make assumptions as some information is not always readily available. Some of the most common assumptions will facility wide, for example atmospheric conditions, but other assumptions, such as equipment insulation, will have a major effect on risk as it relates to the external condition of the equipment and the prevalence of the corrosion under insulation (CUI) damage mechanism. Therefore, these assumptions should be verified, and the data gaps reviewed to ensure the appropriate decisions are being made on the equipment.

Verify risk rankings:

This is one of the more critical steps to executing an RBI program methodology. The risk rankings define and establish how the equipment will be managed and inspected. If the risk is not accurate, then the organization may under inspect equipment or over commit resources by over inspecting the equipment. It is recommended that the organization, following the implementation, revisit the risk ranking of the equipment, to ensure and verify the risk results prior to scheduling inspections. As mentioned previously, if the actions have been completed, and the data assumptions and gaps have been addressed, this may have altered the risk results.

Verifying that the risk is as expected is often an overlooked step for life after an implementation. The consequences of one high risk item being miscategorized as lower risk could drive an early outage causing a loss in production. When reviewing risk, the following are common places to ensure the risk of the equipment is more accurate.

Example Case:

- Equipment Item: Production Separator
- Design: Carbon Steel, Typica Wall Thickness, Manufactured in the 1990s
- Process Environment: Produced Hydrocarbon Service, Operating within Normal Operating Ranges
- Primary Failure Mode: Internal Wall Degradation
- Risk Ranking for the Vessel: High
- What is Driving the Risk: High internal corrosion rate with a high consequence of failure due to the available hydrocarbon inventory associated with the vessel

The risk of this asset was reviewed and verified to be accurate during the RBI implementation. As shown, the primary issue with the vessel is a thinning wall, thus leading to a loss of containment of a hydrocarbon process service. Once the vessel fails, the hydrocarbon will de-inventory and release the hydrocarbon to the atmosphere and causing a potential for safety, environmental, and business impact consequence.

Upon reviewing the results of the study, the measured corrosion rate, for example, was 0.020in/yr. (20 millinches per year). By reviewing the equipment's inspection history, the location that was driving the corrosion rate was an older monitoring location reading due to what was found as an impingement flow causing a localized erosion area within the separator. It was also found that this impingement was mitigated several years prior and that the corrosion rate at this location was within expected ranges for a vessel in this service. During the RBI implementation, the guidance from the operator to the RBI team was to use the historical inspection thickness readings for the corrosion rates of the equipment. Due to the software tool that was being used for the RBI implementation, the "most conservative" rate was used as a default for the RBI analysis and thus the probability of failure (POF) was calculated to be high. By going back and adjusting the corrosion rate to reflect the mitigation of the higher erosion rate, the adjusted risk for this vessel decreased to a medium risk and was no longer a driver for an outage and inspection. This resulted in the inspection interval changing from a 12-month interval up to a 90-month inspection interval, yielding an improvement of 750%, thus saving the organization unnecessary cost, time, and effort.

This is only one typical example of verifying the risk within an RBI program. By doing the extra due diligence and review of the equipment, the operator improves the confidence of the results and ensures that the appropriate risk drives the integrity program for the facility.

Overdue inspections and optimize inspection planning:

The initial RBI implementation will uncover many areas of a mechanical integrity program that may have been overlooked or not considered as part of a time-based regulatory driven inspection program. Some items may be specific inspections for specific damage mechanism, or perhaps the including of pressure equipment considered outside of the MI scope under the previous mechanical integrity program. Therefore, overdue or past due inspections will be identified as inspection activities that must be addressed by the operator.

Not only will overdue inspections be an area that must be addressed, but as a deliverable to an RBI implementation, the operator will receive all inspections to be completed on relevant risk items for the facility. This may result in thousands of inspection activities provided to the facility upon the completion of the implementation. Depending on the software tool's business processes established during the software implementation, thousands of tasks and planned maintenance activities could be released into the maintenance planning system, thus causing an overwhelming scheduling issue for the RBI team. An alternative to this could be an intermediate step where the RBI team reviews the inspection planning results and then optimizes the inspection plans to correspond to budget years, planned outages, inspection campaign cycles, and even optional inspection lists based on the organizations approach. This will ease the impact on the scheduling process and create opportunities for cost savings.

Both the issues of overdue inspections and the large number of inspection plans as a result of the RBI implementation need to be optimized in similar processes. Each of these need to be planned accordingly to address the main intent of the inspection, which is to gather as much relevant data on the equipment as safely and efficiently as possible. Some organizations may lose sight of this goal and will determine that if an inspection is considered "overdue" that they stop everything at the earliest convenience and accomplish this inspection. For some inspections, this behavior may be required, but for most of these types of inspections, they can be completed at the next best opportunity. Likewise, for the large amount of inspection plans generated, it is recommended that the facility review the inspections due and align and organize these inspections based on safety, outage dates, types of inspections, budgets, specific inspection criteria, and similar information to affectively organize the inspections.

Sometimes as a result of an RBI implementation, a group of inspections will be due at the end of the calendar year. This does not necessarily imply that they must be done in December of that year, it may actually imply that the inspections are due sometime before the end of that calendar year. Therefore, these dates should be reviewed with the correct context and planning information such that the inspections are scheduled appropriately for the organization.

Sustaining an RBI program:

Life after an RBI implementation must address the operational aspects to sustaining an RBI program. As an example, RBI does not change the requirements of a normal API 510 pressure vessel inspection, but it may dictate how the inspection results are documented and evaluated, using API 581 inspection effectiveness as an example, as the inspection pertains to the RBI program and its requirements. If the RBI program is more quantitative and not qualitative, the results of the pressure vessel inspection may be recorded and applied differently within the software application and RBI program itself. Thus, to assist in sustaining an RBI program, some considerations should be made for what work processes are required to meet the goals of the mechanical integrity program. Once the work processes are established, documented, put in practice, and kept evergreen, the RBI program will yield significant value through efficiency and optimization for the organization by focusing integrity on the most critical items.

In summary, as discussed throughout these topics, the result of not preparing for life after an RBI implementation often leads to results accuracy, data issues, which leads the organization to potential re-implementations or regression back to a time-based program. By understanding the topics addressed in this paper, the organization can help ensure that their RBI program reaches maximum effectiveness and does not result in a shelved program. Life after a RBI implementation brings value, but to capitalize on the most value, consider these topics as areas to help enhance that value.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Are you struggling with your Asset Integrity program?

Katherine Anderson*, CCPSC
ioMosaic
93 Stiles Rd #102, Salem, NH 03080
*Presenter E-mail: anderson.k.nh@iomosaic.com

Abstract

Asset Integrity (also referred to as Mechanical Integrity) [1] findings remain on top of OSHA's citation list during PSM inspections. Violations most frequently found include failure to address equipment deficiencies, lack of AI written procedures, and failure to perform internal AI inspection(s) and test performance. Establishing systems to collect equipment information to develop proper, effective AI procedures that maintain equipment integrity, schedule inspections, and track deficiency resolutions are a major challenge – especially for smaller companies. This paper describes how electronic database management along with proper information collection practices as well as the use of workflows to track inspection and deficiency status can greatly improve efficiency of an asset integrity program.

Keywords: Management, Mechanical Integrity, Technical Tools, Risk Management Tools

Asset Integrity (AI) findings remain on top of OSHA's citation list during OSHA Process Safety Management regulation 1910.119 inspections. Violations most frequently found include failure to address equipment deficiencies, lack of MI written procedures, and an absence of MI inspections.

Data from 2016-2017 showed asset integrity was the most cited element [1]. The top three cited requirements for asset integrity were [1]:

- AI Inspection and Testing
- AI Written Procedures

[1] Center for Chemical Process Safety (CCPS) refers to OSHA Mechanical Integrity as Asset Integrity in the latest "Guideline for Asset Integrity Management" book and this term will be used throughout this paper.

- AI Equipment Deficiencies

This trend continued in 2018 and these three AI issues were identified in the top ten on the OSHA citation list [2]:

- AI Written procedures (#2)
- AI Equipment Deficiencies (#3)
- AI Inspections and Tests (#7)

Like process design, asset integrity is critical to the safe operations of facilities. Its criticality is demonstrated by the fact that it is one of the 14 elements of the OSHA PSM standard as well as a pillar of the risk management foundation in the risk-based process safety management system. Its implementation is a challenge for companies of all sizes but becomes very hard for smaller facilities with minimal resources. An effective AI program requires a large amount of effort and resources not only to set-up the initial program but also to execute the inspection schedules on time and address any recommendations/deficiencies that were identified. This paper identifies how three key components: electronic database management, proper information collection practices, and the use of workflows to track inspection and deficiency status, can greatly improve the efficiency of an AI program.

The goal of an AI program is to implement elements and steps that establish and maintain safety for processes and equipment in order to prevent failures and accidental releases. The initial set-up of the asset integrity program includes:

- Defining company policies and management system procedures
- Identifying equipment to be included in the program
- Defining equipment criticality
- Defining required inspection types and their frequency

After the initial program is set-up the inspection schedule must be tracked and executed on time, the results have to be analyzed, and identified recommendations/deficiencies have to be corrected in a timely manner.

I. Electronic Data Management System

The biggest struggle in the initial set-up phase is to be able to collect and manage all the information required for proper equipment evaluation. Equipment specifications are required to identify the maximum allowable operating condition. Process conditions are required to identify equipment criticality, possible damage mechanisms, and proper inspection techniques to be used for detection.

Depending on the age of the facility or the systems used for Process Safety Information (PSI) much of this information may not be easily available or may be out-of-date. An electronic data management system can help with this task, however proper set-up must be followed to allow for easy information retrieval. Electronic equipment folders can be used to organize and store information. Naming convention must make sense to the user(s). The electronic folders should be set-up using location, equipment type, and equipment ID number that user(s) are familiar with allowing ease in searchability by any of these identifiers. Using equipment numbers from P&IDs makes it easy for operating personnel to cross reference with Process Hazard Analysis (PHA) and procedures. Identifiers such as functional location in computer maintenance management system (CMMS) can be very cumbersome for information retrieval. Storing information in capital project files may work well during project execution, however it becomes difficult to find by the operating unit personnel after project is completed.

The electronic data system is most useful if it allows users to link the equipment number to its operating conditions, P&IDs referenced, equipment specifications, U-1 forms, safety devices protecting the equipment, and/or sizing calculations as well as all asset integrity information.

II. Proper Information Collection Practices

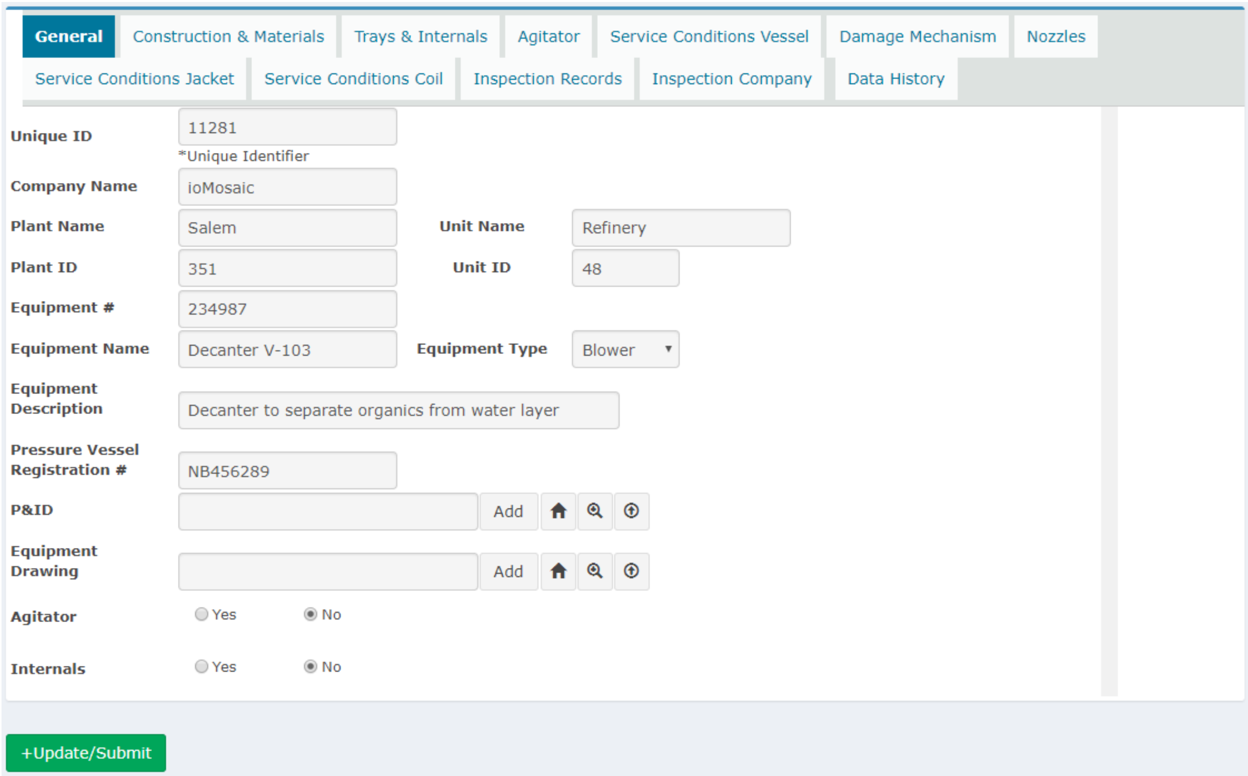
The electronic system should be set-up to allow users easy access to information and also to assure that the information is current or up to date. Given the sheer volume of information surrounding asset integrity, proper information collection practices are crucial during a program start-up. At minimum the asset integrity information should include:

- Equipment criticality
- Possible damage mechanisms
- Type of inspections to be performed
- Frequency of inspections
- Results of inspections
- Corrective actions to be taken
- Status of repairs

Proactive collection and documentation followed by proper storage in an electronic system is key to managing and maintaining an effective and compliant AI program. Allowing for all equipment specific information being accessible to all staff from a single electronic form, including reports and back-up documentation makes the retrieval system more efficient. For instance, pressure relief valve information would automatically be linked to the protected equipment information. Document control of PSI is critical to proper asset integrity implementation. This information should be current and easy to find to ensure it will be used properly and more importantly support compliance.

Figure 1 is an example of how the equipment information can be documented and linked together using an equipment form. Data linked to this equipment form can be stored in electronic document-controlled PSI folders and should also be accessed from the specific equipment form without having to search the folders. This makes identifying equipment criticality and possible damage mechanisms more efficient.

Fig 1 – Pressure vessel equipment form example from Process Safety Enterprise®



Source: Process Safety Enterprise®, ioMosaic Corporation

Facilities should provide guidance on what equipment should be included in the AI program but also provide the electronic means to properly manage the information. Scattered data located in several places increases the time it takes to do proper evaluations of equipment criticality and determine correct inspection techniques and frequencies.

III. Using Workflows to Track Inspection and Deficiency Status

A final common struggle in implementing the program after equipment is identified and inspection frequencies are defined is to manage the inspection program to assure inspections are done on time and results are documented.

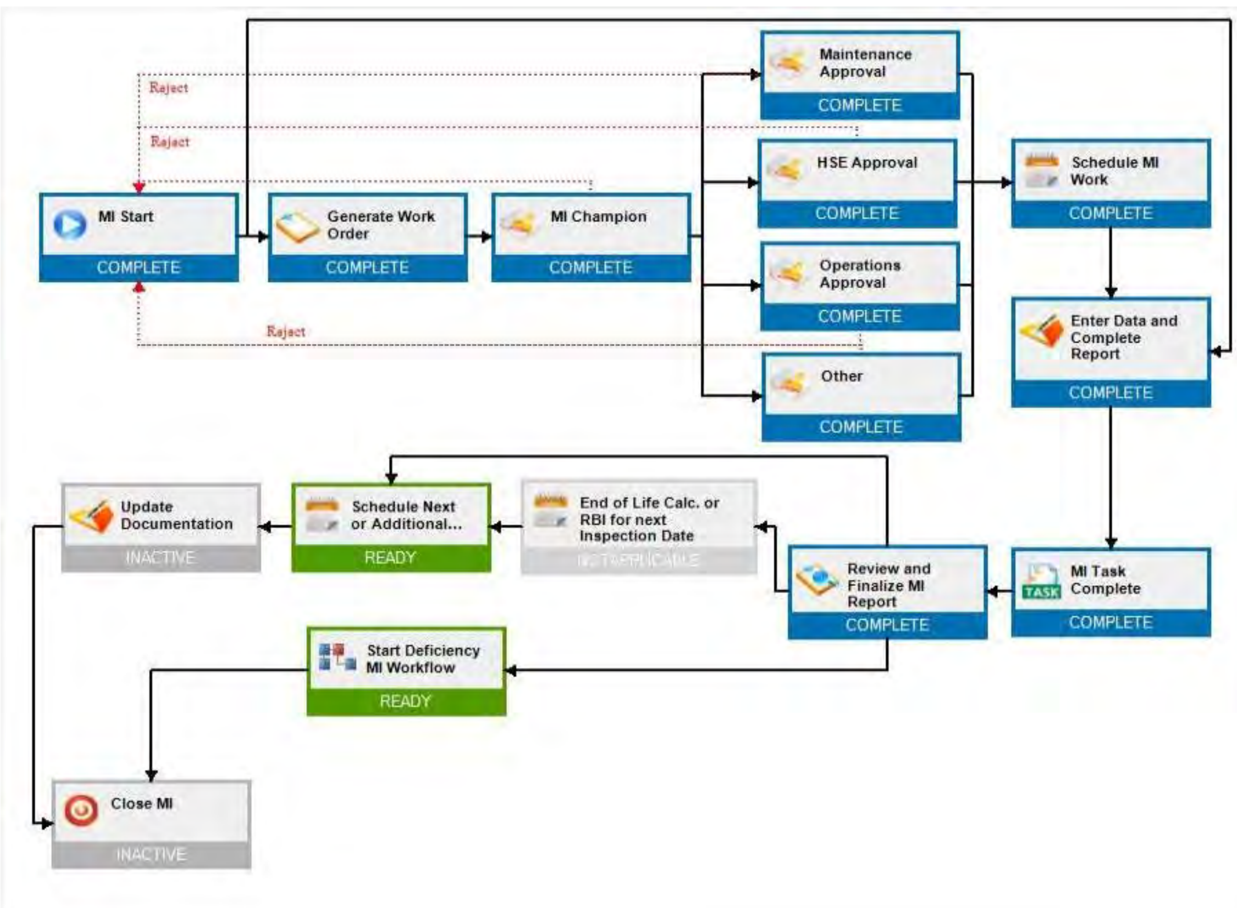
That can sometimes be a challenge within a CMMS depending on the configuration of the work order system. Workflows can be used to manage specific inspection tasks and deficiency corrective actions to improve this management system. Using a workflow to track inspections provides visual progress of the inspection tasks and the automatic reminders for tasks that need to be completed help to resolve issues quickly. Moreover, AI workflows can be used throughout or applied to different stages of equipment life cycle.

Figure 2 is an example of an AI Inspection Workflow that can be used for tracking a specific inspection. Such a workflow or module can simplify RAGAGEP (Recognized And Generally

Accepted Good Engineering Practices) questions by automatically selecting and suggesting applicable RAGAGEP inspection tasks and frequency for each piece of equipment added to the AI program. This type of workflow can still use the CMMS for actual work order generation, but it can also track the status of other steps in the inspection process such as proper approvals, review of inspection data, and equipment end of life determinations.

Steps are identified in the facility's mechanical inspection execution process and a workflow step is created for each individual requirement. Workflow systems can track the status of each step, send reminders to responsible parties to complete their tasks, and keep the workflow open until all actions are completed. This allows the work order for the inspection task in CMMS to be closed and still provides for proper tracking of the inspection related activities. Reports can be run to track inspections progress at every step in the workflow.

Fig 2 – Asset integrity inspection workflow from Process Safety Enterprise®

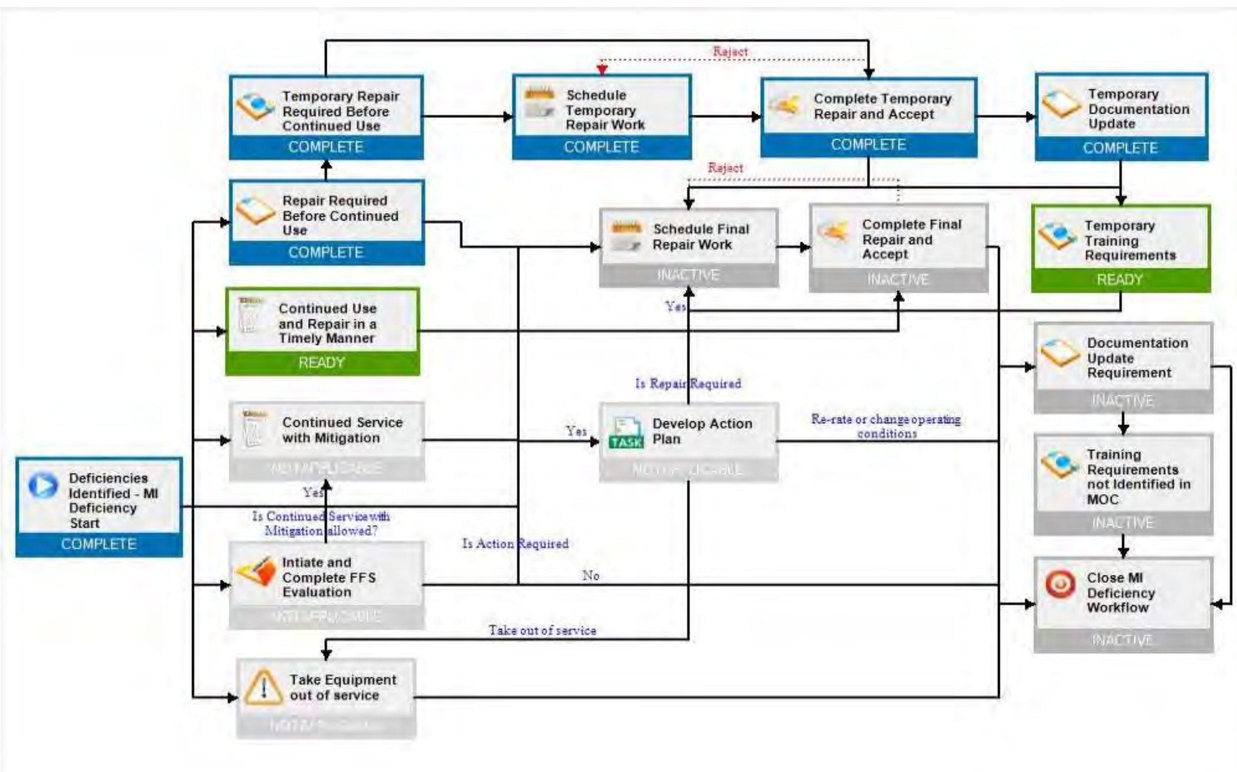


Source: Process Safety Enterprise®, ioMosaic Corporation

The same workflow concept can be used to manage equipment recommendations or deficiencies. The steps needed to take corrective actions are identified based on facility's procedures and workflow created to manage the recommendation to completion. Using a workflow for corrective action can also assure the Management of Change (MOC) procedures are being followed when equipment is repaired, modified, run with mitigation or taken out of service. The deficiency workflow can be set-up not to move forward until proper MOC workflow is created and approved. The workflow also assures that proper documentation was completed. The reminder function of a typical electronic workflow is an important and reliable tool that keeps tasks in front of the personnel responsible for their completion.

Without a workflow in place, it is not unusual to lose track of a temporary repair such as a pipe clamp, because the work order used for the temporary repair was closed and no system was in place to create a final repair plan. A properly implemented workflow system can identify these and other oversights and help to manage backlog more efficiently.

Fig 3 – Asset integrity deficiency workflow from Process Safety Enterprise®



Source: Process Safety Enterprise®, ioMosaic Corporation

Workflows are a great tool to assure proper steps are accounted for and implemented into any process safety management activity and improve the efficiency in execution and reporting. Properly implemented equipment data information storage and AI workflows will minimize the amount of time and effort that personnel have to spend on these activities. To make asset integrity implementation easier and more efficient data should be easily retrievable from a single location. AI tasks should be trackable and their status easily visible with proper reminders to assure completion.

Conclusion

This paper has identified and outlined many of the common challenges companies face when it comes to asset integrity. As one of the 14 elements of the OSHA PSM standard, a thorough AI program is essential for compliance and risk reduction. The overall efficiency and compliance of an AI program can be greatly improved by the three key components that were the focus of this paper: implementation of an electronic database management, proper information collection practices, and the use of workflows to track inspection and deficiency status ultimately ensuring the establishment and maintenance of safe operations. Although these components are recommended to be applied during asset integrity program set-up, they can be successfully applied to any process and to any company size to improve safety.

References

[1] Schmoyer, N. "Review of Recent OSHA PSM Citations". Inspectioneering. 3 January 2019. Inspectioneering.com

[2] Occupational Safety & Health Administration (OSHA). Top 10 Most Frequently Cited Standards for Fiscal Year 2018 (Oct. 1, 2017, to Sept. 30, 2018). Online: https://www.osha.gov/Top_Ten_Standards.html

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Choosing Functional Safety Field Instrumentation - Certified, Prior Use or both? - Fundamentals of VDI 2180

Gene Cammack* & Luis Manuel Fernando Garcia Garcia*
Siemens Industry Inc.
*Presenters' E-mails: gene.cammack@siemens.com, Luisgarcia@siemens.com

Introduction

As a subscriber of the Safety List, which is an International Society for Automation – ISA - open email based forum (SAFETY@ISA-ONLINE.ORG); I was drawn to a very interesting discussion about the selection of instruments to be used in a Safety Instrumented Function (SIF) and the implications that such selection would have in the performance of such a safeguard.

As might be expected, two camps developed as soon as people started sharing their thoughts and experiences. Some colleagues claimed that certified instrumentation was just a ploy from vendors to make more money, and that field data collection and analysis is the only way to select equipment to be used in functional safety applications. Others recognized that many systematic faults could be avoided all together by using properly IEC 61508 certified equipment. One recognized international engineering firm went as far as to indicate that up to 30% of the instrumentation they had analyzed had shown design flaws that would lead to dangerous failures.

What it points out is that determining the equipment to use in safety instrumented systems (SIS) and the rules for maintaining them is one of the most difficult and controversial topics in the industrial SIS marketplace. As is usually the case, there are valid arguments in both sides, but in truth, there is a third approach where both philosophies are needed and, in fact, must be adopted in most cases. This is based on the use of certified equipment which needs to be continuously monitored to weed-out implementation systematic faults.

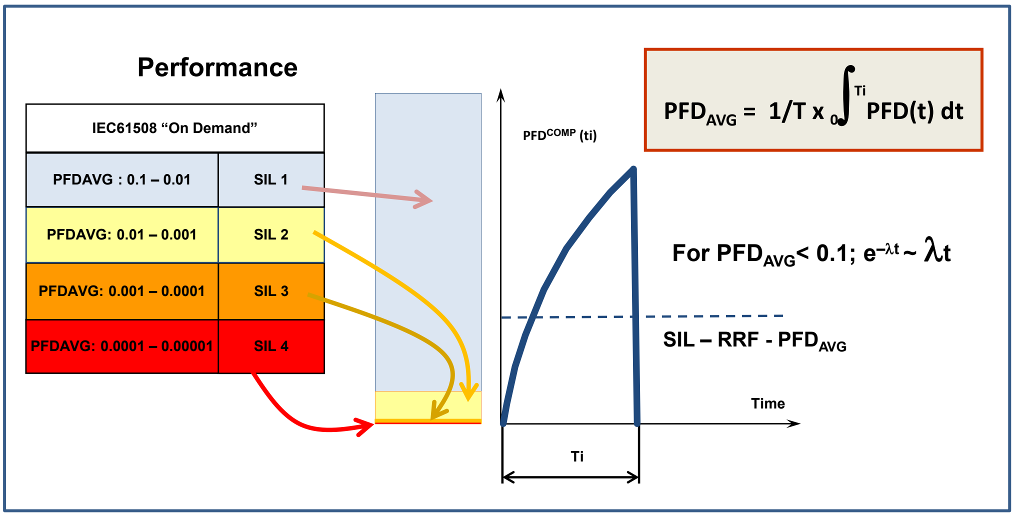
To get to the heart of the matter, we will look at the background of both positions, review the recent changes to the standards, and look at the recommended practices from the German Engineering Association, VDI to calculate performance of different instrument arrangements as subsystems of a Safety Instrumented Function (SIF).

Safety Integrity Level (SIL) of a Safety Instrumented Function

A SIF is a safeguard, designed to take the process to a safe condition if the process functionally exceeds safe operating conditions. As a “safeguard”, it should <u>only</u> function when required. Therefore, equipment used in a SIF needs to reliably operate and execute its function whenever the process exceeds safe operating conditions (a demand). A failure to do that is called a “failure on Demand”

The performance of a SIF and their components are expressed as Safety Integrity Levels (SIL). These are statistical estimations of average probability that they will fail on demand (**PFD$_{AVG}$**). The Average Probability of Failure on Demand (PFD$_{AVG}$) is a function the failure rate of the device (expressed as □□failures per time) and the time between inspections (proof test interval) since a periodic inspection will decrease such likelihood of failure (*Figure*).

SIL calculations for **PFD$_{AVG}$** are also dependent on the architecture of the SIF where redundancy and common cause (□) become factors. One out of Two (1oo2) and Two out of Three (2oo3) architectures are often used to lower the **PFD$_{AVG}$** for a subgroup (Sensors, Logic Solver or Final Elements). Failure of the SIF will occur in the event of failure of **the sensors subgroup <u>or</u> the logic solver <u>or</u> the valves subgroup**. Like a chain, it will fail in its weakest link.



Figure

Performance	Risk Reduction	PFD$_{AVG}$
SIL 1	10 to 100	1 in 10 will fail
SIL 2	100 to 1,000	1 in 100 will fail
SIL 3	1,000 to 10,000	1 in 1,000 will fail
SIL 4	10,000 to 100,000	1 in 10,000 will fail

Table – SIL for Low Demand Mode

But SIL Calculations are based on □ (failures per unit time) which only considers random failures. We must also take into account *<u>Systematic Failures</u>* which could be several orders of magnitude higher than random failures, rendering PFD$_{AVG}$ calculations irrelevant.

A systematic failure is a failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. When designing a SIF, users need to select instrumentation with a clear understanding of their performance.

There are four factors to take into consideration when assessing the SIL an instrument could reach.

1. **PFD$_{AVG}$**: Does the instrument have low enough random failures and high enough inspection frequently to achieve the **PDF$_{AVG}$** required by the SIL level?
2. **Architectural constraints:** Does it meet a minimum level of redundancy?
3. **Systematic Faults:** Have systematic faults been controlled through good design processes and when used as instructed by the manufacturer?
4. **Security:** Is the device secure or hardened against threats?

So, the question is how do we evaluate, prove and document the performance of a SIF component?

SIL Determination of an Instrument – What to use?

There are three possible ways in which a device is evaluated.

Certified - Route 1H: The *instrument manufacturer* may follow Standard IEC 61508; 2010 Route 1H and 1S[i]; then a third party (TÜV, exida, Risknology, FM etc.) certifies the instrument. The process involves:

a) Performing Failure Mode and Effect Diagnostic Analysis (FMEDA), a detail and lengthy analysis of all failure modes of all components of an instrument.
b) Compliance with Safe Failure Fraction (SFF) constraints tables for the level of redundant architecture where the instrument will be used.
c) Using an appropriate group of techniques and measures designed to prevent the introduction of systematic faults during the design and development of the device. This includes evaluation of the device, the design process and the safety manual (architectures, inspection frequencies, operating conditions, etc.)

To certify an instrument, or a component following this process, might take months or years, and the certification entity has a clear incentive of finding mistakes in the instrument, resulting in an improved design.

Certified - Route 2H: The *instrument manufacturer* may follow Standard IEC 61508; 2010 Route 2H and 2S [ii]and/or 3S; then a third party (TÜV, exida, Risknology, FM etc.) certifies the instrument. The process involves:

a) The collection of failure data, following IEC 60300-2-3
b) The analysis of the data following IEC 61649 (2H) and **Proven In Use** (**PIU**)

The goal is to demonstrate, based on an analysis of operational experience for a specific configuration of the instrument, that the likelihood of dangerous systematic and random faults is low enough so that every safety function that uses the instrument in the same conditions achieves its required safety integrity level (Route 2S). This includes pre-existing software components (Route 3S).

The process also might take months or years depending on the data available.

Prior Use: *Users* follow Standard IEC 61511; 2016 Prior Use evidence determination (**PU**). The process involves:

a) **PU** analysis, which consists of data collection and analysis of failure rates in the user's environment with the goal of performing a documented assessment of a device, supporting that it is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments.
b) Understanding how the equipment behaves in its specific operating environment to achieve a high degree of certainty that the planned design, inspection, testing, maintenance, and operational practices are sufficient.
c) Calculating upper bound statistical confidence limit 70 %.

The process might yield too conservative values, as systematic faults are expected to dominate. Replacing by a different design instrument would only introduce different systematic faults.

<u>Possible scenarios</u>

Users are therefore confronted with 4 possible scenarios when selecting critical instrumentation (which was exactly what fired up these discussions in the first place);

Scenario 1 – when IEC 61508 certified instrumentation (either Route 1H or 2H) is available for the specific application. This is the ideal situation. If the user follows the safety manual of the instrument; (like type of application, installation, inspections frequencies, procedures and life of the instrument); expected performance should be achieved, and SIL Calculations, including redundant architectures will be easily performed.

Scenario 2 – when IEC 61508 certified instrumentation is available, but the user application is slightly different to what is recommended by the certification entity. In this case, evaluation of severity of the deviations needs to be analyzed.

Scenario 3 – when certified instrumentation is NOT available, yet failure rates data of instruments used for interlocks and other safeguards in similar environment is available. This scenario is similar to scenario 4 but with a lesser degree of difficulty.

Scenario 4 – when certified instrumentation is NOT available, yet failure rates data of instruments used in process control is available. Then PU evidence of suitability, although in different conditions (process control environment is not the same as functional process safety) should be performed, following IEC 61511-1; 2016. Evaluation should include analysis of:

- Manufacturer's quality management systems;
- Adequate identification and specification of the devices;
- Demonstration of the performance of the devices in similar operating environments;

Performance of redundant instruments subsystems – VDI/VDE 2180

SIL related PFD_{AVG} calculations models take into account all failure modes and how they affect the performance of equipment under study, and consider:

- Time in which each type of failure mode affects performance
- Architecture under consideration
- Influence of common cause (for redundant architectures)
- Time a component of the SIF is bypassed for maintenance.

The dominant factors of the equations are the rates of dangerous failures which cannot be detected by automatic diagnostics ($\square_{DU}$), as well as the common cause ($\square$) in redundant architectures. Therefore, basic reliability formulas could be simplified by considering just these two parameters and the time between manual inspections. The values of $\mathbf{PFD_{AVG}}$ would be more conservative, but by less than 10%.

This is exactly what **VDI 2180** proposes. (VDI is a German Engineers association)[iii]. VDI recently published "Safeguarding of industrial process plants by means of process control engineering (PCE) Recommendations for practical use" [VDI 2180].

In summary it proposes:

A - If devices are either; not certified, operating in different conditions as originally designed for, or there is not experience to determine optimal operating conditions. Then;

a) Collect failure rates data
b) Classify for a clear taxonomy
c) Evaluate for systematic failures,
d) Calculate expected values
e) Apply following equations for different architectures;
   - $\mathbf{PFD_{AVG\ 1oo1} = ½\ \square_{DU}\ Ti}$
   - $\mathbf{PFD_{AVG\ 1oo2} = 1/3\ (\square_{DU}\ Ti)^2 + ½\ \square\ \square_{DU}\ Ti}$
   - $\mathbf{PFD_{AVG\ 2oo2} = \square_{DU}\ Ti}$
   - $\mathbf{PFD_{AVG\ 2oo3} = (\square_{DU}.\ Ti)^2 + ½\ \square\ \square_{DU}\ Ti}$
   - $\mathbf{PFD_{AVG\ 1oo3} = 1/4\ (\square_{DU}.\ Ti)^3 + ½\ \square\ \square_{DU}\ Ti}$

B - If devices are both:

a) Certified
b) Are going to operate as indicated in their safety manual

Then the $\mathbf{PFD_{AVG}}$ of a single device is given in the Safety Manual (nothing to calculate) and for other architectures:

- $\mathbf{PFD_{AVG\ 1oo2} = 4/3\ (PFD_{avg\ 1oo1})^2 + \square\ PFD_{avg\ 1oo1}}$
- $\mathbf{PFD_{AVG\ 2oo2} = 2\ PFD_{av\ 1oo1}}$
- $\mathbf{PFD_{AVG\ 2oo3} = 4\ (PFD_{avg\ 1oo1})^2 + \square\ PFD_{avg\ 1oo1}}$
- $\mathbf{PFD_{AVG\ 1oo3} = 2\ (PFD_{avg\ 1oo1})^3 + \square\ PFD_{avg\ 1oo1}}$

Conclusion

There is a natural simplification in the evaluation of performance of instruments which are used in a SIF if such instruments are **certified as per IEC 61508** and if the user follows the recommended operation and maintenance practices as stated in the instrument safety manual. Alternatively, instruments with **PU evidence of suitability** might be used but analyzing such data could be challenging, forcing very conservative application designs.

VDI 2180 offers a simplified recommended way to calculate performance for both paths;

---

[i] **H** denotes Hardware and **S** denotes Systematic
[ii] IEC 61508;2010 part 7
[iii] [iii] VDI represents all disciplines of the engineering spectrum in Germany going from Agroindustry to Biotechnology applications. VDI organizes conferences, symposiums, exhibitions, subscribes standards and promotes young talents. Founded in 1856, it is the oldest association in Germany with more than 135,000 members.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Leveraging the Power of Industry 4.0: Orm Digital Twin for Process Industry

Abilash Menon*
Sphera Solutions
*Presenter E-mail: amenon@sphera.com

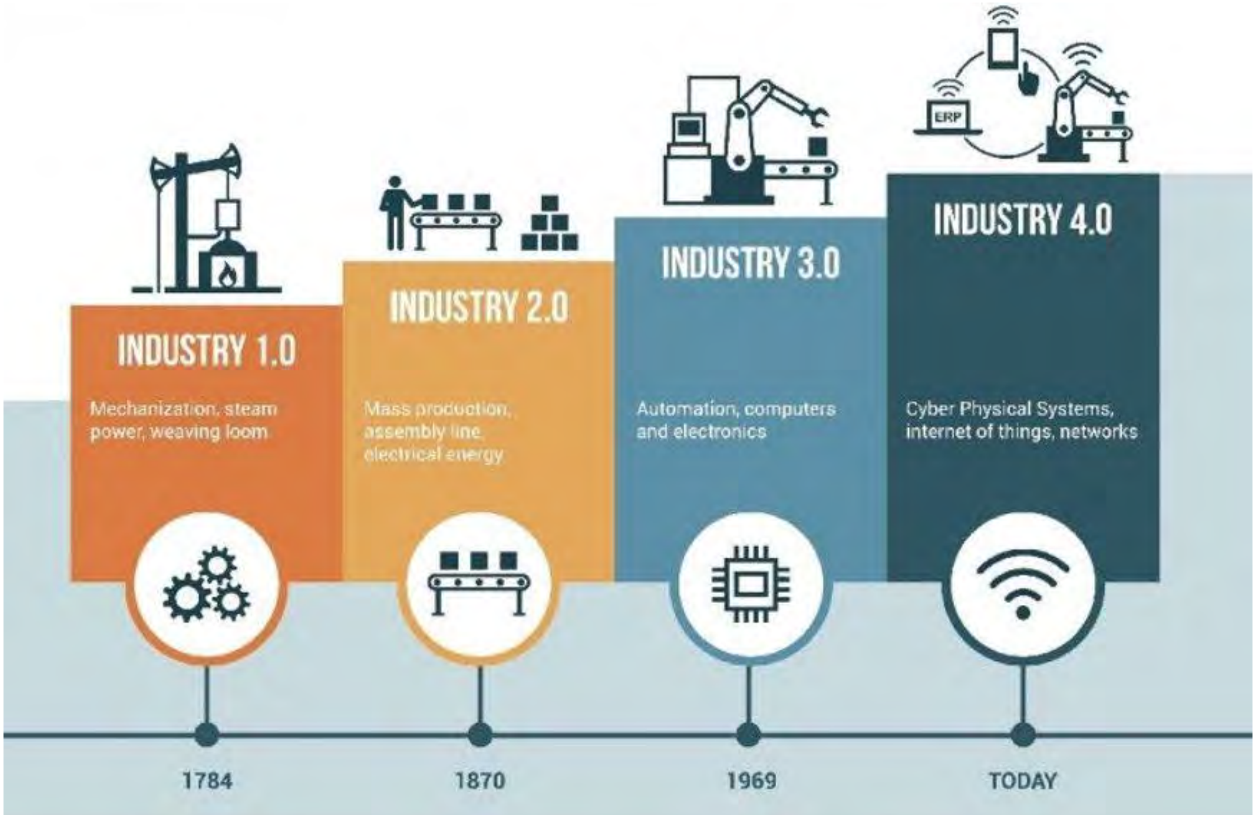
" Houston, we've had a problem here."[1]

When astronaut John Swigert sent this message from the Apollo 13 in 1970 during their attempt to land on the moon, NASA had to find a way for the three astronauts to fix the space vessel quickly before they ran out of oxygen. The team in Houston had to find a way to visualize the exact issue based on the description that the team in space relayed to them from the vessel, and then they had to find a way to help the team in space fix the problem so they could return to earth safely.

It is interesting to imagine how the scientists and engineers at NASA used a physical twin of the Apollo 13 module to conjure up the solution. Since that incident, NASA has invested more and more in technologies that can predict the risk of different failures and the potential resolutions for the same.

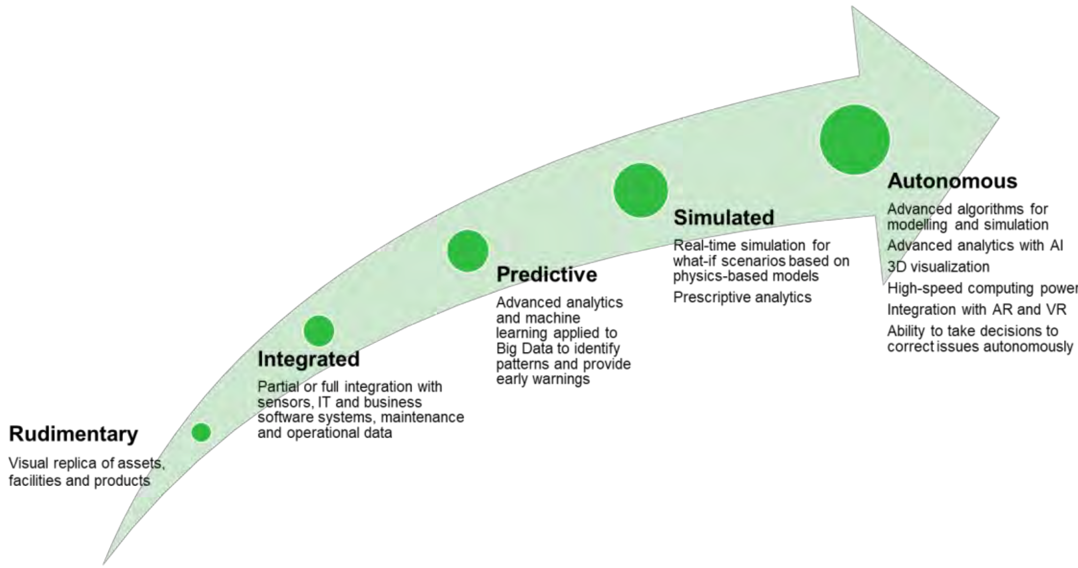
As an engineer, one of the subjects I studied in school was about Finite Element Methods for design purposes. Working as an engineer and building process equipment for the Oil & Gas industry, I now know how equipment is supposed to behave in its operating environment and as part of its operating standards. However, the real-world situation for that well-designed pressure vessel or heat exchanger is very different. Not only does the equipment have differing operating environments, but also they must be able to interact with other equipment, which likely has been designed and engineered in a different way. Once a process plant is operational, the asset is introduced to a variety of risks and uncertainties that, again, were never part of the original design.

The asset has software available that can provide information about the changing parameters for the individual equipment. Engineers can use this data to modify work environments or consider maintenance for the various parts. In the past few decades, Industry 3.0, which is the revolution of automation and computer-operated systems have given plant operators in the hazardous industries a good understanding of what needs to be done for the individual equipment’s safety and performance. However, experience has shown that the majority of incidents do not occur because one particular piece of equipment failed or performed out of its operating window. Accidents and disasters happen when a series of infractions (big and small) come together lining up to make and create a situation where an accident is triggered.



Timeline of the Evolution to Industry 4.0.[2]

Hence, it is important that the asset operators get an overall view of the entire asset and understand how the interaction of the various automated equipment, sensors, probes, etc., along with the human maintenance and operational tasks have a combined effect on the safe working of the asset. Industry 4.0 has emerged and is now at a stage to deliver the promise of the true deployment of the Industrial Internet of Things (IIoT). Using all the information available from the individual sensors and equipment, we can now draw a virtual picture of what the real-life plant status is. We can then overlay information on what human interactions need to happen in the plant to then start to get a better picture of what is the true operational reality of the plant. Once we start to get the picture and we plan our operations, first in the digital space and then in the physical asset, we can start to manage the real Operational Risk of the asset.



Various stages of Digital Twin Technologies Delivering Value[3]

Today's technology allows us to predict and plan for risk at the asset location based on the digital information acquired from it. We can now deliver a true Operational Risk Management Digital Twin of the asset, and operators in the hazardous industries can start to predict what is going to happen in the asset, simulate the changes based on planned operations and then offer a prescriptive behavior of what needs to be managed at the asset to ensure the planned operations are carried out in a safe manner and minimize the chances of a disaster occurring at the asset.

2019 Operational Risk and Process Safety Management Survey

Sphera performed our annual survey of process safety engineers from global organizations and have found some important messages with regards to the state of process safety and operational risk management in the industry. The 2019 Sphera PSM/ORM[4] survey found that most companies do have safety inherent in their DNA. It appears in their corporate culture and includes defined safety goals even though technological shortcomings sometimes cause organizations to spin their wheels when it comes to mitigating risk. Companies understand that a strong safety culture is important to manage Operational Risk and Process Safety.

A significant number of respondents said that there was an increased focus on Operational Risk at their organization. However, oftentimes approaches to managing Operational Risk are too static and not able to connect to the day-to-day challenges organizations need to overcome. Just 40% of respondents said that their organization proactively manages Process Safety, and 77% said that risk increases in some capacity between periodic safety review periods, which is up a robust 21 percentage points from 56% in the previous survey. The numbers indicate that progressively there is an increase in awareness of risk increasing during periodic safety studies.

What organizations need to do next is identify ways to be more proactive in spotting the real-time risks at the asset so that the issues are identified earlier in its lifecycle and clear mitigating measures can be put into place. The results from the PSM/ORM survey, however, suggest that there hasn't been much improvement year over year in terms of companies' ability to manage risks proactively. And in a typical month, only 69% of scheduled asset integrity inspections were achieved, according to the survey.

It is imperative that companies move to a more proactive approach to manage risks at their assets and change the way things are done to change the current status quo. The power of IIoT needs to be leveraged, and companies need to start connecting disparate data systems and the people to enable new end-to-end business processes to help people shift from a reactive approach to enabling operators with real-time insights.

When Dr. Michael Grieves first spoke about the concept of the digital twin in 2002[5], he envisioned a product lifecyle management (PLM) system in a virtual space to analyze and predict the multiple outcomes of a physical entity. During the entire PLM, the physical and digital version would be linked, and the digital version would mirror the processes. Applying this concept to the process industry, you can visualize the entire refinery or a chemical plant with the different processes in a digital space. The data that is provided to the control panel is then translated to a visual means, and you are able to make a prescriptive approach to managing the asset. But now you are able to plan the multiple outcomes that the asset may have based on the planned activities in the future. This digital presence is what enables the frontline operator to be more proactive in their activities and truly delivering the Operational Risk Management Digital Twin for the asset.

The PSM/ORM survey also reveals that companies are taking steps in this direction to ensure the frontline operator is enabled. Four out of five (82%) of the respondents said that their organizations understand the importance of Operational Excellence and continuous process improvement. The key aspect for implementing any program at an organization is to know the people accountable and need to be empowered to proactively manage Operational Risk. he survey found that 57% of the respondents believe the frontline operations and maintenance staff need better information to manage risk. A little less than half (44%) said empowering department heads should be high on the agenda for mitigating risk.

The real world of operations is neither simple nor static. The effects of aging assets, interventions in the plant to operate it or perform maintenance all come together day in and day out to affect the process safety risk on the assets. With risks unavoidably managed in different parts of the organization, the information has become siloed. Dots are not connected and decisions are made without the full context. So, if companies can provide the right information to the right people at the right time, they can make the right decisions.

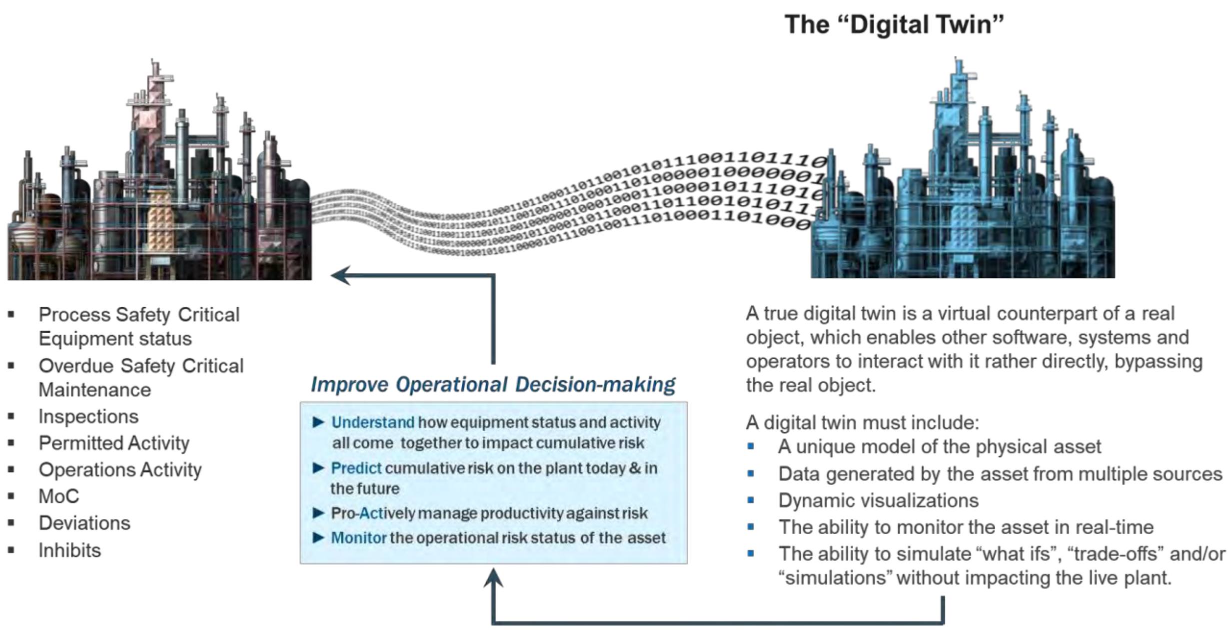
Implementing Digital Twins may be in the relatively nascent stages within organizations, but the implementation of digital transformation projects is not. But organizations are struggling to get going at any scale with their digital transformation. In Gartner's 2019 CIO survey, a full 63% of Oil & Gas companies indicated that they have yet to move beyond the ambition or design phases of their Digital Transformation journey. These numbers mirror Sphera's own numbers from the 2018-19 Operational Excellence survey, which found that nearly 70% of operators are only just starting or beginning to implement their Digital Transformation projects.

One of the biggest reasons why organizations struggle in those areas is because of siloed information, and the numbers back that up. Three-quarters of respondents (75%) said their companies are operating with siloed data and piecemeal insights. And only 10% of the respondents said that they have deployed integrated, digital solutions that record risk-relevant data and execute predictive algorithms for real-time risk identification and management.

An Operational Risk Management Digital Twin Is a Step Toward Closing the Gap

There is increasing focus and attention on the potential for new digitalization technologies to deliver increased value and sustainability in the energy and petrochemicals sectors. Over 90% of industry leaders recognize the power of digitalization to accelerate and provide sustainable Operational Excellence[6]. A reduction in operating costs, broader operational efficiencies and a fundamental transformation of the business are expected. The promises of data connectivity and analytics include continuous uptime, rapid response to risk exposure, incremental revenue gains, opportunities to better utilize assets, ways to coordinate operating and business needs, and opportunities to improve the efficiency of field service groups.

An ORM Digital Twin brings together human, system and sensor-derived inputs in a combined way to provide a continuously updated picture of operational risk on the specific asset.



An ORM Digital Twin Connects Operational Risks to a Fundamental Barrier Model

As hazardous industry operators move toward a fundamental barrier model, based on multiple layers of protection/mitigation, an ORM Digital Twin can bring all the risks together to understand their potential cumulative impact in a practical and tangible manner. The idea is simple: If you have impairments in several barrier groups, risk increases because a major accident is more likely to occur. Note that these barrier groups are not singular barriers; each is a collection of equipment, instrumentation or people-driven processes that collectively fulfill the function of the barrier.

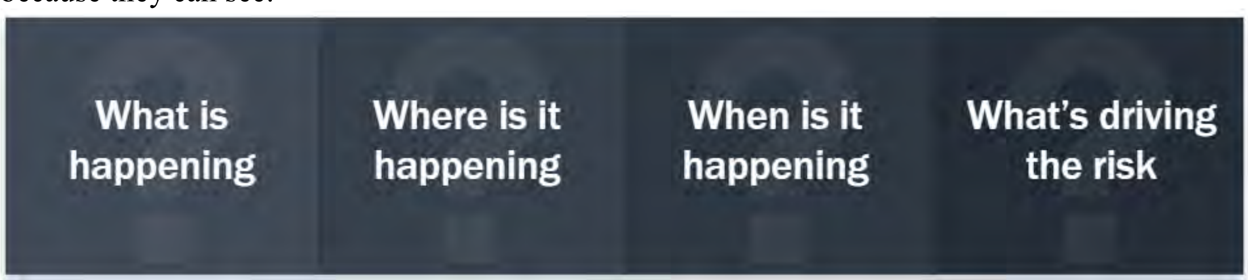
The fundamental barrier model has its origins in James Reason's Swiss Cheese metaphor; the holes in the barriers represent impairments, and when the holes line up, an event can occur and escalate into a major accident. The degree to which risk pathways develop represents the potential level of risk.

The grouping of the barrier systems is important because it allows work teams and process safety engineers to see how the impairment of barriers can line up sequentially with others with the potential to compound risk. For example, if there is an impairment on the *containment* barrier happening at the same time and within the same location as impairment in the *ignition control* barrier, the risk of having an uncontrolled release of hydrocarbons to the atmosphere is higher as is the risk of ignition. Combined, they can result in a fire or explosion from the subsequent failure of more than one barrier group. If the *detect* barrier (e.g., gas and fire detector) is also compromised, and the ability to protect it is compromised as well (e.g., because the water deluge system is inoperable), these additional breaches can result in the potential occurrence of a major event. The degree of escalation and the scale of the consequences will depend on the mitigation barriers or the ability to respond to the incident.

Planned activity on the facility can also introduce risk as it often includes the introduction of hazards into a process plant whether it's work involving spark potential, breaking containment, startups, shutdowns, isolations, de-isolations. All these activities have the potential to increase risk and impact process safety barriers. These activities are typically planned and scheduled in a maintenance management system, and their execution is managed via a work permit processes and supported by task risk assessment or job safety analysis (JSA). In addition, operational activities are managed through a combination of operational procedures and operator rounds practices. The potential barrier impact of this activity can be modeled. For instance, if a planned positive isolation is needed to prepare for a confined space entry, it is reasonable to assume that there is a potential impact on the process containment barrier for the period in which the first line break is undertaken. Similarly, open flame hot work in a unit represents a degradation of the ignition control barrier for the period the permit is issued.

An ORM Digital Twin Provides a Single, Shared View of the Operational Reality

Capturing all the process safety risk data isn't enough. It needs to be connected to the operational reality in a practical and routine way for everyone. An ORM Digital twin can do just that by delivering real-time insights to support daily operational decision-making on the ground. With a single, shared view of the operational reality everyone can make better, more informed decisions because they can see:



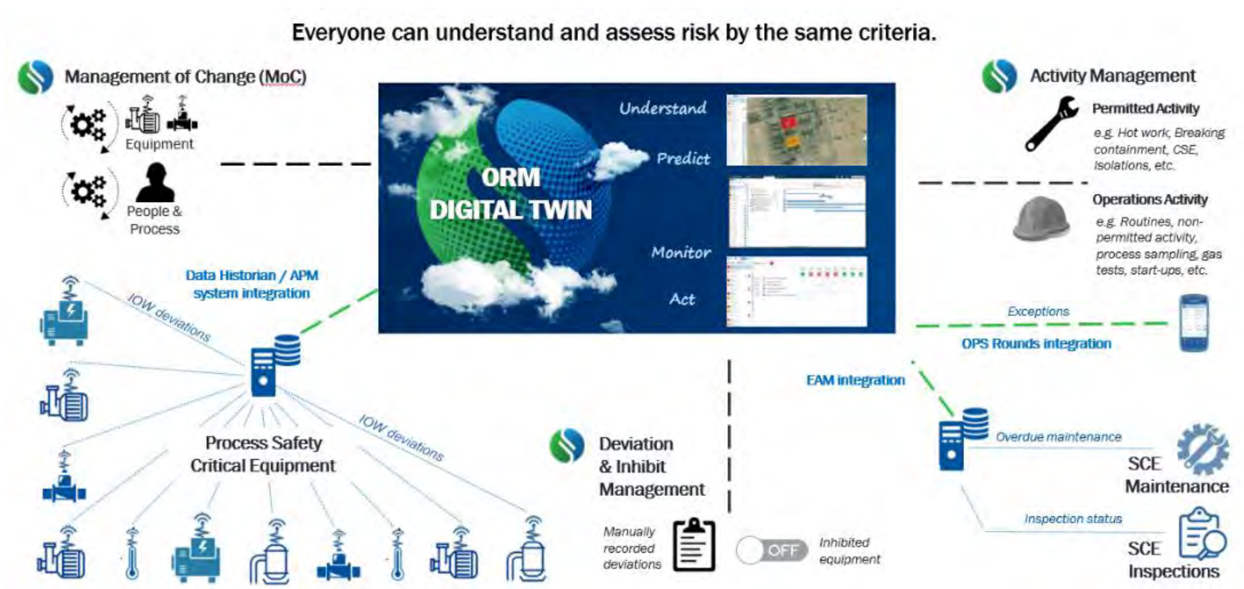
If we think about the daily activities of the frontline worker, there are many situations where providing a common view of the operational reality of the facility—that is, an understanding of where equipment conditions or planned activities may impact operational risk—will help support effective decision-making. By bringing all human and sensor-derived inputs together in a combined way to see their cumulative risk impact on the operational reality of the plant, operators can understand the health status of process safety-critical equipment and the impact of performance deviations and abnormal conditions. With a common view of risk,
everyone can understand and assess risk by the same criteria. This provides a holistic and common means of balancing risk against production at all levels of the operation.

Major accident hazard risk exposure can be made visible, prominent and available in real time. It can be viewed in time, location and in a dynamic process safety barrier model with drill-down capabilities to quickly understand what's driving the risk. Everyone can understand what activities or conditions drive risk and which process safety barriers are affected or impaired by specific work activities, actions and operational requirements. This allows you to proactively manage the health status of safety-critical equipment and the impact of performance deviations and abnormal conditions.

Knowing what is happening, when it is happening and where it is located allows operations staff to understand better how the state of the plant potentially can impact planned activity and how planned activity could potentially impact the state of the plant.

How Does Data Get Into the ORM Digital Twin?

An ORM Digital Twin allows us to connect disparate sources of data that represent all activity, deviations and nonconformances on the facility and generate a "common currency of risk." The cumulative impact of these risks can be modeled to help everyone understand and assess risk by the same criteria, to make better operational decisions, and to proactively intervene to prevent major hazard events. Support for diverse integration needs, ranging from direct point-to-point integration with third-party systems to robust involvement with integration middleware via RESTful Web Service API, Plugins, Messaging (MQ) and custom connectors is key. The diagram below illustrates how insights can be created with the help of an ORM Digital Twin by extracting, translating and aggregating data from sensors, systems and human activity.

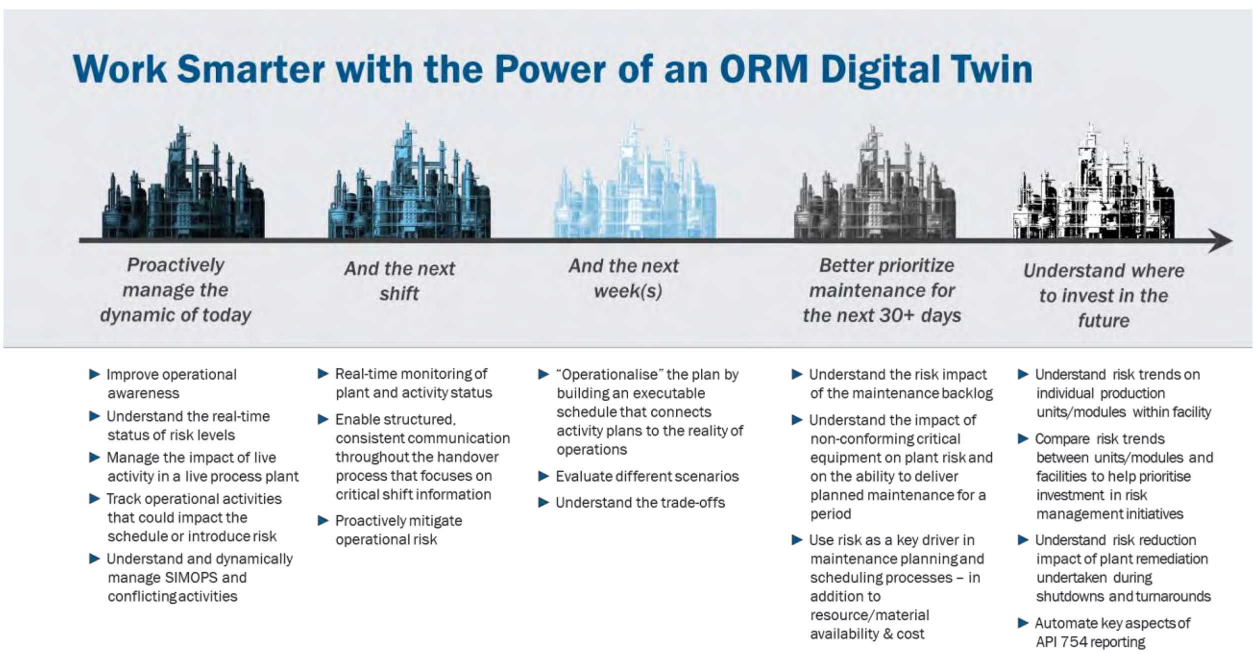


- Make the IIoT operational by connecting the status of process safety-critical equipment sensor (e.g., temperature, pressure, vibration sensors) data to its impact on cumulative Operational Risk with real-time or near-time integration to Historians and APM systems using time-weighted averages.

- Automatically connect overdue and planned maintenance and inspection data with integration to EAM/CMMS and Inspection systems.
- Automatically capture process- and people-related "risk" data with real-time integration of EPTW-CoW, Environmental Health & Safety and other systems.
- Automatically capture the Operational Risk impact of Management of Change (MoC), inspection data, inhibits, emergency-critical and environmental control system statuses.
- Manually raise, risk assess and manage performance deviations for impairments, deferrals, overrides, MoCs or even how well processes, procedures, and drills are followed.

Leverage the Power of IIoT and Manage Process Safety With an ORM Digital Twin

Digital Transformation/Industry 4.0 done right is an ongoing process that will change the way hazardous industries operate. It's fundamentally about new end-to-end business processes empowered by technology to produce positive business outcomes. As we have demonstrated, an ORM Digital Twin with its digital representation of the operational reality can unlock a radically different, far more effective way to visualize and manage activity and risk. By connecting people and processes and closing the loop between operations; maintenance; engineering, Environmental Health & Safety; and other functions, digital solutions can deliver meaningful, actionable insights with powerful visualizations of risk and activity. An ORM Digital Twin can help connect previously disparate business processes in ways that just haven't been possible until now. It can relate the collective performance of your process safety systems to the real, cumulative risk impact on operations at any given point in time.



[1] https://en.wikipedia.org/wiki/Houston,_we_have_a_problem
[2] Founder Institute

[3] Verdantix
[4] 2019 Sphera PSM/ORM Survey – Part 1: The State of Process Safety and Operational Risk Management
[5] Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems (Excerpt) https://www.researchgate.net/publication/307509727_Origins_of_the_Digital_Twin_Concept
[6] Operational Excellence Index 2018/2019

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

On Model-Based Systems Engineering for Design, Management, and Governance of Protective Systems

Antonio Arreola-Risa, Diana Gallart Hamilton*,
M. Sam Mannan, Paul Nelson, Martin A. Wortman
Texas A&M University
College Station, Texas 77843-4113.
Tecnológico de Monterrey Campus Estado de México, México.
*Presenters' E-mails: dgallart@tamu.edu, dgallart@tec.mx

Abstract

Protective systems failure can be catastrophic, and originates in management failure. These systems rely on a document-based approach, which involves handling disjointed artifacts that are expensive to maintain and may become inconsistent and obsolete. We propose a framework for managing process safety that pioneers the modeling of protective systems according to the tenors of model-based systems engineering (MBSE). The framework embeds management and governance, and harmonizes regulations and inconsistent industry guidelines. Potential users include enterprises and regulators in the chemical process safety industry and the energy sector. The framework starts the development of more sophisticated standards to prevent catastrophic protective systems failures.

Keywords: MBSE, Model-Based Systems Engineering, Protective Systems, Management of Change, Managing Process Safety, SysML.

1 Introduction

Designing and operating protective systems is a major engineering endeavor, due to the intricacy and complexity of its technologically enabled physical components, the management system that supports them, and their wide variety of stakeholders. Furthermore, protective systems need to be constantly evolving, in order to remain effective as disruptive technologies emerge, and policies, regulation, operating conditions or requirements change. This constant evolution brings the additional challenge of management of change throughout their lifecycle.

Every year, incidents happen in safety-critical companies throughout the world. While the majority of them are "near misses", others have significant economic and moral implications, as they result in important business interruption costs, property damages, environmental damages, injuries and fatalities among both internal workers and external civilians who may or may not be aware of the risks imposed on them. Regulators and judges therefore require methods and tools to reduce the asymmetry of information, mitigate moral hazard, and induce preventive and protective measures while facing financial and informational constraints and dealing with a large number of agents. Seeking to deter the risk-creators and compensate the victims, they use *ex post* civil liability and *ex ante* safety regulation in its various forms: compliance-based regulation (prescriptive regulation), performance-based regulation, and process-based regulation (integral supervision).

Many minor incidents have quickly escalated into major events, with poorly mitigated consequences (Marsh-Ltd, 2018). Although several other incidents with significantly less damage have the same root causes, all of the largest property-damage losses that have occurred in the last few decades in the hydrocarbon industry, were due to a simultaneous failure of various prevention and mitigation layers in the protective process-safety management system (Marsh-Ltd, 2014).

The failure of protective systems can be catastrophic; and such failures are associated to management failure (Marsh-Ltd, 2018; Jarvis and Goddard, 2017; Summers and Hearn, 2012). Infrequent inspections, lack of preventive and corrective maintenance, faulty designs, lack of needed redundancies, the use of incompatible equipment, materials or protocols after a deficiently planned change, improper resource allocation, careless operation by personnel not properly trained or with excessive workload, and many other issues that can cause a major incident are originated in management.

Nevertheless, managing protective systems requires more than ensuring compliance with practices and procedures. It is extremely difficult for several reasons, including not having enough historical data to analyze (Selvik and Abrahamsen, 2016) or being uncertain about whether systems indeed function properly in the fortunate absence of initiating causes. Models such as the safety pyramid, based on the work of H. W. Heinrich (Heinrich, 1941) and its extensions (Rebbitt, 2014), suggest that focusing on the underlying causes of near misses, where more data exists, can be useful to prevent serious incidents, as their underlying causes are essentially the same. While identifying and addressing the initiating causes of incidents is undeniably beneficial to advance process safety, if protective systems work as intended, the critical consequences of initiating causes can be prevented or mitigated. The usefulness of information provided by the study of near misses is limited, as it may not always be related to aspects affecting protective systems.

Furthermore, the implications of a shared governance, the dynamic nature of technology and people in the system, as well as the multiple interactions among their elements, increase complexity. Safety is an emergent property (Leveson, 2013); this implies that elements that may be safe on their own, do not necessarily constitute a safe system once they interact with other components. As safety-critical technologies evolve and complexity increases, we need tools to improve our ability to manage them.

Protective systems are often characterized by a group of protection layers, such as inherently safer design, control, supervisory, preventive, mitigative, barrier, limitation, and response (Center for

Chemical Process Safety, 2007), intended to reduce the frequency or consequence severity of hazardous events (Center for Chemical Process Safety, 2001; Center for Chemical Process Safety, 2007; Crowl and Louvar, 2011). This representation, similar to the Swiss Cheese Model of Accident Causation, proposed by Dante Orlandella and James T. Reason of the University of Manchester, is used in Layer of Protection Analysis (LOPA), whose primary purpose is to determine if there are sufficient layers of protection against a hazardous scenario to meet an organization's risk tolerance criteria. Given that no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the incident tolerable (Center for Chemical Process Safety, 2001; Dowell, 2011). Modeling protective systems based on their physical layers designed to prevent, and ultimately respond to a loss of containment in the presence of an initiating cause seems appropriate, but this approach is limited, as it does not encompass management issues, such as who the owners and operators of each layer are or who is accountable for them. When the same agent manages two or more layers, this makes them subject to common-cause failures, which makes the assumption of independence between layers is hard to achieve in practice.

Advancing the efficacy of protective systems requires more than focusing solely on improving their physical components, as several engineering research works do; the way they are designed, but also managed and governed is key as well. The paradigm of High Reliability Organizations (HROs), by Todd LaPorte, Gene Rochlin, and Karlene Roberts, of the University of California, Berkeley, links management to safety (Roberts, 1990a; Roberts, 1990b; Roberts and Bea, 2001; Roberts and Libuser, 1993); however, that paradigm does not provide a model suitable for analyses and simulation, and does not encompass regulatory issues. While industrial associations, regulatory bodies, and other disciplines have done a remarkable work to offer guidelines and best practices involving management (Center for Chemical Process Safety, 1994; Center for Chemical Process Safety, 1995; Center for Chemical Process Safety, 1996; Center for Chemical Process Safety, 2007; Center for Chemical Process Safety, 2008; Center for Chemical Process Safety, 2011), there are some inconsistencies among their publications, which complicates integration, and their work still relies on the traditionally used document-based approach. This implies handling and maintaining a large number of disjointed artifacts, which is expensive and time consuming; but more importantly, may lead to inconsistency and obsolescence, thus aggravates the problem of deficient management of change.

MBSE is a relatively new approach, which emerged in the aerospace industry, that significantly reduces the limitations of its document-based counterpart, and has other benefits beyond maintenance, including traceability and impact analysis capabilities. It has been successfully applied in other technologies, but not yet in protective systems.

Our work presents a framework that embeds governance in protective systems, and pioneers the modeling of the multiple dimensions of protective systems according to the tenors of MBSE. It harmonizes regulations, theories, and inconsistent industry guidelines; provides a realistic approach to manage multiple aspects of change; and offers traceability and visualization capabilities.

2 MBSE

2.1 What is MBSE?

Systems Engineering (SE) has many definitions, as those given by the International Council on Systems Engineering (INCOSE) (Walden et al., 2015), the U.S. Department of Defense (DoD) (Office of the Deputy Assistant Secretary of Defense, 2016), the National Aeronautics and Space Administration (NASA) (NASA, 2007), the Federal Aviation Administration (FAA) (Federal Aviation Administration, 2016), among other institutions and authors. They often refer to an interdisciplinary approach or process to design, realize, manage, operate and retire successful systems, document and satisfy requirements, meet the user needs, while taking into account their socio-technical aspects. SE is seen as an effective way to manage complexity and change (Walden et al, 2015). SE approaches can be either document-based, or model-based. The document-based approach has many drawbacks, because it involves having many disjoint artifacts, which can easily become inconsistent and obsolete. In the model-based approach, the main artifact is an integrated, coherent, and consistent system model (Delligatti, 2014), which evolves and is refined using model-based methods and tools (Friedenthal et al., 2015).

MBSE is "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases" (Holt, 2004). The three pillars of MBSE are modeling languages, modeling methods, and modeling tools (Delligatti, 2014). Modeling languages are standardized mediums to communicate model elements and their relationships; modeling methods ensure model consistency; and modeling tools enable the creation of models with elements, relationships, and views, in such way that any change made to a model element on a diagram automatically propagates, instantaneously updating all the other diagrams where that element is displayed.

MBSE practitioners commonly use the Systems Modeling Language (SysML). It originated from an initiative between the Object Management Group (OMG) and INCOSE in 2003, intended to adapt the Unified Modeling Language (UML) for systems engineering applications (Holt and Perry, 2014), allowing to represent the structure, the behavior, and the requirements of a system through nine types of diagrams. Block definition diagrams (BDD) display and categorize elements and their relationships. Internal block diagrams (IBD) show the connections between the internal parts of a block and their interfaces. Parametric diagrams (PAR) express constraints using equations and inequalities. Package diagrams (PKG) display the organization of the model as a package containment hierarchy. Requirements diagrams (REQ) use texts to display requirements, and how other model elements satisfy, verify and refine them. Activity diagrams (ACT) depict the transformation of inputs into outputs and the flow of control through a sequence of actions. Sequence diagrams (SD) specify interactions among blocks via operation calls and asynchronous signals. State machine diagrams (STM) specify the states of a block and possible state transitions in response to event occurrences. Use case diagrams (UC) illustrate the actions that a system performs, as well as the actors that invoke and participate in them (Delligatti, 2014).

2.2 Benefits of MBSE

Modeling a system is useful in characterizing existing systems, designing new systems, conducting impact assessments, and training its operators and maintainers (Friedenthal et al., 2015). Modeling helps to address complexity, lack of understanding, and poor communications. When applied effectively, MBSE is a formidable approach to manage complexity and increase the understanding of a system, and brings important benefits such as consistency, coherence, traceability, a common language that improves communication, as well as the automatic generation and maintenance of system documents (Holt and Perry, 2014). The diagrams and texts used in this approach are views of the underlying system model, not the model itself (Delligatti, 2014), thus, they communicate different aspects of the system model, such as its structure, behavior, requirements, at different levels of granularity, and may suit the information needs of different audiences, while remaining consistent and integrated.

2.3 MBSE and safety

SysML has been employed successfully in the aerospace and defense industry (D'Ambrosio and Soremekun, 2017), with safety applications, particularly during the design phase. Jensen and Tumer (Jensen and Tumer, 2013) used SysML to evaluate the safety of a system under critical event scenarios involving one or more component failures in the design stage of a maneuvering system for a satellite. They included in their system model the object view for the software and hardware components, the view of function for their behavior, and a third view called "safety functions", referring to the property of a system to resist moving from a hazardous state to an mishap state, essentially describing protective systems in a broad sense. The use of SysML extensions has been proposed for improving the modeling of mechatronics specificities such as interconnection components and multi-physical interactions in an Electro-Mechanical Actuator for aeronautics industry (Mhenni, Choley, and Nguyen, 2015). The use of MBSE with SysML has also been proposed for handling the increased complexity of the automotive industry (D'Ambrosio et al., 2017).

3 Conceptual Model of Protective Systems

Our conceptual model of protective systems, depicted in Figure 1, shows the broad, interrelated elements that constitute a protective system. Together, they provide a baseline for the structure of our MBSE framework, referred to as the "system model".

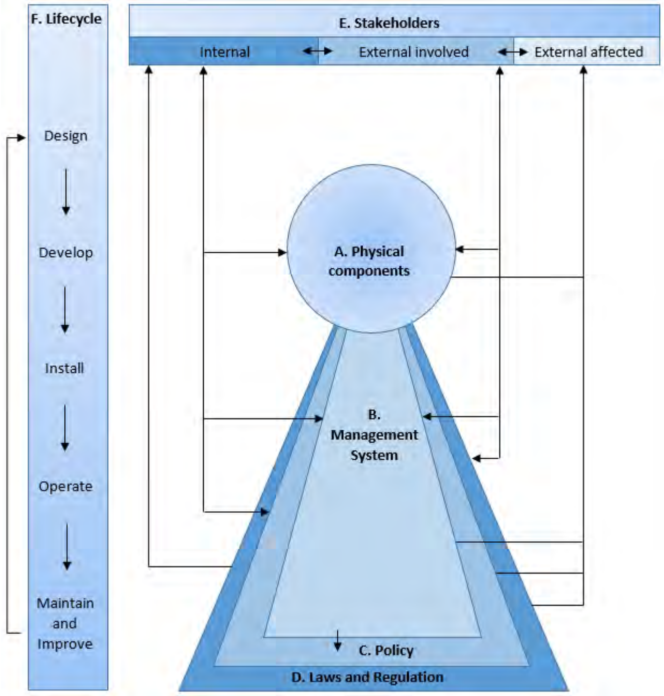


***Figure 1**. A conceptual model of protective systems.*

3.1 Model elements

The *physical components* (A) such as sensors, alarms, relief devices, dikes, water curtains, and emergency shutdown systems, for instance, are present in the preventive, mitigative, barriers, and limitation layers of protection. Physical components are supported by a *management system* (B) that includes operating procedures, control systems, monitoring and supervision activities intended to prevent hazardous events and correct anomalies. Management of change, design procedures, documentation, hazard assessment, processes for reviewing and preserving equipment integrity, human factors, training, audits, incident investigation, and emergency response, among others, are activities of major importance that belong to the management system. Industry standards and guidelines such as those from the CCPS of the AIChE (Center for Chemical Process Safety, 2007), serve as a basis for their identification. This element encompasses the structure, processes and resources contained in the inherently safer design, control, and supervisory layers, but also the management part behind the responsive layer. The management system provides the structure, processes and resources to establish the *operating policy* (C), which must comply with the applicable *laws and regulation* (D). The *stakeholders* (E) can be classified into three categories: internal, external involved, and external affected. The internal ones belong to the company and actively participate in the design, operation and management of the protective system. While the external agents do not belong to the company, some are involved in such activities (e.g. manufacturers, first responders, regulatory authorities), whereas others are not, but can be affected by protective systems failure (e.g. near neighbors).

The *lifecycle* (F) acknowledges that there are various stages that depend on and build upon each other over time. For that reason, the system model artifacts need to show in what stages certain activities occur. The outputs of each stage may become the inputs for the subsequent, which implies that they will inherit characteristics, consequences of decisions or issues to address. When referring to the lifecycle, many SE approaches have a “cradle-to-grave approach”, defining it as the entire spectrum of activity, from the identification of needs to the system retirement and material disposal (Blanchard, 2008), including the stages of observation, failing/concern/opportunity awareness, development, transition, operation, maintenance, enhancement, overhaul, decommission, and disposal. Conversely, the CCPS organizes the protective management system lifecycle in seven phases: (1) planning, (2) risk assessment, (3) design, (4) engineering, (5) installation, commissioning, and validation, (6) operational and mechanical integrity, and (7) continuous improvement (Center for Chemical Process Safety, 2007). While the activities of abandonment of outdated practices and decommission and disposal of obsolete or worn out materials are still implicit in the last two stages, this concept of lifecycle phases is consistent with the evolving nature of protective systems, and follows a “cradle-to-cradle” approach, which is the one we chose for our model.

3.2 Interactions among elements

Besides presenting a structural decomposition of the main types of elements of a protective system, it is important to understand some interactions and dependencies depicted by the arrows in the conceptual model. No individual has full visibility of the whole complex system, and yet, changes in one element could affect others as well. The needs of the stakeholders are refined into requirements for the physical components and the management system. Internal stakeholders can determine policy, and some external stakeholders may affect laws and regulation. Both types of stakeholders may be affected by protective system failure. Internal stakeholders, as well as the external involved, possess more information about the protective system compared to the remaining external stakeholders, as the former work together to design and operate it. Nevertheless, the external stakeholders who are involved, such as the regulatory authorities and the citizen participation groups who represent the near neighbors, can take into account the interests of the external affected stakeholders. These interactions can prevent or mitigate asymmetry of information issues.

The management system (B) supports the physical components (A) and establishes the operating policy (C), which must comply with the applicable laws and regulation (D). The arrow that connects (B) and (C) illustrates that unidirectional dependency. Given that policy does not automatically change when the regulation does, the model does not include an arrow connecting (D) and (C). Instead, laws and regulation can affect the internal stakeholders who are able to change policy directly, and the stakeholders who create or modify laws and regulations can affect the management system that establishes policy. Also, the graphical representation of (B), (C) and (D) as various layers, with (D) as the outer layer reinforces the idea of compliance. Presenting (B) as the base for (A) conveys the idea that the management system supports the physical components. The arrows that connect each lifecycle stage represent how stages depend on and build upon each other. The feedback from the “maintain and improve” stage to the “design” stage is consistent with the cradle-to-cradle philosophy. Given the very low level of granularity in our broad conceptual model, the specific interactions between (F) and (E) are not shown; however, other artifacts in the detailed system model developed after it should indicate what stakeholders participate in each lifecycle stage.

For the sake of simplicity, the conceptual model does not show the possible interactions among elements of the same type, but these clearly exist and must be included in the system model. Physical components interact among themselves: sensors provide inputs for logic solvers and final elements; closing a valve on the discharge of a pump may result in pump damage; opening a pressure control vent valve may affect the amount of released gases that incinerators or flares will need to burn. In the management system, new operating procedures, as well as lessons to learn revealed in incident investigations and audits, have to be communicated in the form of training to personnel and contractors; hazard analysis or evaluation require process safety information, and changes in any element need to be assessed and approved by management of change.

3.3 The dynamic nature of protective systems

Protective systems have a dynamic nature. They must respond to the new demands from the safety-critical technologies they are intended to protect, which evolve over time. Their physical components wear out and become obsolete as technology advances, personnel turnover demands training and documentation, laws and regulations are amended, the needs and requirements of the different types of stakeholders change, affecting the management system and the operating policy. Change is constant and inevitable. Failing to manage it effectively can compromise the efficacy of protective systems.

4 Results and discussion

4.1 A computerized model in SysML

Based on our conceptual model of protective systems that encompasses the physical components, the management system that supports them and determines the operating policy, which must be consistent with laws and regulations, and has different stakeholders participating throughout its lifecycle, we created a computerized model, referred to as "the system model". We used the modeling language SysML, and the software NoMagicMagic Draw 18.3 with its SysML Plugin, and the Paramagic Plugin for simulation purposes. This model details each broad category of elements in order to show their structure and behavior, as well as the relations and interactions among them. It consists of more than 500 blocks, 74 activities, 49 packages, 31 requirements, 77 use cases, and 7 views and viewpoints, sketched in over 65 diagrams. The full diagrams are available from the authors upon request. For its design, we used information extracted and adapted from the CCPS guidelines and Occupational Safety and Health Administration's Process Safety Management of Highly Hazardous Chemicals (OSHA PSM) (U.S. Department of Labor. Occupational Safety and Health Administration, 2000).

4.1.1 LOPA as one of many views of the system model

According to the MBSE approach, the diagrams and other system artifacts are simply views of the system model. They reveal portions of the model at specific levels of granularity. Our system model presents the current characterization of protective systems, which consists of a group of protection layers used in LOPA, as one view of protective systems. Figure 2 conveys the idea that the protection layers, which are inherently safer design, control, supervisory, preventive, mitigative, barriers, limitation, and response, can be affected by initiating causes, such as instrumentation failure, equipment failure, an external event, human error, or utility failure. While this broad representation may be useful to illustrate the main idea behind LOPA, many other views in our model system provide greater detail regarding the structure, behavior, and relationships between each type of the many elements of a protective system.

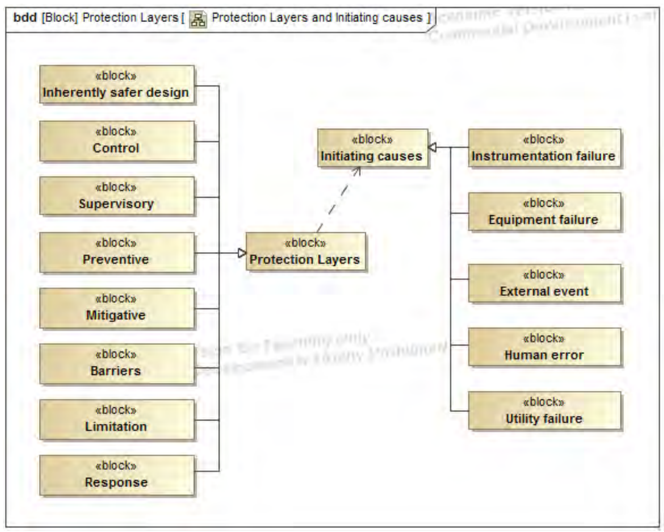


***Figure 2**. Protection layers and initiating causes.*

Diagram 1 shows a BDD with the taxonomy of the protection layers. It presents the generalization between devices and the type of protection layer into which they can be classified. Generalizations show that the subtype is a type of a supertype. This is useful, as all the properties assigned to a supertype are inherited to the subtypes, whereas those from the subtypes are only specific to them. Diagram 2 has a taxonomy of the initiating causes and displays an accepted definition of each for documentation purposes. Diagram 3 provides further details regarding generalizations, composite associations, reference associations and dependencies of such protection layers. In other words, it conveys structural decomposition, depicts existing connections and possible unidirectional or bidirectional accesses among certain elements, and the notion that whenever one element changes, others stated there may change as well.

Figure 3 corresponds to a portion of Diagram 3, which illustrates that the process alarms have both hardware and software, and that changes to alarms hardware may affect alarms software. It also shows that process alarms, as well as basic process control systems, belong to the Control protection layer. Another portion, depicted in Figure 4, exposes the unidirectional connections among pressure relief devices with knockout drums, condensers and incinerators; pressure relief devices and vents; scrubbers and vents; and scrubbers and flares. It also shows the factors that determine the necessary height of the elevated flares: the stack diameter, the distance from the base of the flare, the desired heat intensity, the vapor rate, and the molecular weight of the vapor, each one with their respective units. The corresponding equations, which appear as constraints, are embedded in the model through the use of PAR. Diagram 4 complements Diagram 3 by revealing the functions that these types of mechanical equipment perform in a relief system, in an ACT. A portion of it is shown in Figure 5.

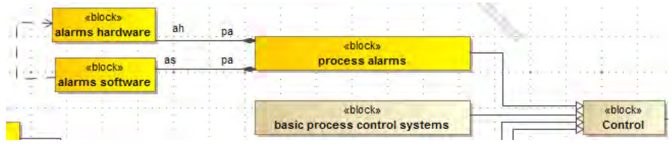


Figure 3*. Portion of BDD in Diagram 3 showing process alarms.*

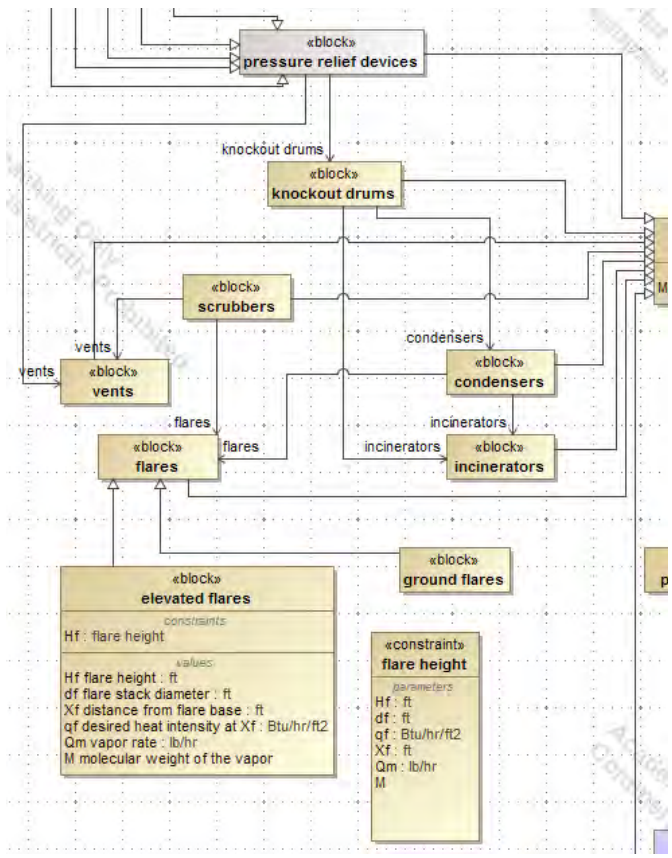


Figure 4*. Portion of BDD in Diagram 3 depicting relations among various types of mechanical equipment.*

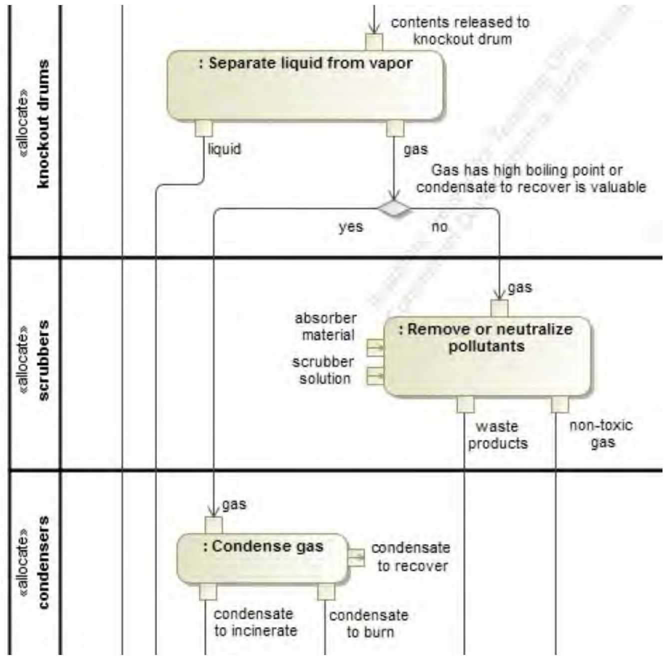


Figure 5. *Portion of ACT in Diagram 4 showing the functions performed by some mechanical equipment.*

4.1.2 Physical components

Many of the elements that constitute the protection layers are physical components. Because of these generalizations, defined in Diagram 5, the structural and behavioral features assigned to the block of physical components are inherited automatically, by transitivity, to all the subtypes. Further properties are assigned only to specific subtypes. Figure 6 illustrates that all physical components have maintenance procedures, installation procedures, and inspection and testing procedures; but only specific physical components have other properties: mechanical equipment has piping and instrument diagrams; various types of pressure relief devices, which are a subset of the mechanical equipment, have a relief system design.

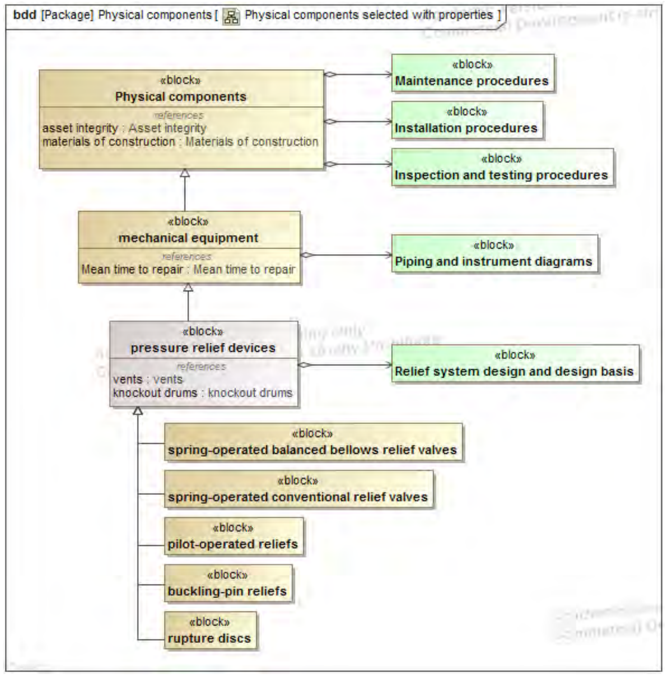


Figure 6. *Selected physical components with properties assigned at various levels.*

4.1.3 Management system

The management system that supports the physical components is represented in our system model in Diagrams 6 through 20, in order to display the various elements present in OSHA PSM, as well as their respective components, which were modeled as parts. Figure 7 shows them summarized, in the form of one block, with its elements displayed as part properties. In Diagram 21, an IBD details the information and objects that flow across the elements of the management system, which reveals possible interactions among themselves. A portion of it can be found in Figure 8. Management of change (MOC) is one of the main components of the management system. Given the multiple interactions that MOC has with other components, as well as its major importance in process safety, it deserves special attention. Our model includes a section related to MOC systems, based on the CCPS guidelines for the management of change for process safety (Center for Chemical Process Safety, 2008). Diagram 22 displays various packages with the inputs and outputs to and from MOC, such as the package in Figure 9. Diagrams 23 through 32 illustrate diverse aspects of MOC, from the commitment required from management to allocating resources and providing training to those involved in activities derived from or affected by changes, the key principles and essential features of MOC, the activities of MOC decision structure, or the tasks that should be performed during the design and development lifecycle stages in order to create a MOC system, to the roles that internal stakeholders play in MOC, the steps followed during MOC, and details about the request for change review and approval procedure. Figure 10, Figure 11, and Figure 12 present portions of such diagrams.

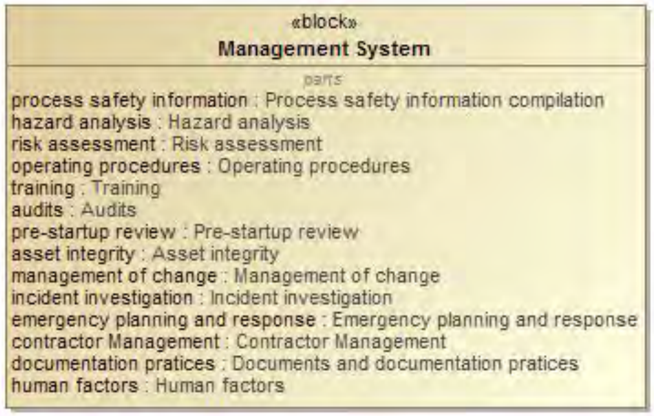


***Figure** 7. Block of the management system.*

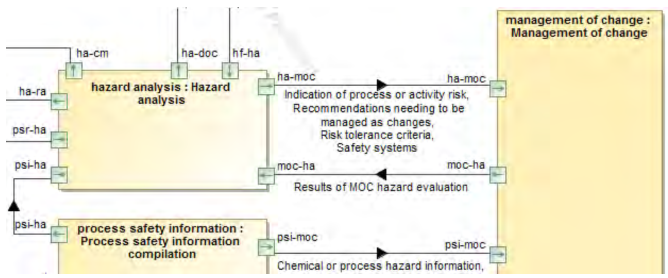


***Figure 8**. Portion of the IBD in Diagram 21 depicting information flow within the management system.*

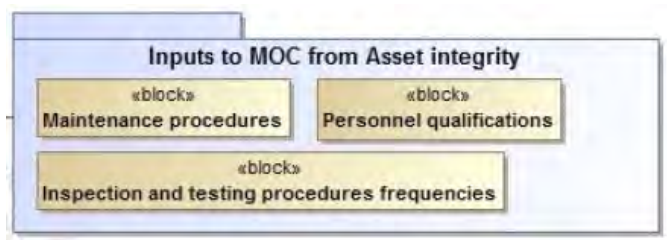


***Figure 9.** Portion of Diagram 22 depicting a package of inputs to MOC from Asset integrity.*

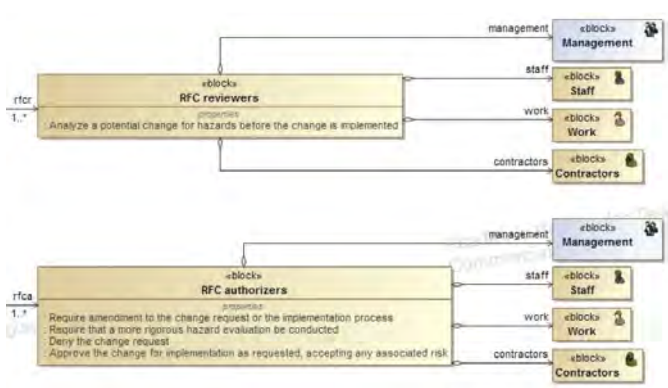


***Figure 10.** Portion of the BDD in Diagram 29 depicting the roles in MOC and the stakeholders who play them.*

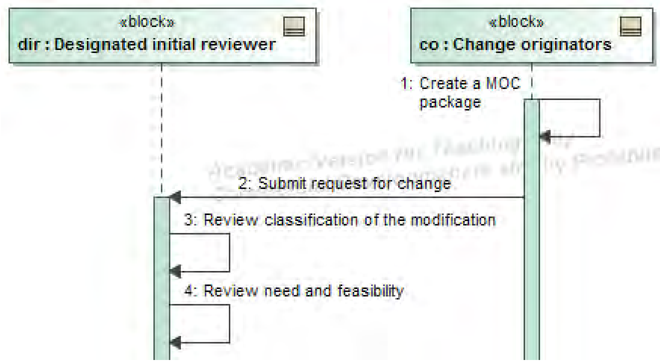


Figure 11. *Portion of the SEQ in Diagram 31 depicting the steps followed during MOC and the interactions among the people playing each role.*

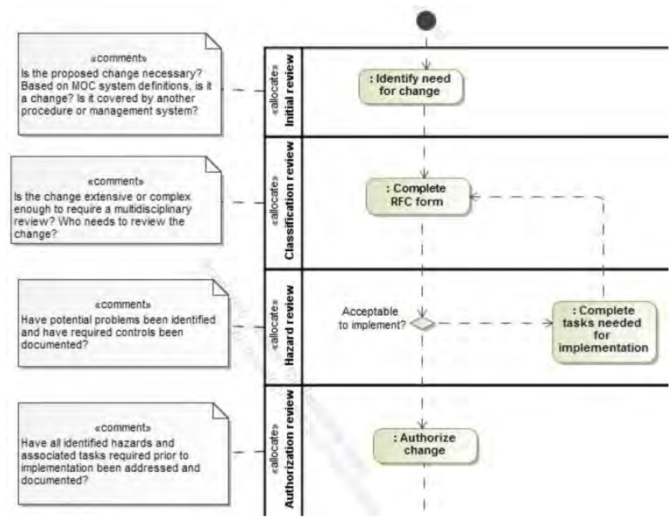


Figure 12. *Portion of the ACT in Diagram 32 depicting the Request for change review and approval procedure.*

4.1.4 Policy, laws and regulation

The policy element from our conceptual model is included in the system model in various ways. The operating procedures part of the management system, detailed in Diagram 16, encompasses many aspects of policy, such as the steps required to correct or avoid deviation in the operating limits, the engineering controls and the administrative controls established in safer work practices, failure responses, compensating measures and procedures to apply in the event that a shutdown fails. Another way to represent policy is through the information that flows across the parts of the management system, since it includes procedures (e.g. inspection procedures, maintenance procedures) and criteria (e.g. risk tolerance criteria, criteria for applying procedures). Some blocks from the taxonomy of the protection layers are also elements of policy.

Policy, laws and regulations also appear in our model in the form of requirements. Requirements may be represented as tables, as part of block diagrams, or as REQ. We also used use cases, with their corresponding activity diagrams, to illustrate courses of action, as in Figure 13. Various relationships among requirements and other model elements, such as containment, trace, derive requirement, refine, satisfy, and verify, provide greater detail and further properties regarding how those requirements are fulfilled or can be traced in the system. In Diagrams 35 and 36 we included examples of applicable laws and regulation, such as OSHA PSM, the Toxic Substances Control Act II, the Risk Management Program of the Environmental Protection Agency (EPA RMP), the Emergency Planning and Community Right-to-Know Act, in the form of requirements. A small portion of diagram can be found in Figure 14. Diagram 37 is a REQ that also shows some use cases and blocks to depict the core attributes of the protection layers. A portion of it is shown in Figure 15.

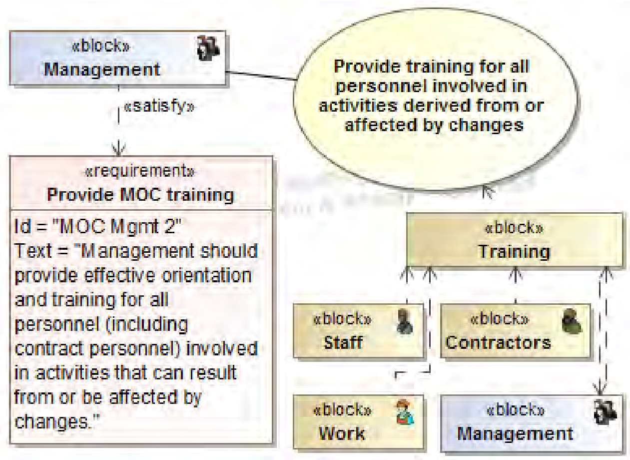


Figure 13. *Policy depicted with a requirement and a use case.*

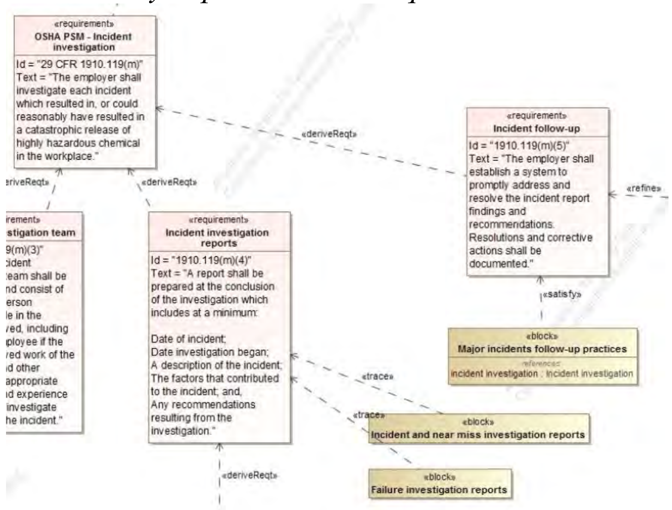


Figure 14. *Portion of a REQ exemplifying laws and regulations modeled as requirements.*

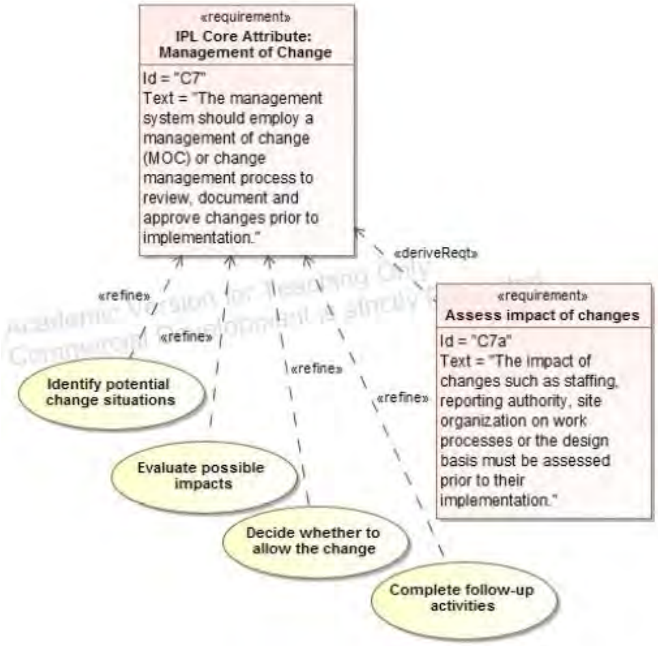


Figure 15. *Portion of Diagram 37 illustrating the use of requirements and use cases to include policy, laws and regulation in the system model.*

4.1.5 Lifecycle

The lifecycle is represented in the system model in various views. The first one, presented in Diagram 38 and Figure 16, shows the lifecycle as an aggregate of various stages. An aggregate, in contrast to a composition, is not responsible for its parts (Weilkiens, 2007). The direct reference associations that link the stages convey the idea that they depend and build upon each other. The position of the arrowheads in the system model, as opposed to those from our conceptual model, do not stand for the chronological flow of information. Instead, according to the standards of the modeling language used, they suggest that the later stages can access information from earlier stages.

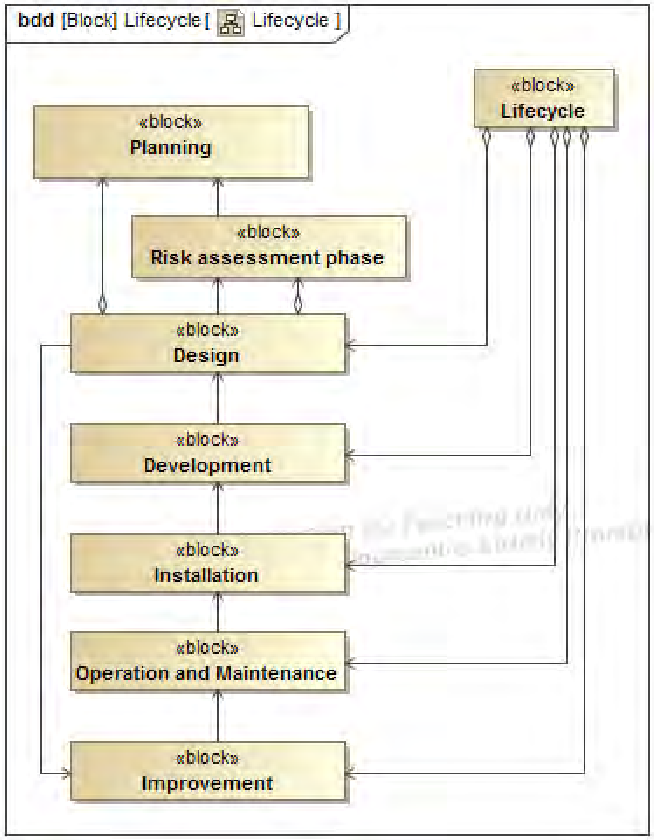


Figure. 16. *Lifecycle stages.*

The lifecycle stages also appear in the model as partitions or swimlanes in Diagram 39, which corresponds to an ACT that allocates major activities to the lifecycle stage where they are expected to occur. The diagram shows the flow of information as object tokens, as well as the control tokens that enable subsequent activities. Each activity has inputs and outputs, which are not just texts; instead, they are referenced to blocks that may appear in other diagrams and reside in a specific repository. They have properties such as parts and references, and may have further capabilities suitable for analysis. Figure 17 shows a portion of Diagram 39.

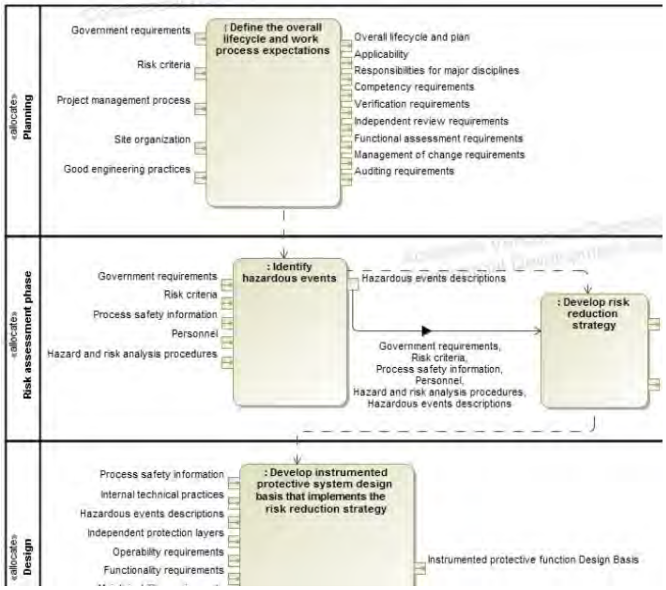


Figure 17. *Portion of Diagram 39 depicting the allocation of activities within lifecycle stages.*

Diagram 40 contains a very large BDD that reveals further information about the inputs and outputs in Diagram 39, including their structural decomposition and the various lifecycle stages to which they are allocated, as some of them are inputs to more than one activity, or outputs from one activity and inputs to another. Diagram 41 contains the same elements as those in Diagram 40, but rearranged as a tulip, in such way that the blocks that appear at the core are those that are used in two or more lifecycle stages, and the blocks in the periphery are used only during one stage. This suggests that the elements at the core deserve more attention due to their greater importance and complexity in the system. These are: hazardous events descriptions, independent protection layers, instrumented protective function design basis, operability requirements, process safety information, reliability requirements, internal technical practices, functionality requirements, maintainability requirements, independent protection layers analysis report, equipment list, and detailed engineering specification.

4.1.6 Stakeholders

The stakeholders are presented in various diagrams. In Diagram 42 and Figure 18, they are classified, as in our conceptual model, into three categories: internal involved, external involved, and external affected. They appear as icons since the software tool allows it, but they are still blocks with their corresponding functionalities. Diagram 43 has a detailed taxonomy of stakeholders, which includes those mentioned in OSHA PSM (U.S. Department of Labor. Occupational Safety and Health Administration, 2000), Rasmussen's framework (Rasmussen, 1977), and various mismatching CCPS guidelines (Center for Chemical Process Safety, 1994; Center for Chemical Process Safety, 1995; Center for Chemical Process Safety, 1996; Center for Chemical Process Safety, 2004; Center for Chemical Process Safety, 2007; Center for Chemical Process Safety, 2008; Center for Chemical Process Safety, 2011). See Figure 19 for a portion of it. We used generalizations to allow the subtypes to inherit the properties assigned to their supertype. Diagram 44 is a PKG that summarizes the stakeholders that participate in each lifecycle stage, and their respective concerns, according to the guidelines for safe and reliable instrumented protective systems (Center for Chemical Process Safety, 2007). A portion of it is shown in Figure 20.

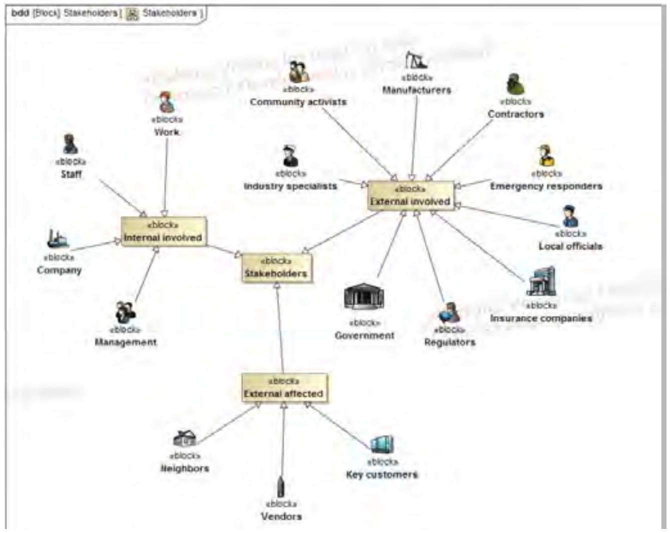


Figure 18. *Protective system stakeholders.*

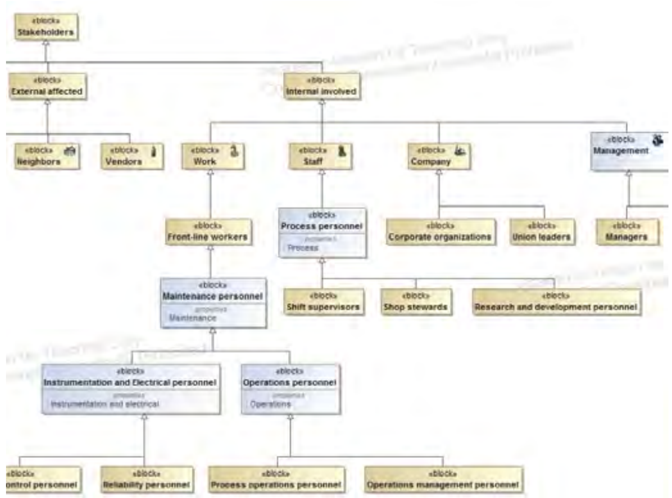


Figure 19. *Portion of Diagram 43 depicting a taxonomy of stakeholders.*

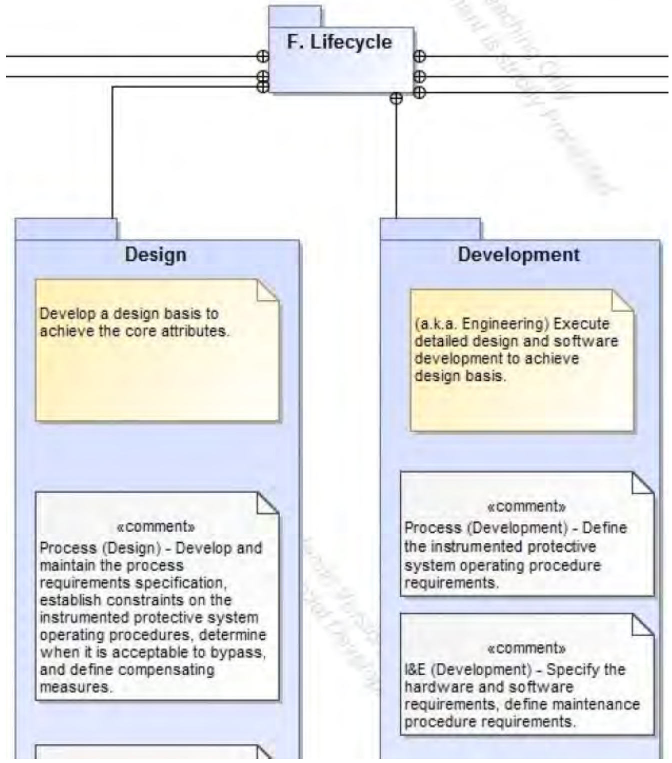


Figure 20. *Portion of Diagram 44 depicting stakeholders' concerns through different lifecycle stages.*

SysML allows to model views and viewpoints. Views are packages that selectively import various diagrams, packages, model elements, etc., which constitute an aspect that is of interest to a particular set of stakeholders (Delligatti, 2014). Viewpoints specify the stakeholder, the concerns, the purpose, the languages, and the methods. Diagrams 45a and 45b present two ways in which the stakeholders' views and viewpoints can be modeled. Not only do they show in which lifecycle phases they participate, allowing a visual comparison, but they also specify what model information is relevant to them. Figure 21 exemplifies the views and viewpoints of two stakeholders. Diagrams 46 through 52 detail packages that contain all the model elements allocated or associated to lifecycle phases.

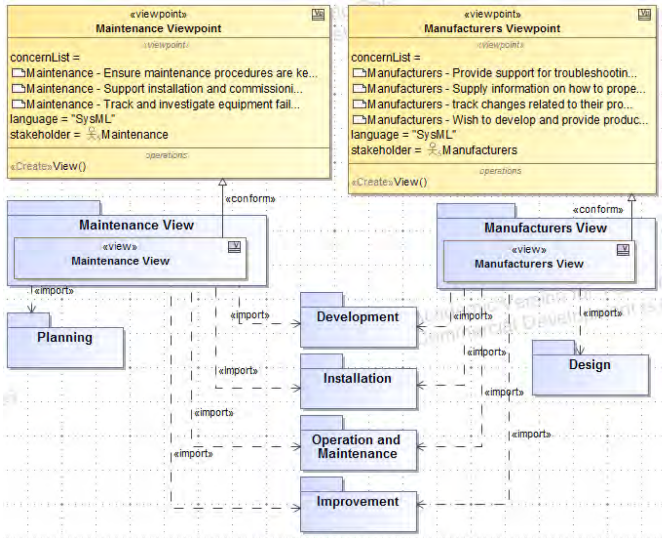


Figure 21. *Views and viewpoints of two stakeholders importing packages.*

4.2 Tools for impact analysis and management of change

Software tools that work with SysML can provide users, including designers, managers, and regulators, with tools for impact analysis and management of change. In the event we wanted to make a change in one of our model elements, it would be important to determine whether that change would impact other parts of the system. The software tool we have chosen can quickly identify in which diagrams the object appears, open them and show the element location, or navigate through the diagrams. Besides knowing the usage of a specific element in other diagrams, before making any changes to it, we need to identify what other model elements interact with it, and the kind of relationships that they have, in order to assess possible impacts. With the software modeling tool we used, it is possible to display in the current diagram the related elements from other diagrams, or display a list with the elements of the model that use it or depend on it. It is also possible to generate a dependency report in Microsoft Word, which will list all the model elements that have any kind of declared relation with the element, the type of relation, or if it is a connector that conveys information from one node to another. Although the dependency report can specify relations such as containment, dependency, allocation, association, direct association, aggregation, direct aggregation, composition, direct composition, generalization, and applied stereotypes including imports of packages, it does not show the direction of the arrows in the relations, that is, it does not specify whether the related element is a client or a supplier, and it does not display inherited relationships, that is, those assigned to a supertype. Nevertheless, these two limitations can be overcome by opening the specification of block properties for the desired blocks.

Some alternatives provided by the tool are to generate either a dependency matrix in Microsoft Excel, or an allocation matrix in NoMagic MagicDraw. A portion of an allocation matrix is shown in Figure 22. These matrices display all the elements in the model in the first row and column vectors, and the existing relations among them in the appropriate entries. Models with many unrelated elements generate sparse matrices. Since both types of matrices have the same limitations from dependency reports, we recommend to use the specification of block properties in conjunction with the matrices. If the model only declares dependencies between elements A and B, and between elements B and C, the user of dependency reports, dependency matrices or allocation matrices may be able to infer that element C could be indirectly affected by element A. Having the big picture that these matrices provide can be beneficial for impact analysis and management of change, as long as the model is well constructed and declares the relations between elements.

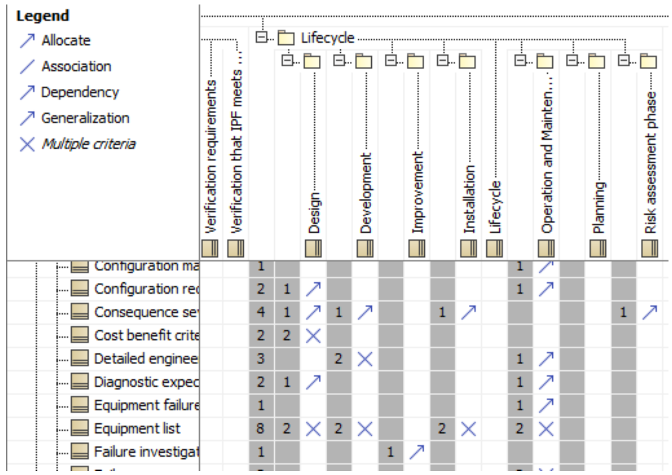


Figure 22. *Portion of an allocation matrix*

4.3 A model and a method for impact analysis in the context of MOC

One of the key principles and essential features of management of change is to evaluate possible impacts (Center for Chemical Process Safety, 2008). Impact analysis requires a model and a method. The model of protective systems we have presented, which can be adapted to the characteristics of the industries where it will be used, offers the stakeholders tools to perform this activity. Its outputs include lists and matrices that show dependencies and other relations among its elements. The software functions allow the user to identify where each element is used.

Our proposed method for impact analysis with our model recommends the following steps: First, use the software tools to identify where a model element is used, in order to ensure that a possible change that seems pertinent according to a diagram is indeed suitable in the remaining diagrams. Second, refer to the outputs of the model and check what are the other elements that have any dependencies or other declared relations with the element whose impact is being analyzed, and what kind of relation exists among them. If there are dependencies with other elements, the user should go further and identify the dependencies that those related elements have with other not already considered elements. Dependencies communicate that a change in the supplier element (at the arrowhead end) may result in a change to the client element (at the tail end). Therefore, the user must pay attention to the direction of the dependency to determine whether the element is a client or a supplier.

4.4 Cross-sections, views and viewpoints for shared governance and multiple stakeholders

Although many of the model elements are organized according to the lifecycle stages in which they occur, in order to be part of a model library that can be shared with the stakeholders involved, or be imported by another model that encompasses further aspects related to that time frame, in order to understand and address better the concerns of each stakeholder, regardless of the amount of lifecycle stages where they participate, it is possible and convenient to have a subset of the model that contains the parts that are relevant for them. The use of packages or package diagrams allows partitioning the model and presenting it as cross-sections, offering views that filter the model according to the point of view of each stakeholder, or specific aspects intended to address.

A cross-sectional modeling style, combined with the capability of the modeling language to show many views and viewpoints, is beneficial in the context of shared governance, as it can help to specify and clarify the roles and responsibilities of each group of multiple stakeholders, understand the needs and concerns of other groups, and identify possible gaps. It is also possible to create a single view of the elements that two or more types of stakeholders have in common, in order to facilitate collaboration. Creating views that import selected packages only can allow external stakeholders to obtain the information they need to know, without giving them access to aspects of the company that should not be disclosed, such as classified information, confidential business information, and trade secrets. This approach can therefore mitigate asymmetry of information without compromising sensitive information.

4.5 Implications of having a computerized model for maintenance

With regard to maintenance, the MBSE approach offers many advantages compared to its document-based counterpart. Instead of having as system artifacts several disjointed manuals, spreadsheets and other text-based files that need to be updated every time the system changes, with the difficulties inherent to keeping track of all the places in which a modified element appears and the time and resources needed to ensure that all the documents are properly updated, at the risk of having inconsistencies among the updated and outdated artifacts, leading to the obsolescence of the latter if any misses occur, the MBSE approach that our model of protective systems follows allows a fast and inexpensive maintenance that prevents inconsistencies caused by leaving one or more artifacts outdated by mistake, as any changes made to an element of the model are automatically propagated to each and every place where that element appears.

Nevertheless, this advantage also has its drawbacks. It is very dangerous to change an element of the model based solely on one of the diagrams where it appears, because all the other diagrams in which the element to update is present will instantly be modified as well, and perhaps the change may not always be desirable or compatible, or could impact other elements not previously considered. For that reason, besides being cautious about who is given the authority to modify the system model, as well as the timing for the updates, managers should always follow a proper procedure of management of change, which must include the impact analysis discussed earlier. The model should be updated only after the proposed changes have been evaluated and approved. Special attention must be paid at the moment of the update in case the change only took place in some instances of the model element, in order to adjust the model accordingly and avoid the modification of all the instances at once. For example, instead of renaming or modifying the properties of a block that is used in two or more diagrams, which would propagate the changes throughout all the diagrams where it is used, we recommend to replace the block subject to change only in the affected diagram with a new block with a different name and properties.

4.6 Benefits for managers and regulators

Managers can benefit from this model in many ways. It can lower the cost of system documentation maintenance; it provides tools for impact analysis and management of change; it can be used in training, and be used to increase awareness and understanding about the interactions and information flows among physical components, the management system, policies, procedures and requirements from laws, regulation, and recommendations from professional associations; the activities to perform during each lifecycle stage, with their corresponding inputs and outputs; as well as the notion of who the stakeholders are and what are their main roles an concerns.

Besides acknowledging governments and regulators as stakeholders of protective systems, this model also provides them with tools to mitigate moral hazard and asymmetry of information, and perform activities related to loss prevention and the preservation of public safety. Regulators have the authority to enforce the adoption and use of protective systems, but they may also suggest, promote, or demand the use of MBSE to facilitate companies to comply with prescriptive regulation, such as those in OSHA PSM, EPA RMP, or any other applicable. The adoption of MBSE practices may also facilitate audits and inspections, since companies would be able to provide the authorities with the current status of the company regarding the implementation of protective measures, as well as their processes and equipment. Regulators may also benefit from this model as it may help them to keep in hand the specific needs and concerns of the near neighbors and general population they seek to protect, summarized and captured as the views and viewpoints of the external affected stakeholders. Also, having a model that illustrates the structure and behavior of the protective systems that companies use could help them determine what information they should request in order to mitigate moral hazard and answer questions to the public. At the same time, companies can satisfy the requests of regulators by creating packages with the information to disclose to external stakeholders, consistent to their concerns.

5 Conclusions

This work presents a MBSE framework that advances the state of the art in safety-critical protective systems, by integrating the management and governance dimensions. Our model is still consistent with the current characterization of protective systems as a group of protection layers used in LOPA, but it is also suitable for combined design, operation and regulation. It reduces the cost of maintenance of its artifacts and offers tools for impact analysis and management of change. Potential users include any agents invested in the design and management of protective systems, especially enterprises and regulators from the chemical process safety industry and the energy sector. This work significantly reduces the pitfalls of its document-based predecessors, by offering a visual, organic model with traceable, integrated and consistent elements, whose changes automatically propagate throughout every part where the modified element appears, instead of a set of disjointed texts, which are prone to errors, expensive to maintain, or may become inconsistent and obsolete as the system evolves. This framework encompasses the views and viewpoints of multiple owners, whose roles vary throughout the system lifecycle. Therefore, it supports shared governance, and can be used by multiple agents within and beyond the enterprise premises. While it mitigates information asymmetry, since all of its users share the same model, it also renders the possibility to provide its specific audiences with tailored views, at different levels of granularity, filtered according to their roles and concerns. Future publications about the simulation part of this work will encompass its computational and analytical capabilities, which may allow its users to comply with and support the development of both prescriptive and performance-based regulation. The multiple benefits that the use of MBSE standards provides to safety-critical companies and its many stakeholders, at a very low expense, support our conclusion that it should be a regulatory requirement for managing process safety.

6 Acknowledgement

This work was supported by the Mexican National Council of Science and Technology *Consejo Nacional de Ciencia y Tecnología (CONACyT)*, the Mexican Ministry of Public Education *Secretaría de Educación Pública (SEP)*, and *Tecnológico de Monterrey Campus Estado de México*.

7 References

Blanchard, B. S. (2008). System engineering management. Wiley series in systems engineering and management. Hoboken, NJ : John Wiley & Sons, Incorporated.

Center for Chemical Process Safety (1994). Guidelines for implementing process safety management systems. Center for Chemical Process Safety/AIChE.

Center for Chemical Process Safety (1995). Plant guidelines for technical management of chemical process safety. Revised edition. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (1996). Guidelines for integrating process safety management, environment, safety, health, and quality. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2001). Layer of Protection Analysis - Simplified Process Risk Assessment. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2007). Guidelines for safe and reliable instrumented protective systems. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2008). Guidelines for the management of change for process safety. Hoboken, NJ : Wiley-Interscience.

Center for Chemical Process Safety (2011). Guidelines for auditing process safety management systems. 2nd ed. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Crowl, D. A. and Louvar, J. F. (2011). Chemical process safety: fundamentals with applications. Upper Saddle River, NJ : Prentice Hall.

D'Ambrosio, J., and Soremekun, G. (2017, October). Systems engineering challenges and MBSE opportunities for automotive system design. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2075-2080). IEEE.

Delligatti, L. (2014). SysML distilled. A brief guide to the systems modeling language. Upper Saddle River, NJ : Addison-Wesley.

Dowell, A. M. (2011). Is it really an independent protection layer? Process Safety Progress, 30(2):126–131.

Federal Aviation Administration. (2016). National Airspace System System Engineering Manual. https://www.scribd.com/document/98230420/NAS-Systems-Engineering-Manual-Vol-1. Accessed: 2016-08-30.

Friedenthal, S., Moore, A., and Steiner, R. (2015). A practical guide to SysML : the systems modeling language. Waltham, MA : Morgan Kaufman.

Heinrich, H. W. (1941). Industrial accident prevention : a scientific approach. 2nd ed. New York, NY : McGraw-Hill.

Holt, J. (2004). UML for systems engineering : watching the wheels. 2nd ed. London : Institution of Electrical Engineers.

Holt, J. and Perry, S. (2014). SysML for systems engineering – A model-based approach. 2nd ed. London : The Institution of Engineering and Technology.

Jarvis, R., and Goddard, A. (2017). An analysis of common causes of major losses in the onshore oil, gas & petrochemical industries. *Loss Prevention Bulletin*, (255).

Jensen, D. C. and Tumer, I. Y. (2013). Modeling and analysis of safety in early design. Procedia Computer Science, 16(2013 Conference on Systems Engineering Research):824 – 833.

Leveson, N. (2013). The Drawbacks in Using The Term 'System of Systems'. Biomedical Instrumentation & Technology. Association for the Advancement of Medical Instrumentation. http://sunnyday.mit.edu/papers/system-of-systems.pdf. Accessed: 2015-09-30.

Marsh-Ltd (2014). The 100 Largest Losses 1974-2013. Large Property Damage Losses in the Hydrocarbon Industry. 23rd edition. https://uk.marsh.com/Portals/18/Documents/100%20Largest%20Losses%2023rd%20Edition%202014.pdf. Accessed: 2015-02-02.

Marsh-Ltd (2018). The 100 Largest Losses 1978-2017. Large Property Damage Losses in the Hydrocarbon Industry. 25th edition. https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/100-largest-losses.pdf. Accessed: 2019-03-15.

Mhenni, F., Choley, J. Y., and Nguyen, N. (2015, September). SysML extensions for safety-critical mechatronic systems design. In *2015 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 242-247). IEEE.

NASA (2007). Systems engineering handbook. Washington, DC : National Aeronautics and Space Administration.

Office of the Deputy Assistant Secretary of Defense. (2016). Systems Engineering. http://www.acq.osd.mil/se/initiatives/init pp-sse.html. Accessed: 2016-08-30.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3):183 – 213.

Rebbitt, D. (2014). Pyramid power. Professional Safety, 59(9):30 – 34.

Roberts, K. H. (1990a). Managing high reliability organizations. California Management Review, 32(4):101 – 113.

Roberts, K. H. (1990b). Some characteristics of one type of high reliability organization. Organization Science, 1(2):160 – 176.

Roberts, K. H. and Bea, R. G. (2001). When systems fail. Organizational Dynamics, 29(3):179.

Roberts, K. H. and Libuser, C. (1993). From Bhopal to banking: Organizational design can mitigate risk. Organizational Dynamics, 21(4):15 – 26.

Selvik, J. T. and Abrahamsen, E. (2016). How to classify failures when collecting data for safety-instrumented systems in the oil and gas industry. Journal of Risk Research, 0(0):1–11.

Summers, A. E. and Hearn, W. H. (2012). Risk criteria, protection layers, and conditional modifiers. Process Safety Progress, 31(2):139–144.

U.S. Department of Labor. Occupational Safety and Health Administration. (2000). Process Safety Management. https://www.osha.gov/Publications/osha3132.html. Accessed: 2016-03-15.

Walden, D. D., Roedler, G. J., Forsberg, K., Hamelin, R. D., and Shortell, T. M. (2015). Systems engineering handbook : a guide for system life cycle processes and activities. 4th ed. Hoboken, NJ : John Wiley & Sons, Incorporated.

Weilkiens, T. (2007). Systems engineering with SysML / UML : modeling, analysis, design. Amsterdam ; Boston, MA : Morgan Kaufmann OMG Press / Elsevier.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Analysis of Reliability Mapping in Refining Industry: Identification of Critical Regions and Interventions in Complex Production Systems

Cassio Brunoro Ahumada[2], Érica Cayres[1], and Salvador Ávila Filho[1]*
[1]Federal University of Bahia, Polytechnic Institute,
Rua Professor Aristides Novis, 2,
40210630, Salvador, Brazil
[2]Mary Kay O'Connor Process Safety Center,
Texas A&M University, Bizzell St. 400,
TX 77843, College Station, United States of America
*Presenter E-mail: avilasalva@gmail.com

Abstract

The article aims demonstrate the importance of reliability mapping for decrease risks of shutdown and accident in critical activities. For mapping is needed to know the operational context, considering culture and deviations that between with other factors will be occasion total failure. The analyses of sociotechnical reliability need of mapping of human, operational, process and equipment reliability to occur, besides considering the system complexity and the social attractiveness, for that this way be possible the elaboration of efficient barriers. The reliability mapping demands tools in the area of social and human risk analysis, analysis of the task with the evaluation of the environment of the activities, project of work, analysis of human factors, identification of work behaviour for cultural transformation, leadership style for process safety, culture of guilt and fair culture, dynamic risk management, energy reliability and good energy practices. The Socio Technical Reliability Analyses – STRA is a more complete tool for the analyse of systems and decrease of risks. With this mapping, it is possible to identify the industrial areas that have the greatest influence on the losses occurred in the industrial context, after that it is possible use the information for make an using fault tree analyses & decision diagram. That provides for the manager makes decisions with a solid knowledge base. The methodology aims through application of tool, demonstrate the use in analyses of parameters and construction of sociotechnical reliability mapping, identifying the tasks, equipment and process that cause shutdown. After reliability assessment, it continued with barriers analysis using fault tree analyses & decision diagram tool. The conclusion is about understand different cause considering STRA and demonstrate the decision-making processes importance to take corrective and preventive actions.

Keywords: Reliability; Operations; Reliability, Factors;

1 Introduction

The article aims to demonstrate the importance of reliability mapping for industry sustainability through a case study in the application of the Socio Technical Reliability Analyzes (STRA) tool. In this paper, the mapping will indicate which vulnerabilities impact on Refining unit reliability. It is intended to elaborate tactical procedure for decision making about the contributing factors in the reliability of this system. By identifying the causes, priorities and impacts, it is possible to decide on actions in a timely manner by returning the industrial unit to its normal state, that is, operating at full load, specified quality and positive image maintained. Finally, it is proposed to provide a tool to assist in the maintenance of Organizational Resilience.

For this analysis to be carried out effectively, it is necessary to know the operational context, identifying cultural aspects, such as normalization of deviations, aspects of operational discipline, technical-organizational changes and communication, as well as process and equipment characteristics.

As discussed by Ávila [1], the STRA tool aims to increase the competitiveness of the production systems analyzed, reducing the number of failures and increasing the socio-technical reliability. Sociotechnical reliability, also known as integrated reliability, is calculated from knowledge of the operational context, human factors and technological constraints.

This paper continues to investigate reliability, but from a strategic point of view come into the discussion on organizational resilience. The STRA bases are applied to cases of the oil refining industry, with information from articles, interviews and actual data, making decision-making more evident regarding the resulting scenarios (normal situation, process uncontrollability, controlled stop and accident).

It should be noted that in complex systems, such as the refinery case, the risk is dynamic and involves a variety of task, process, equipment and human factors. In order to avoid deviations that generate accidents, a detailed risk analysis must be done, which will entail the construction of barriers with incisive action in the cause of the problem. Even though it is human, social and or technological in nature.

The complexity of this system comes from operational routine inserted in process characteristics, communication difficulties and inadequate task planning. This scenario indicates the existence of systemic failure in the operation. This failure can lead to reduced performance in production, downtime or in extreme cases accidents and disasters. Thus, being very important the case study as presented in this article, where will be made a link between all these factors in decision making and their consequences in the refinery.

1.1 Systemic Failure

Industrial technological development has been used to increase production and diversify the quality and types of products demanded by the Company. This increase in scale while preserving the image of accidents and environmental impact has brought the characteristic complexity of systems and organizations [2].

The technical complexity comes from new intricate and interconnected processes [3] that require a high level of automation. The reliability of complex systems may therefore not meet the standards expected by the Organization [4]. That is, in this type of industry there will be systemic failures (operation, equipment, instruments and or operators will suffer from failures).

The failures that occur in complex industrial systems represent losses, which can be financial, imaging and even human, on a large or small scale. Oliveira, Paiva and Almeida [5] state that although no system is indifferent to failures, in some cases failure is not an option as it can result in catastrophic events. Considering this, efforts must be made to identify inaccuracies and create barriers to prevent failures and to prevent emergencies and accidents.

Early diagnosis of process disturbances, equipment malfunction and other unwanted events plays an important role in terms of safety as well as improving process / equipment efficiency and providing better results in product quality assurance [6]. Thus, demonstrating the importance of a study of socio-technical reliability, indicating which areas are most at risk and finally how to proceed after the analysis, investing in the prevention and contingency of failures.

According to Gagliano [5], the most commonly used techniques such as Failure Mode and Effect Analysis (FMEA), Failure Tree Analysis (FTA), Cause and Effect Diagram, Pareto Diagram, Five Whys, among others, cannot always reach the root cause because they address the immediate cause, especially when physical, equipment, or process causes are identified. Thus, neglecting the impact of human and organizational interactions on the system, the socio-technical mapping then appears as an alternative to remedy this lack by analysing the entire physical and cognitive set.

1.2 Risk and reliability

According to Bharatiya [7] an example of industrial hazards is the handling of flammable products, which can cause fire, explosions and impact workers and surrounding areas as well as economic losses, plant downtime, environmental impact, damage to equipment, damage to company image. Therefore, it is necessary to analyse the risks to avoid the occurrence of failure events using physical barriers (PSV for example), cognitive barriers (redundancy in communication) and management barriers (more assertive decisions).

According to Ávila [8] the operational risk management model requires that technical and social aspects be correlated at different levels of normality / abnormality of processes with the consequences and impacts they produce on their own business, the environment and society. Keep in mind that risks are dynamic and must consider the influence of the ever-changing process, tasks, equipment, culture, and human factors for a good definition of management strategies.

1.2.1 SPAR-H

It is important to recognize the influence of human factors in the calculation of integrated reliability in the operational context. A complex industrial unit needs people who have the experience, the mind to avoid deviation and to make decisions. However, it is known about the variety of psychological stressors that influence the quality of information for the operational routine. This can lead to human errors, deviations or incorrect decisions.

SPAR-H [9] is a document that discusses human performance factors (PFS's), the relationship between these factors and the failure of the operation and may even involve accidents. SPAR-H describes eight PSF's for calculating human reliability: time available, stress level, complexity, experience / training, procedures, ergonomics, work ability and work process.

These factors, although classified as human, involve organizational, managerial aspects and depend on the type of process and product technology involved. On the basis of the discussion on sociotechnical reliability, technology and culture should be fully known to the reliability investigator.

According to Ávila [10], the Organization should understand about cultural events that cause variation in behavior and, if not perceived by the leadership, creates a climate of coexistence with deviations. These initial deviations if left untreated can lead to disaster. Therefore, in the construction of the study made in this article, using the bases of STRA [1], the human reliability in the refining process is calculated.

In this case, it is noted that due to the operational context differentiated by geographical, cultural and technological issues, the indicators resulting from reliability will differ from those resulting from human factors.

The relationship employees have with the company and its organizational culture will reflect on how the employee validates and understands the company's mission, vision and values, affecting its performance and satisfaction [11]. Considering that published employee policies are supported by leaders through real-world examples and that tools are available to carry out best practices in the operating routine, it facilitates agreement on organizational values by validating the company's mission and vision.

It should be remembered that the organizational climate may or may not improve employee productivity, a strong organizational culture, will have leaders who make quick and assertive decisions, and willing and committed employees.

1.2.2 Sociotechnical Reliability

Ávila [12] proposes that industrial reliability should not be analyzed independently and in isolation, that it is necessary to make a calculation that includes human, equipment, process and operational reliability through equations defined after complexity analysis and calculation.

The evaluation and calculation of integrated reliability, using the proposed method [12], has the function of showing that human failure has a considerable contribution to equipment failures. Built-in reliability enables better visualization of the operational context for decision making, without its decisions will only have a localized effect, not reaching the root cause of the problems.

Considering this, [1] proposed the STRA tool, which is represented by a block diagram to map sociotechnical reliability. This map assists management decisions made to improve productivity and industrial safety. The proposed equations (Table 1) for calculating human, process, equipment, operational and socio-technical reliability [12] will be used in this case study. In addition, it is necessary to classify the level of complexity and social attractiveness.

Table 1 – Sociotechnical Reliability Calculation

Cx= (1)*(2)*(3)*(4)*(5)*100000	STR=(PR)²*ER* (HR*OR)^1/2	HR = NHEP* PSFc / NHEP*(PSFc-1)+1
OR=(100-(LOG(LC)/4)*100))	PR = (R/ΔL)	
Cx= Complexity OR =Operational Reliability	STR = Sociotechnical Reliability PR = Process Reliability ER= Equipment Reliability	HR= Human Reliability NHEP = Nominal human error probability PSF = performance-shaping factors

1.3 Oil Refinery

According to [13],

> *Refineries are continuously challenged to produce more and cleaner products from a broader range of feeds, preferably with limited or no capital investments. In the short term, changes in spot market prices for both crude oil and products have forced refiners to reevaluate their process options and planned investments in search of higher operational flexibility.*

Processes are always being reviewed and improved to increase the sustainability of refining units, in this case hydrocracking technology. This paper analyses the reliability of the assertive decision regarding the best plant availability and the smallest number of operational deviations.

This challenge of producing more and with differentiated input qualities requires high levels of skill and knowledge in the operating team demanding better team and leadership competency.

Combining improvements in technology and human performance factors avoids increased production costs due to reduced rework, reprocessing and unplanned downtime, avoiding double power consumption and labour application.

The new hydrocracking technology brings cost savings and increases profit margins and is a key factor in achieving faster setup change and keeping in sync with market fluctuations [13]. This chemical process is complex and requires great reliability to maintain quality production and financial return without process losses.

According to [14]:

> *the industry interconnections and controls complexity can bring characteristics that make it difficult to control processes and variabilities that are hidden in the system connections, flow information, and large data that travel through control signals present in the chemical industry.*

Refining technology is included as energy intensive where reliability concerns are increased. Since poor performance and downtime causes high energy loss [15].

Hydrocracking is highly exothermic indicating that temperature reduction is critical control for safety and production costs [16]. In the case of security events, fires and explosions can occur, bringing together the issues of management decision, technology and human error that cause accidents and plant shutdowns.

2 Methodology

The methodology of this work (figure 1) serves the Manager of Complex and High-Risk Industrial Units for safety events and production cost.

The initiation of the investigation requires (1) operational context analysis and complexity level classification with details on Process and Product Technology. To build the operational context, it is also necessary to study or analyse the level of safety and organizational culture. Safeguards already installed should be identified and the operating routine as well.

In the operational context, a preliminary identification will be made of the types of failure of this operating unit that cause downtime or loss of performance, thus indicating the functions, equipment, tasks and critical regions.

The operational context analysed will also be used for (2) the construction of reliability mapping. This mapping uses the bases of STRA [1], through the calculations and estimation of the integrated reliability. Expert knowledge and literature will identify the main systems that cause the refining industry to fail.

From the reliability diagram we investigate the most frequent and most severe type of failure due to technology, culture and impact on human factors. The (3) fault tree is made with systems with probability of explosion in case of sequential errors.

Safeguard operating modes (4) are discussed and analysed after the fault tree has been created. It is necessary for the manager to understand the modes that the failure can generate. With this knowledge, be able to discern the best option to maintain the normal functioning of the plant or return to the state of full availability.

The strategic point of view of this work culminates in the elaboration of the (5) Decision tree with actions. From this tree managers will be more likely to take the necessary steps to keep Resilience operational.

Figure 1 - Methodology

3 Case study and Discussions

This paper discusses a case study in a Brazilian oil refinery industry that uses hydrocracking technology. The database for the discussion of the results will be built on expert opinion, previous research data and articles already published.

In the application phase, an exercise was performed in a refining unit with hydroprocessing and hydrocracking technology (Figure 2). Refineries have constant challenges in using cleaner technologies. In addition, crude oil price fluctuations force them to re-evaluate the process [13]. As a result, refinery investments have focused on the hydrocracking process with catalytic systems.

These low-cost changes are related to operational flexibility, the industry's need to receive raw materials of varying purity and deliver different products. These changes are also used to increase the return on investment.

To meet these challenges, it is also necessary to study the socio-technical reliability. Despite this, equipment reliability is the most widely used for refineries based on the serial reliability of the hydrocracking process and its fractionator. What this article intends is to analyze reliability in an integrated way, using the combination of human, operational, process and equipment factors.

Equipment reliability is still the most widely used aspect for refinery reliability calculation, based only on the frequency of failures and the failure mode discussion (FMEA) [18]. Although this discussion is extremely important, social aspects are not considered together with the technicians, in other words, the analysis of human and organizational factors in conjunction with equipment and task analysis is not considered. For this, STRA [1] was used to construct a reliability diagram.

In this way we understand that the reliability diagram becomes more complex including the social and technical aspects at the same time. This makes fault analysis, decision tree and system reliability insight more complete to make managerial decision making more assertive.

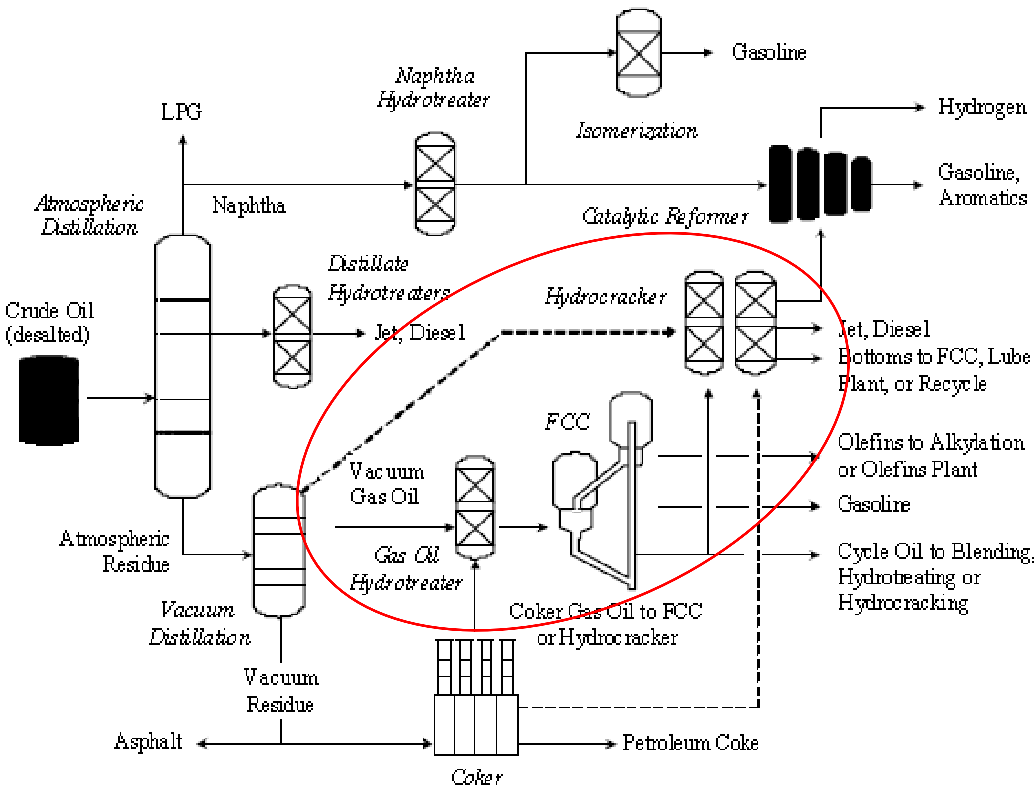


Figure 2 – Hydroprocessing Diagram

For the discussion of the case, the part of the plant highlighted with a red circle in figure 2 will be considered. Contemplating the hydrocracking, hydrotreating processes and the fluidized catalytic cracking unit.

3.1 Operational Context

The first step of the study is to know the operational context in which the analysis will take place, based on literary references and expert knowledge. Using the information required according to the STRA [1], it is important to describe that the refinery is in Latin America, Brazil, has an installed production capacity of approximately 320,000 bbl / d, started operations in 1950. Currently 31 types of products are refined daily, in a continuous process with 8-hour shifts and 10 days of scheduled shutdown per year.

With the need for better profit margins despite being an old plant, the technology was upgraded. In this article, the discussion will considering only these newer units, which use hydrocracking technology, so they have more automation and high complexity.

In this context it is important to emphasize the complexity of the refining unit, considered high according to the STRA guidelines. For integrated reliability analysis this is essential information.

Regarding cultural and management aspects, it is known from experience that underreporting and centralizing information to a slight degree is identified in regional culture. A certain conflict between policies and practices that cause failures, and there may be cultural and barrier degradation.

3.2 Reliability Diagram

Using the bases of STRA [1], it is necessary to map the main functions / activities / processes that affect production. That is, they cause a plant shutdown or greatly decreases production.

For the reliability analysis and better application of the study, a specific part of the hydroprocessing plant was limited. The studied part is composed by hydrotreating, the FCC unit and the hydrocracking, their union in the production process determines a system of high complexity and its stopping implies severe loss of production.

From the know-how of experts and the literature on the subject for the analysis, table 2 was built. It takes into consideration the characteristics of the treatment of deviations and failures in the routine, mapping the main points of production loss and risks of the operation.

Table 2 – Reliability analyses (only <10%)

Systems	Loses %	% functions/processes/activities
Maintenance	20	9% valves and pumps; 55% compressors; 9% pressure vessels; 8% pipe flanges; <10%
Process	30	20% FCC Unit; 8%Distillation; 9% Coker; 40% hydrocracking; <10%
Management/Culture	10	20% Performance reduction by inappropriate decision; 9% unreporting;
Utilities/ Efluents	5	; 20%wastewater treatment; <10%
Operational	15	25% LPG Sulfur Level; 30% Planning and Production Control; <10%
Safety	10	30% H2 Leak; <10% others

Table 2 defines the 8 main functions / activities / processes that affect sociotechnical reliability. Only those with a greater than 10% influence on losses are considered. We then proceeded to calculate the reliability through the equations (table 1) previously defined by Ávila [11], resulting in the block diagram (figure 3) that makes up the result of STRA [1].

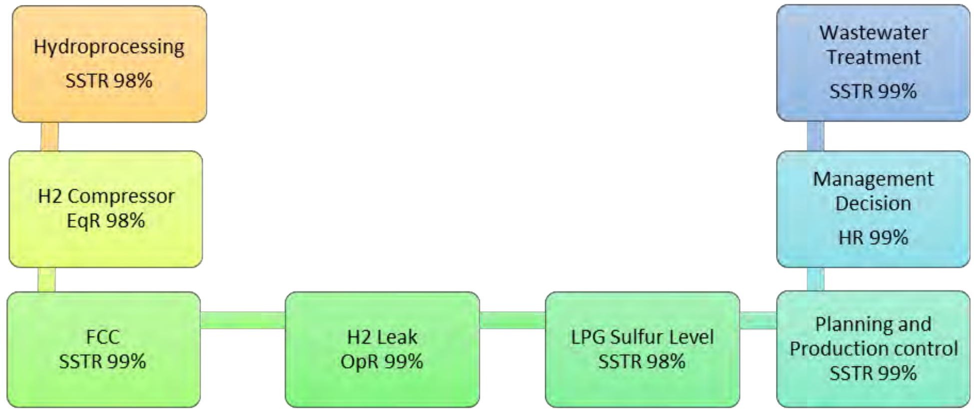


Figure 3 - Reliability Block Diagram of Hydroprocessing

Considering the diagram with established values based on articles and interviews with experts, the final result of reliability diagram is: 89.5%. This result indicates that the plant in this case study operates with a process runaway, which will be analyzed later.

3.3 Fault Tree

From reliability diagram formulated in the previous step, a fault tree was constructed (figure 4). For this the blocks with the highest risk of disaster were chosen, those that together with a spark generate explosion.

The blocks chosen were the hydroprocessing, the compressor and the FCC unit. These units, besides being vital for the maintenance of industrial resilience, also have a high risk. The union of uncontrolled leaks in these areas with small sparks can cause catastrophes, with loss of equipment, image and worse, lead to deaths.

For this explosion not to occur, there must be high reliability and a well formatted hazard containment decision process. This article counts on the construction of this process to help with the management decision.

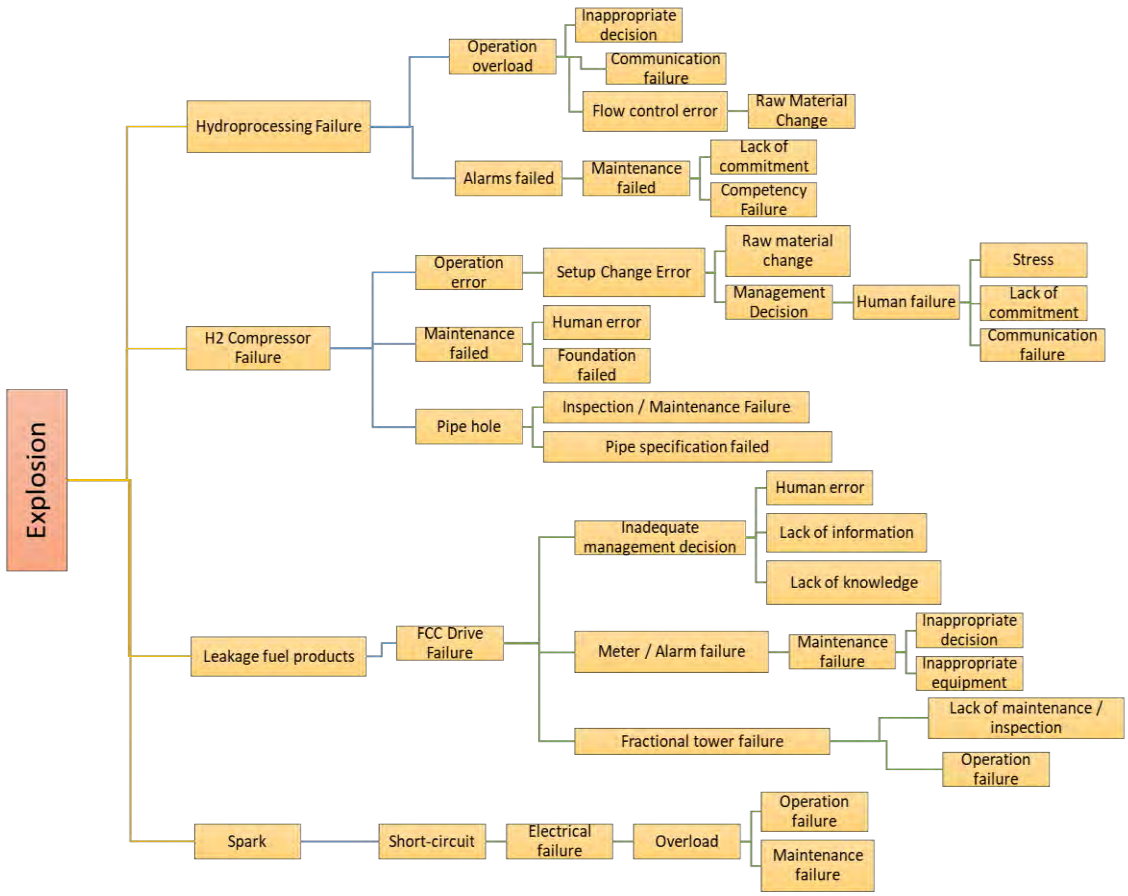


Figure 4 – Simplified Fault Tree

3.4 Modes of Operation

This article considered four modes of operation during the process. In the first case (1) the operation is normal, with no fault intensity, with maximum availability, performance and reliability. (2) After failure, there is a slight lack of control in the process, which decreases reliability and performance rates while maintaining availability, in which case there may be a decrease in production, but the plant is still in operation and decisions have been made correctly.

The third case (3) is controlled stop, after severe failure, the plant could not be resumed and the necessary maintenance leading to a controlled stop as a protective barrier, in this case often human error and / or delay in first decision to resume normality.

In the fourth case (4), the failure occurred and the decision to decrease or stop the plant in a controlled manner or to use an efficient barrier were inefficient or nonexistent, which led to the collapse of the process. Having an uncontrolled or exploding shutdown, financial loss of image and in worst cases the lives of surrounding employees or residents. The modes of operation are described in figure 5.

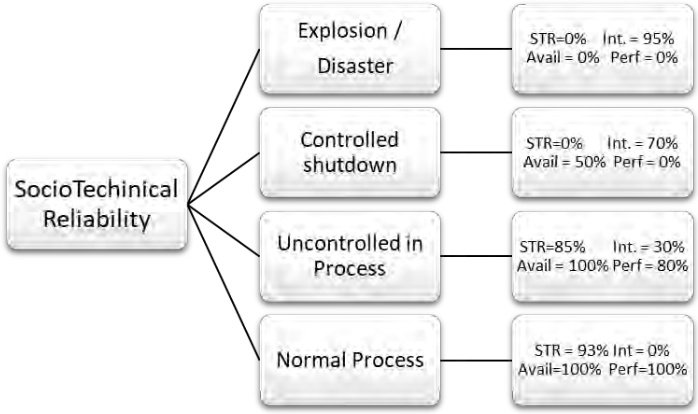


Figure 5 – Modes of Operation

Normal operation has an estimated socio-technical reliability above 93%, performance in this case is 100%, in other words, the plant operates at 100% production load, and 0% intensity as there is no severity of failures during operation. normal operation.

In the emergency with the correct operational control, in time and well done the reliability drops to values between 85% to 93%, that is, the case study of this article, which estimates a socio-technical reliability of 89.5%, is in uncontrolled process also has a fault intensity of 30%. In this case it is still possible to achieve non-stop recovery by only decreasing throughput (80% performance).

For the process to return to normal operation, management decisions must be made based on the cause of the failures. For this case study, management decisions will be exposed in the decision diagram (figure 6). In addition, other risk containment barriers should be used, such as preventive equipment maintenance, staff training, procedural review and operational discipline program.

The third case the operational control fails due to human factors (forgetfulness, lack of competence, incorrect maintenance) the action that would safeguard the plant did not happen and the shutdown will occur to not happen the accident or disaster, in this 3 stage there is a redundancy that is the plant shutdown.

Considering the case studied, an analysis is made for the failure of the hydroprocessing unit. When the quality of the raw material used changes from light, low sulphur oil to higher sulphur, recirculation should increase, so the hydrotreating inlet flow should decrease.

If a decision error occurs, the input stream for a single process can be maintained and an overload can be generated. Increasing the material level in the equipment and consequently the risks of leakage, equipment failure, deteriorated process quality. In order to avoid a decrease in product delivery, spare equipment must be put into operation. If this decision does not occur, the plant may become unbalanced and a forced decrease may occur through the decision.

Another possibility is the decision not to be made, equipment to overload and alarms or meters to fail. In this case, communication between panel and area operators can identify the problem and the management decision to stop the reality restoration operation being made.

If, in addition to overloading and alarm failure, human communication failure occurs between operators in the same class or in shift crossings. The case may not be perceived, thus continuing with the system overload, leading to collapse, a leak accompanied by spark that leads to an explosion, leaving the plant completely unavailable.

3.5 Decision Tree

The decision diagram was designed as a way to keep management safe to take the necessary stances to contain hazards or re-establish order through planned shutdown.

With the reliability diagram, fault tree and knowledge of operating modes, it was possible to construct a decision diagram that should be used by plant leaders to avoid critical situations and explosions. This tree was made based on hydroprocessing failure.

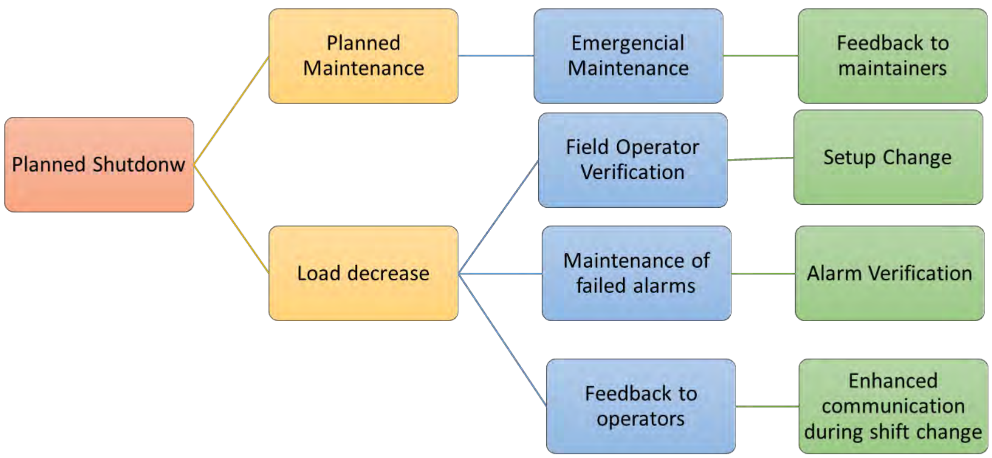


Figure 6 – Diagram Decision

4 Conclusion

This article aims at operational resilience of the plant, assisting managers in decision making intending to avoid the loss state or to return to normal operation. For this it is necessary to go through several steps followed in the methodology.

First, we need to know the operational context, the technology, analyse the risks, the human factors. So that you can calculate the reliability and see the critical areas and functions where the biggest causes of loss are. From then on, decide what are the best actions to take to maintain operational resilience and move to execution with the resources and expertise required to avoid rework.

The article followed the steps until the decision. It is important to know that the data were analysed based on knowledge of experts and literature on the subject, it is expected an approximation consistent with reality.

For this reason, the article demonstrates the need for the approximation between the university and the Brazilian refining industry, which has a great opportunity to improve reliability. With the decision making and the assertive analysis of the current reliability, it would be possible to increase the profit level of the industries and increase the effectiveness of the containment barriers through the execution of the presented points.

5 References

1 Ávila, S. Management Tool for Reliability Analysis in Socio-Technical Systems - A Case Study. Proceedings of the AHFE 2019 International Conference on Human Error, Reliability, Resilience, and Performance, Washington D.C., USA ,2019

2 Johnsen, S. O.; Kilskar, S. S.; Fossum, K. R. Missing focus on human factors – organizational and cognitive ergonomics – in the safety management for the petroleum industry. Journal of Risk and Reliability, vol. 231, iss. 4, p. 400-410, 2017.

3 Perrow

4 Gagliano, M. Analysis of the reliability of the CO2 compression system in a petrochemical plant considering the technical and human factors, Master Dissertation, Postgraduate Program in Industrial Engineering, Polytechnic School, Federal University of Bahia, Brazil, 2018

5 Oliveira, U. R.; Paiva, E. J.; Almeida, D. A. Integrated fault mapping methodology: a proposal for the joint use of process mapping with FTA, FMEA techniques and expert analysis. Revista Produção, v. 20, n 1, p. 77-91, 2010.

6 Galicia, H. J.; He, Q. P.; Wang, J. Statistics pattern analysis-based fault detection and diagnosis. In: Proceedings of CPC Conference, 8., 2012. [S.l.: s.n.], 2012.

7 B. K. Bharatiya. Project Hazard Analysis in Hydrocarbon Processing Industry. Proceedings of 4 th Latin American Conference on Process Safety - CCPS. Rio de Janeiro, 2012.

8 Ávila, S. Dynamics Operational Risk Management in Organizational Design, the Challenge for Sustainability. Global Congress on Process Safety, Houston, EUA, 2016

9 Boring, R., Blackman, H.: The Origins of SPAR-H Method's Performance Shaping Factors Multipliers. Idaho – EUA, 2007

10 Souza L., Ávila S., Cerqueira I., Santino C. and Ramos A., "Analysis of failure cases in the operational control and recommendations for task criteria and man-process interface design", Applied Human Factors and Ergonomic Conference, Florida, EUA, 2018

11 Ávila, S. Reliability model analysis for interdependent failure mode, a discussion of human error, organizational and environmental factors. National Congress of Mechanical Engineering, Salvador, Brazil, 2018

12 Ávila, S. Reliability analysis for socio-technical system, case propene Pumping. Journal of Engineering Failure Analysis **56** (2015) 177-184

13 Dave Brossard; Natalia Koldachenko; Theo Maesen; Dan Torchia; H. Alex Yoon.. Hydroprocessing to Maximize Refinery Profitability. Chevron Lummus Global. AFPM, San Diego, CA, 2012

14 Maria Lorena Souza, Salvador Ávila Filho , Rafael Brito, Ivone Cerqueira , Jade Avila, Discussion about criteria for the management of alarms and cognitive limits for the chemical industry Applied Human Factors and Ergonomic Conference, Florida, EUA, 2018

15 José F. M. G. Ferreira, Carla V. M. Galvão, Jean M. P. Silva, Salvador Ávila Filho Análise do Impacto da Baixa Confiabilidade Operacional nos Indicadores de Energia de uma Refinaria de Petróleo, Abrisco, Rio, 2017

16 Robinson, Paul & Dolbear, Geoffrey. (2007). Hydrotreating and Hydrocracking: Fundamentals. 10.1007/978-0-387-25789-1_7.

17 Nakamanuruck, Itthipol & Rungreunganun, Vichai & Talabgaew, Sompoap. (2017). Reliability Analysis for Refinery Plants. The Journal of King Mongkut's University of Technology North Bangkok. 10.14416/j.ijast.2017.01.002.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Practical Considerations for Overfilling Scenario Application

Houston Haile, Robert (Bob) Siml*
Siemens Energy, Inc.
4615 Southwest Freeway, Suite 900,
Houston TX 77027
*Presenter E-Mail: Robert.Siml@Siemens.com

Abstract

As a result of the BP Texas City explosion, industry recognized overfilling as one of the most important overpressure scenarios to be considered. Atmospheric release of flammable liquids above their flash point is no longer an accepted industry practice. Additionally, overfilling with combustible liquids often leads to mist formation, which may be easily ignited. Overfilling applicability is a critical factor in deciding whether to tie-in a relief system to a closed disposal system; for example, large liquid loads, especially those which are flashing, can affect knockout drum and flare capacity, radiation, etc.

This paper addresses practical considerations in determining if overfilling leads to overpressure. Subtle but important practical factors determine overfilling applicability, and the analysis requires an in-depth understanding of the process, instrumentation, and procedures. How the feed pressure reacts during overfilling must be carefully reviewed. Deciding if overfilling applies typically involves determining if an independent high-level alarm (IHLA) is present and whether there is adequate time for operator intervention. In some facilities, pressure transmitters are ranged to span the entire equipment height, giving additional redundancy in level alarms. As a result, an informal Layer of Protection type Analysis (LOPA) may eliminate overfilling as a source of overpressure, by serving to limit the maximum upstream feed pressure or serving as an IHLA. In some cases, the equipment will simply overflow to high capacity systems, such as a header system, such that no overpressure will occur. In other cases, the flow may have to fill multiple vessels; therefore, overpressure by overfilling is not credible based on multiple level alarms. These factors are each described and careful consideration can guide the overfilling applicability determination.

Keywords: Safety, Pressure Relief Analysis, Overfilling, Vapor Cloud Explosion

1. Introduction

In 2005 the BP Texas City refinery overfilled the raffinate splitter in the Isomerization unit during startup[1]. The relief valves discharged into a "blowdown drum with an atmospheric stack." The intent of the system was to allow vapor flashing off liquids to be vented at an elevated discharge location for dispersion and collect the remaining liquid. The use of a blowdown drum with an atmospheric stack was recognized as an antiquated practice but had not been routed to a flare system. The atmospheric blowdown drum was subsequently overfilled with liquid above the flash point.

The liquid above the flash point resulted in evaporation which increased due to droplet formation from liquid falling on equipment. The resulting vapor cloud was likely ignited by an idling truck resulting in the 15 fatalities and 180 injuries.

Two of the Chemical Safety Board (CSB) findings[2] can be summarized as:
- Potential for overfilling must be considered.
- Atmospheric release of liquids above the flash point is not accepted practice.

2. Applicable Codes and Standards

The applicable standard for evaluating overfilling for pressure vessels is API Std 521.

As a result of the 2005 Isom Explosion, API issued the API 521 5th ed 2008 Addendum[3] which added significant guidance on overfilling in §5.23 Overfilling Process or Surge Vessel. (The overfilling guidance was subsequently modified slightly and moved to §4.4.7 in the API 521 6th ed – 2014[4].) Key aspects are:

1) Startup and other non-normal modes of operation must be considered.

2) If the source of pressure can exceed the equipment design / relief device set pressure, options include, but are not limited to:

   Eliminate overfilling with vessel design / relief device set pressure
   - Ensure there is adequate margin between the relief device set pressure and maximum operating pressure, otherwise design the relief device and disposal system for the liquid release.
   - Consider the foundation, vessel design, and piping in overfilling.

   Design the relief system for overfilling
   - Ensure the relief device and disposal system can handle the liquid release.
   - Consider effects of two-phase flow and potential for autorefrigeration.
   - Consider the foundation, vessel design, and piping in overfilling.

   Install a Safety Instrumented System (SIS)
   - Safety Integrity Level (SIL) rating based on risk analysis.
   - Consider availability of instrumentation for SIS activation.

3) Evaluate the risk associated with discharge location (e.g. Atmosphere, process, flare.)

4) Considerations for level instrumentation include:
   - If safeguards are on different taps from process control system;
   - Susceptibility of instrumentation to common mode failures;
   - Tendency for level to show low or high when out of range;
   - Tendency for level to show low during overfilling; (e.g. Overfill top leg of dP cell.)
   - Impact of composition or temperature on density for dP cells;
   - Whether instrumentation is proven for the specific application;
   - Whether any instrumentation can span an extended range;
   - Whether instrumentation is suitable for non-normal operation.
   - Maintenance and testing frequency;

3. Other Industry Accepted Methods

It is common industry practice to exclude overfilling based on an independent high level plus adequate operator response time. Although it is easy to interpret this as a simplistic guideline that does consider the potential failure of operator intervention, the minimum acceptance criteria in context with API Std 521[5] is:

<u>To exclude overfilling based on an independent level alarm and operator intervention</u>
- Ensure an independent level alarm plus 10 – 30 minutes operator response time.
- Consider the availability and independence of instrumentation.
- Ensure training and procedures include expected behavior of instrumentation.
- Ensure operators agreement that procedures can be safely relied upon.
- Evaluate the risk associated with failure of operator intervention. Potential effects are included in Table 1:

Table 1: Potential Effects Associated with Discharge Location

Discharge Location	Potential Effects
Process	Other process relief
Flare	Backpressure, knockout drums, radiation
Atmosphere	Toxic or flammable release

The time for operator response must be determined by the owner operator based on the complexity of the operation and the time for the operator to diagnose / mitigate the problem. Factors should include the potential for "operator overload" due to multiple alarms in complex situations. Training must include written procedures and corrective actions.

Evaluating the risk associated with the failure of operator intervention is based on the operating company's risk evaluation and acceptance criteria. The range of criteria include:
1) Evaluating the risk / potential overpressure when routed to a closed system.
2) Determining the layers of protection required for routing to atmosphere.

4. Summary of Commonly Accepted Overfilling Protection Practices

All of process design is ultimately geared toward the most cost-effective process design and most cost-effective risk reduction. In some cases, the risk is quite low and can be easily managed. In other cases, the risk-based engineering analysis is quite complex.

The order of preference of dealing with overfilling, given in Table 2, is generally:

Table 2: Order of Preference in Dealing with Overfilling

Mitigation	Preference
Eliminate overfilling with vessel design / relief device set pressure	Highest
Exclude overfilling based on company's risk acceptance criteria	↓
Design the relief system and disposal for overfilling	
Install a safety instrumented system (SIS)	Lowest

For new and existing facilities, the preference is to eliminate overfilling with the equipment design, if economically feasible.

If it is not economically feasible to eliminate overfilling by design, then the focus shifts to determining if the relief and disposal system is adequate for overfilling or if overfilling can be excluded with additional safeguards to meet the company's risk acceptance criteria.

It can be successively argued that overfilling is not applicable because of the nature of the system or the risk has been sufficiently reduced to meet the company's risk criteria in a variety of cases, including:

- Closed loop systems during charging and normal operation.
- Cases where overfilling (overflowing) will not cause overpressure.
- Cases where overfilling is so disruptive that it must be corrected to operate.
- Cases where overfilling cannot occur based on a thorough understanding of the pump calculations.
- Cases involving design changes to eliminate overfilling. (Inherently Safer)
- Cases where overfilling can be excluded by a PHA or LOPA.
- Cases where additional layers of protection have been added to exclude overfilling.

5. Closed loop systems

Closed loop systems are intended to operate with a fixed inventory circulating in a loop. Although seeming simple systems, extensive work is involved in designing a closed loop system. Besides designing for normal operation, the designer must also calculate the required charge and decide if the inventory will be stored in one vessel or if the bulk of the inventory will reside in the loop during maintenance.

During charging, overfilling / overpressure is generally not expected to apply if well-established procedures are followed.

During normal operation, overfilling / overpressure is also not expected. However, a systematic evaluation is required to ensure that upsets such as inadvertent closure of a block valve will not result in overpressure. Furthermore, if the intent of the design is to store the entire charge in one vessel, the inventory of the system versus vessel volume should be verified.

Examples of closed loop systems where overfilling is expected to be designed out of the system during startup / normal operation is given in Table 3:

Table 3: Closed Loop Systems – Overfilling Designed Out

Hot Oil System	Equipped with an expansion tank designed with "fill to cold" and "operating hot" levels. Overfilling due to thermal expansion is designed out.
Refrigeration	A refrigeration system is designed for a fixed inventory and charging is well-defined. Overcharging is designed out.
Amine Systems	The inventory of an amine absorbent system is well designed. Overfilling due to overcharging amine is typically not considered.

Consideration must be given to abnormal flow into the system causing overfilling. Possibilities include:
- Tube leak / broken tube scenarios
- Control valve failure cases

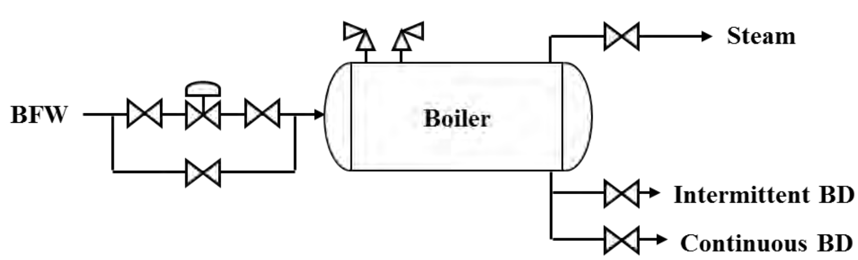
Examples of a control valve failure scenario that can cause overfilling is liquid hydrocarbon breakthrough to an amine treating or sour water

6. Overfilling (Overflowing) Will Not Cause Overpressure

In some cases, equipment is open to utility headers or downstream equipment; therefore "overfilling" (overflowing) will not cause overpressure.

Example 1: Normally Open Path to Downstream Header
A boiler is typically open to the downstream steam header. A simplified boiler is shown in Figure 1.

Figure 1: Simplified Boiler



ASME Section I[6] prescribes the relief system design requirements as the design steaming rate of the boiler. The underpinnings are that for BFW feed control valve fail open or inadvertent opening of the bypass, the boiler is open to the header.

Similarly, for process steam generator built according to ASME Section VIII[7] and the potential overpressure evaluated by API Std 521[8], the BFW feed control valve failing open (or inadvertent opening of the bypass) and the outlet being blocked at the same time is typically considered "double jeopardy."

A brief pressure relief analysis of a boiler in given in Table 4.

Table 4: Typical Boiler Pressure Relief Analysis

Scenario	**Relief System Design Basis?**	
Blocked Outlet (Steam)	Yes	Normal steam flow
Blocked Outlet (C-BD)	No	Slightly wet steam to header
Blocked Outlet (I-BD)	No	NC - Intermittent use
Control Valve / Bypass	No	Overflow to the header

Different companies have different policies on how to treat overfilling in these situations:

- Assume the path to the header is adequate.
- Perform hydraulics to ensure the path to the header is adequate.
- Design the relief system capacity for overfilling.
  (Discharge of relief system must be routed to a safe location.)

When credit is taken for flow to the header, a hydraulic analysis should be considered to ensure the path is adequate without exceeding allowable accumulation. In addition, the steam line should be supported for liquid / two-phase flow.

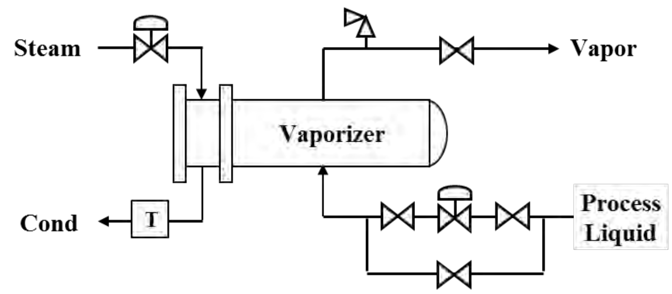
A common position is that the boiler feedwater will flow to the steam header and the relief valves on the boiler will not lift. The steam header is typically quite large compared to the capacity of an individual BFW control valve failing open. A good case can be made that the "overfilling" (overflowing) of the boiler will be detected via the effects on the operation of the steam system (i.e. loss of heat transfer in the process, rotating equipment stops working, etc.) long before overpressure occurs.

Damage can occur due to steam hammer and liquid flowing into turbines. However, the damage cannot be prevented with a relief valve. Minimizing equipment damage is typically considered part of Loss Prevention.

<u>Example 2: Vaporizer Normally Open to Downstream Header</u>

Another common example of a piece of equipment that is open to a downstream equipment or distribution header is a process vaporizer. A common vaporizer is shown in Figure 2.

Figure 2: Process Vaporizer



The minimum relief system design basis for a vaporizer that is normally open to the header is the vapor generation rate for blocked outlet.

The process feed control valve failing open, inadvertent opening of the bypass, loss of heat input, or a broken tube are overfilling concerns, but the vapor valve being blocked-in at the same time is typically considered double jeopardy.

When credit is taken for flow to the downstream equipment, a hydraulic analysis should be considered to ensure the path is adequate without exceeding allowable accumulation. In addition, the vapor line should be supported for liquid / two-phase flow.

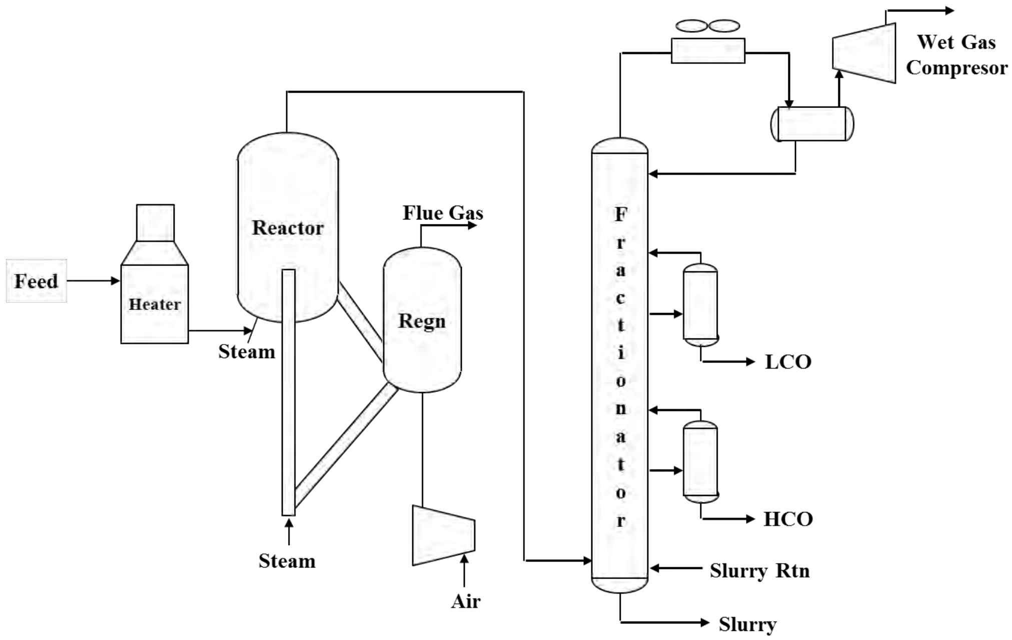
Whether the downstream system can absorb the additional flow must also be considered. If the downstream system cannot absorb the additional flow, the relief system on the vaporizer or downstream system must be designed for the additional flow.

7. Overfilling is So Disruptive that it Must be Corrected to Operate

In some cases, the owner operator may decide that the onset of overfilling is so disruptive that the process cannot continue to operate and must be shutdown.

Example 3: Overfilling is not Possible Based on System Behavior
An example of a system where it might be argued that overfilling is not credible because it is so disruptive to the process is a Fluidized Catalytic Cracker (FCC) – Main Fractionator. A significant part of the driving force of the process is the air blower to the regenerator. If the main fractionator were to try to overfill the blowers must support the entire column of liquid which also has the effect of backing out the air blowers which is a major upset to the process. A simplified FCC – Main Fractionator is shown in Figure 3.

Figure 3: FCC Main Fractionator



Discussions with engineering and operations on potential for overfilling of a Fluidized Catalytic Cracker – Main Fractionator can be summarized as:

> "The effects of the Main Fractionator starting to overfill are so obvious that the unit cannot keep running. We must shutdown and restart."

This reflects a complex understanding of the operation including high levels in multiple vessels, higher pressure drop through the process causing the air blower to back out, etc.

The decision that overfilling can be excluded on the basis that the effect on the process is so obvious that the process cannot continue to operate must be made by a qualified individual (e.g. superintendent) or preferably a group knowledgeable in the operation of the unit and documented accordingly.

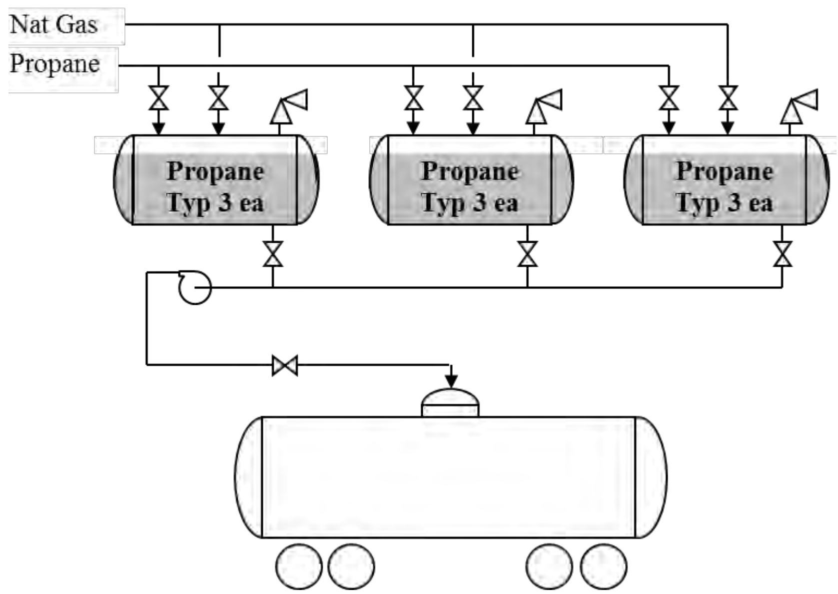
8. Overfilling Cannot Occur with Thorough Understanding of Calculations

Most overfilling cases involve pumps. A key aspect of evaluating overfilling is understanding how the upstream pressure reacts when the pump is effectively deadheaded into a downstream system.

<u>Example 4: Pumps with a Well-Defined Maximum Upstream</u>

Some pumps will have a very well-defined maximum upstream pressure. An example is a rail car, tank car, or transfer operation. See Figure 4.

Figure 4: Loading Operation with Well-Defined Upstream Pressure



$$Pump\ Discharge\ P_{Max} = P_{Normal} + \frac{\rho}{144}\left(\frac{g}{g_c}\right)(H_{Deadhead} + H_{Static})$$

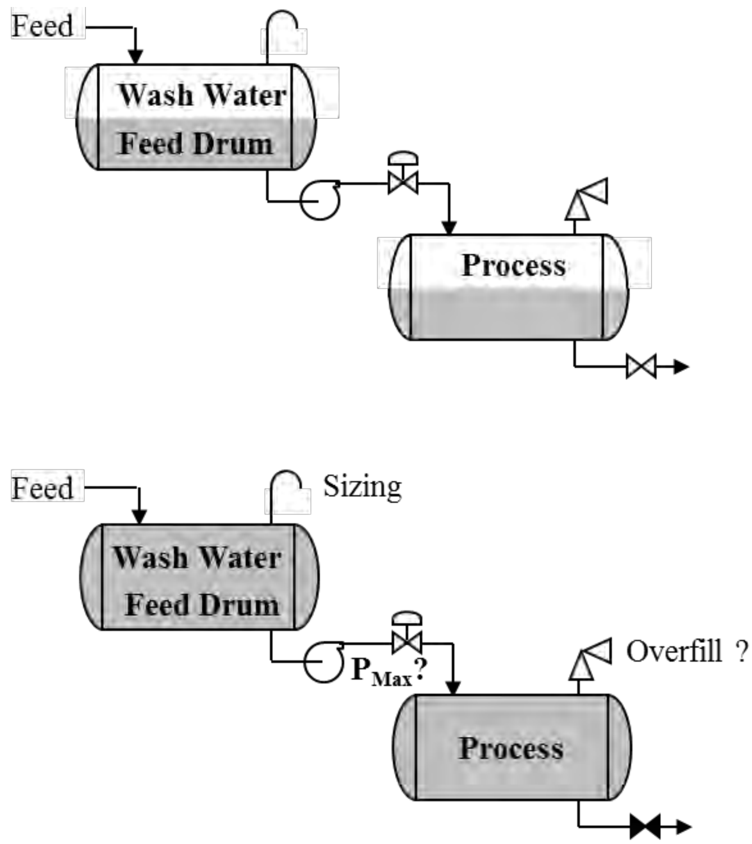
Observations

- It is unusual to feed into and pump out of storage vessels at the same time for inventory control purposes. (e.g. Low-pressure tanks, bullets, spheres.)
- Inadvertently blocking the flow to the rail car loading operation will not result in overfilling of the bullets. (Overfilling may apply for other modes of operation.)
- Railcars and tank cars are equipped with relief devices.
- The maximum discharge pressure of the loading pumps is based on the highest normal operating pressure of the bullets. (In cold climates, the bullets may be padded with natural gas in the wintertime.)

It is expected that rail car and tank car loading operations are "inherently safer" designs such that the maximum pump discharge pressure cannot exceed the pressure rating of the rail car or tank car but must be verified with a thorough understanding of the loading operation.

Example 5: Pumps Associated with Vessels with Open Vents
Calculating the maximum pump pressure associated with a vessel with an open vent can be deceptive. In the case of a basic API 650 tank, the maximum static head is well defined. Occasionally, a pressure vessel will be equipped with an open vent. The observer might be tempted to assume the vessel is at "atmospheric pressure." However, there is a maximum feed pressure/sizing basis for the open vent which must be taken into consideration. See Figure 5.

Figure 5: Maximum Upstream Pressure with an Open Vent



$$Pump\ Discharge\ P_{Max} = P_{Relief} + \frac{\rho}{144}\left(\frac{g}{g_c}\right)(H_{Deadhead} + H_{Static})$$

<u>Observations</u>

- Feed drum will overfill.
- The potential for overpressuring the process depends on the pressure used for sizing open vent.

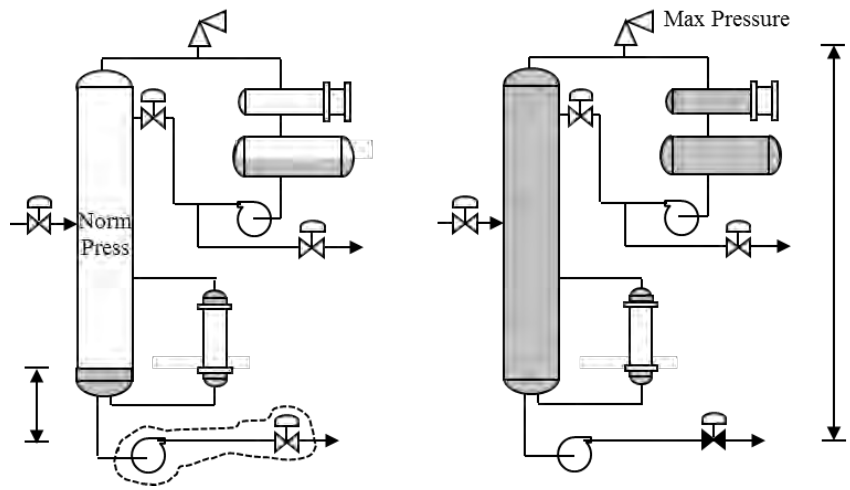
In this case, inadvertently blocking the outlet of the process will back the pump up the curve. The feed drum will overfill. The potential for overpressuring the process can depend on the sizing basis of the open vent.

It is possible to have a case where the downstream vessel relieves moving the pump back out on the curve / lowering the suction pressure such that the system will oscillate between relieving upstream and downstream. The preference is to size the open vent (and choice of the pump) so the wash water drum will relieve water instead of the process relieving for an "inherently safer" design.

Example 6: Complex Overfilling Considerations

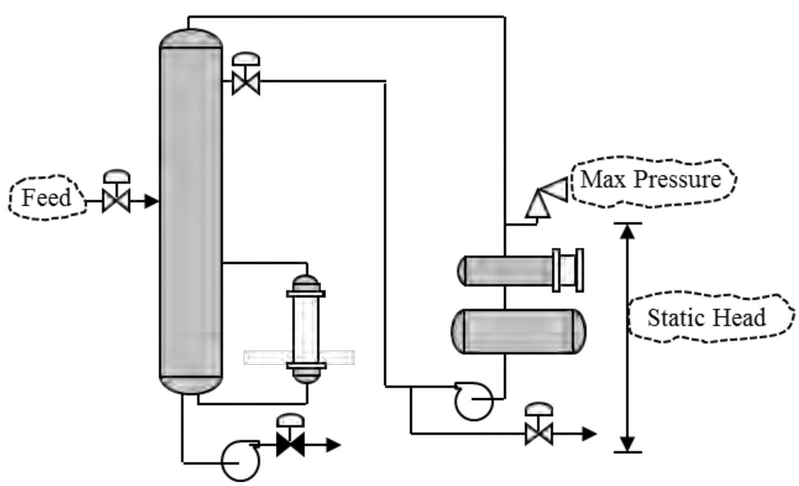
Overfilling of a column system entails filling the entire column system. This example assumes the initiating event is the bottoms control valve failing open. See Figure 6.

Figure 6: Overfilling of a Distillation Column



Assumptions that should always be checked in determining the maximum discharge pressure of the pump include considering relief valve location / sizing basis and how the feed pressure / flow will react when the column pressures up. See Figure 7.

Figure 7: Factors Involved in Bottoms Pump Discharge Pressure



Factors include:

<u>Feed</u>

- How does the feed flow rate change?
- How does the feed pressure change?

Static head Considerations

- Is the column relief device located on the overhead line near the top of the column or close to the condensers?

Maximum Relieving Pressure

- Is the relief device set at limiting MAWP or lowered to account for static head?
- If relief device is located below the top of the column, did sizing include the additional pressure from static head for overfilling? (Rare)
- Will overfilling result in a loss of cooling plus continued heat input?

Ultimately

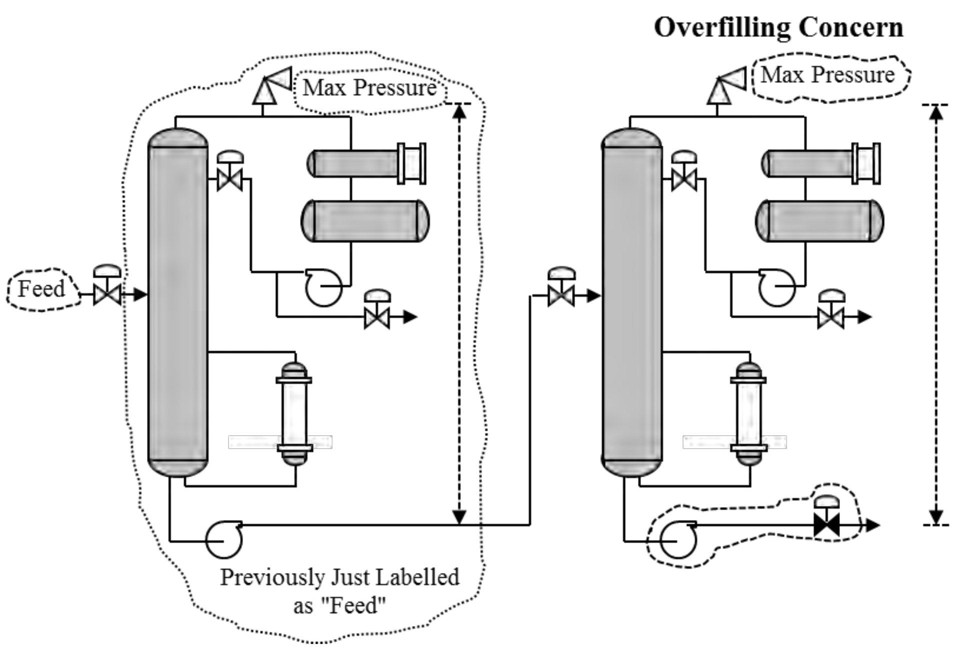
- Can a lower relieving pressure be justified?

  If the relief system is oversized:

  - Can one device be used instead of multiple devices?
    (10% versus 16% accumulation)
  - Is the device a pilot?
    (Full open at set pressure = Calculated accumulation versus 10% accumulation.)

A seemingly "basic" overfilling concern can involve significant complexity in determining how the upstream pressure will react, static head, and set pressure considerations. Consider multiple columns in series. See Figure 8.

Figure 8: Multiple Columns in Series:



Observations

- Credit can potentially be taken for forward flow for both sets of overheads pumps.
- The first system could potentially relieve before the downstream column relieves.

− The static head included on the bottoms pump for the first column is partially offset based on the static head to the relief device on the second column.
− Elevation of the equipment and static head effects are not included in this example.

Conclusions

1) A seeming basic overfilling scenario can be quite complex.
2) If the relief device and disposal system are inadequate based on easy assumptions, the pump discharge flowrate and pressure can potentially be significantly refined.

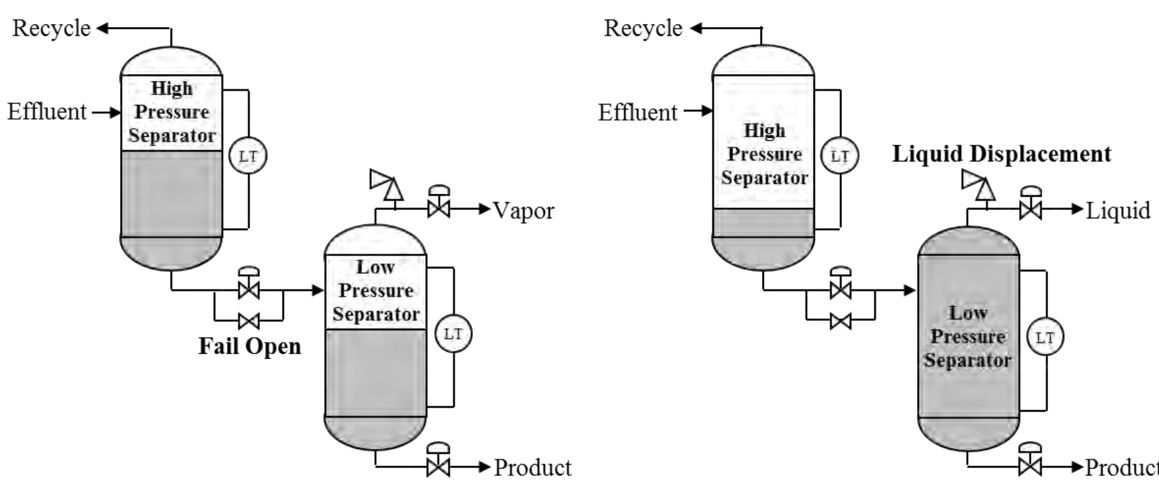
9. Changing the Design to Eliminate Overfilling (Inherently Safer)

If a relief valve discharges to atmosphere or the relief device / disposal system are inadequate for overfilling, a valid approach is permanently changing the operating envelope to eliminate overfilling:

Example 7: Excluding Overfilling of a Low-Pressure Separator

A common design criterion in the design of a hydrotreater is to ensure the high-pressure separator cannot overfill the low-pressure separator when the high-pressure letdown valve fails open or the bypass is inadvertently opened. If the low-pressure separator is full of liquid and high-pressure gas enters the system, liquid will be displaced at the vapor volumetric expansion rate. This is known as “liquid displacement” or “bottom venting.” The required relief area for displacing liquid at the vapor volumetric rate can easily be 10 times higher than expected for the vapor by itself even if credit is taken for continued outflow through the vapor and liquid control valves from the low pressure separator in their normal position with no credit for positive response by the control system. See Figure 9.

Figure 9: Control Valve Fails Open Resulting in Liquid Displacement.



Besides simply preventing the low-pressure separator from becoming liquid full, the preference is to limit the maximum level to ensure the relief system is adequate based on 2-phase disengagement models and a check for liquid re-entrainment.

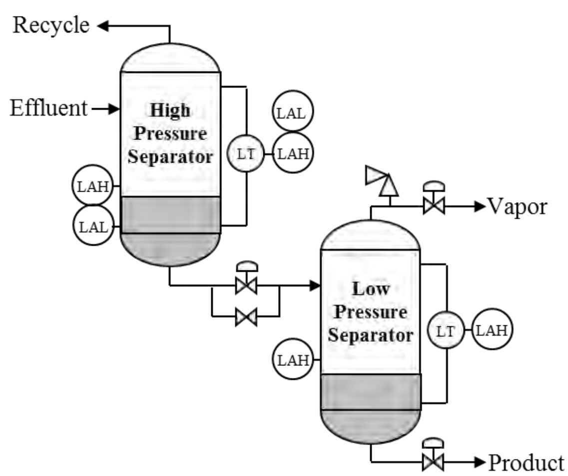
In one case, the high-pressure separator was replaced with a larger vessel, but the low-pressure separator was not. The relief system was significantly undersized for liquid displacement.

This case involved extensive discussions with operations with two objectives:

1) Avoid potential liquid displacement and otherwise limit the maximum level in the low-pressure separator to ensure the relief system is adequate when 2-phase disengagement and the potential for liquid re-entrainment is taken into consideration.
2) Minimize the potential to inadvertently lose level in the high-pressure separator causing vapor displacement (also known as "gas blowby") even through the relief system was adequate.

The agreed upon changes were additional independent instrumentation to include both high, high-high, low, and low-low level alarms. Although the changes can be viewed as a layer of protection analysis, the better understanding is a permanent shift in the operating envelope to eliminate potential overfilling for the low-pressure separator. See Figure 10.

Figure 10: Change Operating Envelope to Exclude Overfilling / Liquid Displacement



Other cases that were considered separately:
- Gas blow-by (vapor based on disengagement models)
- Blocked outlet (two-phase)

10. Overfilling Excluded with a PHA or LOPA

A Process Hazard Analysis (PHA) is a team of qualified individuals from engineering and operations. Based on an in-depth review of the system, a PHA team may include or exclude overfilling as a relief system design scenario based on the collective knowledge of the team.

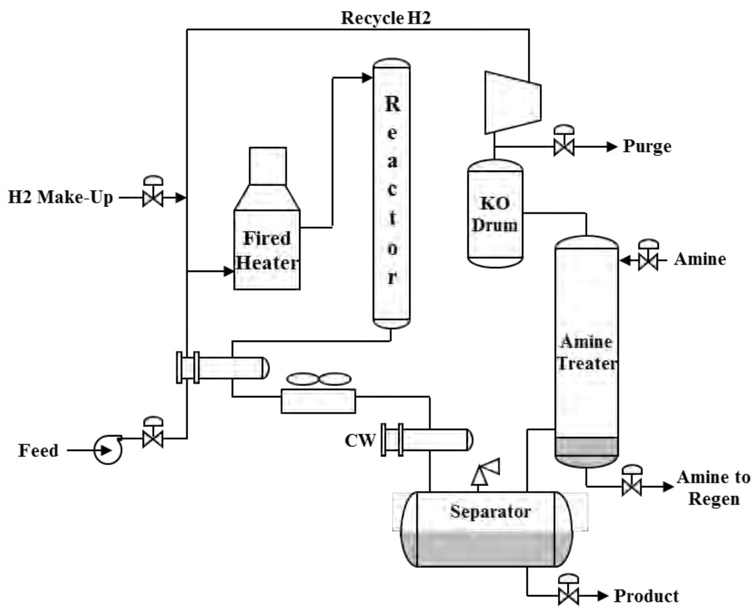
<u>Example 8: Excluding Overfilling of a Hydrotreater by a PHA</u>
Hydrotreating and hydrocracking are two similar but separate processes under the broad category of hydroprocessing.

Hydrotreating removes impurities such as sulfur (to hydrogen sulfide H_2S) and nitrogen (to ammonia). In addition, some cracking generating to methane occurs. In the process, olefins are saturated which raises the octane rating of gasoline and cetane rating of diesel.

Hydrocracking breaks larger molecules into smaller ones.

There are several configurations but both processes involve reacting the material at high pressure and temperature with hydrogen in the presence of a catalyst. A basic hydrotreater design is shown in Figure 11.

Figure 11: Basic Hydrotreater



The reaction is sometimes liquid phase and sometimes supercritical depending on the design. The combined feed to the fired heater and flow after the cross exchanger is 2-phase.

Assuming the charge pump is capable of overpressuring the system, the relief system is often designed for overfilling for blocked product outlet from the separator. How to handle the hydrogen is a discussion issue.

<u>Recycle Hydrogen</u>
Some companies include the recycle hydrogen. Other companies consider the recycle compressor as stopping; therefore, the recycle hydrogen stops.

<u>Make-Up Hydrogen</u>
The make-up hydrogen is largely consumed but some H_2S, ammonia, and methane is generated. Since the process is no longer operating normally, the most common design

basis is to include the make-up hydrogen with the product flow as if no hydrogen is consumed.

Even a basic hydrotreater is a still a large complex process. If the relief or disposal system is inadequate, a valid question is:

> "Is overfilling a relief system design scenario based on levels in multiple pieces of equipment, the behavior of the process, etc.?"

The results from a PHA team from engineering and operations on potential overfilling of this hydrotreater can be summarized as:

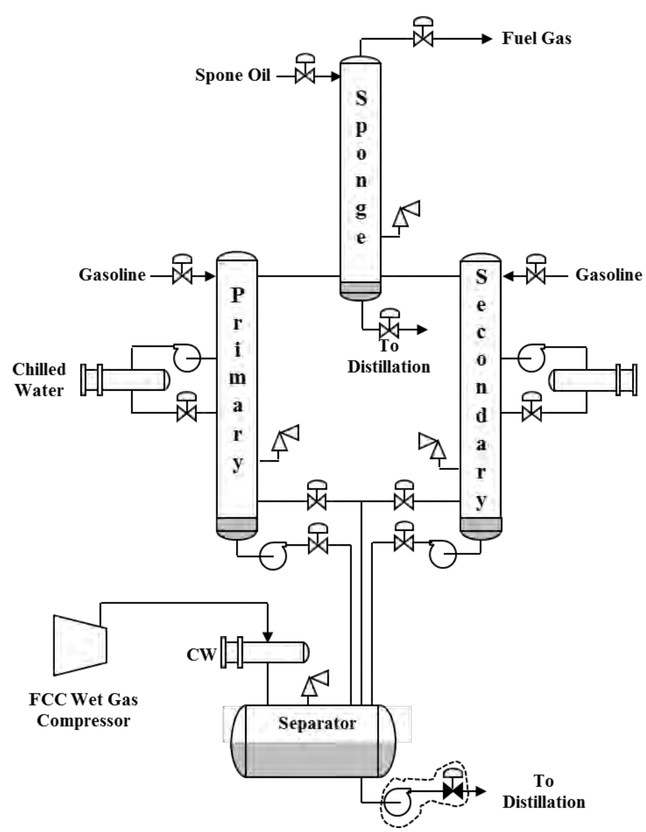
> "Overfilling / overpressure of the hydrotreater will not occur because of multiple level indications, the behavior of the equipment, and calls from downstream unit losing feed."

This reflects an understanding of the complex behavior of the unit and the layers of protection to prevent overfilling.

<u>Example 9: Excluding Overfilling Light Ends Unit by a PHA</u>

One type of Vapor Recovery Unit after the Fluidized Catalytic Cracker involves absorbing the cracked gases as shown in Figure 12.

Figure 12: FCC Absorption Vapor Recovery Unit



Overfilling of this system due to blocked liquid outlet of the separator would require overfilling four vessels, with the associated high-level indications from each vessel and the associated process upsets. The pressure in the equipment would only build due to static head and some additional pressure drop until the liquid finally reaches the control valve to the fuel gas system. Once the liquid finally reaches the control valve to the fuel gas system, the pressure would spike, and overfilling / overpressure would occur.

Blocked liquid outlet of any of the other liquid paths requires overfilling of at least three vessels with the associated high-level indications. (The vapor control valves are much larger than the liquid control valves. The separator and its level instrumentation would typically also be involved.)

A PHA team consisting of engineering and operations personnel decided that the risk of overfilling was sufficiently low that overfilling was not a relief system design scenario for overpressure protection.

11. Adding Layers of Protection to Exclude Overfilling

In the event the PHA includes overfilling as a relief system design scenario, an option is a Layer of Protection Analysis (LOPA). A LOPA also consists of qualified team to quantitively assess the risk, determine the number of layers of protection present, and the number of layers required to reduce the risk to the owner operator's risk acceptance criteria.

Layers of protection could range from adding an independent high-level alarm (IHLA) to a Safety Instrumented System (SIS) with a Safety Integrity Level (SIL) to add a sufficient number of layers based on the probability of failure on demand.

If no independent high-level alarm is present, adding one could provide one layer of protection with credit for operator response. However, if a high-level alarm is already present, then simply adding another one typically does not add another layer because the operator is in common. For additional credit, entire layers of protection must be added.

In the case where there are multiple alarm points present, a written management system which includes training of additional outside operators, inside operator, and/or the shift foreman to respond to different alarm points if corrective action hasn't been taken may constitute additional layers of protection. Factors that would be included are evaluation of the response times, the corrective actions to be taken, actions to be taken during loss of communication with the primary outside operator, etc.

Example 10: Adding Layers of Protection to Exclude Overfilling

After the Isom explosion (referred to in Section 1) some companies recognized:

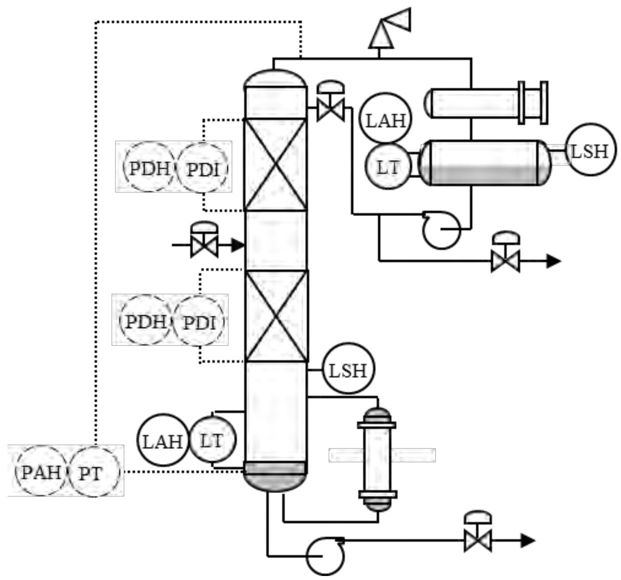
- An independent high-level alarm was not present or subject to common mode failure.
- The range of level transmitters were only intended for normal operation.

As a result, one of the strategies used a (LOPA) type analysis to ensure the level would always be detectable and provide multiple indications of overfilling. See Figure 13.

Changes often included:

1) Adding differential pressure transmitter spanned for the entire height of a column to ensure the level was always detectable if the level overfilled the high tap on the normal dP cells used for level control instrumentation.
2) Adding high level alarms
3) Using high differential pressure alarms over beds to provide multiple indications of potential overfilling.
4) Implementing level deviation alarms comparing level instrumentation with level information predicted from the differential pressure instrumentation.

Figure 13: LOPA Implementation to Reduce Risk of Overfilling



12. Conclusions

1) Overfilling typically does not apply to Closed Loop Systems.
   (A systematic analysis is still required.)

2) Overfilling to a utility system will typically not result in overpressure.

3) Overfilling to other process equipment may not result in overpressure.
   (The ability of the downstream system to absorb the flow must be checked.)

4) In some cases, the onset of overfilling is so disruptive it can be excluded as a scenario.

5) Pump discharge pressure calculations require a thorough understanding of the system.

6) A PHA or LOPA may exclude overfilling as a design scenario.

7) Additional layers of protection can be added to excluding overfilling as a scenario.

8) The preference is to design out overfilling with equipment design. In some cases it is possible to ensure the operating envelope is so narrow that overfilling is not a scenario.

13. References

[1] CSB: U.S Chemical Safety Board (2007) Report 2005-04-I-*TX Refinery Explosion and Fire,* Available https://www.csb.gov/assets/1/20/CSBFinalReportBP.pdf p.17.

[2] Ibid, p. 21 - 23

[3] API Standard 521:2008, *Pressure-relieving and Depressuring Systems, p. 65-66*

[4] API Standard 521:2014, *Pressure-relieving and Depressuring Systems, p. 21-22*

[5] Ibid, *p. 13*

[6] ASME BPVC, Section I:2017*, Rules for Construction of Power Boilers, p. 61*

[7] ASME BPVC, Section VIII Div 1:*2017, Rules for Consruction of of Pressure Vessels*

[8] API Standard 521:2014, *Pressure-relieving and Depressuring Systems, p. 13*

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Refrigerated tanks base plate-heating hazards – A case study of Ethylene tanks

Mahmoud Mohamad Hassan[2], Mahesh Murthy*[2], Pulak Pal[4], Gys Van Zyl[1],
Integrity Engineering Solutions[1], SABIC[2], Global EHSS, SADAF[4]
*Presenter E-mail: murthym@sabic.com

Abstract

Cryogenic storage tanks are commonly used for the storage of refrigerated liquids at sub-zero temperatures. Such tanks are often of double-wall construction with thermal insulating material in the annular space between the two tanks. These tanks commonly employ foundation heating (electrical or steam) to prevent freezing of the soil beneath the tank and the associated risk of frost heave. Frost heave occurs when water beneath the tank freezes and unevenly expands leading to structural damage. A case study presented in this paper is for a storage tank where liquid ethylene is contained at -104°C , in which the foundation heating system conduits were found to be severely corroded. This resulted in Class 1, Division 2 violation of Hazardous Area Classification Code of the company's engineering standards and also potential for frost upheave and structural damage of ethylene tank.

Thermal finite element analysis was used to estimate the temperature distribution beneath the tank and the potential for frost heave. In the analysis, the effect of parameters like soil conductivity, soil temperature, environmental temperature and insulation conductivity on soil temperature was evaluated. Sensitivity analysis was used to determine the critical parameters and field temperature measurements were used to quantify these parameters through best fit with analysis results.. Ground water table heights were measured at wells in the area and local historical data. Detailed analysis indicated that the heat transfer from ethylene tank to the soil did not result in sub-zero temperatures beneath the tank and would not cause frost heave. As a result, the foundation heating was discontinued utilizing Management of Change processes. In addition to compliance with Hazardous Area Classification, substantial heating costs were also saved as an outcome of this study. Details are reported in this paper.

Keywords: Process Safety Management, Cryogenic, Hazard, Hazardous Area Classification, Frost heave and Ethylene

Background:

During routine preventive maintenance inspection, conduits carrying electrical cables were found severely corroded underneath the ethylene tank. The conduits contain electrical heating elements that are used to maintain the foundation temperature above 0°C. This is required to prevent freezing of the ground water which would result in frost heave due to uneven expansion of the soil. The damaged conduits also posed a hazardous area classification breach of Class I, Division II, as per the company's engineering standards [1] .

The storage tanks contain liquid ethylene at -104ºC), much lower than the ambient temperature for Saudi Arabian soil conditions [2] . Given the hazards of frost upheave and hazardous area classification breaches, there were two options available. Option 1 was to empty the ethylene tanks, repair the defects and put it back to service. Option 2 was to undertake a detailed engineering study to determine soil temperatures beneath the tanks and evaluate the actual need for foundation heating.

Option 1 was found to be extremely expensive considering extensive periods of shutdown. Option 2 was chosen and the results of the Finite Element Analysis (FEA) is presented in detail in this paper.

Study methodology:

Soil temperature distribution by thermal FEA

Heating elements are provided in the soil beneath the cryogenic ethylene storage tanks, with the objective of preventing damage to the tank due to frost heave. A large number of the heating elements and conduits had been damaged, and effective repair was extremely difficult to implement. Furthermore, considering typical high environmental temperatures in middle-eastern region, the likelihood of frost heave should be significantly less than in cooler climates [3] . Finite element thermal analysis was performed in order to evaluate the possibility of sub-zero temperatures beneath the tank (and specifically beneath the concrete ring-wall)

A schematic outline of Ammonia tank is given is Figure 1.

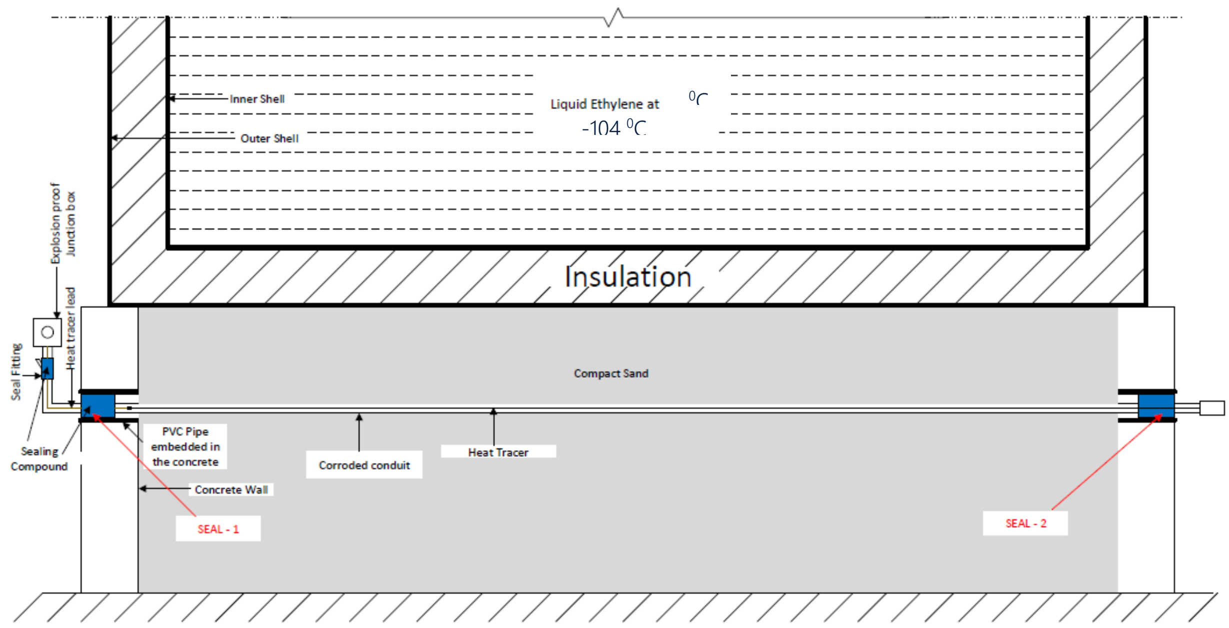


Figure 1 – Schetatic outline of Ethylene tank

An axisymmetric finite element model of the lower parts of the tank was created. Primary components as illustrated in Figure 2 below:

- Carbon steel shell and floor (inner and outer)
- Concrete ringwall and layer on outer tank bottom plate
- Dry sand (below inner tank bottom plate)
- Foam glass insulation between inner and outer tank bottoms
- Perlite insulation (between inner and outer tank shells)
- Saturated sand (soil beneath tank)

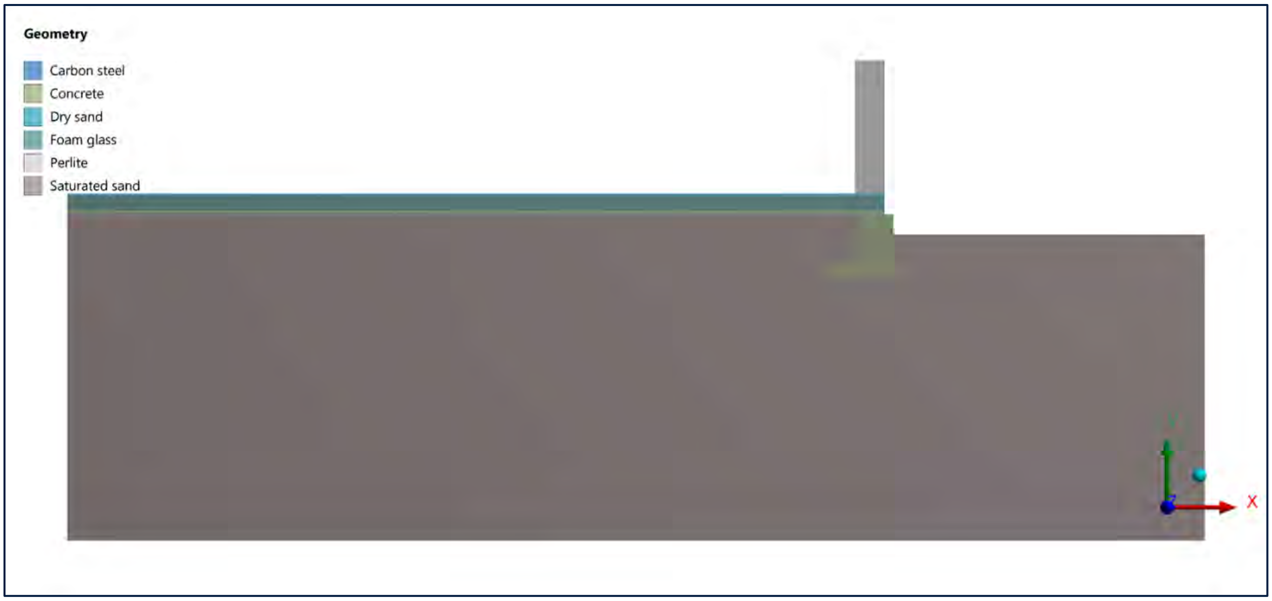


Figure 2 - Geometry and primary components of finite element model of tank bottom parts

The finite element mesh consisted of quadrilateral elements and is illustrated in Figure 3.

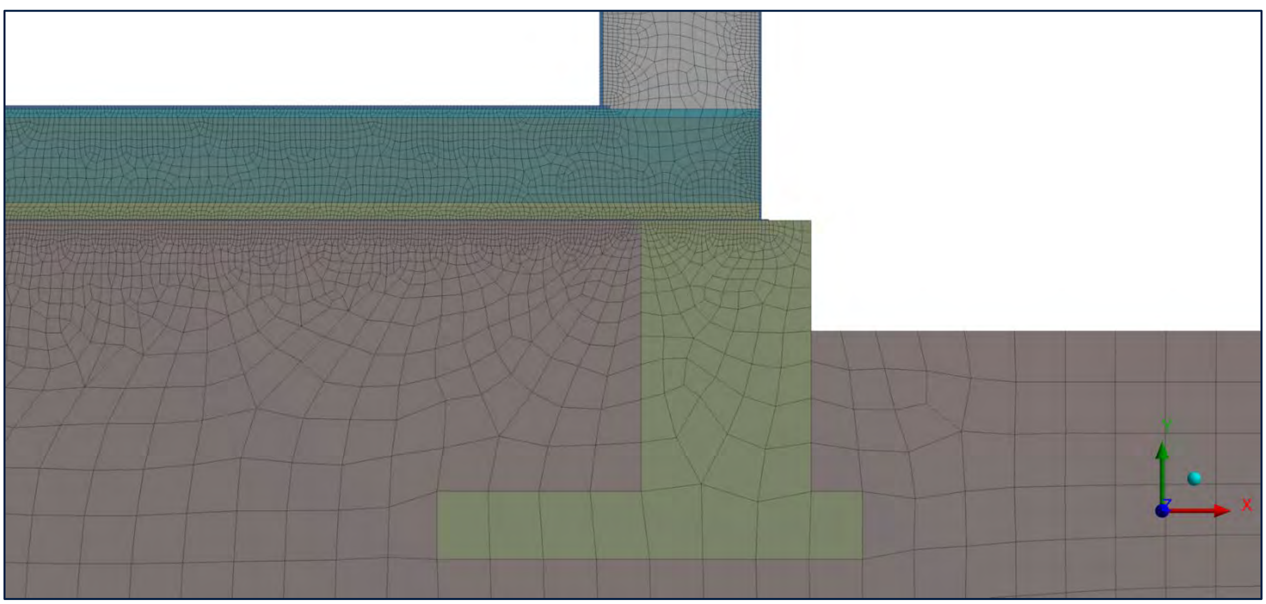


Figure 3:Finite element mesh

Boundary conditions used in the analysis are:

- Temperature inside inner tank (-104°C)
- Convective heat loss to ambient (10 W/m^2°C, ambient temperatures were varied)
- Soil temperature remote from tank (29°C, based on measurements)

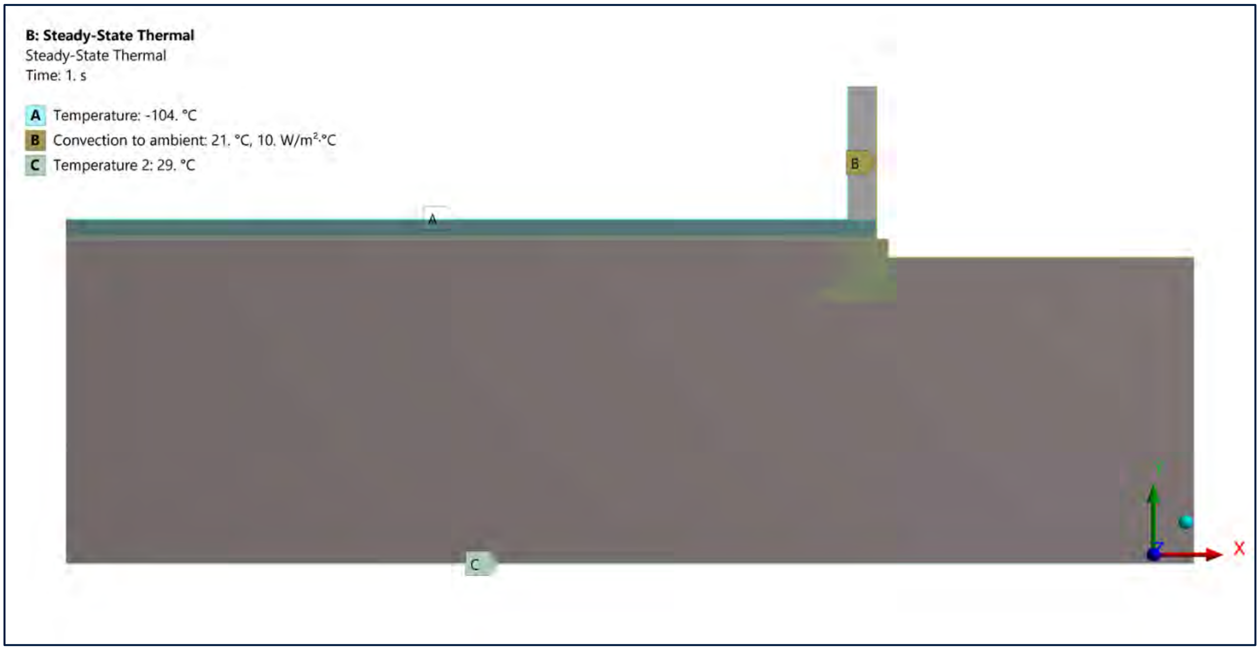


Figure 4: Boundary conditions used in thermal analysis

Parameters influencing heat transfer rates

Heat transfer rates are influenced by the following parameters;

- Soil temperature and
- Thermal conductivity

Soil temperature and thermal conductivity of the soil had high impact on the heat transfer rates . Thermal conductivity of foam glass and environmental temperature had a medium impact on the model. Thermal conductivity of concrete and saturated sand had a low impact on the heat transfer rates. The heat transfer analysis parameters are given in Table 1 below;

FEA Analysis parameters	Baseline	Range	
		Min	Max
Thermal conductivity, W/m.K			
Concrete	1	1	1.8
Dry sand	0.15	0.15	0.25

Saturated sand	3	2	5
Foamglass	0.05	0.048	0.056
Soil temperature, ºC	29	15	50
Environment temperature, ºC	21	0	50

Table 1 – Finite Element Analysis parameters

Parameters best fit

A number of model parameters in the finite element model influence the calculated temperature distribution:

- Thermal conductivity of:
    - Concrete
    - Dry sand
    - Saturated sand
    - Foam glass insulation
- Soil temperature
- Environment temperature

Data was not available to accurately quantify these parameters; therefore, a combination of temperature measurements and sensitivity analysis was used to estimate them. Figure 5 shows that the predicted depth of freeze beneath the tank is most sensitive to soil temperature and thermal conductivity.

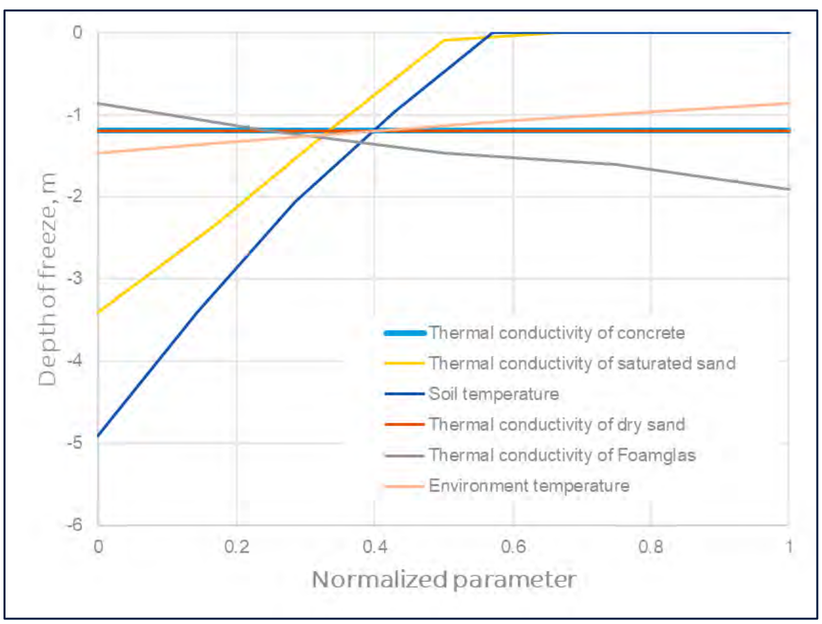
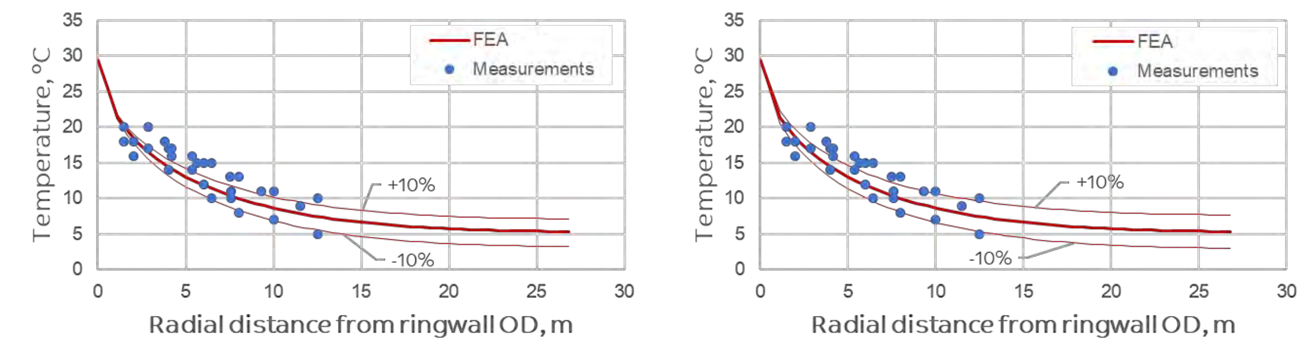


Figure 5 :Sensitivity of parameters to the prediction of depth of freeze beneath the tank

Temperatures measurements were performed on two tanks, after deactivating the heating elements. Thermal parameters in the FEA were adjusted until good correlation with measurements was achieved. Figure 6 illustrates the correlation between FEA results and temperature measurements for variations in the two most sensitive parameters.



Soil conductivity | Soil temperature

Figure 6: Illustrating soil conductivity and soil temperature parameters best fit with temperature measurements

Table 2 lists the values of all parameters used in the analysis that were determined by the sensitivity analysis and correlation with soil temperature measurements beneath the tanks.

Table 2: Best fit parameters

Thermal conductivity, W/m.K	
Concrete	1.8
Dry sand	0.15
Saturated sand	4.3
Foamglass	0.05
Soil temperature, °C	29
Environment temperature, ºC	Varies

Using the best-fit parameters, FEA was used to predict the soil temperature distribution beneath the tank in the event of a 0°C environmental temperature (50 year recurrence interval) and with deactivated foundation heating elements. The result provided in Figure 7 shows that no sub-zero temperature is predicted in the soil beneath the tank.

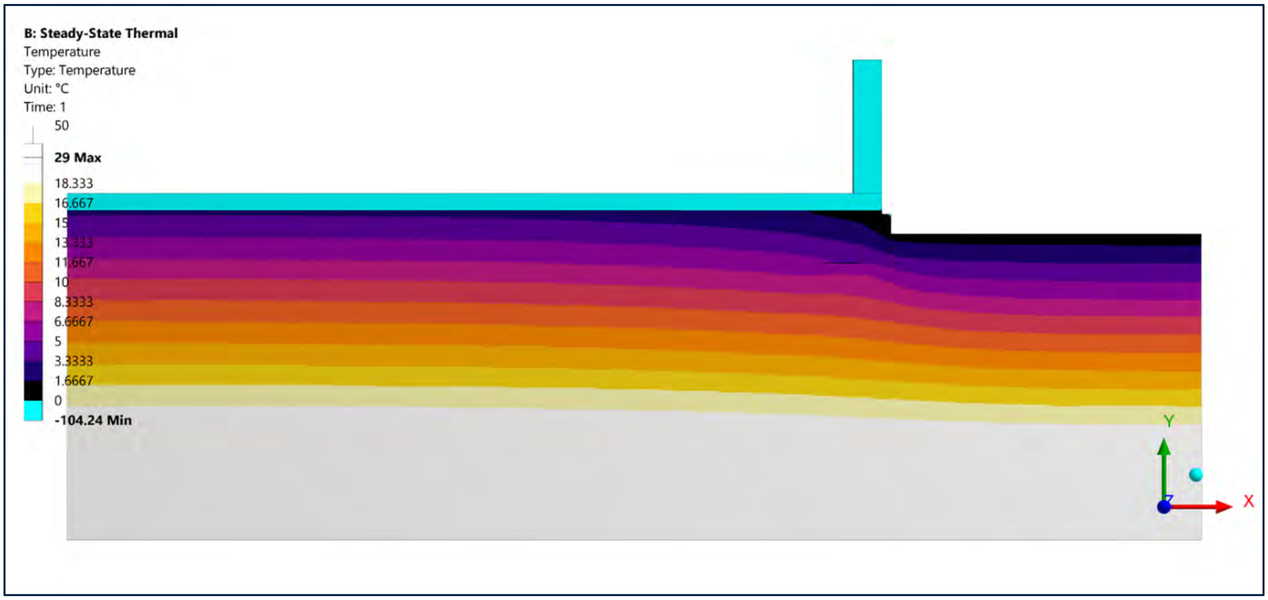


Figure 7: Temperature distribution with 0°C environmental temperature and best-fit parameters.

The study concluded that sub-zero temperatures are not expected beneath the tank under any realistic condition, and with this result as one of the considerations in a broader risk analysis, it was decided to disable the foundation heating on the two tanks.

Recommendations

- Turn off the base plate heater
- Approach of using FEA

Thermal finite element analysis was effectively used as a tool to obtain a more detailed understanding of the temperature distribution in the foundation of the storage tanks, which resulted in an informed decision to disable foundation heating, thereby eliminating a known safety hazard while reducing energy costs.

End notes

- Hazardous Area Classification hazard was eliminated due to de-activation of igition source. SABIC technical safety alert was also issued based on the case study [4]
- Frost heave was ruled out as credible scenario, given the context of Ethylene tanks.
- The FEA approach led to energy savings 122 kilo- watt, or an estimated equivalent of $ 40,000 for two ethylene tanks.
- Estimated indirect costs for repairing and restoring the foundation heaters were in the range of USD 70 million.
- 24 similar tanks were identified across SABIC that could be potentially be applied with similar approach. Estimated energy savings was in the range of 11085 Mega Watt Hour per annum.

References:

1. SABIC Engineering Standard Hazardous Area Classification – S02-E05, Rev 0, June 2017
2. Typical ground water temperature in Saudi Arabia, accessed via http://webcache.googleusercontent.com/search?q=cache:ftp://ftp.ncdc.noaa.gov/pub/data/EngineeringWeatherData_CDROM/engwx/riyadh_sa.pdf, accessed via website https://www.ncdc.noaa.gov/; on 23 August 2019
3. Mansour Almazroui et.al. , 2013, Trends of temperature extreames in Saudi Arabia, International Journal of Climateology Published online in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/joc.3722
4. Global EHSS Bulletin # 64, 15 May 2018, Issued by SABIC Internal Communications Department

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

A Practical Approach to Preventing Systematic Error in the Maintenance of Instrumented Safeguards

Eloise Roche and Dr. Angela Summers*
SIS-TECH Solutions
12621 Featherwood Dr. Suite 120, Houston, TX 77034
Presenters E-mails: asummers@sis-tech.com*, eroche@sis-tech.com

Abstract

Instrumentation and electrical (I&E) maintenance is typically managed using site-wide policies, practices, and procedures. Since I&E equipment is part of the control system and nearly every other layer of protection, the cumulative impact of poor I&E performance can be a significant contributor to major events. Systemic problems in managing I&E equipment reliability lowers process safety performance across a site.

Practical guidance is needed on how to assess the vulnerability of existing sites to instrumented safeguard failure due to maintenance deficits. This paper leverages Reason's organizational accident model as a framework to discuss site-specific factors that impact a site's susceptibility to maintenance error. A table of more than 60 human factors covering I&E maintenance activities was developed and organized by 4 elements of causality: organizational processes, workplace practices, personnel traits, and enabling conditions. The human factors table can be used to rate an industrial site on a negative-to-positive scale, highlighting those areas where systemic changes would likely improve maintenance performance and instrument reliability.

Keywords:
Instrumentation, safety instrumented systems, electrical systems, maintenance, human factors, human error, systematic

1 Leading or Lagging Indicators

The process industry depends on I&E equipment maintained in a manner that sustains the equipment's ability to act as required, when required, to prevent process safety incidents. While this responsibility is mandated by process safety regulations, it is simply a wise business practice to be proactive in managing instrument reliability. At many facilities, any one of thousands of instruments could cause operational problems. High reliability organizations understand that tackling these challenges head-on yields the best process availability.

Yet, assessments conducted by the UK's Health and Safety Executive (HSE) [1] and the US's Occupational Safety and Health Administration (OSHA) [2, 3] have found that some companies in the process sector have problems with their maintenance programs, as evidenced by the percentage of maintenance-related findings (Figure 1). These findings echo those published as a series of case studies in Guidelines for Safe Automation of Chemical Processes (Safe Automation) [4].

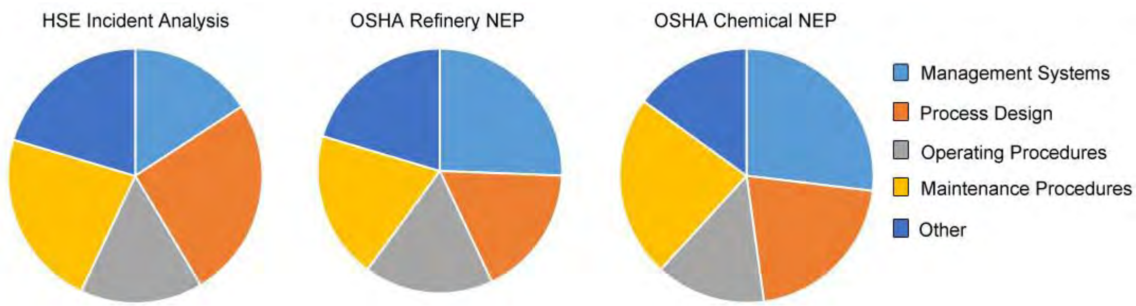


Figure 1. HSE Incident Analysis [1], OSHA Refinery National Emphasis Program (NEP) [2], and OSHA Chemical NEP [3] Findings

Government and industrial organizations have recommended metrics for monitoring the effectiveness of process safety management, including the Health and Safety Executive [5] the Center for Chemical Process Safety [6], and the American Petroleum Institute. API 754 [7] established 4 tiers of indicators (Figure 2). The bottom 2 tiers are leading indicators, because they are measures of the operating discipline, equipment integrity and safety culture. When these tiers are well-managed, it is far less likely that an event will happen. Safe Automation's case studies show that the top 2 tiers are often events where Tier 3 and 4 metrics were not implemented, and site practices did not identify and correct systemic problems.

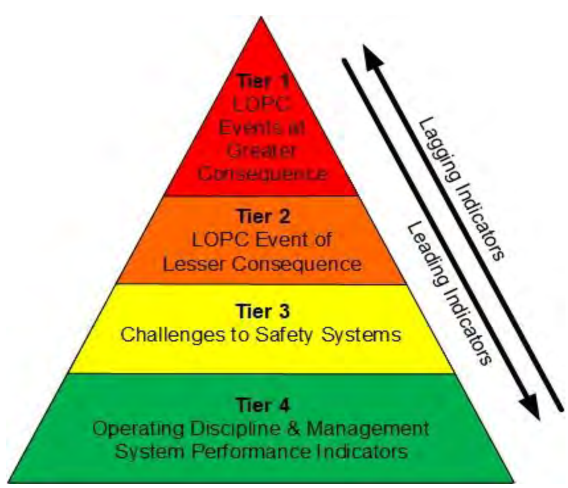


Figure 2 API 754 Metrics

International standards on instrumented safeguards provide more detailed guidance on performance metrics. ISA 61511 [8] requires monitoring the safety instrumented system (SIS) reliability parameters, which are Tier 3 metrics. Quite a few more Tier 3 metrics are recommended by ISA TR84.00.04 in Annex R [9]. Tier 4 indicators, such as using maintenance records as a predictive tool for reliability issues, were introduced into the 2012 edition of ISA TR84.00.03 [10] on asset integrity management of SIS. Recent ISA 84 meetings have included workshops on reducing systematic errors during SIS implementation and discussions on preventing systematic errors during maintenance.

2 Incidents are an Organization Failure

Human factors often play an out-sized role in poor I&E reliability. Safe Automation's case studies demonstrated strong links between the incidents and the failure to manage the on-going reliability of instrumentation and controls [4, 11]. These incidents ultimately were attributed to a series of failures that lined up in a dangerous manner. To prevent incidents, effort is required to sustain the asset integrity of the site's I/E equipment [12]. The errors, violations, and systemic failures in one system, whether control or safety, often repeat in other instrumented systems. If SIS equipment is not maintained, it is highly likely that other I/E reliability deviations are occurring. Systematic issues in maintenance can easily cause a breakdown of multiple IPLs (Independent Protection Layers), even if the IPLs are deemed independent based on an analysis of the equipment and system architecture [13].

The latest industry-published guidance on reducing maintenance errors through diversity is not really helpful. While theoretically attractive, there is no evidence that equipment diversity, staggered testing, or diverse maintenance teams can address the predominant underlying problems that are frequently cited by I&E technicians (Table 1). Rather, the proposed diversity would tend to make many field issues worse by increasing the complexity of the design, installation, testing, and maintenance.

Table 1 Problems commonly cited by I&E Technicians [13]

Unclear roles and responsibilities	Poor procedures
Lack of up-to-date documentation	Lack of warnings or cautions
Poor planning	Poor installation and configuration

3 A Practical Approach to Determining Site Risk for Systematic Error

James Reason, the father of the accident causation model, also known as the "swiss cheese" model, stated "Blaming people for their error is emotionally satisfying but remedially useless [14]." Errors are not inherently bad. There are a multitude of industry stories of errors that birthed significant innovations.

Errors can be made by the best people. No one intends to make them. The more competent the person is, the more likely they will commit a very serious error. This is because the most competent people will seek out assignments with the greatest challenges and risk. All employees should be competent enough to do at least the average job, so error management is not equivalent to competency management. Rather, error management is about understanding what promotes errors and changing the situation presented to the employee to discourage them instead.

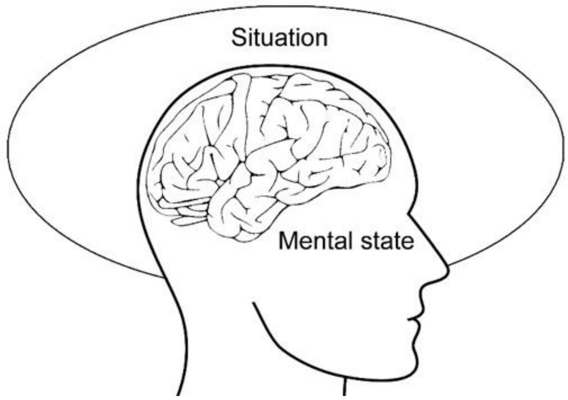


Figure 3 Errors Involve A Mental State and A Situation

Errors are affected by the mental state of the individual and the situation presented to the individual (Figure 3). Functional safety principles cannot control the individual's mental state, but they can influence the individual's decision-making processes. Everyone weighs the costs versus the benefits of complying to policies, procedures, and practices (Figure 4).

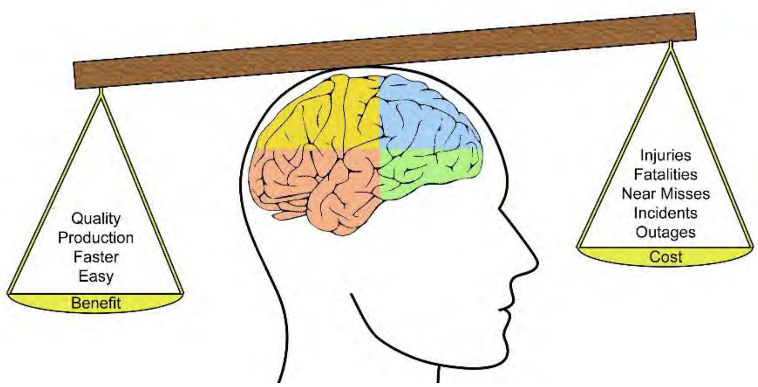


Figure 4 Humans Balance Costs and Benefits When Making Decisions

The perceived costs might include accidents, injuries, and damages, but these may seem like unlikely future events compared to the benefits of doing something an easier way or saving time today. In most cases of non-compliance, the benefits are easy to see immediately with little obvious negative impact.

The cost/benefit balance is rarely shifted by increasing the penalties for non-compliance, because these penalties are already known to be severe in the case of process safety events. Instead, greater influence on decision-making might be achieved by investing more time in acknowledging the important benefits of compliance.

In contrast to the mental state, the situation can be controlled and managed by functional safety management. The situation can be viewed as what maintenance personnel face when executing the work. The situation involves 4 elements: organizational processes, workplace practices, personnel traits and enabling conditions (Figure 5).

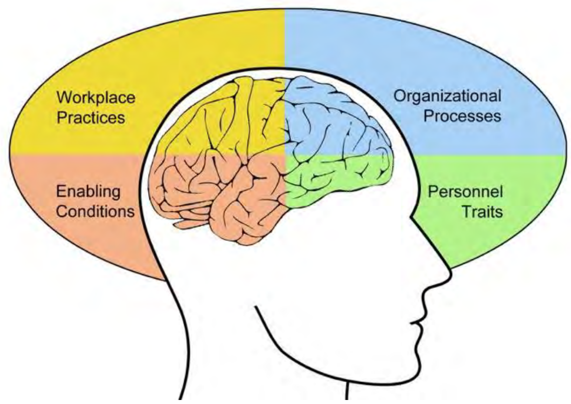


Figure 5 Situations Involve 4 Elements

These elements are external to personnel, but they influence the decision-making process. The situation can vary significantly in ways that promote or discourage human error. For example, the situation could involve a task that is well-planned with detailed procedures in place to achieve quality work execution. Or the situation could involve troubleshooting unexpected behavior with unfamiliar technology in a poorly lit room with no up-to-date specification.

Reason's organizational accident model (Figure 6) used the 4 elements to illustrate the underlying causality [14] of human errors and incidents. Errors occur when a planned action does not achieve the desired result. For example, the maintenance procedure did not define who takes responsibility for the equipment being returned to service, so this critical task was not done. In contrast, violations occur when deviations from an approved practice are intentionally taken.

Violations are rarely malicious acts and are often intended as positive with respect to some aspect of the task. An optimizing violation occurs when someone does something that seems to accomplish the same thing but is easier or faster than the planned way. For example, the deviation meets the deadline or budget, demonstrates a high level of skill, or is simply easier. Routine or optimizing violations can become part of the site maintenance culture when an owner/operator rarely punishes deviations or fails to frequently reward compliance [15].

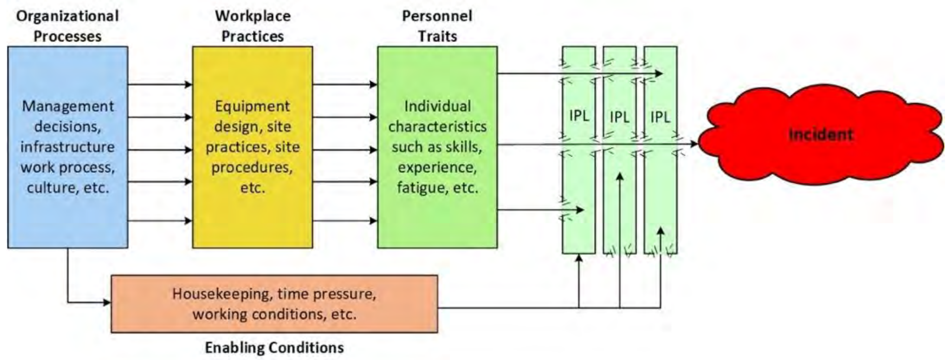


Figure 6 Anatomy of an Organizational Accident (adapted from [14])

Organizational processes focus worker attention on certain behaviors and metrics, while workplace practices impact the quality and consistency by which maintenance activities are accomplished. Organizational processes determine what is considered important or not. These processes feed into management decisions that directly impact the day-to-day work of planning, forecasting, budgeting, communicating, monitoring, and auditing. Many accidents begin with negative organizational processes that promote poor workplace practices and tolerance of poor instrument reliability. For example, effective communication between maintenance and engineering is critical to ensure that reliability issues are addressed comprehensively. The likelihood of unresolved, long-term reliability problems significantly increases when communication breaks down between engineering, operations, and maintenance.

Workplace practices are the written instructions that govern how maintenance is executed. Poor practices, like inadequate instructions, missing specifications, obsolete procedures, and ineffective interface design, increase the likelihood of errors and violations [16]. For example, a test procedure that does not define the required equipment function becomes a source for maintenance error even though the maintenance person has a high degree of skill with the technology.

Personnel traits are intrinsic to the person executing the task. The most important traits are possessing the skills and experience necessary to complete assigned tasks correctly. Hiring competent personnel is essential but sustaining competency as I&E technology changes can be challenging. High turnover can make it difficult to ensure that personnel have the in-depth knowledge of the system design needed for troubleshooting problems or evaluating the impact of management of change activities. Competency can also be off-set when fatigue or poor health impacts decision-making. Accidents become even more likely when poor workplace practices are combined with negative personnel traits, such as inexperience, poor skills, or being tired.

Enabling conditions make errors impacting multiple protection layers more likely. These conditions are triggered by organizational decisions that promote errors and violations, such as high work load, time pressure, unreasonable schedules, poor housekeeping, and poor quality tools. Other task-specific conditions, such as ill-fitting personal protective equipment, dim lighting, poor housekeeping and missing labeling can also exist due to management policies and resource allocations. These enabling conditions potentially increase the likelihood that error will occur regardless of how optimal the organizational processes and workplace practices may be.

The 4 Elements of Causality were used as a framework to develop a list of 61 positive and negative human factors for maintenance activities. The list is based on personal experience and was enhanced by lessons-learned discussions at the Instrument Reliability Network [17], ISA 84 and ISA 61511 committee meetings. A summary of the systematic error sources, subtopics and human factors is provided in Table 2. The detailed human factors table is provided in Appendix A.

Table 2. Hierarchy of Human Factors in Maintenance

Sources	Subtopics	Specific Human Factors
Organizational Processes	Communications	• Clarity of responsibilities • Engineering and maintenance communications • Operations and maintenance communications • Teamwork and communications • Emergency communications
	Instrument Reliability Program	• Process demand tracking • Maintenance priority • Out of service/bypass management • Repeat failure/bad actor management
Workplace Practices	Maintenance Instructions	• Task complexity • Procedure clarity and detail • Return to service procedures • Change management • Quality control and record keeping
	Maintenance Equipment/Interfaces	• Specification and installation drawing availability • Maintenance feature/facility design
Personnel Traits	General	• Knowledge, skills and experience • Fatigue
	Competency Assessments	• Verification of knowledge and skills
Enabling Conditions	General	• Personal protective equipment • Tools and equipment • Working conditions • Housekeeping • Time pressure

Each human factor listed in Table 2 has multiple prompts in Appendix A. These prompts describe negative and positive human factor attributes. Some negative organizational attributes often cited in incident reports are as follows:

- Instrumented safeguard maintenance is frequently delayed, behind schedule, or not prioritized.

- Frequent bypassing of instrumented safeguards with little oversight, time limits, or risk assessment. Bypasses include operator bypasses, manual operation, changing setpoints, and forces.

- High tolerance for poor process control and upsets leading to frequent demands on the instrumented safeguards.

- High tolerance for poor instrument reliability. Unresolved issues, long-term out-service, and frequent fault conditions accepted.

In contrast, the positive organizational attributes associated with these are:

- Instrumented safeguard maintenance is prioritized, executed as scheduled, and is rarely delayed for operational reasons.

- Instrumented safeguards only bypassed under strict controls, including compensating measures and time limits. Bypasses include operator bypasses, manual operation, changing setpoints, and forces.

- Low tolerance for poor instrument reliability. Proactive attitude to taking action to improve reliability.

- Low tolerance for poor process control; particular focus on reducing frequency of process upsets and process demands on the instrumented safeguards.

The attributes can be rated on any desired scale. This paper takes a binary approach where the site is assessed as displaying either negative or positive human factors. Another approach is to use an analog scale of 1 to 5 with 1 being mostly negative and 5 being the mostly positive. The intent is to provide a means to assess the current status of the strategies, processes and activities used by a site to identify and prevent systematic errors.

4 Applying Human Factors Evaluation to a Case Study

Process safety management provides multiple opportunities to assess the adequacy of I&E equipment, including hazards and risk analysis, risk assessments, maintenance monitoring, management of change, and audits. The use of the positive and negative human factor table in Appendix A can be triggered as a result of findings from these activities. Using the table as part of a corrective process is a good way to get started and to demonstrate immediate benefits. However, it does mean that the site is already experiencing sufficient systemic impact to warrant a deeper dive. This is a classic feedback, or lagging indicator, approach to process safety [16]. Another approach would be to use the table as a self-assessment tool to understand site vulnerability to maintenance error before negative performance data piles up.

To illustrate the methodology, the human factors table was applied to the incident commonly known as "Buncefield." The incident occurred at the Hertfordshire Oil Storage Terminal, which was located in Hemel Hempstead north of London England and was part of a complex of tank terminals known as the Buncefield Depot. The depot had an estimated capacity of 60 million gallons, making it the 5th largest oil depot in the UK [18]. The depot served as a major distribution center for the UK oil pipeline network [18]. It provided fuel to Humberside, Merseyside, as well as to Heathrow and Gatwick airports [19].

An explosion occurred on December 11, 2005, which injured 43 people and devastated the Hertfordshire Oil Storage Terminal, which was jointly owned by Total UK Ltd and Chevron Ltd [19]. Residences and commercial buildings in the area were structurally damaged with some requiring demolition. The economic impact on regional businesses is estimated to be in the range of ₤130–170 million [19]. Total losses may have been as much as ₤1 billion [19, 20].

The incident occurred when the Automated Tank Gauging (ATG) system for one of the terminal tanks failed (Figure 7). The loss of level control allowed fuel to be fed into the tank for 11 hours [21]. The fuel overflowed through the tank conservation vents for approximately 40 minutes [22] prior to ignition, producing a large vapor cloud estimated to be 8 hectares in size [23]. The vapor cloud ignition resulted in the largest peacetime explosion in European history [18] producing a tremor measuring 2.4 on the Richter scale and blowing out windows five miles away from the site [23].

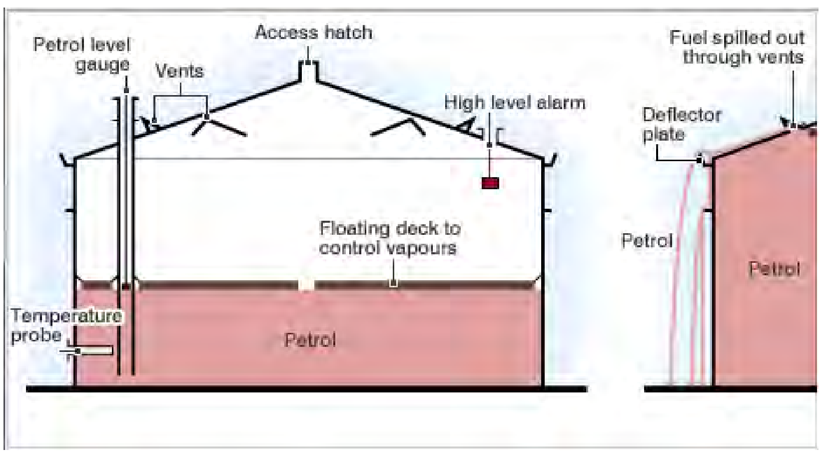


Figure 7. Simplified Graphic of Buncefield Tank

Gasoline was being delivered to the tank on the day before the incident. Early the next morning, the ATG displayed an unchanging level, although the tank continued to fill. By practice, the operator controlled the tank level by terminating transfer upon receipt of the ‘user’ alarm. However, the 'user', 'high', and 'high high' level alarms used the same transmitter. The failure of the shared transmitter rendered all three alarms inoperative. Since the ‘user’ alarm never activated, the operator did not take action to terminate transfer.

An independent high-level switch, set above the ATG high-high level, was designed to close inlet valves and activate an audible alarm, but it also failed. The high-level switch had been disabled when the maintenance organization, due to lack of understanding of the relatively new technology and to insufficiently detailed procedures, did not reinstall a lock on the switch test arm. Without the lock, the level switch was not activated when the float was lifted. By late afternoon, the tank overfilled and contents spilled out of tank roof vents. A vapor cloud was formed and noticed by tanker drivers and by people outside the facility. The fire alarm was activated and firewater pumps were started. An explosion occurred a short time later, likely ignited by the startup of the firewater pumps.

Reviews of the readily available literature on the incident identified significant problems with I&E equipment. The analog level involved in the incident had 14 dangerous failures (stuck) in the 3.5 months preceding the incident. It appears that the site had a high tolerance for poor process control and poor instrument reliability. The three "failed" alarm measurements came from the same faulty level device, which is an example of a common cause failure for the intended protection layers. The review also identified quite a few organizational and workplace issues:

- Confusion of responsibilities and expectations
- Poor communication between operations and maintenance
- Lack of consistency on who did what and when
- Lack of timely communication between maintenance technicians and supervision
- No reporting structure for escalation of unresolved problems
- Inaccessible installation drawings, specifications, and functional requirements
- No review of installation and configuration of instrumented safeguards after initial validation

The available information in reports on the Buncefield incident were used to assess the site against the human factors in Appendix A. Nearly half (28 of the 61) of the negative attributes were identified. It is also likely that other negative attributes were present; however, these contributors are not discussed in the available literature. The assessment suggests that the organizational processes, workplace practices, personnel traits, and enabling conditions at the Buncefield site significantly increased the likelihood of systematic issues. The negative human factors made an overfill event much more likely than would have been predicted by hazards and risk analysis.

5 Summary

Safe Automation's case studies describe incidents where instrumented safeguards should have intervened in the incident propagation but did not. The underlying causes of these failures were often systematic rather than random. These underlying causes likely impacted the potential for incidents across the site, and perhaps the entire organization. A practical first step in preventing systematic error in instrumented safeguard maintenance can be to perform a qualitative evaluation of the existing maintenance human factors. This evaluation identifies the areas in which the organization might be vulnerable to such errors and where there might be more value to focusing additional organizational resources. A table of positive and negative human factors was created to allow assessment of a site's vulnerability to systematic errors during maintenance. As an illustration, the table was used to assess the Buncefield incident. Based on the published reports, nearly half of the 60 negative human factors were present.

6 References

[1] HSE, Health and safety laboratory report, Loss of Containment Incident Analysis, Great Britain (2003).

[2] OSHA, Process Safety Management for Petroleum Refineries - Lessons Learned from the Petroleum Refinery Process Safety Management National Emphasis Program.

[3] OSHA, Process Safety Management for Chemical Plants - Lessons Learned from the Chemical Process Safety Management National Emphasis Program.

[4] CCPS/AIChE, Guidelines for Safe Automation of Chemical Processes, Second Edition, American Institute of Chemical Engineers, NY, (2017).

[5] Health and Safety Executive, "Developing process safety indicators," 1st edition, (2006) ISBN 978 0 7176 6180 0.

[6] CCPS/AIChE, Guidelines for Process Safety Metrics, Wiley-Interscience, New York (2009).

[7] API, Recommended Practice Process Safety Performance Indicators for the Refining and Petrochemical Industries, RP754, API, Washington D.C. (2016).

[8] ISA, ANSI/ISA 61511-1-2018, Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), Research Triangle Park, NC (2018).

[9] ISA, Guidelines for the Implementation of ANSI/ISA 84.00.01- Part 1, TR84.00.04-2015, Research Triangle Park, ISA, (2015).

[10] ISA, Asset Integrity of Safety Instrumented Systems, TR84.00.03-20012, Research Triangle Park, ISA, (2015).

[11] Summers, Angela, E. Roche, H. Jin, M. Carter, "Incidents That Define Safe Automation," 61st International Instrumentation Symposium, Huntsville Alabama, May 2015.

[12] Summers, Angela, "Risk Assessment Challenges to 20:20 Vision," Process Safety Progress, pages 119-125, June 2015.

[13] Summers, Angela E. and Eloise Roche, "Mobile Interfaces on the Plant Floor," 73rd Instrumentation and Automation Symposium, Texas A&M University, January 2018.

[14] Reason, James and Alan Hobbs, Managing Maintenance Error: A Practical Guide, Ashgate Publishing Company, Hampshire England (2003).

[15] Reason, James, Managing the Risks of Organizational Accidents, Ashgate Publishing Company, Hampshire England (1997).

[16] CCPS/AIChE, Guidelines for Safe and Reliability Instrumented Protective Systems, 1st edition, American Institute of Chemical Engineers, NY, (2014).

[17] Instrument Reliability Network, Mary Kay O'Connor Process Safety Center, Texas A&M University.

[18] Wikipedia, "2005 Hertfordshire Oil Storage Terminal Fire," http://en.wikipedia.org/wiki/2005_Hertfordshire_Oil_Storage_Terminal_fire.

[19] Buncefield Major Incident Investigation Board, "The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board," ISBN 978 0 7176 6270 8, (2008).

[20] British Broadcasting Station, "Buncefield blast could cost £1 bn," December 11, 2008, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/england/7777539.stm.

[21] British Broadcasting Station, "Buncefield tank was overflowing," May 9, 2006, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/4752819.stm.

[22] The Daily Mail, "Petrol tank 'overflowing' before Buncefield blast," May 9, 2006, United Kingdom, http://www.dailymail.co.uk/news/article-385607/Petrol-tank-overflowing-Buncefield-blast.html

[23] The Guardian, David Fickling, "Faulty fuel gauge caused Buncefield Explosion," United Kingdom, http://www.guardian.co.uk/uk/2006/may/09/buncefield.davidfickling

Appendix A - 4 Elements of Causality

Table 1. Organizational Processes

Topic	Positive Human Factors	Negative Human Factors
Communications		
Clarity of responsibilities	Expectations communicated and rules are consistently enforced	Confusion on expectations or inconsistent enforcement
Engineering and maintenance communications	Clear communication between maintenance technicians and engineering to resolve instrumented safeguard issues	Maintenance lacks support from engineering; tolerance for unresolved instrumented safeguard issues
	Timely communication of negative findings by maintenance to I&E engineering/reliability	Poor or lack of communication of negative findings by maintenance to I&E engineering/reliability
Operations and maintenance communications	Clear communication of instrumented safeguard status between operations and maintenance technicians	Poor/unclear communication of instrumented safeguard status between operations and maintenance technicians
	Reliable operator-to-maintenance technician communication equipment (two-way radios, telephone, etc.) with alternative means	Unreliable, no alternative, may not work in an overloaded situation
	Good communication between operations and maintenance technicians	No/not expected communication between operations and maintenance technicians
Teamwork and communications	Formal communication with turnover log when maintenance shift changes occur. Includes communication of active bypasses, overrides, faulted devices, and other issues relevant to safe completion of tasks.	Informal communication when shift changes occur. No defined expectation on what to communicate at shift change.
	Frequent supervisory reviews and quality assurance checks	No/incomplete supervisory reviews or quality assurance checks
	Good communication of new findings related to instrumented safeguard health, such as obsolescence, end-of-life, and any identified installation, commissioning, or functional issues	Lack of timely communication of new findings related to instrumented safeguard health, so that identified issues are not addressed systematically across a site
	Routine reporting of repeat failures (e.g., bad actors) to maintenance supervision	Lack of timely communication of repeat failures to maintenance supervision
Emergency communications	Clear, unambiguous site-wide emergency warning system	No distinction in emergency warnings based on areas or event types. Not audible or reliable in some locations.
Instrument Reliability Program		
Process demand tracking	Low tolerance for poor process control; particular focus on reducing frequency of process upsets and process demands on the instrumented safeguards	High tolerance for poor process control and upsets leading to frequent demands on the instrumented safeguards
Maintenance Priority	Maintenance priority is established based on device criticality and level of functional impairment	Maintenance priority does not consider device criticality; redundant instrumented safeguard equipment essentially treated as "spares;" level of functional impairment not understood
	Spare parts management program considers the time required to acquire specialized instrumented safeguard equipment and the need to remain within the assumed mean time to restoration	Spare parts purchased on failure detection without regard to lead time and planned mean time to restoration
	Instrumented safeguard maintenance is prioritized, executed as scheduled, and is rarely delayed for operational reasons	Instrumented safeguard maintenance is frequently delayed, behind schedule, or not prioritized
	Instrumented safeguards only bypassed under strict controls, including compensating measures and time	Frequent bypassing of instrumented safeguards with little oversight, time limits, or risk

Topic	Positive Human Factors	Negative Human Factors
Out of service/bypass management	limits. Note: Bypasses include operator bypasses, manual operation, changing setpoints, and forces.	assessment. Note: Bypasses include operator bypasses, manual operation, changing setpoints, and forces.
	Low tolerance for poor instrument reliability. Proactive attitude to taking action to improve reliability.	High tolerance for poor instrument reliability. Unresolved issues, long-term out-service, and frequent fault conditions accepted.
Repeat failure/bad actor management	Minimal false or spurious alarms	Many false or spurious alarms or alarms ignored or disabled
	Instrumented safeguards are known to be reliable and effective	Instrumented safeguards are known to be unreliable or ineffective
	Identified failures are investigated and repaired in a timely manner	Failed equipment remains in-service; repeated failures are not investigated
	Failure reporting and escalation notification for unresolved issues is clearly defined	No/poor reporting structure for identified failures; no escalation of unresolved problems

Table 2. Workplace Practices

Topic	Positive Human Factors	Negative Human Factors
Maintenance Instructions		
Task complexity	Required tasks are well-defined and regularly performed	Infrequently performed or repeated/rapid changes in task expectations
	Manufacturer installation and maintenance manuals are reviewed to ensure that maintenance procedures agree with intended application; manuals are accurately translated, written in native language and written from the perspective of the maintenance technician	Manufacturer installation and maintenance manuals are not reviewed for consistency with application; manuals are not clearly written, in wrong language, or poorly translated
	Units of measure are consistent between provided documents and equipment configuration	Units of measure are not consistent between provided documents and equipment configuration
Specification, installation drawing availability	Procedures include verification of installation and configuration of instrumented safeguards against specification	No review of installation and configuration of instrumented safeguards after initial validation
	Installation drawings, specifications, and functional requirements are accessible when needed	Installation drawings, specifications, and functional requirements are not accessible
Procedure clarity and detail	Procedures are at the right level of detail to ensure consistent execution and record keeping	Too general or too detailed leading to inconsistent maintenance, a tendency to skip steps, or poor maintenance records
	Procedures are written in concise, imperative language	Wordy, inconsistent style
	Procedures include notes, cautions, and warnings where errors could result in impaired equipment	Lack of hazard awareness, unknown impact of error
	Notes, cautions, and warnings set off from procedural steps (e.g., in text boxes placed immediately before applicable steps)	Task criticality not clearly identified
	Procedures/checklists used in the performance of task	Task sequence done by memory
	Procedures contain clear pass/fail criteria	Maintenance determines acceptability based on ad hoc criteria
Return to service procedures	Maintenance procedures include return to service verification by operations	No operations cross-checking or verification of return to service for instrumented safeguards

Topic	Positive Human Factors	Negative Human Factors
Change management	Procedures address change management and version control	Maintenance corrects problems without engineering involvement or change management review
Quality control and record keeping	Procedures include appropriate supervisory checks	No supervisory cross-checking or verification
	Data governance is used to ensure record quality	No data governance
Maintenance Equipment/Interfaces		
Maintenance feature/facility design	Instrumented safeguard equipment is easily accessible for maintenance or accessibility issues are addressed in the maintenance procedures	Instrumented safeguard equipment is not easily accessible; maintenance is known to be delayed by access issues
	Maintenance facilities designed for purpose, arranged in logical order, easy to use, well-labeled, and in-service status is easy to detect	Maintenance facilities are confusing, complicated, unreliable, disablement possible without detection, or in-service status difficult to detect

Table 3. Personnel Traits

Topic	Positive Human Factors	Negative Human Factors
General		
Knowledge, skill and experience	Minimal turnover of maintenance technicians resulting in significant experience with site instrumented safeguards and a high degree of personal knowledge of site systems	High turnover of maintenance technicians resulting in less experience with site instrumented safeguards and less personal knowledge of site systems
	Hiring qualifications are defined and include specific requirements for instrumented safeguards	Hiring qualifications are not defined or do not include specific requirements for instrumented safeguards
	Technicians are well-trained, experienced, and good at troubleshooting the technologies used on site	Technicians are not well-trained, are inexperienced, or lack troubleshooting skills with the technologies used on-site
	Technicians are well-trained on safe work practices, such as lock-out/tag-out, electrical safety, job safety analysis, etc.	No specific/unclear requirements for training on safe work practices, such as lock-out/tag-out, electrical safety, job safety analysis, etc.
	Technicians are well-trained on instrumented safeguard maintenance and required record keeping. Training program includes periodic refresher training.	No specific/unclear training on instrumented safeguard maintenance and record keeping.
Fatigue	Overtime limited by defined policy that ensures reasonable and regular rest breaks	Overtime is extreme and does not ensure sufficient rest
	Permanent shift assignments	Shift rotations
Competency Assessments		
Verification of knowledge and skills	Training verification includes both test and observations	No/inadequate verification of learning

Table 4. Enabling Conditions

Topic	Positive Human Factors	Negative Human Factors
Personal protective equipment	Required PPE does not affect performance of tasks	PPE is heavy, cumbersome, gets in the way of performing tasks.
Tools and equipment	Test equipment is high quality, equipment calibration is verified	Poor quality test equipment; lax tracking of calibration records
Working conditions	Noise level low enough to easily communicate	Hearing protection is required. Noise level hinders ability to hear or use communication equipment.
	Provided with protection from weather; including rain, snow, wind, and sun	Not provided with protection from weather, including rain, snow, wind, and sun
	Task conducted in climate-controlled environment	Task conducted in high temperature and/or humidity extremes
	Clear visibility where task is being executed	Poor visibility where task is being conducted, including fog, smoke, or other sight obscuring element
	Lighting is sufficient to conduct task, including being able to read tags, critical information, procedures, or other documents	Lighting is insufficient to conduct task or to read documents
Housekeeping	Equipment is clearly and uniformly labeled	Equipment is mislabeled or not labeled
	Equipment is installed in the field as would be expected (A to C are upstream to downstream)	Equipment is installed in an unexpected order (C to A are upstream to downstream)
	Equipment criticality is easily distinguished in the documents and in the field	Similar equipment in same area or grouped together without any indication of criticality
	Clearly communicated identifier/location for instrumented safeguard equipment	Ambiguous identifier/location for instrumented safeguard equipment
	Consistent tagging between procedures, P&IDs, and equipment	Inconsistent tagging between installation and documents
	Installation shows discipline toward good labeling, tight wiring connections, and consistent installation practices	Installation shows poor discipline, such as loose wiring connections, lack of consistent labeling, or inconsistent installation practices
Time pressure	Number of tasks well-matched to work force	Required tasks exceed resources
	Pace of tasks is not rushed. Little time pressure on step execution.	Multiple tasks are executed in rapid succession and under time pressure

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Managing an Instrumented Protective Systems Program for a Petrochemical Facility

J. Gregory Hall*
Eastman Chemical Company
*Presenter E-mail: jghall@eastman.com

INTRODUCTION

An Instrumented Protective Systems (IPS) program reduces the risk associated with health and safety effects, environmental impacts, loss of property, and business interruption costs in a petrochemical facility. IPS are composed of any combination of sensor(s), logic solver(s), and final element(s) used to implement protective functions that detect abnormal or unacceptable operating conditions and take action on the process to achieve or maintain a safe state. The objective of the program is to identify the activities necessary to ensure the design, operation, and maintenance of IPS throughout their life cycle, from inception through decommissioning, and to ensure the functional safety requirements of identified Safety Instrumented Systems (SIS) are met.

Upper management support is necessary for an IPS program to be successful. The program is managed by a group of personnel committed to process safety. Operating facilities are driven to make production quotas while managing process safety risk. The IPS group helps operating departments comply with company IPS policies, procedures, and standards. Upper management is the authority of jurisdiction to ensure the operating departments comply.

IPS PROGRAM ELEMENTS

An IPS program is based on a RAGAGEP (Recognized and Generally Accepted Good Engineering Practice). Typically, North American petrochemical company programs are based on ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector –Part 1: Framework, Definitions, Systems, Hardware and Software Requirements”, NFPA standards, API practices, and other practices and standards. The ISA standard specifically addresses safety instrumented systems (SIS) but can be broadened to include all IPS including SIS, safety, and non-safety interlocks. The following IPS program elements were adapted from the ISA standard.

1. Hazard and Risk Assessment

   The hazard and risk associated with each IPS interlock is assessed by the safety department using the appropriate methodology (e.g., formal safety reviews, Process Hazard Analyses (PHA), Layers of Protection Analyses (LOPA)).

2. IPS Classification Assignment

   Each IPS interlock is assigned an IPS classification based on the hazard and risk assessment see Figure 1.

3. IPS Classification Requirements

   Each IPS interlock is designed, documented, installed, commissioned, operated, tested, and maintained to specific requirements.

4. Design and Engineering Requirements

   Each IPS interlock is designed to company standards. SIS and safety interlocks are reviewed by the IPS group before being issued for construction. Any changes during a project that affect an IPS classification are reviewed to determine if the classification is valid or must be changed.

5. Application Software Requirements

   Each IPS interlock is configured and programming to specific requirements. Security and access to the logic solver software is important to the integrity of each interlock.

6. Installation, Commissioning, and Validation Requirements

   Each IPS interlock is installed according to the drawings and other documentation. Commissioning includes full functional testing. Each SIS interlock is validated to ensure compliance with LOPA requirements.

7. Operation Requirements

   The operating department ensures all IPS are operated, maintained, and tested as required.

8. Maintenance Requirements

   Each IPS interlock that can be defeated or bypassed during normal operation has an operating procedure describing operator action when defeated or bypassed. On-line calibration and maintenance capability of interlocks is provided for processes that operate continuously and are only shutdown during planned outages.

9. Proof Test Requirements

A proof test procedure is developed for each SIS and safety interlock to perform a proof test per the specified time interval. A copy of each completed test is stored in a instrumentation computer database.

10. Modification

Any modification to an IPS interlock is reviewed by the IPS group to ensure the IPS classification remains valid.

11. Information and Documentation

Each IPS interlock is properly documented and recorded in an instrumentation computer database.

12. Grandfathered Safety Interlocks

Each grandfathered safety interlock is properly documented and tested on a specified time interval. Any modification to a grandfathered interlock is reviewed to determine if the interlock can remain grandfathered.

RESPONSIBILITIES

It takes a coordinated effort of different departments and groups to manage an IPS program. This effort is managed by the IPS group with the backing of upper management.

1. IPS Group

The IPS group is responsible for managing all aspects of the IPS program, developing policies, procedures, and standards regarding the design, construction, maintenance, verification, and testing of IPS, and assisting operating departments with compliance to company policies, procedures, and standards.

The group is composed of different engineering disciplines and expertise.

- IPS design engineer
- Safety department engineer
- Safety department LOPA expert
- Instrument engineer

- Process technology engineer
- Process control engineer
- DCS/PLC engineer
- Other members as needed

2. Safety Department

   Safety department representatives work with each operating department to assess and classify IPS interlocks within their responsibility. They perform the hazard risk analysis including LOPA when required.

3. IPS Design Engineer

   The IPS design engineer is responsible for ensuring IPS interlocks are properly designed, SIS interlocks meet LOPA requirements, and SIL verification calculations are completed. They work with all parties involved to develop and maintain procedures regarding the design, construction, maintenance, verification, and testing of IPS.

4. Operating Department

   Each operating department is responsible for developing and maintaining procedures regarding the design, construction, maintenance, verification, and testing of IPS in their area. They work with the maintenance department to ensure instrument calibrations and interlock testing is done within the required time intervals.

5. Maintenance Department

   The maintenance provides qualified technicians who are properly trained to perform maintenance, calibration, and testing of IPS interlocks and all associated instrumentation. Failure information is documented and recorded in a computer data base.

6. Documentation Services

   Documentation services create and update instrument and interlock records in a computer data base. Failure data is reported to the engineering, operating, and maintenance departments to correct any deficiencies with existing instrumentation and interlocks.

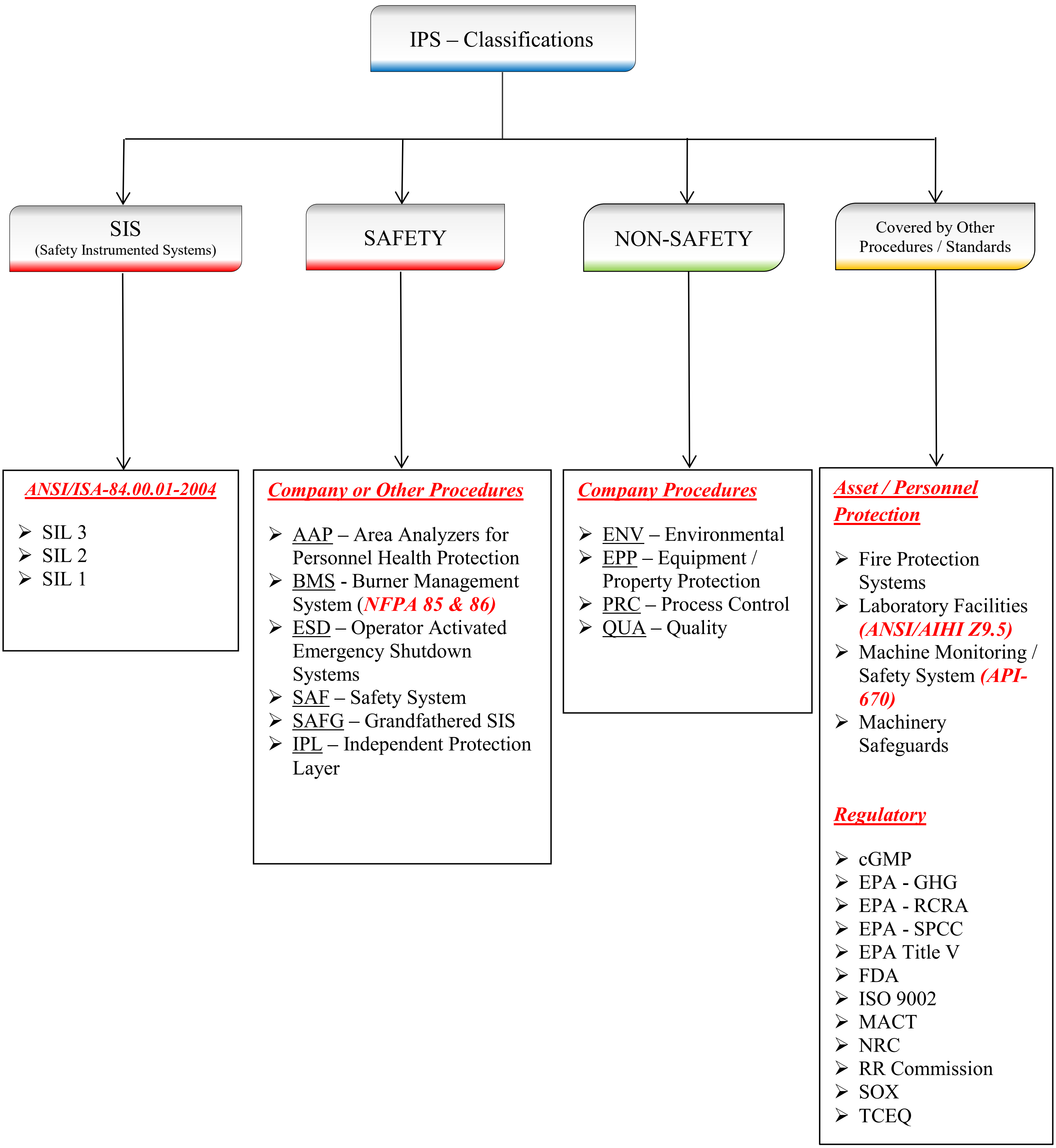
7. DCS/PLC Group

   The DCS/PLC is responsible for the configuration and programming of all IPS to ensure consistency and standardization throughout the plant site.

CONCLUSION

It is not an easy task to manage a life-cycle IPS program for a petrochemical facility that operates 24/7. Different departments, and groups must work together to ensure all parts of the program are covered. Upper management provides necessary personnel, training, equipment, computer resources, and expertise to ensure the program is successful. The IPS group is the key to managing the program. The maintenance and operating departments provide feedback used to improve the design, installation, commissioning, and operation of IPS interlocks. A successful IPS program reduces the potential risk associated with health and safety effects, environmental impacts, loss of property, and business interruption costs.

Figure 1 – IPS Classifications



MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

PPE – Can you have too much of a good thing?

Brenton L. Cox, Sean J. Dee*, Russell A. Ogle, and Matthew S. Walters
Exponent, Inc.
4580 Weaver Parkway, Warrenville, IL 60555 USA
*Presenter E-mail: sdee@exponent.com

Abstract

Specifying Personal Protective Equipment (PPE) after a hazard has been identified is a critical aspect of a facility's ability to protect their workers. In a chemical manufacturing facility, manual operations and maintenance activities have the potential to expose workers to hazardous chemicals and flammable atmospheres. Even though it is generally recognized to be one of the least effective safeguards in the hierarchy of controls, PPE is often the last line of defense, and sometimes the only feasible defense, that isolates workers from potential hazards. As a result, companies may lean toward putting workers in higher levels of PPE to provide additional protection. However, in many cases higher levels of PPE may introduce new hazards associated with limited worker mobility, fatigue, unreliable job performance, or limited egress. Therefore, PPE specification should focus not only on what is necessary to protect the worker, but also what is appropriate for a given job task. In this paper, a risk-based approach to PPE selection, specification, and use will be presented. Discussion will focus on potential hazards that can be inadvertently introduced because of PPE over-specification. Studies related to the impact of PPE on worker performance will be presented to help demonstrate the potential negative impacts of over specifying PPE. Lastly, a case study will be presented where a PPE specification was questioned, and the impact of increasing the PPE specification for a job task was evaluated.

Keywords: Operational Integrity, Personal Protective Equipment, PPE, Risk Assessment, Qualitative Risk Matrix

1 Introduction

All workplaces contain some inherent level of risk — defined as the potential for loss or injury — to which workers are exposed.[1] In the process industry, engineers and safety professionals manage risk to employees through the process of hazard control. Hazard control is the recognition,

[1] Speegle, M. *Safety, Health, and Environmental Concepts for the Process Industry, 2nd Ed.* Delmar, Clifton Park, NY, 2013, Chapter 11.

evaluation, and minimization of hazards. A hierarchy of hazard controls is typically followed, listed below in the order of most to least desirable:[2]

1. Elimination (removal of the hazard)
2. Substitution (replacing the hazard with a lower risk hazard)
3. Engineering Controls (equipment-related methods of control)
4. Administrative Controls (documented rules and procedures)
5. Personal Protective Equipment

Personal protective equipment (PPE) is the last line of defense protecting workers from known hazards.[3] However, properly specifying PPE is often complex because each protective device has limitations. Gloves, for example, can protect workers from a chemical, thermal, puncture, or abrasion hazard as well as provide other specialized protective functions. Selecting the correct PPE for a job is a process that involves a combination of experience, hazard identification and risk assessment (HIRA), and general safety knowledge regard the process hazards, job task, and PPE functionality. PPE is commonly used in combination with other elements of the hierarchy of hazard control, so the functionality and reliability of engineering or administrative controls may be critical to PPE selection. For example, a lockout-tagout (LOTO) program is an administrative control that can reduce the potential hazard exposure to a worker, thereby lowering the PPE requirement for a specific task.

In some cases, laws or regulations impose PPE requirements. The U.S. Occupational Safety and Health Administration (OSHA), for example, specifies four levels of PPE protection for Hazardous Waste Operations and Emergency Response (HAZWOPER) operations:[4,5]

- Level A: Supplied-air respirator and fully encapsulating chemical-resistant suit
- Level B: Supplied-air respirator and chemical-resistant clothing
- Level C: Air-purifying full-face respirator and chemical-resistant clothing
- Level D: Coveralls or fire-resistant clothing

While most work in normal plant operations can be safely performed with Level D protection, it may be tempting to specify the highest level or multiple types of PPE to ensure worker protection during non-routine maintenance or operation. However, PPE that is uncomfortable or cumbersome to the worker could pose additional risks. This paper explores the implications of PPE over-

---

2 ANSI-ASSE Z590-3 *Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes*, American Society of Safety Engineers, 2011.

3 Speegle, M. *Safety, Health, and Environmental Concepts for the Process Industry, 2nd Ed.* Delmar, Clifton Park, NY, 2013, Chapter 13.

4 Appendix B to 29 CFR § 1910.120 - Hazardous waste operations and emergency response.

5 The equipment specified for each level within this list only includes examples of distinct PPE features. Other PPE requirements not specified in the list may include but are not limited to boots, safety glasses, hardhat, gloves, and/or radio.

specification and provides a case study that reviews the impact of increasing the PPE specification for a job task.

2 General PPE Selection Guidance

In any given chemical manufacturing facility, there will a range of jobs and worker responsibilities. Some of these activities are routine and some may be unique occurrences. Similarly, a worker may encounter a range of hazards depending on the work activity in which they are engaged. To protect workers from these hazards, it is important that a job hazard analysis has been performed to identify, evaluate, and control the hazards.6 In any work assignment, various hazard controls can be implemented to protect the worker. PPE is a frequent choice as one of those safeguards.

2.1 Hazard Identification and Risk Analysis

PPE selection begins with the identification of the hazards to be encountered. These hazards can harm different parts of the human body, and thus various kinds of PPE may be required to control these hazards. In this paper, the focus is on the combined hazards of chemical and flammability exposure. Other hazards, such as mechanical, thermal, electrical, and biological, will be omitted only for the sake of brevity. A general discussion on PPE selection can be found in standard occupational safety and health references.7

As previously discussed, a range of engineering and administrative controls that may eliminate or mitigate the hazards involved should be considered prior to the specification of PPE. However, the hierarchy of controls is not a mandatory prescription which must be followed without the benefit of critical thinking. On the contrary, the hierarchy of controls is a powerful and useful guideline for evaluating the pros and cons of different types of safeguards. Although PPE is generally recognized as one of the least effective safeguards in the hierarchy of controls, PPE is often the last line of defense, and sometimes the only feasible defense, that isolates workers from potential hazards. If engineering and administrative controls cannot reduce the residual risk to an acceptable level, then the use of PPE is justified.

In the chemical process industries, it is not unusual to identify both chemical and flammability hazards in a work assignment. This combination of hazards can complicate PPE selection. The physical characteristics of PPE that best control chemical hazards may not offer any protection from flammability hazard such as a flash fire exposure. Similarly, the PPE that best protects a worker from a flash fire hazard may provide little or no protection from chemical hazards. While there are garments that provide protection from chemical exposure with an optional capability to provide escape protection from chemical flash fire hazards during hazardous materials incident response,8,9 the flame resistance and thermal protection requirements for these garments are not as robust as those that satisfy the NFPA standards for flame-resistant or arc-rated

---

[6] OSHA 3071 *Job Hazard Analysis*, Occupational Safety and Health Administration, 2002.

[7] Plog, Barbara A., Jill Niland, and Patricia Quinlan. *Fundamentals of Industrial Hygiene, Fourth Edition*. Chapter 18 Methods of Control. Ithaca, NY: National Safety Council, 1996.

[8] NFPA 1991 *Standard on Vapor-Protective Ensembles for Hazardous Materials Emergencies and CBRN Terrorism Incidents*, 2016, Section 7.7.

[9] NFPA 1992 *Standard on Liquid Splash-Protective Ensembles and Clothing for Hazardous Materials Emergencies*, 2018, Section 7.6

garments.10,11,12 Hence, if at all possible, it would be preferable to eliminate either the flammability or the chemical hazard to permit a simpler selection of PPE garments.

If one must protect against both chemical and flammability hazards, one option to consider is a more complex, layered clothing ensemble. This complex PPE ensemble can present significant physiological and psychological burdens on the worker (this issue is explored further in the next section of this paper). It is also critical to understand the limitations of the various layers of the ensemble, to ensure that interior layers do not become compromised by the presence of an outer layer. For example, a flame-resistant fabric may stipulate that its protective functionality is only valid if it is the outer garment. Because PPE selection is so important to the protection of the worker, the selection process must be predicated on a sound basis.

Chemicals may present multiple hazards for the worker including toxicity, corrosivity, or carcinogenicity. Chemical clothing PPE is intended to limit or prevent exposure to these hazards. Typically, chemical protective clothing consists of one or more polymer layers. The primary purpose of chemical clothing PPE is to prevent dermal contact with hazardous chemicals. Two factors drive the evaluation of chemical clothing PPE: the fluid state of the chemical exposure (liquid or vapor) and the compatibility of the garment material with the chemical. The fluid state is important because that determines how the chemical is presented to the garment, either by liquid splashing or by vapor intrusion.

For liquid splashing the garment design must be impermeable to liquid entry at the surface of the garment. Furthermore, the garment design must prevent entry or accumulation of any liquid through the garment seams or the interface of the skin and garment. Generally, liquid-splash protective garments will provide a much lower level of protection from vapor intrusion (if any at all). The performance requirements for liquid-splash protective garments are presented in NFPA 1992 (cited previously).

The potential for vapor intrusion presents a more stringent design constraint. Generally, to prevent vapor intrusion, the garment must be fully encapsulating. These garments also provide protection from exposure to liquid splashing. The performance requirements for vapor-intrusion protective garments are presented in NFPA 1991 (cited previously).

2.2 Fabric Evaluation

The compatibility of a garment material with a chemical of concern depends on the ability of the garment to resist the permeation (diffusion) of the chemical through the polymeric material. Permeation through polymeric materials depends on the chemical composition of the polymer, the thickness of the polymeric material, the molecular properties of the chemical of concern, and other environmental factors (temperature, pressure, exposure time, etc.). The permeation of a chemical through the garment surface can be evaluated through chemical resistance tables provided by the manufacturer. These tables will usually indicate whether the garment material is suitable for the

---

[10] NFPA 2112 *Standard on Flame-Resistant Clothing for Protection of Industrial Personnel against Short-Duration Thermal Exposures from Fire*, 2018.

[11] NFPA 2113 *Standard on Selection, Care, Use, and Maintenance of Flame-Resistant Garments for Protection of Industrial Personnel against Short-Duration Thermal Exposures from Fire*, 2020.

[12] NFPA 70E *Standard for Electrical Safety in the Workplace*, 2018.

chemical of concern, and if it is, a breakthrough time is reported. The breakthrough time is the time duration over which the garment will offer protection following an exposure to the chemical. Alternatively, one can determine the compatibility of a polymeric material with a chemical of concern by consideration of the Hildebrand solubility parameter for both the polymeric material of the garment and the chemicals of concern.[13]

2.3 Training

Simply selecting the correct PPE fabric for chemical protection is not sufficient to protect workers. Workers must also be trained in the proper donning, use, decontamination, and doffing of their PPE garments.[14] Prior to donning of PPE, the worker should inspect the garment for punctures, tears, or other defects that might permit entry of the chemicals of concern past the protective boundary of the garment. The worker should also read any labels, warnings, or instructions provided with the garment or on the garment tags. In donning the PPE, the worker must be careful to avoid damaging the garment and ensure that it is properly assembled. It is often helpful for a second worker to assist with the inspection after donning to ensure a full 360-degree inspection. During the use of the PPE, the worker must note the nature and duration of any direct exposures with chemicals of concern as this may limit the useful life of the garment (i.e., the garment should not be worn for a period exceeding the permeation time of a chemical of concern). Finally, the worker should be familiar with necessary decontamination and doffing procedures for the PPE. If an exposure occurs, the worker must carefully guard against exposure to the chemicals of concern which may have adhered to or penetrated the PPE garment prior to and during removal. Decontamination protocols and inherently safer doffing procedures (e.g., remove contaminated gloves by rolling them inside-out off of the hand, touch PPE garments only with gloves and not bare hands) can prevent or at least mitigate chemical exposures during the doffing of PPE.

2.4 Complex Specifications: Flammability and Chemical Hazards

Flammability hazards in the chemical process industries are manifested as flash fires, liquid pool fires, and jet fires. Flash fires are caused by the ignition of a diffuse fuel cloud followed by a flame sweeping through the cloud without causing significant overpressure damage.[15] Flash fires tend to be transient events with a duration measured in seconds. A liquid pool fire is caused by the ignition of a discrete accumulation of liquid fuel into a region of finite extent called a pool.[16] A pool fire rapidly achieves a steady burning rate and will continue burning until the fuel supply is consumed. A jet fire occurs when a flammable gas, vapor, or liquid is released under pressure from its containment.[17] The jet fire can persist until the discharge of fuel is stopped or the fuel supply is exhausted.

One important feature of flammability hazards is the duration of the exposure. Both pool fires and jet fires can present sustained fire hazards and therefore require PPE that is quite different from that required to protect against a flash fire. The workers most likely to be exposed to sustained

---

13 Moseman, J. "Are these the right gloves?" *Professional Safety*, pp. 40-47, April 2016.

14 NIOSH. *Occupational Safety and Health Guidance Manual for Hazardous Waste Site Activities*. National Institute for Occupational Safety and Health, Chapter 8 Personal Protective Equipment (PPE), 1985.

15 NFPA 921 *Guide for Fire and Explosion Investigations*, 2017, Section 3.3.87 and 6.3.7.11.2.

16 NFPA 921 *Guide for Fire and Explosion Investigations*, 2017, Section 5.7.3.

17 NFPA 921 *Guide for Fire and Explosion Investigations*, 2017, Section 23.8.2.2.5 and 23.18.6.

fires are firefighting personnel. Turnout gear or aluminized fire suits are the PPE of choice for firefighting activities. In comparison to pool fires and jet fires, flash fires present a hazard of much shorter duration. Therefore, PPE for protection from flash fires tends to be much lighter and less bulky than the full firefighting turnout gear employed for combatting sustained fires. Flash fire PPE garments are typically labeled as flame-resistant clothing (FRC).

Flash fires cause burn injuries by heating the skin tissue to injurious temperatures. Flash fires can lead to essentially two types of thermal exposure: direct flame impingement (related to convection) and radiant heat. The potential for thermal injury is characterized by the incident heat flux, the duration of the exposure, and the total energy deposited into the skin. FRC must satisfy six different thermal performance criteria as determined through standardized testing to successfully demonstrate that the garment will offer protection from these thermal damage mechanisms.[18] One common FRC garment uses cotton fabric treated with flame retardants. FRC is often intended to be reused on a routine basis much like a work uniform. To preserve the protective features of FRC, the user must follow the manufacturer's instructions regarding the laundering, inspection, and reuse of these garments.

NFPA requires that a hazard analysis for flash fire hazards be performed for the determination of whether FRC PPE is required, and if so, what performance characteristics it must satisfy.[19] An example of a flash fire hazard analysis procedure has been developed by BASF.[20] It is based on a consideration of the hazardous properties of the materials involved, the process area or equipment location where the work is to be performed, and the job task to be performed. The determination and specification of FRC PPE requirements follows from this hazard analysis. The BASF hazard analysis identifies three material hazard thresholds:

- Is it a flammable gas?
- Is it a liquid being handled or processed above it flashpoint?
- Is it a combustible dust where the particle size less than 75 µm, the minimum explosive energy is less than 100 mJ, and the moisture content is less than 10%?

The considerations for the process area are the following:

- Evaluation of the area's flash fire history and near-misses
- Are flammable gases, vapors, or combustible dusts present in the atmosphere during normal operations?
- Are potential ignition sources present?
- Is there a potential for personnel to be present in the vicinity of a flash fire event?

---

18 NFPA 2112 *Standard on Flame-Resistant Clothing for Protection of Industrial Personnel against Short-Duration Thermal Exposures from Fire*, Appendix B Properties for Evaluating Flame Resistant Garments, 2018.

19 NFPA 2113 *Standard on Selection, Care, Use, and Maintenance of Flame-Resistant Garments for Protection of Industrial Personnel against Short-Duration Thermal Exposures from Fire*, 2020.

20 BASF. Flash Fire FRC Assessment Tool, 2010. Accessed at http://www2.basf.us/DocSearchWeb/displaydoc?docbase=Wyandotte_MI_US&cabinet=EHS&folder=Publish/WSTD&docname=WYN032.007a&rend=pdf.

Finally, the considerations for the job task are the following:

- Credible release scenarios
- Exposure potential: does the task involve the potential for exposure to the material of concern or are there other activities nearby that could create a flash fire potential?
- Ignition potential: does the task introduce an ignition source for the material of concern or are there other ignition sources nearby?

Based on this hazard analysis, if it is concluded that there is a potential for both exposure to the material of concern and its ignition, then FRC may be required.

Generalizations about PPE selection must be tempered by the specific circumstances encountered at each worksite and each work assignment. Given that caution, some generalizations are reasonably indicated. First, if a worker must be protected from both flash fires and chemical hazards, then the in most cases the outerwear for their PPE clothing should be the flash fire protection (the FRC). In the event of a flash fire, the FRC will not only provide protection for the worker, but it will also provide some protection for the chemical hazard PPE. Thus, the worker will still be protected from chemical hazards.

On the other hand, if the worker is exposed to a chemical hazard, the FRC may be degraded or contaminated by the exposure event. If the chemical exposure is an unexpected, acute exposure, the condition of the FRC should be immediately evaluated. The condition assessment of the FRC in this circumstance may require an interruption of the work assignment. For example, if a flammable liquid splashes onto the worker, the chemical PPE clothing may protect the worker from a chemical exposure. But the saturation of the FRC fabric with a flammable liquid could compromise its effectiveness. In fact, the saturation of FRC fabric with a flammable liquid clearly increases the magnitude of the fire hazard presented to the worker. Whether the work should be discontinued will depend on several factors. One example of an important factor in this scenario is the quantity of liquid splashing onto the worker. A spill onto FRC fabric equivalent to one cubic centimeter of flammable liquid is likely an acceptable risk. The spill of a liter of flammable liquid onto the worker presents a higher, and likely unacceptable, fire risk. The manufacturer's instructions and warnings should also be consulted for potential guidance regarding contamination of PPE.

Following the work activity, the condition of both the FRC and the chemical PPE should be assessed for potential reuse. The ability to reuse the FRC will depend on the degree to which the FRC can be decontaminated or repaired. To prevent damage to the FRC, the laundering and maintenance instructions should be closely followed.[21,22,23,24] The ability to reuse the chemical PPE

---

21 Hoagland, H. "How to properly care for flame-resistant garments," *Welding Journal*, pp 38-40, November 2008.

22 ASTM F1449-08 Standard Guide for Industrial Laundering of Flame, Thermal, and Arc Resistant Clothing, 2015.

23 ASTM F2757-09 Standard Guide for Home Laundering Care and Maintenance of Flame, Thermal and Arc Resistant Clothing, 2016.

24 NFPA 2113 Standard on Selection, Care, Use, and Maintenance of Flame-Resistant Garments for Protection of Industrial Personnel Against Short-Duration Thermal Exposures from Fire, 2020.

will depend on the manufacturer's recommendations. Many, if not most, of chemical protection garments are intended for one-time use only.

Finally, it must be emphasized that combining PPE for both flash fire and chemical hazards results in a complex PPE ensemble. This complex PPE ensemble can present significant physiological and psychological burdens on the worker and may introduce new hazards that must be managed.

3 Potential Negative Impacts of PPE

As previously discussed, PPE is the critical last line of defense to protect workers from chemical, physical, and biological hazards, but the trade-off for this protection primarily impacts the worker through a reduction in performance, efficiency, and stamina. The proper selection of PPE requires a consideration of these trade-offs to ensure the worker is adequately protected without unknowingly introducing new hazards, or otherwise unduly impacting their ability to perform the job. As OSHA cautioned in an appendix the HAZWOPER standard, 29 CFR 1910.120, "The use of PPE can itself create significant worker hazards, such as heat stress, physical and psychological stress, and impaired vision, mobility, and communication."[25] While adequate protection for an employee is critical, "over-protection, as well as under-protection, can be hazardous and should be avoided where possible."[26] The impact of chemical protective equipment on human performance has been the subject of extensive studies funded by the United States military due to the threat of chemical warfare, which can require the use of chemically protective clothing during combat.[27] Chemical warfare protective combat clothing bears many inherent similarities to the PPE employed in industrial settings, consisting of a non-encapsulating over-garment and a full-face respirator with a hood, gloves, and boots.[28] The military studies have identified the following primary causes of performance degradation experienced by soldiers wearing chemical warfare protective combat clothing:[29]

- *Heat stress due principally to the weight, insulation, and low moisture vapor permeability of the overgarment.*
- *Reduced manual dexterity due to the constraints imposed by the gloves, overgarment, and boots.*
- *Restricted vision due to the design and optical characteristics of the mask, e.g., reduced field-of-view and poor optical quality of the mask faceplate.*
- *Restricted communication (hearing and speaking) due to the mask and hood.*
- *Respiratory stress due to air resistance of mask filters and outlet valves.*

---

[25] Appendix C to 29 CFR § 1910.120 - Hazardous waste operations and emergency response.

[26] *Ibid.*

[27] Taylor, H.L. and Orlansky, J. The Effects of Wearing Protective Chemical Warfare Combat Clothing on Human Performance. Institute for Defense Analysis, IDA Paper P-2433. August 1991.

[28] Grugle, N.L. An investigation into the effects of chemical protective equipment on team process performance during small unit rescue operations. Master's Thesis. pp. 37-41.

[29] Taylor, H.L. and Orlansky, J. The Effects of Wearing Protective Chemical Warfare Combat Clothing on Human Performance. Institute for Defense Analysis, IDA Paper P-2433, April 1991. p. I-4.

These causes parallel the hazards identified by OSHA and underscore the fact that the process of PPE selection is truly one of risk management: balancing the hazards posed by PPE against the external hazards the PPE is intended to control.

3.1 Heat Stress

Heat stress is an obvious and widely discussed concern relative to PPE that cannot be overemphasized. Any level of additional clothing can increase the risk of the worker developing heat stress, and the amount and type of PPE worn directly influences the magnitude of this risk.[30,31] Garments designed to protect against physical and chemical agents are most often highly impermeable to water vapor, which imposes a considerable restriction on the body heat balance.[32] As a result, once PPE has been selected, it may be necessary to impose limitations on work duration and require mandatory rest periods to manage the risk of heat stress.

3.2 Mobility

Wearing a chemically protective ensemble may also impair dexterity and mobility. This fact has been recognized by the National Fire Protection Association (NFPA), which publishes standards on PPE for fire fighters and other emergency responders during incidents that involve hazardous material operations. Again, much of this PPE is comparable, if not identical, to the PPE used in the chemical process industry. As previously discussed, the NFPA 1991 and NFPA 1992 standards cover vapor-protective and liquid splash-protective ensembles, respectively. Both NFPA 1991 and NFPA 1992 directly address the loss of hand dexterity due to wearing gloves by requiring a standardized test and setting limits based on a comparison to a barehanded control test.[33,34] The standardized test compares the time required for a user to place a series of pegs into a specifically designed pegboard while wearing the protective equipment versus barehanded. The measure of dexterity is reported as "percent increase over barehanded control," where a value over 100 percent indicates that a greater time was required to accomplish the task while wearing gloves. For liquid splash-protective gloves, the average percent increase over barehanded control must be less than 200 percent, and for vapor-protective gloves, the average percent increase of barehanded control must be less than 600 percent. In other words, depending on the type of protection deemed necessary, it can increase the amount of time required to complete a manual task by a factor of between 2 and 6. Thus, workers may need to spend more time in high hazard locations to accomplish the same task.

3.3 Vision

Vision can also be significantly impaired by PPE, which can diminish visual acuity (sharpness or clarity of vision) and limit the field of view of the user. NFPA 1991 and NFPA 1992 require a minimum visual acuity of 20/35 for garments where hoods with visors are provided, and 20/100

---

30 Hazardous Waste Operations. National Institute for Occupational Safety and Health (NIOSH). 1985.

31 Cheremisinoff, N.P., and Graffia, M.L. Environmental and Health and Safety Management: A Guide to Compliance. 1995. pp. 446-447.

32 Holmer, I. Protective Clothing in Hot Environments. *Industrial Health*. **44**, pp. 404-413, 2006.

33 NFPA 1991 *Standard on Vapor-Protective Ensembles for Hazardous Materials Emergencies and CBRN Terrorism Incidents*, 2016, Section 7.4.6, 8.17, and A.7.4.6.

34 NFPA 1992 *Standard on Liquid Splash-Protective Ensembles and Clothing for Hazardous Materials Emergencies*, 2018, Section 7.2.6 and 8.13.

for ensembles with flash fire escape protection.[35,36] Consider a scenario where a worker who has 20/20 visual acuity is required to wear a vapor-protective ensemble with flash fire escape protection. Objects that were clearly visible to the worker at 100 feet without PPE may now need to be as close as 20 feet from the worker to be clearly visible while wearing the ensemble.[37] For reference, a visual acuity of 20/100 is comparable to the ability to read only the first two lines on the typical Snellen Eye Chart used by many American optometrists and ophthalmologists. Thus, the decision to provide PPE to protect against vapor and/or splash hazards may result in a measurable loss of visual acuity, and simultaneous protection from a flash fire hazard can cause a significant trade-off in visual acuity.

3.4 Psychological Effects and Decision Making

In addition to the physiological effects that PPE can impart on a worker, studies have also suggested that protective clothing can impact a person's decision making and psychological effects. The previously referenced military studies of soldiers wearing chemical warfare protective combat clothing also found that clothing could result in symptom intensification, and general deterioration of mood. [38] This included intensification of feelings of sleepiness, dizziness, and unhappiness, while aggressiveness, friendliness, and clear thinking decreased. When combined with other factors, such as heat stress, cognitive performance has been shown to markedly decrease, primarily due to errors of omission.[39]

3.5 Summary

Depending on the level of PPE necessary, each of these factors may also significantly impact the industrial worker in chemical protective clothing. Take for example the consideration of respiratory protection. The options can range between no PPE, carrying an escape respirator, wearing a half-face or full-face air-purifying respirator, wearing a self-contained breathing apparatus with supplied air via a hose or a tank, or wearing a fully-encapsulated suit with supplied air. Additionally, due to the impact of psychological and physiological stresses imposed using PPE, wearers may require medical clearance and surveillance before, during, and after its use.[40]

4 Case Study: Reevaluation of PPE for Line Breaks

After an injury or near-miss, personnel may find themselves questioning the resiliency of their safeguards. The following case study discusses a facility that reevaluated the PPE specified for line break activity following an exposure and chemical burn injury to a maintenance operator. The incident occurred during installation of temporary drain piping on an ethylene oxide header. The background of the incident, the root cause of the exposure, and the role of PPE and safe work

---

[35] NFPA 1991-2005, Sections 7.1.2(3) and 7.8.2.

[36] NFPA 1992-2005, Sections 7.1.2.2 and 7.6.2.

[37] "Low Vision and Legal Blindness Terms and Descriptions." American Foundation for the Blind. url: https://www.afb.org/blindness-and-low-vision/eye-conditions/low-vision-and-legal-blindness-terms-and-descriptions

[38] Taylor, H.L. and Orlansky, J. The Effects of Wearing Protective Chemical Warfare Combat Clothing on Human Performance. Institute for Defense Analysis, IDA Paper P-2433, April 1991. p. I-4.

[39] Fine, B.H. and Kobrick, J.L. Effect of Heat and Chemical Protective Clothing on Cognitive Performance. US Army Research Institute of Environmental Medicine, Report M4/86, November 1985.

[40] Personal Protective Equipment (PPE). Chemical Hazards Emergency Medical Management, National Institute of Health. U.S. Department of Health and Human Services. url: https://chemm.nlm.nih.gov/ppe.htm.

practices will be reviewed. The facility's reevaluation of the PPE for line breaks will then be discussed.

4.1 Ethylene Oxide — Hazard Overview

Ethylene oxide (EtO) presents multiple types of hazards to workers, equipment, and the environment. EtO has a wide flammability range, forming flammable mixtures in air from 2.6%–100%.[41] Aqueous solutions of >4 wt.% EtO are flammable with flashpoints reported between -2℃ to -57℃. In addition to its flammability, EtO is also extremely reactive and can react with other materials exothermically or decompose explosively in air or inert atmospheres. It also poses carcinogenic, reproductive, mutagenic, and neurotoxic hazards through inhalation, eye, or skin contact. Extended skin exposure from continuing to wear contaminated clothing can cause blistering, frostbite, and chemical burns. It is also toxic to microorganisms and marine life in the environment. It is typically stored as a liquid under pressure, with a boiling point of 10.8℃ at atmospheric pressure. As a result, leaks and releases may include both liquid and vapor depending on the ambient conditions.

4.2 Line Break Overview: Temporary Piping Installation

At the facility, EtO was supplied to process equipment via a pressurized (200 psig), insulated, 24-inch diameter header. The header ran along a pipe rack that was elevated approximately 20 feet off the ground in an area outside of the manufacturing building as shown in Figure 1. As part of a scheduled shutdown, the EtO header was scheduled to be drained and purged so a temporary blind could be installed to isolate the EtO source from the process unit during maintenance. The EtO header was de-inventoried and depressurized to 50 psig. The next step of the job involved installation of temporary drain piping on a 2-inch diameter drain line on the header as shown in Figure 2. The temporary drain piping would be routed to a closed head drum on the ground so the remaining heel of EtO vapor and liquid in the header could be back flushed with inert gas.

---

[41] S. Rebsdat and D. Mayer, Ethylene Oxide, Ullmann's Encyclopedia of Industrial Chemistry, 2012.

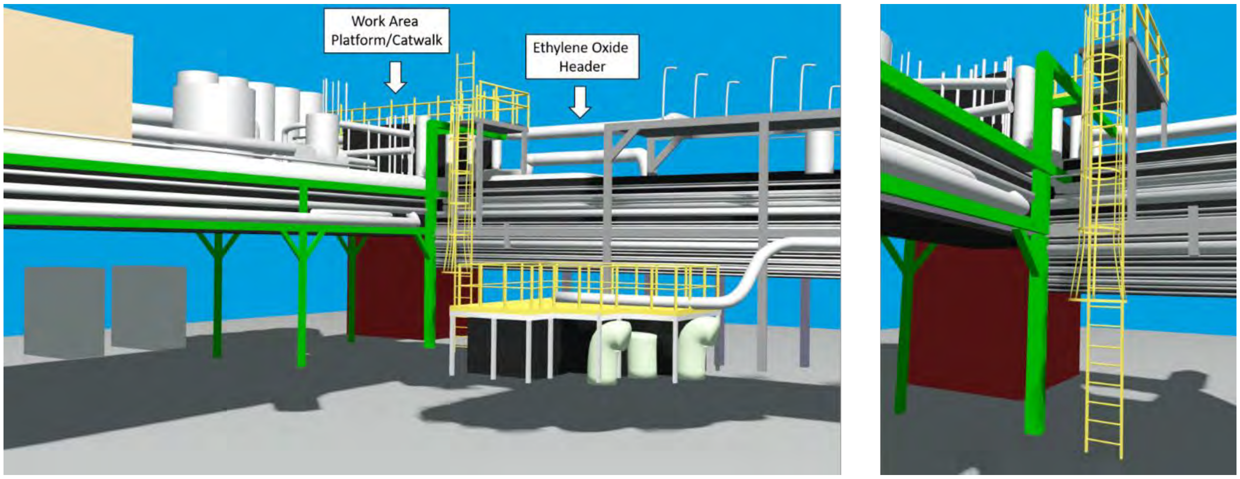


Figure 1. *Ground view of the elevated work area (left) where the platform and catwalk were located to access the drain line on the Ethylene Oxide Header. Close-up view of the ladder and cage (right) to access the elevated platform.*

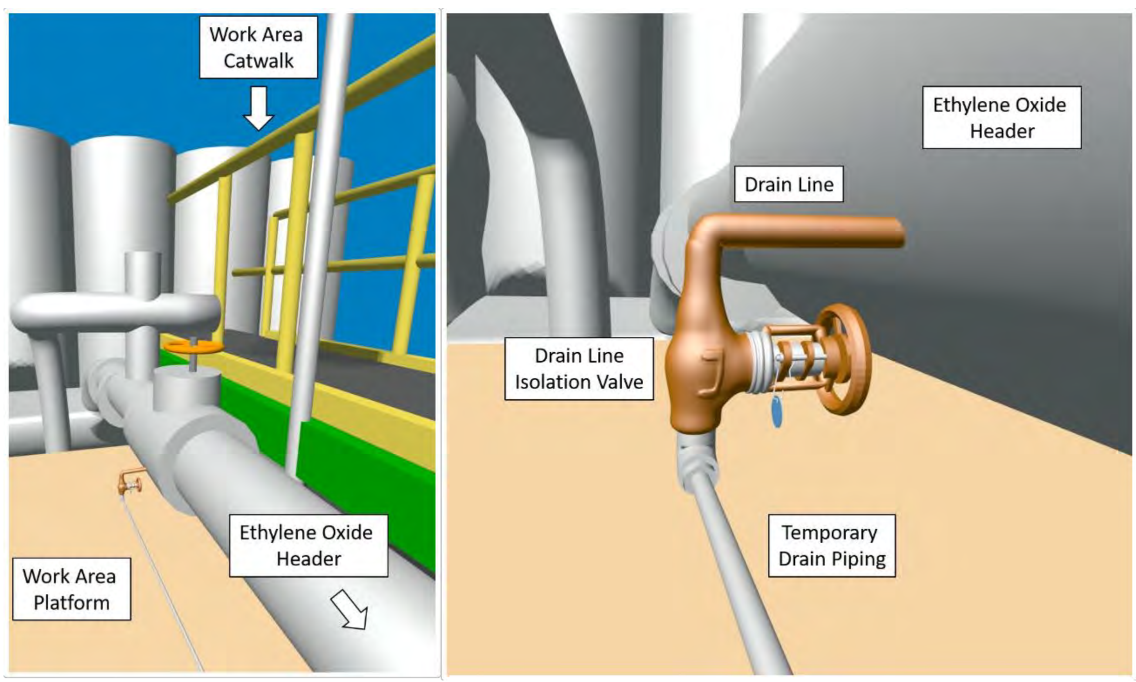


Figure 2. *View of the work area from the elevated catwalk (left) with a close-up view of the isolation valve and temporary piping that was to be installed (right). Prior to installation of the temporary drain line piping, the isolation valve had a removable plug screwed into the discharge end.*

Installation of the temporary drain piping required that a plug be removed from the discharge of an isolation valve on the header's 2-inch drain line, immediately followed by installation of the temporary piping. The facility considered the removal of the plug on the discharge of the valve a line break because there could be a small amount of pressurized EtO liquid or vapor between the drain isolation valve body and the plug. Pre-job planning paperwork with maintenance, engineering and operations staff was completed including a safe work permit, a LOTO form, a job hazard analysis, and a pre-job walk through.

The facility line break procedure specified several layers of PPE to protect workers from both vapor and liquid EtO. The Line Break Procedure at the facility specified PPE including a full body chemical suit with booties/socks, air supplied respirator, boots, butyl gloves, and a personal grounding strap. The specified full body chemical suit and gloves were made of materials that listed permeation breakthrough times of 480 minutes for vapor EtO, and 15 minutes for liquid EtO. The model of chemical suit provided to workers also included a tight-fitting respirator hood. The facility viewed this level of PPE appropriate for line breaks and had determined that fully-encapsulating suits (such as those worn by emergency responders in Level A PPE) were unnecessary based on a job hazard analysis performed prior to the incident.

4.3 Incident Overview

Two technicians from a maintenance contractor were assigned to the work order for the temporary piping installation. Since the facility did not perform line breaks often, the maintenance contractor viewed the installation of the temporary piping as an opportunity to train and qualify a newly hired maintenance technician on the procedure for performing a line break in EtO service. The newly hired technician was to learn the procedure by shadowing the job with his supervisor. As previously discussed, the pre-job planning paperwork was completed, and the job was staged. Non-sparking tools, two supplied air hoses and full-face respirators, and a 1.5-inch water hose were placed on the elevated platform near the ladder and catwalk approximately 10 feet from the work area. The two maintenance technicians donned their chemical suits, gloves, and grounding straps in the nearby locker room. Both technicians placed their chemical suit's attached booties/socks over their steel toed work boots, and then walked through the gravel parking lot to the ladder to ascend to the elevated catwalk and platform.

The plan was for each technician to don their respirator on the catwalk and then cross check that their coworker had properly donned their PPE. One technician would then provide a fire-watch with the water hose, while the other technician verified the drain isolation valve was closed and affixed his personal lock to the valve. This would complete the LOTO procedure (with the verification and personal lock of the person performing the line break completing the LOTO process). After completing LOTO, the technician would then remove the plug (break the line) and install the temporary drain piping. As shown in Figure 1, staff at ground level had an obstructed view of the work area. The technicians could be seen on the catwalk, but the work platform, drain line, isolation valve, or the technicians as they performed the line break were not visible.

The inexperienced technician climbed the ladder first and donned his respirator. His supervisor followed next and was in the process of donning his respirator on the catwalk when he heard a pressurized release. He turned and saw the inexperienced technician laying on his back near the drain line and a small blue flame under the platform. The supervisor used the water hose to extinguish the fire while the inexperienced technician stopped the release. Both technicians then removed their respirators, partially doffed their PPE (i.e. removed their butyl gloves and unzipped their chemical suits) and climbed down the ladder.

At ground level, operations and engineering staff could not see what happened, but saw the small blue flame. The inexperienced technician stated that he had mistakenly opened the isolation valve before removing the plug. Once he realized his mistake, he closed the isolation valve stopping the release. Both technicians confirmed there was not an active release, and that the fire had been extinguished. When asked by staff on the ground if EtO had contacted their PPE, both maintenance technicians from the platform said no. Staff on the ground reiterated that EtO, particularly in liquid form, can permeate chemical suits, and both technicians confirmed that EtO had not contacted their PPE. Staff then asked if the maintenance technicians could perform a field survey for EtO to confirm the leak was isolated while estimations were made regarding the amount of EtO that had been released. The field survey was conducted by the inexperienced technician, who rezipped the chemical suit he was wearing, and then put on his standard work gloves. The survey confirmed there was no EtO in the area. Staff on the ground estimated that the amount of EtO released was less than a gallon (a few pounds).

The inexperienced technician walked back toward the breakroom where he took off his work gloves, then removed his chemical suit and boots, before disposing of his chemical suit in a bin for used PPE. Over the course of the next 4 hours, he began to complain of a burning sensation on his hands, legs, and feet. He eventually admitted to emergency staff that EtO liquid and vapor had contacted his respirator face shield, gloves and suit during the line break. He was taken to the hospital and treated for chemical burns.

4.4 Root Cause Analysis

Following the injury, the facility conducted a root cause analysis of the exposure. During the investigation it was noted that several safe work practices had been violated during the line break:

- LOTO – The isolation valve on the EtO drain line was not closed and locked out prior to removing the plug. This exposed the technician to a larger potential volume of EtO than anticipated during the line break.
- Line of Fire – The technician was positioned underneath the valve, directly in the line of fire, as he removed the plug. When EtO was released, liquid and vapor contacted the technician's respirator face shield and chemical suit. The technician then wiped his face shield and suit with his gloves.
- Incident Reporting – The technician who was exposed to EtO failed to report his exposure to his supervisor or other staff at ground level. As a result, he was not properly decontaminated after his exposure.
- PPE Donning and Doffing – Both technicians did not properly don or doff their PPE while performing the work. The instructions, warnings, and labels on the chemical suit clearly indicated that the attached boots were not intended as boot covers and could tear if worn improperly over work boots. Both technicians also removed their gloves prior to removing other pieces of PPE, potentially resulting in cross contamination through their hands. The inexperienced technician also continued to use/reuse his PPE after it had been

contaminated with EtO, extending the potential exposure time and breakthrough risk. He also used his work gloves instead of a new set of butyl gloves while performing the field survey after the release.

Based on the information above, it was determined that the root cause of the injury was the failure to perform necessary safe work practices during the line break. This resulted in a worker being exposed to a larger amount of EtO than the amount anticipated when the PPE was specified. It was concluded that the injury occurred due to either improper PPE donning/doffing, or extended contact from lack of decontamination and removal of contaminated PPE.

4.5 Reevaluation of PPE for Line Breaks

The facility recognized additional layers of PPE (such as a fully encapsulating suit) could have provided a higher level of protection during the line break. However, there was concern associated with heat stress and more specifically the ability of the workers to access the platform, or egress in the event of an emergency if wearing a fully encapsulating suit. The site also questioned whether it was inappropriate to wear the chemical fabric over the FRC clothing. However, the site ultimately concluded that there was not a significant flammability hazard because safe work practices (LOTO) limited the amount of flammable material that could be released, the location was well ventilated because it was elevated and outdoors. Therefore, the site viewed the additional protection potentially provided by fully encapsulating suits as being marginal compared to the hazards presented by decreased accessibility and mobility of the workers at the job site.

The facility realized that safe work practices were a critical component of hazard mitigation during the line break. LOTO would have limited the amount of EtO release to a few drops (if any) because it would have isolated the worker from the source of hazardous energy. If a small amount of EtO was released when the plug was removed, employees had a very small risk of exposure if they remained out of the line of fire, since EtO liquid would rapidly vaporize and dissipate in the work area. It was also determined that the amount of liquid that could be trapped between the valve body and plug would not be sufficient to form a flammable mixture that would envelop the worker. If EtO contacted the gloves or suit of the worker, the fabrics were rated for 480-minute and 15-minute breakthrough times for vapor and liquid EtO, respectively. This provided ample time for employees to receive decontamination and remove the contaminated PPE. The facility also recognized that higher levels of PPE would still be ineffective if workers did not properly wear, use, or remove the equipment during work.

The facility also consulted industry regulations, literature, and references related to proper PPE and specific requirements for EtO service. These references stressed that PPE should not be relied upon to provide complete protection from hazards and instead should be used in conjunction with other safeguards such as engineering controls and administrative controls (e.g. safe work practices). As a result, the facility determined the PPE had been appropriately specified for the job and would not be changed. Instead, the facility focused on training workers on the importance of safe work practices and PPE donning/doffing/decontamination procedures for EtO service.

5 Conclusions

PPE, though often viewed as the least effective safeguard, can also be the last line of protection between workers and the hazards they encounter in chemical processing facilities. In this paper, several aspects of PPE specification, and the trade-offs of various forms of PPE were presented. The key conclusions were:

- PPE specification begins with hazard identification and risk assessment. The assessment should include a review of the materials/chemicals, the job tasks that will be performed in the PPE, and details of the performance of the PPE fabrics and materials. This helps a facility document the assumptions and decisions that were made in specifying the PPE for their employees.
- Training is a critical component of a robust PPE program. Workers need to recognize the hazards they encounter and the benefits/limitations of the PPE they wear. They must also understand how to properly don, doff, and decontaminate their PPE if it becomes contaminated.
- PPE specification can be very complex and complicated. Sometime, PPE intended for one hazard will be ineffective to another hazard encountered at a work facility. Multi-layer ensembles must be carefully evaluated to ensure that each layer is being used properly.
- Over-specification of PPE can negatively impact workers in various ways. Heat stress, decreased mobility and vision, and the psychological impacts of PPE were discussed in detail. Ultimately, it is important that the PPE specified is both adequate for protection, and practical for implementation.
- It is important to read and understand the documentation provided by the manufacture of the PPE. Their instructions and warnings often contain important information regarding the proper use of PPE. If questions arise, many manufacturers include contact information and will provide input based on their expertise.
- PPE is often a safeguard that is used in combination with other engineering and administrative controls, such as safe work practices. If other safeguards, such as a LOTO procedure, are compromised, then workers may be at a higher risk of injury due to exposure to larger quantities of chemicals or flammables. Facilities may benefit from stressing the importance of safe work practices in the context of the PPE specified for a hazardous task.

All work places, including chemical processing facilities, contain some inherent level of injury risk. PPE is one aspect of a safety program that can protect workers from harm, but it is important to critically evaluate PPE specified for a job in the context of the task and hazards. Facilities should not blindly increase PPE requirements without evaluating the hazard that PPE can pose to the worker. Facilities should also seriously consider whether engineering and administrative controls (in combination with PPE) would be more reliable or effective at protecting the worker.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Behaviour-Based Safety

Dr. Ramesh V.M.
BPCL-Kochi Refinery
*Presenter Email: rameshvm@bharatpetroleum.in

Abstract

As advocates of safety at workplace, our primary goal is to statistically assign the number "Zero" against the variable "Number of Accidents" every single day. Towards this, one is obviously prompted to identify the causes behind an accident. "Accidents" are deadly and we have heard stories of several disastrous accidents.

Once upon a time, accidents were attributed to fate which is beyond our control. As decades passed by; we tried to identify the "accident-prone" worker(s) who was given the label "the harbinger of misfortune". Soon, we learnt to find flaws with the system design and the infrastructure associated with our workplace. Later, we observed that a flawed man-environment interaction can be disastrous. Since early 1980's, Behaviour-Based Safety slowly emerged as an approach that sees unsafe behaviour as the main cause of accidents.

BBS calls for fine-tuning our behaviour to bring about a revolution in our safety culture to ensure that "our behaviour is safe even when no one is watching". The present talk will provide a fresh perspective to the concept of BBS from an industrial framework and beyond. This magnifying lens seeks to add more depth and clarity to BBS in our lives.

The observation of BBS Walk can be utilised in Safety training. The BBS will bring down the Near Miss reporting pattern.

Keywords: Behaviour-based Safety, Safety Culture, Value-based Safety

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Effective Remedies for Enhancing Safe Operations Through Analysis of Organizational Safety Climate

[b]Shawn Bayouth, [a]Matthew E. Harvey, and [a*]Nir Keren
[a]Department of Agricultural and Biosystems Engineering, Iowa State University
Department of Agricultural and Biosystems Engineering
Iowa State University, 1620 Howe Hall
Ames, Iowa 50011, USA
[b]Department of Disaster Preparedness and Emergency Management, Arkansas State University
*Presenter E-Mail: nir@iastate.edu

Abstract

While multiple definitions are suggested for organizational safety climate, the theme that goes through all these definitions is that safety climate is the shared perception employees have with regard to the priority safety has as an organizational operational goal. While tremendous efforts are devoted to the study of organizational safety climate, not often do these efforts identify effective measures that can be facilitated in order to address low-level and weak organizational safety climates.

The proposed paper will review fundamental factors of organizational safety climate for the manufacturing industry, the mechanisms by which these factors affect employee engagement (or lack thereof) in safe practices, and various measures that organizations can pursue in order to mitigate low-level safety climates.

Keywords: Safety, climate

Background

Organizations devote significant resources toward developing policies and procedures, hiring employees with appropriate training and experience, and investing in equipment for their operation. These three elements are facilitating the formal management system. For decades it was believed that it is almost impossible to fail when an appropriate formal management system is present. However, many organizations have faced a reality check with their operations, although their formal systems were robust. The magnitude of influence of the informal management system – the Organizational Climate – on the organization's ability to maintain appropriate operations and production became obvious in the late 80's. Despite this awareness and its importance, this area is still often ignored.

Framework

The inception of Safety climate as an academic and practical framework started early in the 1980s (Zohar, 1980).

Despite almost four decades of research, some aspects of safety climate are ambiguous (Beus et al. 2019) and, at times even controversial. Studies on safety climate assessment methodologies are yet to demonstrate predictive power of the relationship between safety climate and safety behaviors. The lack of cohesive framework where predictive relationship between safety climate and safety behaviors exist and is robust, may be one significant cause for hindering adoption of safety climate as a managerial tool among practitioners.

Keren and colleagues (2009) conducted decision making simulations in a manufacturing facility, and their results demonstrated that level of safety climate predicted selection of safer choices. Further, their results indicated that the likelihood of selecting safest line of action was highest in employees with perception of "very high" level of climate.

Zohar and Erev (2007) presented three cognitive biases from which employee unsafe behaviors may stem:

(1) Underweighting delayed outcomes (melioration)

(2) Underweighting low likelihood outcomes (recency bias)

(3) Underweighting social externalities (free ride)

Put in simple language, these biases can be describes as follows:

(1) The melioration bias suggests that the benefits of engaging in unsafe behavior in the short term outweighs the perception of negative outcome of these unsafe behaviors, if these outcomes will occur much later in life.
(2) The recency bias is a cognitive error that creates the perception that current consequence (or lack thereof) of engaging in unsafe behavior, will continue to occur in the future.
(3) Free riders represent workers that benefit from good outcomes without contributing their fair share for the occurrence of the good outcomes.

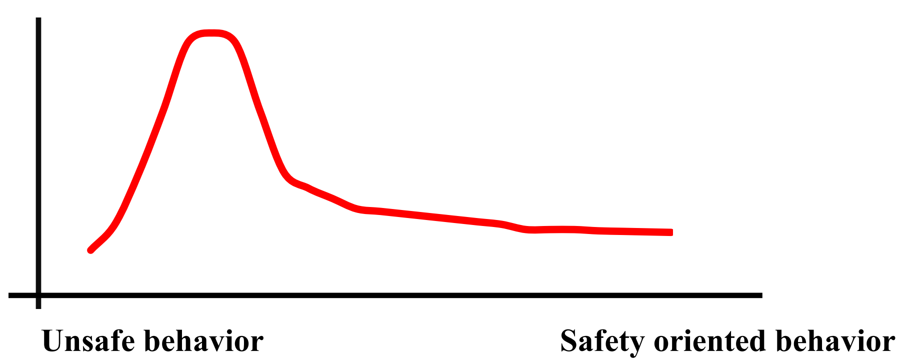


Figure 1. Personal Value Function for safety behavior continuum.

As figure 1 portrays, these biases yield a personal value distribution function where unsafe behavior is of higher value.

When projecting the implications of these biases on a safety climate framework, it is possible to identify practices that will increase engagement in safe practices in the workplace.

Remedies
Strategy for implementing effective safety leadership

The discussion above identified a variety of factors that require attention when strategizing an approach for increasing the safety climate level in a facility. The most critical factors, which will have a significant impact on employee behaviors, reflect management's commitment to safety. One approach recently proved effective includes three components (see figure 2):

- Enhancing visibility of top management safety leadership
- Implement supervisory-based safety program
- Implement supervisory accountability program. This component is the 'glue' that couple top management commitment with supervisory–based system to an overall system which enhances performance.

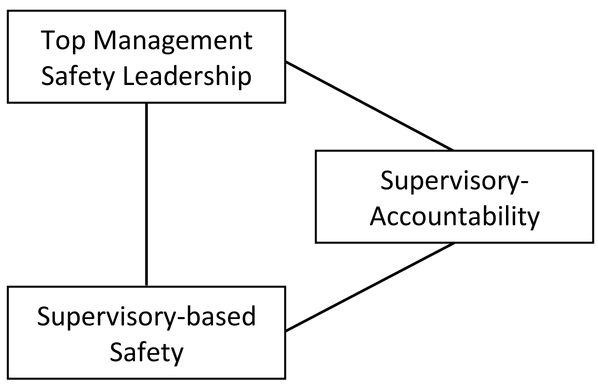


Figure 2. Model for effective implementation of management commitment program.

Enhancing top management visibility and interactivity

Effective occupational hazard protection and prevention requires top management commitment; for safety climate purposes, this commitment must be visible.

The following list consists of items that can increase safety leadership visibility. It is recommended that these items be led by a highly ranked manager in the facility:

- Coordinate a regular (weekly is suggested) safety tour with each one of the supervisors in her/his area.
    - This tour should be dedicated to safety and health operations.

    - The tours will allow supervisors to share their safety concerns, barriers to safety, and constraints to achieving safety goals, along with their strategies to address these concerns.
    - Provide front-line employees with opportunities to discuss their concerns with you during these tours. If necessary, afford the opportunity speak about concerns in private to better facilitate openness, but it is important to conduct these and other efforts with all shifts.
- Conducting unannounced inspections/walk arounds; becoming particularly aware of shortcuts in safe work procedures.
- Establishing a “partnership” program between managers and supervisors that encourages employees to speak out when they witness unsafe conditions.
- Establishing and **chairing** a Central Safety and Health Committee. Announce safety goals and a follow-up routinely to measure outcomes. Monthly meetings are an appropriate frequency for this function.

Implement Supervisory-based Safety (SBS) Program

Zohar (2002) and Zohar and Luria (2003) developed intervention titled, Supervisory-Based Safety (SBS), that aimed at improving supervisory safety practices as leverage for modifying employees’ safety behaviors. They used integrated feedback and a goal-setting protocol for increasing supervisory practice; they also collected individual feedback concerning the frequency of their safety-oriented interactions with subordinates. Their results indicated a steady, synchronized increase in frequency of both supervisory safety interactions and workers’ safety behavior during intervention. Furthermore, improvement continued during the follow-up months (i.e. after the end of intervention) until it reached a plateau, without apparent signs of extinction.

It is recommended to adopt and implement this approach. Since the intervention is only in the supervisory level, changes in workers’ behavior are attributable to a modified values function for safety behavior that stems from frequent and timely supervisory referrals.

As the new supervisory safety practices will become the norm, the three biases from which unsafe practices-oriented behavior stem are counteracted.

Significant elements of SBS can be pursued and accomplished by the enhancement of visibility of safety leadership above, and by implementing supervisory accountability program below. Formalizing the process by which supervisors provide reinforcement contingencies, specify performance goals, and provide frequent and timely feedback (positive and negative) concerning goal attainment are the fundamentals to the expected interaction in SBS.

Implementing Supervisory Accountability Program

Organizations set policies and operating procedures that guide operations through many operational scenarios. Thus, there is a margin for supervisors to be either safety oriented or not safety oriented. Often, due to the cognitive biases described above, supervisors are less likely to be safety oriented.

A supervisory accountability program holds supervisors accountable for their safety and health responsibilities by counterbalancing the recency and free ride biases. Wise implementation of a supervisory accountability program will result in supervisors that are likely to develop solutions for safety concerns, rather than become barriers to safety resolutions. Accountability encourages positive involvement! Implementing the suggestions below can establish appropriate accountability programs:

A top manager conducts bi-weekly safety overview meetings with each one of the supervisors. These meetings should be dedicated to reviewing safety performance **only**, beginning with the supervisor reporting safety status in her/his area.

- Set (in writing) measurable, achievable goals for the next month. For example:
  - Reduce injuries requiring first aid by 20%
  - Conduct a weekly safety awareness meeting for employees in their area
  - Conduct weekly hazard inspections and eliminate these hazards
  - Conduct at least one job safety analysis between two consecutive meetings with top management and devise solutions for the results of the analysis.
- Follow up on accomplishments from the previous month in each meeting. For objectives not accomplished, ask the supervisor for a written plan for accomplishing these objectives by the time of your next review meeting.
- Strongly (**!!**) emphasize safety performance in supervisors' performance evaluation and promotion.

Incorporating safety performance in periodic evaluations and promotion considerations

- Incorporating safety performance into employee evaluations and emphasizing safety performance when considering employee promotion will enhance the perception of safety as a dominant factor in the organization. This measure will target the damaging impact of the Recency and the Melioration biases
- It is important that the implementation of these changes be widely communicated in meetings and through presentation of the new/modified employee evaluation forms, on message boards, and through emails if feasible.

Implementing employee safety appraisal program

Establishing a reward program where safety efforts are recognized, and exceptional efforts are rewarded will support the notion that safety matters. The program should establish opportunities for employees to get engaged in safety efforts.

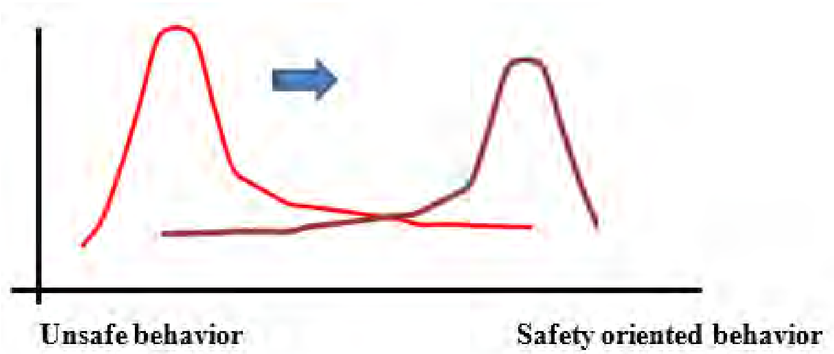
Implement communication enhancement program

Installing a message board in a common area that is dedicated for communicating safety items is effective. Presenting current safety status (e.g., quarterly OSHA recordable analysis of a specific safety incident(s) and the resolution), goals and expectations for safety for the next quarter, and announcement of launching new safety initiatives. It is important to emphasize the positives at least as much as the negatives – a facility of 1,000 employees that experienced an injury, also experienced 999 employees that have not been injured.

- One common 'trap' in attempts to enhance communication is the use of technology. Installation of large TV screens/monitors that continuously present these types of communication may result in resentment toward the use of technology. Responses such as "this is what they spend the money on…" are quite common in response to the use of these modes of communication. Communication that is perceived personal will serve best. Communicate the safety climate enhancement as a safety initiative
- Participating in safety committees and leading safety improvement efforts are good examples of items to recognize.
- Safety efforts information should be periodically collected, with token-level awards (a mug, T-shirt, certificate, and similar) s presented to the winner(s).
- Introducing higher level recognition acts, such as going to dinner with the owner/Plant Manager (once a year), can further strengthen the sense that safety efforts are recognized and awarded. Employees tend to highly regard this gesture.
- Another motivating factor would be announcing safety employees of the month. Rewarding multiple (three would be a good number) employees monthly enhances the 'sense of likelihood of getting awarded', and thus counter effects the bias associated with rareness of feedback.

Items in this category will mainly counterbalance the effects of Recency bias.

Implementing programs based on screening for challenges through safety climate assessment and identifying solutions based on their effects on the three cognitive biases may transform the personal value distribution function from an encouraging 'unsafe behaviors' to supporting 'Safety Oriented Behaviors' (see Figure 3).



References

Beus, J. M., Payne, S. C., Winfred, A., & Munos, G.(2019). The development and validation of a cross-industry safety climate measure: resolving conceptual and operational issues, *Journal of Management*, 45(5), 1987-2013.

Keren**, N**., Mills, T. R., Freeman, S. A., & Shelley, M. C. (2009). Can level of safety climate predict level of orientation toward safety in a decision-making task? *Safety Science* 47(10): 1312-1323.

Zohar, D., 1980. Safety climate in industrial organizations: theoretical and applied implications. Journal of Applied Psychology, 65 (1), 96–102.

Zohar, D. (2002). Modifying supervisory practices to improve subunit safety: A leadership-based intervention model, *Journal of Applied Psychology*, 87(1), 156-163.

Zohar, D., & Luria, G. (2003). The use of supervisory practices as leverage to improve safety behavior: a cross-level intervention model, Journal of Safety Research, 34(5), 567-577.

Zohar, D., Erev, I., 2007. On the difficulty of promoting workers' safety behavior: overcoming the underweighting of routine risks. International Journal of Risk Assessment and Management, 7 (2), 122-136.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Engaging Your Safety Culture Appreciatively

Dana Cooper*
Cooper Hayes LLC
Stevensville, MI
*Presenter E-mail: dana@cooperhayesllc.com

Abstract

Engaging your Safety Culture Appreciatively. We will demonstrate the use of Appreciative Inquiry tools in addition to methods for enhancing your social media and crisis management plans. Plans that are integrated through all areas of your business are key to the success. This is an invitation for individuals to co-create a safety culture in which they want to live. An exceedingly comprehensive approach to generate learnings that translate those learnings into practical innovations.

We will review the value of top management involvement and visibility. Senior managers focus on EHS in enterprise goals, materiality metrics, treasure hunts, and operations reviews. Many companies have developed a method for monitoring through the formation of an Advisory Council to listen and understand the activities of Voluntary Teams. We will ask, "How many companies have a Social Media Plan in your Crisis Management Program"? Doing the right thing is essential. The presentation will provide tools and activities to take back to facilities for enhancing and developing opportunities.

Keywords: Safety Culture, Social Media, Appreciative Inquiry, Employee Engagement, Crisis Management, Advisory Council

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Crude Oil by Rail Accidents: Cross-industry Learning for High Hazard Sectors

Gabor Posta*
Arup
London, United Kingdom
*Presenter E-mail: postagabor@gmail.com

Abstract

A sharp increase in fracking in 2008 sent crude oil production in North America soaring, leading to production quickly outgrowing existing pipeline capacity and record volumes of crude oil being hauled by rail. The high-profile crude oil train disaster at Lac-Mégantic (Canada) in 2013 was an unfortunate reminder of the dangers associated with this method of transportation and led to a permanent change in public perception alongside a re-examination of the regulatory approach. At the same time, opposition to pipeline projects such as Keystone XL meant that there remained a heavy reliance on the transportation of crude oil via rail, and there was significant resistance from rail operators towards retrofitting safety features and upgrading their rolling stock.

Six years on from the accident at Lac-Mégantic, have the right lessons been learned and applied? This paper discusses the challenges behind the transportation of crude oil by rail, identifying and examining some of the universal learning opportunities for both established and emerging high hazard sectors.

Keywords: learning from accidents, ALARP, high hazard, knowledge sharing

1. INTRODUCTION

Crude oil transportation via rail came into the public spotlight in 2013 when a freight train hauling over 70 tank cars of crude oil derailed in the Canadian town of Lac-Mégantic after an unattended brake failure resulted in the train rolling downhill from its parking spot. The significant death toll and spectacular nature of the accident (involving large fires and explosions immediately after the derailment) received widespread global media coverage. This paper discusses the challenges behind the transportation of crude oil by rail, identifying and examining some of the universal learning opportunities for both established and emerging high hazard sectors.

2. BACKGROUND

In the early 2000s, advancements in drilling technology combined with the use of hydraulic fracturing resulted in an increase in oil production from unconventional assets across the world, particularly in North America (Canada and the American states of Texas and North Dakota).

Oil extraction from the Bakken shale formation in North Dakota via hydraulic fracturing led to the North Dakota oil boom, resulting in record amounts of crude oil being produced. The oil underwent onward transportation to refineries and this was initially largely achieved through pipelines. However, production outstripped pipeline capacity by approximately 2010 [1], and combined with the economics of Bakken shale crude (where the high quality resulted in selling of the oil to east coast refineries for an increased profit margin) [2] resulted in an increased reliance on crude oil transportation via rail.

Whilst crude oil transportation via rail was not a new approach for the shipping of crude oil at the time, the increase over the space of less than a decade was that of almost two orders of magnitude in some cases. Association of American Railroads data [3][4] show that approximately 9,500 rail tank cars of crude oil were shipped in the USA in 2008, increasing sharply to a peak of approximately 493,000 rail tank cars in 2014. A graphical summary of this data for 2009-2018 can be seen in Figure 1 for US Class 1 railroads i.e. major railroads with annual carrier operating revenues of approximately $447 million or more [5], representing approximately 70% of the total track miles in the US [6].

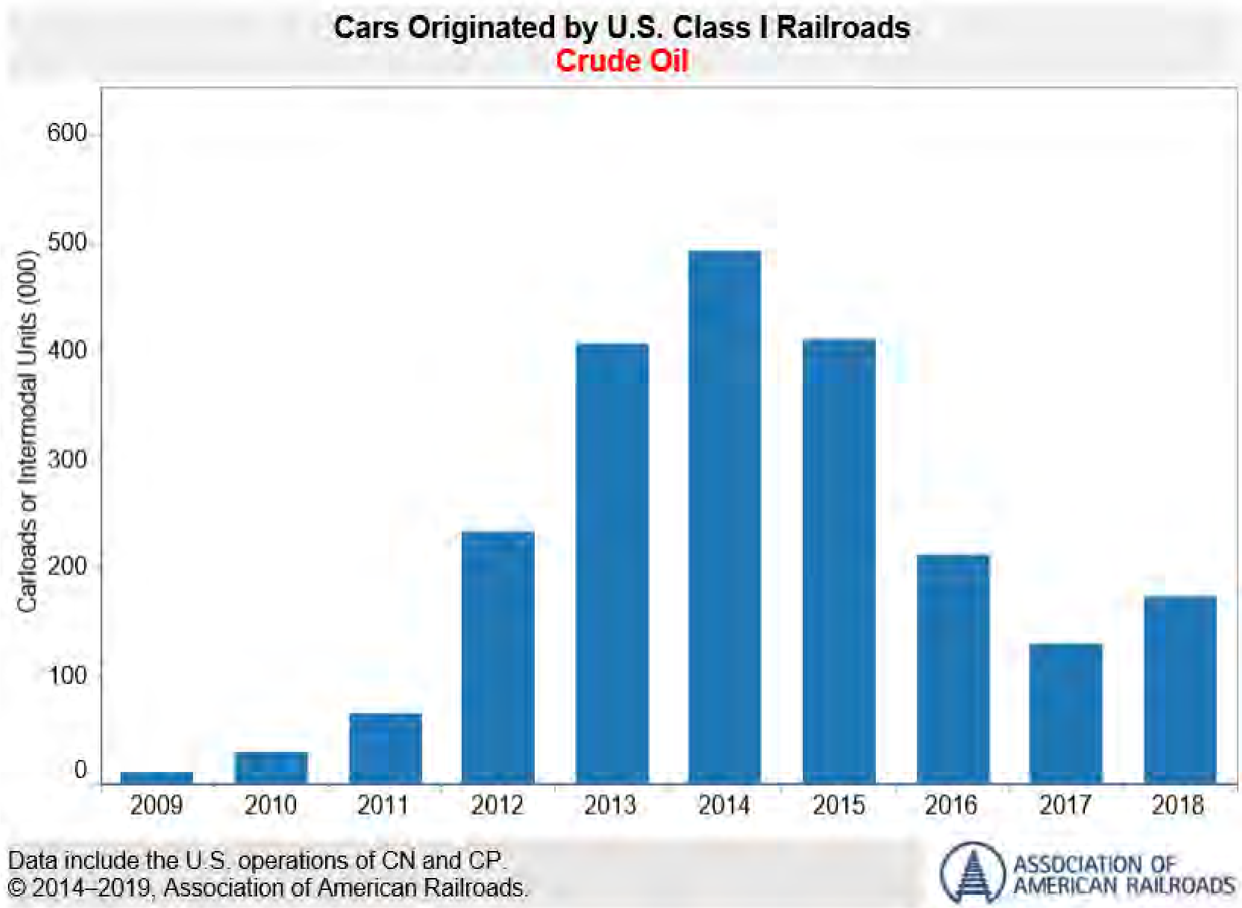


Figure 1. Rail tank cars of crude oil hauled from US Class 1 railroads [3]

Similar data are available for Canadian railways in a raw format from the Canada Energy Regulator [7], although the basis for the data is volume of crude oil exported from Canada via railway rather than volume of crude oil originating in Canadian Class 1 railways. Using a volume of 113,970 litres per tank car as a basis for this analysis (i.e. assuming that all tank cars are of DOT111A100W1 specification, a common rail tank car design), the available data summarised in Figure 2 shows a similar trend to the US data for years 2012 to 2016. A slight deviation between the trends in the two datasets can be seen, where the amount of crude oil transported in Canada experienced an earlier resurgence in 2017 and 2018 compared to that in the US dataset, largely related to the differential in price between West Texas Intermediate (WTI) and Western Canadian Select (WCS) crude oils, which determined the profitability of transporting WCS from Canada to the US.

Raw data are not freely available from the Association of American Railroads and as such a more direct comparison cannot be made in this paper. However, the general trends and numbers allow a useful comparison to be made regardless, demonstrating that similar sharp surges in crude oil transportation volumes were experienced in both countries in the 2010s, noting that the aim of this paper is not to investigate and explain the underlying drivers for the fluctuation of crude oil transportation via rail, other than to provide sufficient context for the reader regarding the origin of these crude oil by rail accidents.

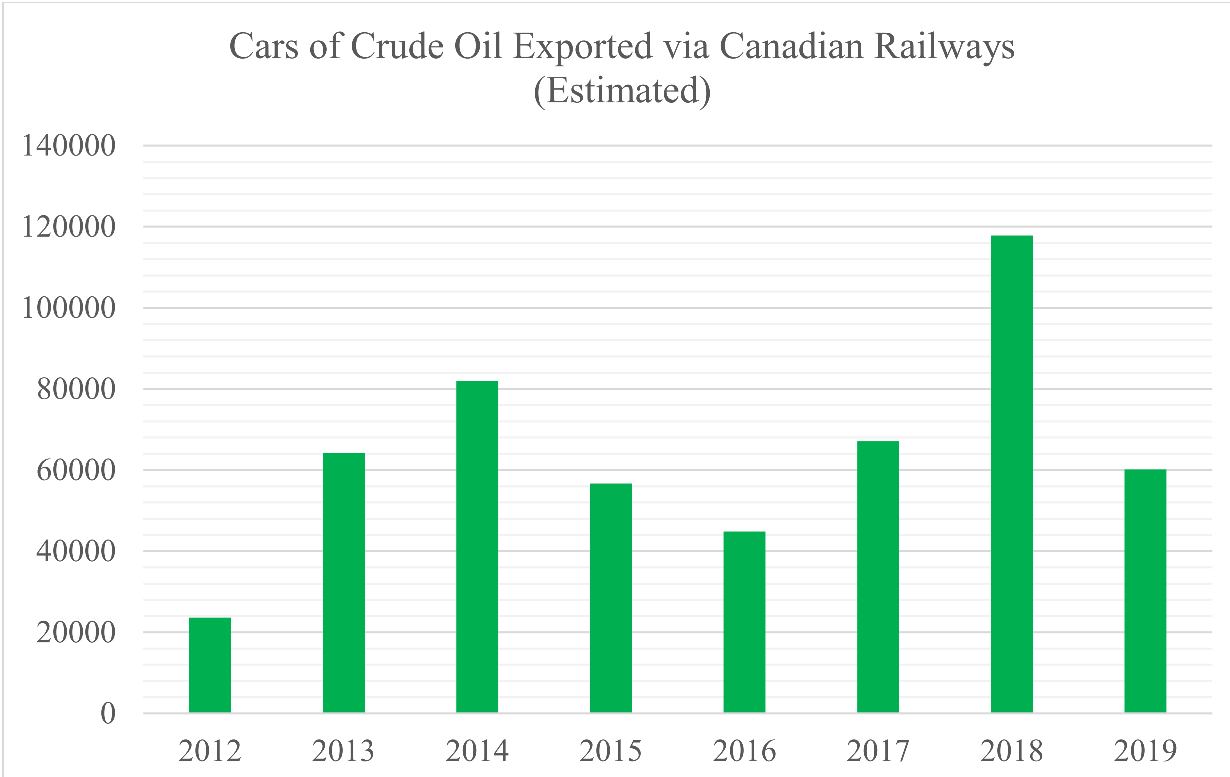


Figure 2. Estimated rail tank cars of crude oil exported from Canada

3. LAC-MÉGANTIC ACCIDENT

Montreal, Maine & Atlantic Railway freight train MMA-002 was used to transport 72 tank cars of petroleum crude oil originating from oil wells in the Bakken formation ("Bakken crude") between Farnham (Quebec, Canada) and Saint John (New Brunswick, Canada). On the 5th July 2013, the train stopped on a slight gradient at Nantes (Quebec, Canada) where a new crew was to continue its journey eastward in the morning after addressing some mechanical issues that were being experienced over the preceding days.

In the early hours of 6th of July 2013, a small locomotive fire on MMA-002 resulted in fire and rescue services attending the scene, extinguishing the fire, and securing the locomotive. Shortly thereafter, the unattended MMA-002 train began to roll down the slight gradient due to gradual brake failure, culminating in the derailment of 63 tank cars containing crude oil in the town of Lac-Mégantic some 10 kilometres downhill from the initial parking position.

The resulting fires and explosions resulted in the death of 47 people, the destruction of a large section of the downtown area (shown in Figure 3 and Figure 4), and environmental contamination of the nearby land and lake water due to the spill of crude oil.

Figure 3. Fire following the train derailment in the city centre [8]

Figure 4. Lac-Mégantic town centre post-accident, showing widespread damage [9]

4. REGULATORY AFTERMATH AND ACCIDENT TREND

There was widespread criticism of crude oil transportation via rail in the years following the Lac-Mégantic accident, focusing on topics such as freight train routing through heavily built-up areas, the high volatility of Bakken crude, and the low design standards for rail cars.

A common rail tank car type used in North America is the Department of Transport (DOT) Class 111 (DOT-111) model, a basic and out-dated design of which approximately 98,000 cars were still used to transport flammable liquids in 2013. Key vulnerabilities are highlighted in Figure 5:

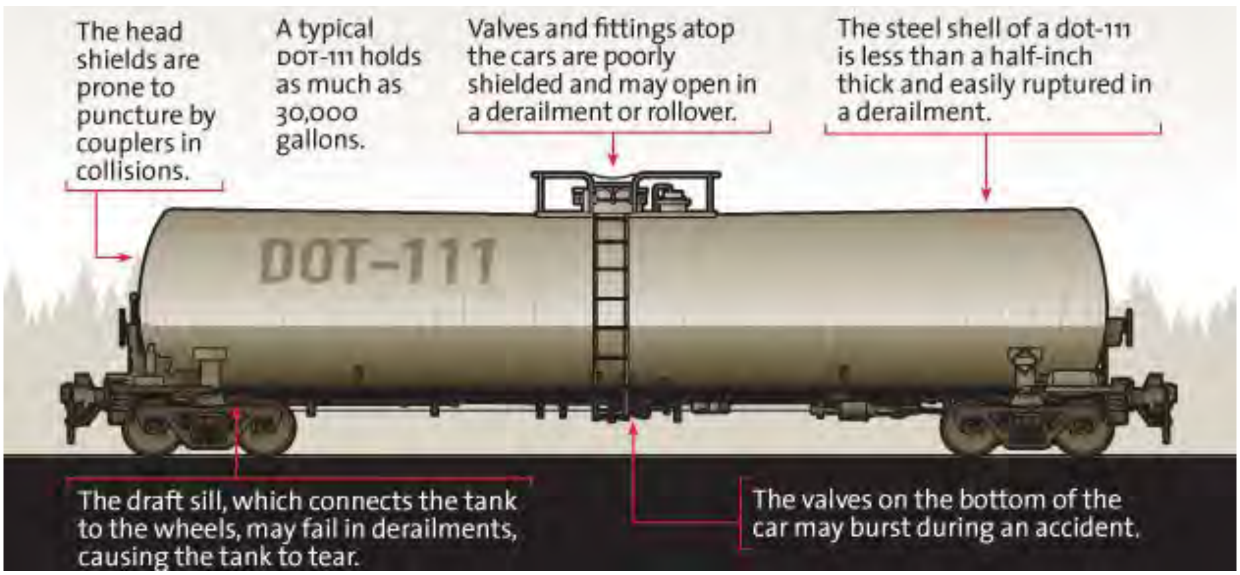


Figure 5. DOT Class 111 rail tank car design issues. [10]

Criticism of the DOT-111 cars was widespread even before 2013, with a US National Transportation Safety Board (NTSB) accident report on the 2009 Cherry Valley (Illinois, USA) crude oil train accident already stating that *"[...] if enhanced tank head and shell puncture-resistance systems such as head shields, tank jackets, and increased shell thicknesses had been features of the DOT-111 tank cars involved in this accident, the release of hazardous materials likely would have been significantly reduced, mitigating the severity of the accident."*[12] 'Good-faith' industry efforts towards upgrading these tank cars had already begun by 2013, with the modified DOT-111 cars (branded CPC-1232) implementing some of the upgrades recommended by the NTSB.

By December 2013, following the Lac-Mégantic accident, the NTSB's stance was that *"[...] recent railroad accidents have shown that using DOT-111 tank cars to ship flammable liquids creates an unacceptable public risk."* [13] Based on data from the Pipelines and Hazardous Materials Safety Administration (PHMSA), more crude oil had leaked from trains in 2013 than all the years since 1971 combined.

The Transportation Safety Board of Canada took a similar view, identifying a series of specific improvements for crude oil transportation via rail through their official accident report [9], formalised via five official recommendations (one of which dealt specifically with DOT-111 cars).

Retrofit and phase-out programmes were recommended by the NTSB in favour of the newer DOT-117 cars, but in some cases, this was met with significant resistance from rail operators on the basis of cost. National Steel Car (a Canadian rail car builder) confirmed that *"some of the retrofits cost more than the actual car."* [14]

A new rule created by the PHMSA in 2016 implemented the requirements of the Fixing America's Surface Transportation (FAST) Act 2015, including all major recommendations that had been advocated for by the Railway Supply Institute (RSI), an all-inclusive trade association for railway suppliers. The new PHMSA rule set deadlines for a transition from the DOT-111 to the DOT-117 standard, with an associated cost estimate of approximately 500 million USD [16]. Crude oil transportation in DOT-111 cars was to be completely stopped by 2025.

The RSI estimates that a 65% reduction in tank car fleet conditional probability of release (CPR) has taken place from 2013 to 2017 for crude oil transportation via rail as a result of a mixture of reduction in DOT-111 shipments, reduction in non-jacketed CPC-1232 shipments and an increase in jacketed CPC-1232 shipments [11]. It is anticipated that this trend in CPR will continue with the increased uptake of DOT-117 cars.

However, the momentum of gradual improvement since 2013 has been broken on a number of occasions. Most recently, braking provision requirements instituted through the FAST Act (requiring upgrading to electronically controlled pneumatic (ECP) braking from 2021 onwards) were rescinded in December 2017 on the basis of cost-benefit analysis by the PHMSA [15]. ECP braking would allow freight trains to achieve faster braking over reduced total braking distances.

Additionally, the overall improvement trend in accident rates per million miles travelled (see Figure 6) has been significantly outweighed by the concurrent sharp increase in actual distance travelled toward the end of the period analysed, which has resulted in continued accidents since 2013. Reliable data for more recent years is difficult to locate and analyse due to the widely differing bases used for data recording (i.e. the various bodies' judgement of what constitutes an accident or a spill), but it appears reasonable to extrapolate from the data in Figure 6.

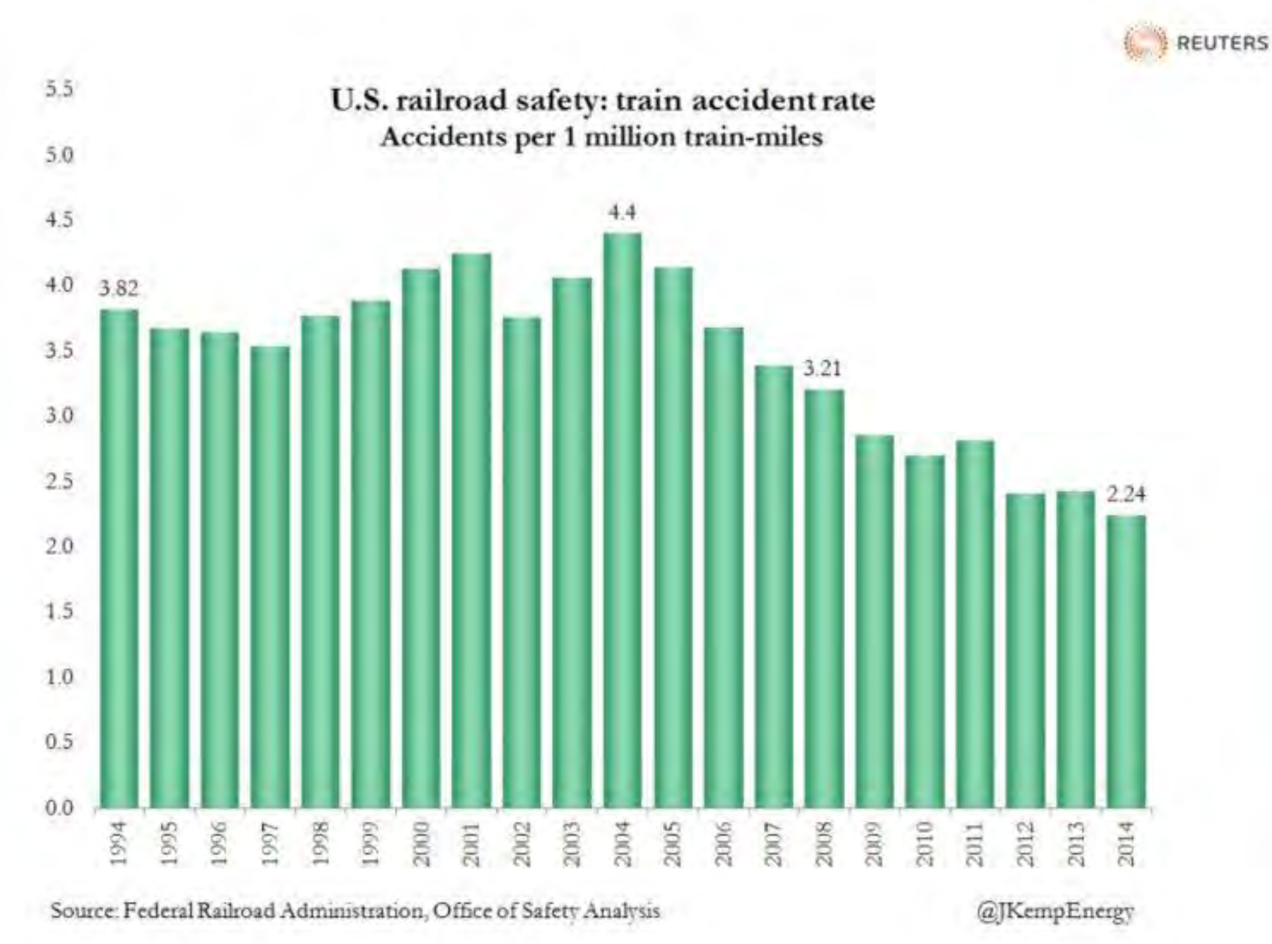


Figure 6. Train accident rates for US railroads [17]

An online literature review conducted for this paper has identified 21 crude oil by rail incidents and accidents in North America since the Lac-Mégantic accident in 2013, summarised in Table 1 below. Incidents and accidents were excluded where the crude oil tank cars were either empty, and where the train was predominantly carrying other cargo (with crude oil constituting a minority of the cargo). Some of the major accidents identified in Table 1 e.g. the Gogama accident in March 2015 bear a significant resemblance to Lac-Mégantic from an accident sequence perspective, and it is readily apparent that such accidents in North America are still relatively commonplace since 2013.

Table 1. Crude oil by rail incidents and accidents, June 2013 to August 2019

Year	Month	Location	Explosion and/or fire?
2013	October	Edmonton (Alberta, Canada)	Yes
2013	November	Aliceville (Alabama, USA)	Yes
2013	December	Casselton (North Dakota, USA)	Yes
2014	January	Plaster Rock (New Brunswick, Canada)	Yes
2014	January	Philadelphia (Pennsylvania, USA)	No
2014	February	Vandergrift (Pennsylvania, USA)	No
2014	April	Lynchburg (Virginia, USA)	Yes
2015	January	South Philadelphia (Pennsylvania, USA)	No
2015	February	Timmins (Ontario, Canada)	Yes
2015	February	Mount Carbon (West Virginia, USA)	Yes
2015	March	Gogama (Ontario, Canada)	Yes
2015	March	Galena (Illinois, USA)	Yes
2015	May	Heimdal (North Dakota, USA)	Yes
2015	July	Culbertson (Montana, USA)	No
2015	November	Watertown (Wisconsin, USA)	No
2015	November	King of Prussia (Pennsylvania, USA)	No
2016	February	Pocatello (Idaho, USA)	No
2016	June	Mosier (Oregon, USA)	Yes
2017	April	Money (Mississippi, USA)	Yes
2017	June	Plainfield (Illinois, USA)	No
2018	June	Doon (Iowa, USA)	No

Comparisons have also been made between the safety of transporting crude oil via rail versus pipeline. Analyses such as that submitted to the International Association for Energy Economics (IAEE) Energy Forum [18] have generally concluded that the conveying of crude oil via rail carries higher risk than pipelines. Some studies [19] appear to indicate that the safety aspects are approximately equal, but such conclusions should be treated with care as most such studies have been commissioned by the railway industry and thus may be demonstrating an underlying bias.

It is important to note that comparisons can be undertaken on a range of bases, with this paper focusing on preventable injuries and deaths rather than the associated (often very severe) environmental impacts of crude oil leaks.

Finally, whilst the analysis in this paper is focused on crude oil transportation specifically, there have been some major non-crude-oil chemicals trains accidents prior to 2013 bearing remarkable similarities to the Lac-Mégantic accident. The Neyshabur (Iran) train disaster in 2004 also involved a runaway train carrying flammable and explosive substances. The train rolled 20 kilometres down a hill after a parking failure (cause unknown to this day) at a railway siding at the highest point of the local area, derailing and catching fire in a city centre and finally undergoing a delayed explosion during clean-up operations. It is estimated that the TNT equivalent of the explosion was 180 tonnes [26], resulting in the death of over 300 people (largely through blast injuries up to 500 metres from the explosion centre [27]) and a blast wave that was perceptible up to 70 kilometres from the accident site [28].

5. SUMMARISING CAUSAL LINKS

Due to the wide range of factors contributing to the Lac-Mégantic accident, systems engineering and systems safety is judged to be the most suitable discipline approach for reviewing the accident. A range of system safety analysis and visualisation techniques can be used to visually represent the contributing factors to an accident, including techniques such as:

- Causal Analysis using System Theory (CAST) stemming from Systems Theoretic Accident Model and Process (STAMP), developed by Leveson [20];
- Functional Resonance Analysis Method (FRAM), developed by Hollnagel [21];
- Human Factors Analysis and Classification Systems (HFACS) developed by Shappell and Wiegmann [22]; and
- AcciMap, developed primarily by Rasmussen and Svedung [23][24].

The AcciMap tool is judged to be most suitable for this paper for its benefits in providing a simple, clear visual overview of the case at hand and for this paper's focus on distilling lessons from existing information, rather than aiming to uncover any new accident root causes (where more complex techniques such as CAST may be more suitable). A coarse AcciMap has therefore been constructed for this paper (see Figure 7) based on some of the contributing factors listed in the official accident investigation report [9] as well as a wider literature review on the subject.

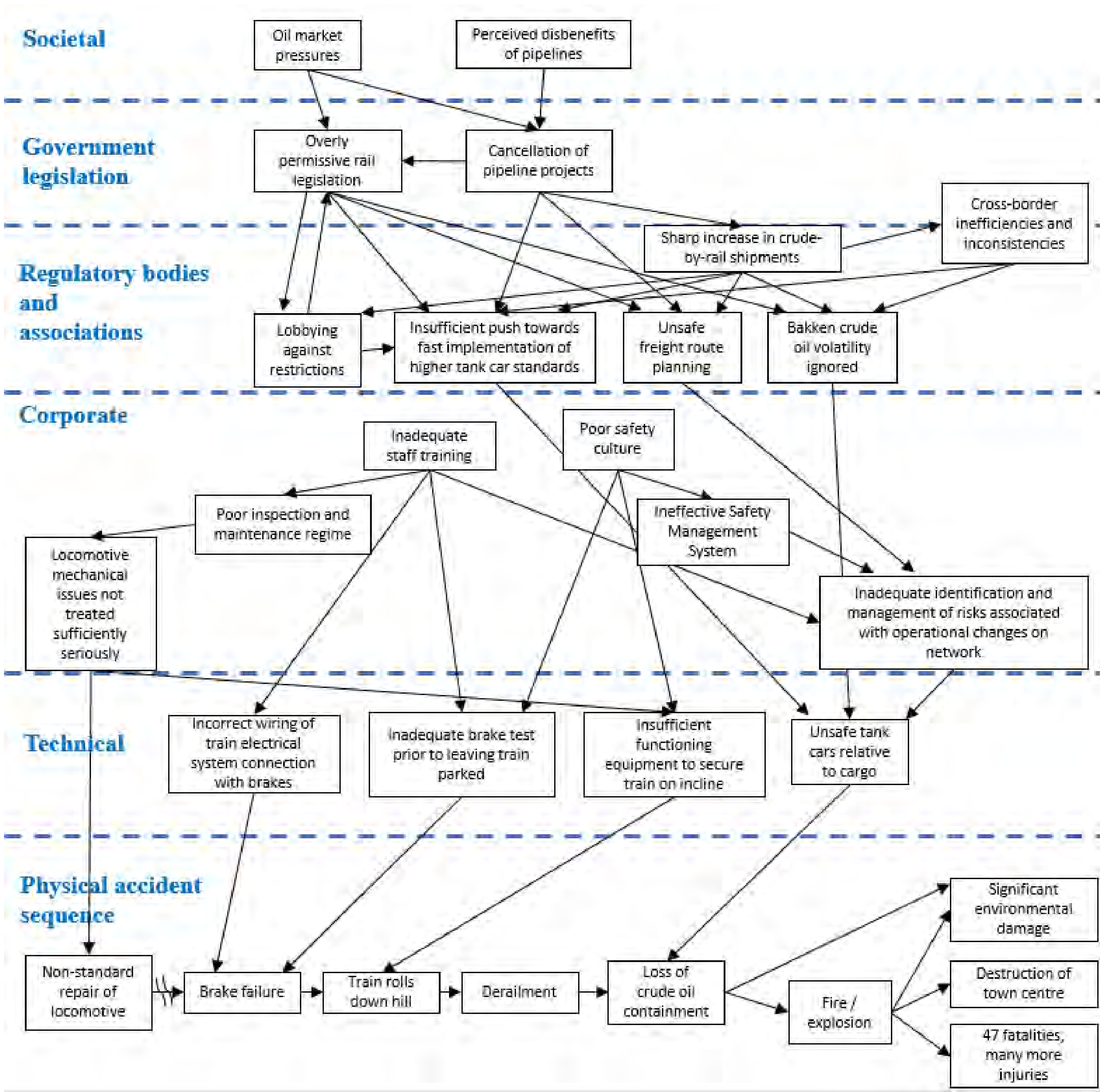


Figure 7. Coarse AcciMap of Lac-Mégantic accident

6. LEARNING OPPORTUNITIES

When investigating a major accident, there is an understandable focus on the details of the circumstances, reconstructing a detailed accident sequence such that specific causal links can be identified and rectified within the sector where the accident (and subsequent learning opportunity) occurred, and the official Lac-Mégantic accident report [9] thoroughly undertakes these tasks. However, it is important to consider whether there is commonality across many high hazard sectors in terms of both accident root causes and also high-level cross-industry lessons that can be distilled and learned.

Emerging sectors such as connected and autonomous vehicles do not traditionally fall under the 'high hazard' umbrella; nevertheless, new accidental and malicious risks related to e.g. use of artificial intelligence (AI) [30] may pose novel and unique low frequency, high consequence event types, whilst potentially also still showing some vulnerabilities which have parallels to older malicious attack vectors such as that used to infect Iranian nuclear centrifuges with the Stuxnet computer worm in 2010 [31]. Industry groups, researchers and intelligence organisations have become increasingly vocal regarding the security deficiencies of industrial control systems [32][33] connected to the internet with the advent of the Internet of Things, and it is important that continuous improvements are made in the interface between safety and security.

Safety professionals all have a part to play in this by actively disseminating lessons through leveraging connections with colleagues working in other sectors and lobbying their professional engineering institutions to make this an explicit aspect of engineering competencies required to achieve and maintain chartered engineer / professional engineer status. Disseminating inter-sector learning opportunities should be seen as an additional key indicator of a successful safety culture within an organisation.

Five key high-level learning opportunities are identified in this paper:

I. **Rate of change**
The rate of change of volume of crude oil transportation via rail was excessive and should have triggered a significant review of safety arrangements. Increases of over an order magnitude in any parameters within a relatively short timescale should automatically prompt review of whether a system has been correctly engineered and is being correctly managed at all levels, and whether any further changes should be made (either in parallel with the operations continuing or making the decision to halt the activity pending review) to ensure ongoing safety. Such a sudden surge in a process parameter (e.g. temperature) would not be acceptable in a process plant, and the same logic should be applied to 'process parameters' on a systems level in a broader sense.

II. **Characterisation of properties**
The volatility of (and therefore the degree of explosion risk posed by) Bakken crude was severely underestimated through assuming that it would be similar to more conventional types of crude oils, meaning that the safety measures in place (such as those on DOT-111 cars) were inappropriate for the hazard posed. The handling of (tangible or intangible) 'materials' with such significant unknown properties via processes with a different design basis should not be accepted without checks being undertaken to confirm suitability. A nuclear decommissioning plant would not feed legacy waste materials through without conducting a proper assay, and machine learning applications should be wary of the quality of learning datasets (whether of insufficient quality by chance or actively poisoned by malicious threats).

III. **Self-regulation**
Regulatory bodies being increasingly stretched thin has resulted in a general trend over the past decades toward allowing increased self-regulation across numerous sectors. The Lac-Mégantic accident and the recent Boeing 737 MAX accidents have shown that, whilst

conceptually useful, self-regulation should be used very sparingly, and only under the right conditions, taking full cognisance of the human factors limitations (such as normalisation of deviance within an organisation).

IV. Ethical lobbying and advocacy

The accident at Lac-Mégantic may have been avoided had a much larger network of pipelines been constructed, against public opinion (now labelling the trains in question as "bomb trains"). Studies have demonstrated that blocking of pipeline projects does not decrease crude oil production, and instead shifts the burden of transportation onto rail [34], increasing the overall risk. Public engagement and communications are now more important than ever to mitigate the hurdles posed by the general public towards sectors involving emotive subjects e.g. nuclear energy and biotechnology. This is exacerbated by the current 'post-truth' political climate worldwide. Companies and organisations across all sectors should allocate significant effort towards (ethical) lobbying and advocacy to achieve outcomes that are objectively beneficial for society.

V. Dynamic ALARP on a holistic level

There is a tendency in 'as low as reasonably practicable' (ALARP) demonstrations to focus on a single system being assessed, not adequately considering how system interfaces may affect the holistic risk profile. Risk reduction to an ALARP level should be demonstrated through consideration of e.g. all levels of an AcciMap diagram (especially focusing on societal, organisational and regulatory considerations) to provide evidence that residual risks have been balanced appropriately.

7. CONCLUSIONS

Crude oil transportation via rail over the last decade has proven problematic despite a comparatively low accident rate due to the high frequency of train derailments, very high probability of loss of containment in case of a derailment, Bakken crude oil posing a significantly higher hazard than initially anticipated, slow regulatory support and response, and

Periodic decreases in crude oil by rail accidents have largely been driven by the temporary decreases in volume transported i.e. the decreases have not been as a result of a significantly improved accident rate per unit distance travelled. Demand still significantly outstrips pipeline capacity, and thus transportation via rail is likely to remain the main mode of crude oil transportation for the foreseeable future, despite the associated risks.

It is important that, in the process of striving for improving the safety performance of this sector, wider endeavours are undertaken to apply any learnings (whether specific or high-level) to other sectors, both established and emerging.

High hazard sectors can encompass not only existing established 'traditional' sectors such as nuclear and oil & gas, but also emerging sectors and technologies such as connected & autonomous vehicles and hydrogen for domestic uses where the low frequency, high consequence type accidents can still result in significant numbers of injuries and fatalities, and where rapid development of the technologies and their implementation could lead to the repeating of past mistakes in unrelated sectors.

When looking to identify lessons, there is also a risk that overly specific lessons are identified, missing an opportunity to identify and disseminate the higher-level learning opportunities across sectors, and thus a concerted effort is needed from safety specialists across all sectors. Whilst adoption rates from lessons learned vary by several orders of magnitude across sectors, there are nevertheless significant success cases (e.g. the adoption of aviation-style checklists during surgical procedures) even in industries such as healthcare, where the adoption rate of new processes is traditionally extremely slow.

Traditional safety and risk analysis techniques are still largely relevant to the modern world, but the current fast pace of technological change can sometimes mean that there is a reduced ability to learn from past experience, and it is therefore more important than ever that all major learning opportunities are utilised to their full potential regardless of the originating sector.

8. REFERENCES

[1] **U.S. Energy Information Administration (2012)**, 'Williston Basin crude oil production and takeaway capacity are increasing', *Today in Energy*, 17 April. Available at: https://www.eia.gov/todayinenergy/detail.php?id=5870 (Accessed: 12 July 2019).

[2] **Sider, A. (2014)** 'In Dakota Oil Patch, Trains Trump Pipelines', *The Wall Street Journal*, 03 March. Available at: https://www.wsj.com/articles/dakota-oil-producers-embracing-rail-over-proposed-pipelines-1393892490?tesla=y (Accessed: 18 August 2019).

[3] **Association of American Railroads (2019)**, 'Annual Rail Traffic Data', *Railroad 101*. Available at: https://www.aar.org/data-center/rail-traffic-data/ (Accessed: 12 August 2019).

[4] **Grant, C. (2017)**, 'Off the Rails: Preparing communities and responders for crude oil train derailments', *NFPA Journal*, 01 March. Available at: https://www.nfpa.org/News-and-Research/Publications-and-media/NFPA-Journal/2017/March-April-2017/Columns/Research (Accessed: 01 July 2019).

[5] **Surface Transportation Board (2019)**, 'Economic and Industry Information', *FAQs*. Available at: https://www.stb.gov/stb/faqs.html (Accessed: 07 August 2019).

[6] **Trains (2006)**, 'Class 1 Railroads', *Railroads*, 01 June. Available at: http://trn.trains.com/railroads/2006/06/class-1-railroads (Accessed: 07 August 2019).

[7] **Canada Energy Regulator (2019)**, 'Canadian Crude Oil Exports by Rail – Monthly Data', *Energy Information*, 19 August. Available at: https://www.cer-rec.gc.ca/nrg/sttstc/crdlndptrlmprdct/stt/cndncrdlxprtsrl-eng.html (Accessed: 29 August 2019).

[8] **CTV News Montreal (2014)**, 'Lac-Megantic coroner reports: 47 violent deaths that could have been avoided', *News*, 08 October. Available at: https://montreal.ctvnews.ca/lac-megantic-coroner-reports-47-violent-deaths-that-could-have-been-avoided-1.2044859 (Accessed: 24 August 2019).

[9] **Transportation Safety Board of Canada (2014)**, 'Runaway and main-track derailment - Montreal, Maine & Atlantic Railway - Freight train MMA-002 - Mile 0.23, Sherbrooke Subdivision - Lac-Mégantic, Quebec - 06 July 2013' *(Railway Investigation Report R13D0054*), 18 June. Available at http://www.tsb.gc.ca/eng/rapports-reports/rail/2013/r13d0054/r13d0054.pdf (Accessed: 24 August 2019).

[10] **Robbins, M (2014)**, 'Why Do These Train Cars Carrying Oil Keep Blowing Up?', *Mother Jones*, 27 May. Available at: https://www.motherjones.com/environment/2014/05/oil-tank-trains-bakken-crude-accidents/ (Accessed 01 August 2019).

[11] **Railway Supply Institute (2018)**, 'RSI Committee on Tank Cars Activity Update', 11 September. Available at: https://www.rsiweb.org/Files/Committees/RSICTC-Update-9-11-2018.pdf (Accessed 29 August 2019).

[12] **National Transportation Safety Board (2012)**, 'Derailment of CN Freight Train U70691-18 With Subsequent Hazardous Materials Release and Fire Cherry Valley, Illinois, June 19, 2009', *Accident Report NTSB/RAR-12/01*, Washington DC.

[13] **National Transportation Safety Board (2007)**, 'Safety Recommendation R-07-004', *Safety Advocacy*. Available at: https://www.ntsb.gov/safety/safety-recs/_layouts/ntsb.recsearch/Recommendation.aspx?Rec=R-07-004 (Accessed: 04 August 2019).

[14] **Renshaw, J. (2015)**, 'U.S. oil-rail flux means no retrofit bonanza for tank car makers', *Reuters*, 06 October. Available at: https://www.reuters.com/article/crude-rail-regulations/u-s-oil-rail-flux-means-no-retrofit-bonanza-for-tank-car-makers-idUSL1N11Y20U20151006 (Accessed: 22 August 2019).

[15] **Pipeline and Hazardous Materials Safety Administration and Federal Railroad Administration (2017)**, 'Electronically Controlled Pneumatic Braking – Regulatory Impact Analysis', *PHMSA-2017-0102*.

[16] **Federal Register (2016),** 'Hazardous Materials: FAST Act Requirements for Flammable Liquids and Rail Tank Cars'. Available at: https://www.federalregister.gov/documents/2016/08/15/2016-19406/hazardous-

materials-fast-act-requirements-for-flammable-liquids-and-rail-tank-cars (Accessed: 29 August 2019).

[17] **Ferro, S. (2015),** ‘US oil train accidents won’t go away any time soon’, *Business Insider*, Mar 20. Available at: https://www.businessinsider.com/crude-oil-train-derailments-2015-3?r=US&IR=T (Accessed 01 August 2019).

[18] **Mason, C. (2018)**, ‘A Comparison of the Risk of Transporting Crude Oil: Rail vs. Pipeline’, *IAEE Energy Forum Second Quarter 2018*.

[19] **Oliver Wyman (2015)**, ‘Canadian Crude Oil Transportation – Comparing the Safety of Pipelines and Railways’.

[20] **Leveson, N. (2011)**, ‘Engineering a Safer World: Systems Thinking Applied to Safety’, The MIT Press, Cambridge, Massachusetts.

[21] **Hollnagel, E. (2012)**, ‘FRAM – The Functional Resonance Analysis Method’, Ashgate, Farnham, UK.

[22] **Shappell, S. and Wiegmann, D. (2000)**, ‘DOT/FAA/AM-00/7 - The Human Factors Analysis and Classification System – HFACS’, *Office of Aviation Medicine*, Washington, DC.

[23] **Rasmussen, J. (1997),** Risk management in a dynamic society: a modelling problem. *Safety Science*, 27, 183-213.

[24] **Svedung, I. and Rasmussen, J. (2000),** Proactive Risk Management in a Dynamic Society. Karlstad: Swedish Rescue Services Agency.

[25] **Branford, K. (2011)**, ‘Seeing the Big Picture of Mishaps: Applying the AcciMap Approach to Analyze System Accidents’, *Aviation Psychology and Applied Human Factors; Vol. 1(1):31–37*

[26] **Banerji, A. (2011)**, ‘*Worldwide Railways Accidents, 2000-09*’.

[27] **Jahangiri *et al.* (2018)**, ‘Pattern and nature of Neyshabur train explosion blast injuries’, *World Journal of Emergency Surgery*, 13:3.

[28] **United Nations Office for the Coordination of Human Affairs (2004)**, ‘Iran - Chemical Train Derailment and Explosion OCHA Situation Report No. 1’, OCHA/GVA – 0024.

[29] **Natural Resources Canada (2016)**, 'Pipelines Across Canada', Energy, 25 July. Available at https://www.nrcan.gc.ca/energy/infrastructure/18856 (Accessed: 22 August 2019).

[30] **Brundage, M. *et al* (2018)**, 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'.

[31] **Kerr, P. *et al* (2010)**, 'R41524 - The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability', *Congressional Research Service*.

[32] **Kaspersky Lab (2018)**, 'Threat Landscape for Industrial Automation Systems in H2 2017', *ICS CERT.*

[33] **National Cyber Security Centre, Government Communications Headquarters [GCHQ] (2018)**, 'Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies.'

[34] **Covert, T. and Kellogg, R. (2017)**, 'Crude by rail, option value, and pipeline investment' *National Bureau of Economic Research (NBER) Working Paper Series – 23855*.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Are biases towards the recent past causing us to unintentionally expose personnel to increased levels of risk?

Alexander I. Fergusson, Karen R. Vilas*
Baker Engineering and Risk Consultants, Inc.
11011 Richmond Avenue Suite 700, Houston, TX 77042
*Presenter E-mail: KVilas@BakerRisk.com

Abstract

This paper focuses on the consideration of an unbiased approach to assessing risk to push the industry towards proactively addressing risk rather than reactively allowing cognitive biases to drive process safety culture and personnel risk management solutions. Scientifically proven to affect the way we process and interpret the world around us, cognitive biases allow us to shortcut the complexities of the world when making decisions. In some cases, biases can be surprisingly accurate, while in other instances they can lead to making poor judgements and decisions based on the limited information available to us. Specifically damaging in the process safety industry are the *availability heuristic* and the *confirmation bias,* which together cause us to focus on information that comes to mind quickly, justifies our opinions, and favors our existing beliefs.

With recent industrial accidents that have resulted in fatalities and a push toward regulatory change in response to explosion events, we have seen a rise in the availability of blast resistant structures such as BRMs and hardened stick-built buildings to protect onsite personnel from explosions. The availability of such blast hardened structures has produced an unfortunate trend of moving personnel back in closer to processing areas. Recent advancements in full-scale testing and computer modeling capabilities suggests that even though such buildings may protect for some level of blast hazards, this approach may result in increased levels of personnel risk from other hazard types, specifically impinged jet fires and toxic exposure. This raises the question: are employees being placed in risky locations in a BRM or hardened building with a false sense of security?

Keywords: Managing Process Safety, Learning from Incidents, Safety Culture, Flammability, Thermal Radiation, Explosions, Toxics, Cogitative Bias, Blast Resistant, Risk, Process Safety, Facilities, Personnel Protection, Safe Refuge Location

Introduction

On March 23, 2005, a vapor cloud explosion (VCE) at the BP Texas City refinery initiated the momentum behind a shift in the fundamental way in which the petrochemical industry views facility siting of temporary and permanent occupied structures (see **Figure 1** for a view of facility damage). In this tragedy, 15 workers were killed and nearly 200 were injured as a result of an ignited vapor cloud that formed from a release of flammable liquid hydrocarbons. (Safety+Health: The Official magazine of the NSC Congress & Expo, 2015) While numerous lessons were learned from this incident and many recommendations were made, arguably the most influential lesson learned was regarding the location of temporary trailers, commonly used for construction and turnaround events, to potential blast events.

Figure 1. BP Texas City, Chemical Safety Board

The BP Texas City incident was not the first VCE to have a significant impact that subsequently influenced industry regulations. In 1974, 28 deaths resulted from a cyclohexane explosion that damaged 1,821 homes and 167 commercial buildings. Approximately 10 years later, the Center for Chemical Process Safety (CCPS) was established. In 1989, a VCE with an initial blast registering 3.5 on the Richter scale caused 24 deaths at the Phillips Petroleum Houston Chemical Complex in Pasadena, Texas. The event led to the establishment of the Mary K. O'Conner Process Safety Center (MKOPSC) and subsequent creation of OSHA Process Safety Management (PSM) in 1992. Shortly after the BP Texas City incident, a VCE in Buncefield, England, was heard up to 125 miles away. (Fitzgerald, Accessed August 2019) These events, which have created a lasting impression on the petrochemical industry, are easily recalled by industry professionals due to their influential nature. As a result of the ease at which these events can be called to mind, there is a tendency for process safety individuals to focus on blast (specifically VCE) as the main hazard of concern for facility siting activities.

This paper explores the impact of the BP Texas City VCE on industry regulations within the US and the subsequent trends with respect to facility siting due to individual biases. The example case study presented is based on the author's experience in performing both consequence and risk-based facility siting studies and is intended to promote discussion around balanced hazard protection. That is, this paper is intended to promote protection for blast, thermal, toxic, and other applicable hazards by removing individuals' natural tendencies towards cognitive biases.

The Interplay of Cognitive Biases with Process Safety

While powerful, the human brain is subject to limitations in processing and interpreting information in the world around us. Cognitive biases, which help us make sense of the input we are receiving and to reach decisions with relative speed, are the brain's attempt to simplify information processing. As such, while we as individuals believe we are being objective, logical, and capable of evaluating all available information, we are constantly taking mental shortcuts (known as heuristics) that creep in and influence the way we see and think about the world. (Cherry, 2019)

It is easy to see how cognitive biases can influence perceptions in all areas of life. This even includes the area of petrochemical process safety, where attempts are made to overcome individual cognitive biases whether we are consciously aware of this or not. Examples include team Process Hazard Analyses (PHAs) with external facilitators, leveraged knowledge shares and lessons learned reviews, and development of accident databases and incident summaries. Regardless, history is lost with time and only the most recent or most impactful events are remembered. To put it as succinctly as George Bernard Shaw, "most new discoveries are made regularly – every fifteen years!" (Maitland, 2015)

We encourage readers of this paper to investigate their cognitive biases and how those biases play a role in daily decision making in our roles. This paper incorporates concepts relating to *confirmation bias* and the *availability heuristic* with respect to historical accidents and facility siting. Confirmation bias is more straightforward of the two and states simply that an individual favors information that supports existing beliefs while discounting evidence that does not conform to that approach. Confirmation bias suggests that an individual actively seeks evidence that supports existing beliefs, which prevents looking at situations objectively. (Cherry, 2019) The authors anticipates that we can all remember a situation where a team member has stated, "that event isn't credible, it has never happened here" or "we've never tested them, but our shelter in place buildings are leak tight" or "the gas cloud will ignite before it gets that large".

The availability heuristic places greater value on information that comes to mind quickly – greater credence is given to this information and as a result, probability and likelihood of similar things happening in the future is overestimated. (Psychology Resource and Reference, 2019) With a recent historical focus on industry VCE events resulting in heavy asset damage, long downtimes, loss of life, and regulatory change, the tendency of petrochemical professionals is to focus on blast events and downplay potential fire and toxic events when discussing facility siting and personnel protection. The availability heuristic leads individuals as well as teams to believe that VCEs are likely to be large and destructive whereas fire and toxic releases are perceived to be smaller and easily isolated with limited personnel impact.

Even with the reference to the Bhopal, India methylisocyanate (MIC) gas leak in the preamble to the PSM standard, toxic hazards continue to be minimized due to the limited number of recent events. This 1984 event led to the death of approximately 5,200 people and permanent or partial disabilities in several thousand more individuals, yet it is mentioned most typically in passing, with a feeling that "something similar wouldn't happen today". (Union Carbide Corporation, 2018) However, some operating companies are recognizing these hazards and proactively replacing toxic chemicals where possible to remove the hazard (e.g., replacement of chlorine for water treatment) as well as establishing mitigation and secondary containment systems with a last resort to provide robust toxic shelter and evacuation programs to protect their personnel. Unfortunately, this is still the exception and not the norm.

With just a few examples, one can see how *confirmation bias* and the *availability heuristic* can greatly influence thoughts on process safety, specifically facility siting. As Trevor Kletz has famously said, "Organizations have no memory…" and "Don't bother to write an accident report, I'll send you one from my files!". (Maitland, 2015)

Impacts of BP Texas City on Facility Siting

Before the VCE incident, the BP Texas City refinery had conducted a site-wide siting analysis in 1995 and again in 2002 to establish layouts for trailers and other temporary structures. With the 5-year PSM refresh cycle in place, an update was due to take place in 2007, except for any changes to siting falling under the management of change (MOC) process. In late 2004, plans were made to place contractors in 9 single trailers and 1 double-wide trailer adjacent to the ISOM unit beginning in 2005; however, an analysis to determine risk for this proposed plan to locate the trailers in accordance with American Petroleum Institute Recommended Practice (API RP) 752, "Management of Hazards Associated with Location of Process Plant Buildings" hadn't been completed at the time of the incident. (Wikipedia, 2019)

After the 2005 BP Texas City incident, The U.S. Chemical Safety and Hazard Investigation Board (CSB) issued an urgent recommendation acknowledging that while BP was compliant with API 752 because the trailers were temporary structures, the CSB recommended that API either update API 752 or issue a new Recommended Practice to ensure the safe placement of occupied trailers and similar temporary structures away from hazardous areas of plant processes. In June 2007, API RP 753, "Management of Hazards Associated with Location of Process Plant Portable Buildings", was published. (U.S. Chemical Safety and Hazard Investigation Board, 2007) In addition, a 3rd Edition of API 752 was released in 2009 to address the Texas City incident, OSHA comments, and NEP findings.

The revised API RP 752 and new API RP 753 included several changes that would impact industry's approach to facility siting, most notably language that transforms facility siting into an ongoing process as well as changing the occupancy basis from a 'man hours per year" calculation to an “intended for occupancy” approach. (Baker, 2011) Both API RP 752 & 753, however, were written to provide companies flexibility in how to assess personnel protection depending on a consequence (simple or detailed) or risk approach as well as allowing for company definition of maximum credible event (MCE). Furthermore, while language was added specifying that thermal and toxic risk should be reviewed as part of facility siting, very little guidance was provided on how to do so; while language was added to require quantitative evaluation of explosion hazards, qualitative or spacing table approaches could continue to be used for thermal and toxic hazards.

The release of these two API RPs resulted in two initial major impacts on facility siting for the petrochemical industry. The first major shift is captured in API RP 753’s guiding principles: “locate personnel away from covered process areas consistent with safe and effective operations”. This is reflective of the trend to move occupied structures from close by the process units to a distance at which personnel would be protected, particularly from blast events. The second major shift was in the rationale behind “maximum credible event” (MCE): companies were no longer allowed to use so called “credible” high frequency smaller release events (flange leaks and plug failures) but instead needed to consider larger loss of containment events associated with pipe and full connection failures. (American Petroleum Institute, 2009) and (American Petroleum Institute, 2007) Along with a shift towards inclusion of larger events for facility siting modeling came a shift from consequence-based siting to risk-based siting, which brought in the element of frequency in addition to the consequence of identified events.

The Rise of the BRM

With the release of the revised API RP 752 and new API RP 753, traditionally constructed permanent buildings (e.g., masonry, unreinforced concrete, pre-engineered, etc. buildings) as well as temporary structures (e.g., modular buildings and wood trailers) were being pushed farther away from process units. Furthermore, due to site real estate restrictions, often consequence results were indicating that weaker structures may even need to be located offsite. While in some situations this had minor impact on site operations, in many cases distance creates a challenge for turnaround/construction crews as well as essential site operations and maintenance personnel. A demand for a solution that would achieve a higher level of personnel protection without having to locate personnel in logistically challenging locations was created in the marketplace.

Blast Resistant Modules (BRMs) entered the marketplace, slowly at first and then in high volume, to fill this demand. BRMs, typically of modular steel construction, are designed to American Society of Civil Engineers (ASCE) building design codes for low (localized damage), medium (widespread damage), or high (loss of structural integrity) response. Depending on the rating of the BRM and the manufacturer, BRMs are designed for a range of maximum pressure loads for a given duration, with the most common BRMs rated as 3, 5, and 8 psi structures with varying impulse sensitivity depending on design/construction. Most purchasers of BRM’s and the BRM vendors focused on the overpressure rating of the BRM structure and used that rating to place it outside of the overpressure zone.

With the rise of the steel BRM, facilities had a product to meet the growing demands for blast protection within the petrochemical industry. BRMs, which can be temporary or permanent in nature, began showing up on sites across the US as well as internationally. With the ability to rent, lease, or purchase these structures, site owners began moving facility personnel closer to processing units using traditional blast contours as guides for siting. However, it is important to understand the vulnerability associated with the structure for a given load (impulse as well as pressure) and not just the response rating – a fact that is often missed by most, resulting in a false sense of protection from blast hazards. Therefore, while utilizing these structures may be compliant with the letter of API RP 752 and 753, BRMs may not meet the intent of protecting the occupants of these structures. But the petrochemical industry tends to be reactive, not proactive, when it comes to safety, and biases had created an unintended focus on the structural survivability of the heavily influential VCE events discussed above.

While the structure of an empty metal BRM may be rated for blast events, BRMs typically provide little thermal or toxic protection for sites with other hazards of concern without additional costly design considerations. Typically, standard BRMs are metal paneled structures which may have windows and standard air handling units and may have less thermal and toxic protection than a traditional plant stick-built structure. However, with preliminary design considerations such as intumescent coatings (thermal), elevated air intake and HVAC shutdown systems (toxic), and removal of windows / installation of protective seals (thermal and toxic), BRMs may be able to provide improved protection required for personnel located near operating units. As a market product, these additional protective features are not standard offerings with BRMs and result in an increased cost per square foot, introduction of secondary hazards resulting in unsafe internal environments, additional complexity in retrofit requirements, and increased maintenance costs.

A Case Study for Balanced Hazard Protection

As a result of a bias towards siting for VCEs, blast resistant structural design and implementation has matured into a reasonably well understood field. In comparison, toxic and thermal performance is lagging due to the lack of emphasis on these hazards, with solutions intended to address these hazards applied, but at a lower level of rigor.

The following case study highlights the concepts described above. This case study focuses on the conceptual consequence and risk associated with locating a trailer, a traditional 3psi long duration / medium response BRM, an enhanced BRM for toxic and thermal protection, and a stick-built building designed for balanced hazard protection for an existing facility.

Building Location

In this case study, the client wants to site a permanent structure (shown in green in **Figure *2***) for contractors and employees to use as an operator shelter and permit writing area. While API 752 and API 753 both allow for either consequence or risk-based siting, this client wants to site based on consequence criteria for personnel protection. The structure will be utilized for contractor and employee offices, change rooms, and restrooms.

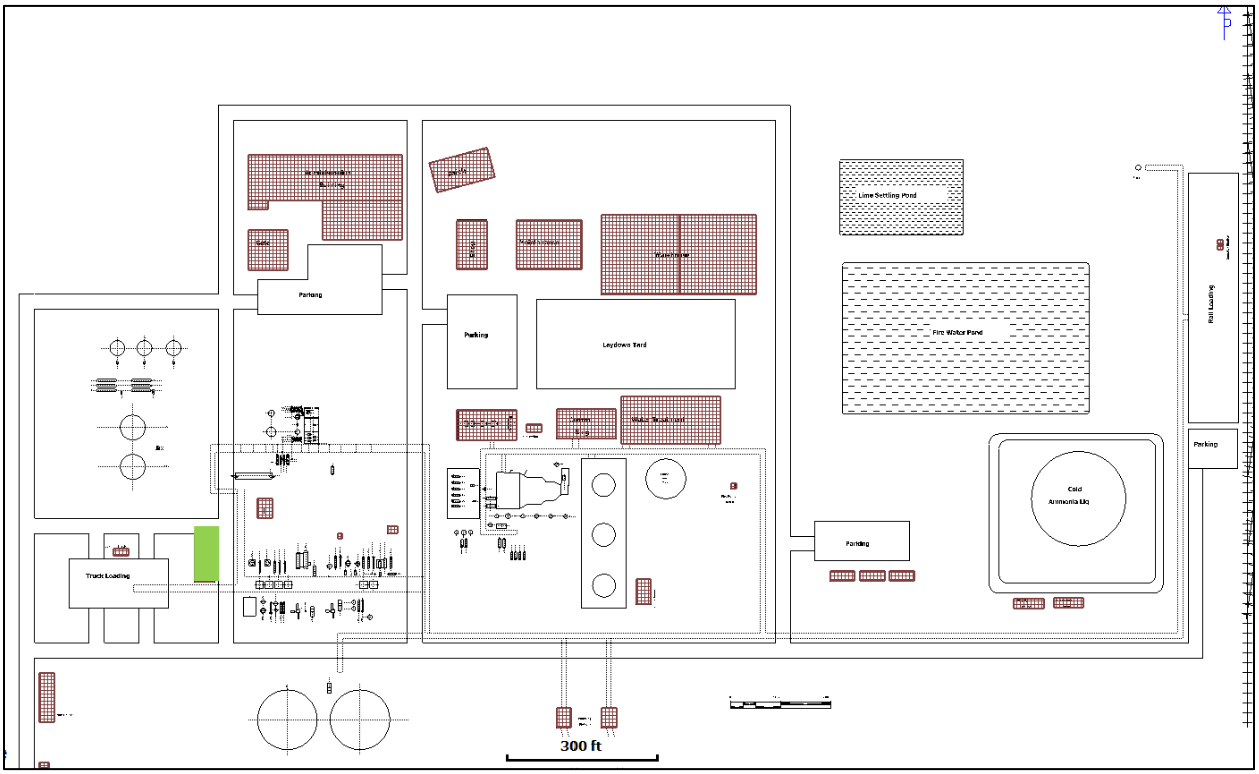


Figure 2. Facility Plant Plot Plan (Building Location Shown in Green)

The client is considering three different building construction types: a traditional wood trailer, a 5psi long duration / medium response BRM, and a stick-built building designed for balanced hazard protection. In addition, they are considering a fourth option as a retrofitted BRM to have additional thermal and toxic protection for personnel. A summary of the building options is shown below in Table 1, with a representation of level of protection by hazard type as well as a representation of relative cost.

Table 1: Building Option Summary

Building Option	**Hazard Resistance**			**Relative Cost**	**Additional Details**
	Blast	*Thermal*	*Toxic*		
Wood Trailer	Low	Low	Low	$	Traditional off-the-shelf trailer.
BRM	Medium	Low	Low	$$	Standard blast resistant building, designed for medium response at 5psi long duration.
Retrofitted BRM	Medium	Medium	Medium	$$$	Windows have been removed and intumescent coating has been applied to BRM. HVAC has automatic shutdown on gas detection and building has elevated air intake.
Stick-Built Concrete	High	High	High	$$$	5spi long duration, low response concrete structure without windows. Doors have been designed with thermal and leak tight seals and the building has interior SIP room with separate, isolatable air handling system and elevated air intake.

Figure *3* shows the overpressure contours (i.e., blast contours) for the facility operations, with pressure thresholds of 0.6, 0.9, 3, 5, and 10 psig. Note that the desired building location falls within the 0.9 psig pressure threshold but outside of the 3psig threshold. Assuming a corresponding long duration event, this location is not suitable for a wood trailer based on blast exposure. In addition, while the BRM is rated up to 5psi, it is designed for medium response indicating that the building may experience significant deformation, potentially resulting in internal debris/projectiles and a subsequent level of increased occupant vulnerability. The custom designed stick-built concrete structure is predicted to receive minor damage at the specified location and is likely immediately available for occupancy post event. *Note that for simplicity, the author is not addressing the importance of impulse in this paper; however, when designing for overpressure, governing loads along the pressure-impulse curve need to be addressed.*

Based on the specifications of the API Recommended Practices, the wood trailer, whether intended to be permanent or temporary, is unacceptable at this location following the detailed analysis approach based on predicted blast overpressures, while the BRM and stick-built structures in

Table 1 would meet the blast requirements specified by API 752/753.

Figure 3. Blast Contours for Facility

It is not uncommon when locating buildings for contractors and temporary employees to use available consequence contours, which most typically are retained onsite as blast contours. For sites employing this process and locating buildings based on blast contours alone without undertaking a robust facility siting MOC process, an off-the-shelf 5-psig BRM would appear to be a satisfactory, cost-effective option for personnel protection. The decision to use a BRM would be reinforced by the *availability heuristic* and *confirmation bias* in two ways: the typically held belief that explosions are the most likely hazard and maximum credible event for personnel exposure as well as the idea that personnel are protected by a Blast Resistant structure. In fact, how often have we all heard these structures mistakenly called "Blast Proof", thus reinforcing biases?

On the other hand, a site following the full intent of the API Recommended Practices and treating facility siting as a living analysis that covers a full range of potential hazard types (explosion, thermal, and toxic) would want to review the vulnerability of personnel in the BRM from blasts as well as the thermal and toxic exposures of additional potential MCEs.

Figure *4* shows that the desired building location falls within the >37.5 kW/m^2 thermal radiation threshold, which is the point at which steel begins to lose its mechanical strength. This is well above the 12.5 kW/m^2 threshold for piloted ignition of wood, further ruling out the usage of an off-the-shelf wood trailer in this location. In addition, a prolonged thermal exposure of this magnitude would not only significantly impact the structural integrity of a standard steel BRM, but also result in significant heat rise within the structure. This leaves two potential options for consideration: a retrofitted BRM with thermally sealed doors, intumescent coating, and no windows, or a stick-built concrete structure with thermally resistant seals and no windows.

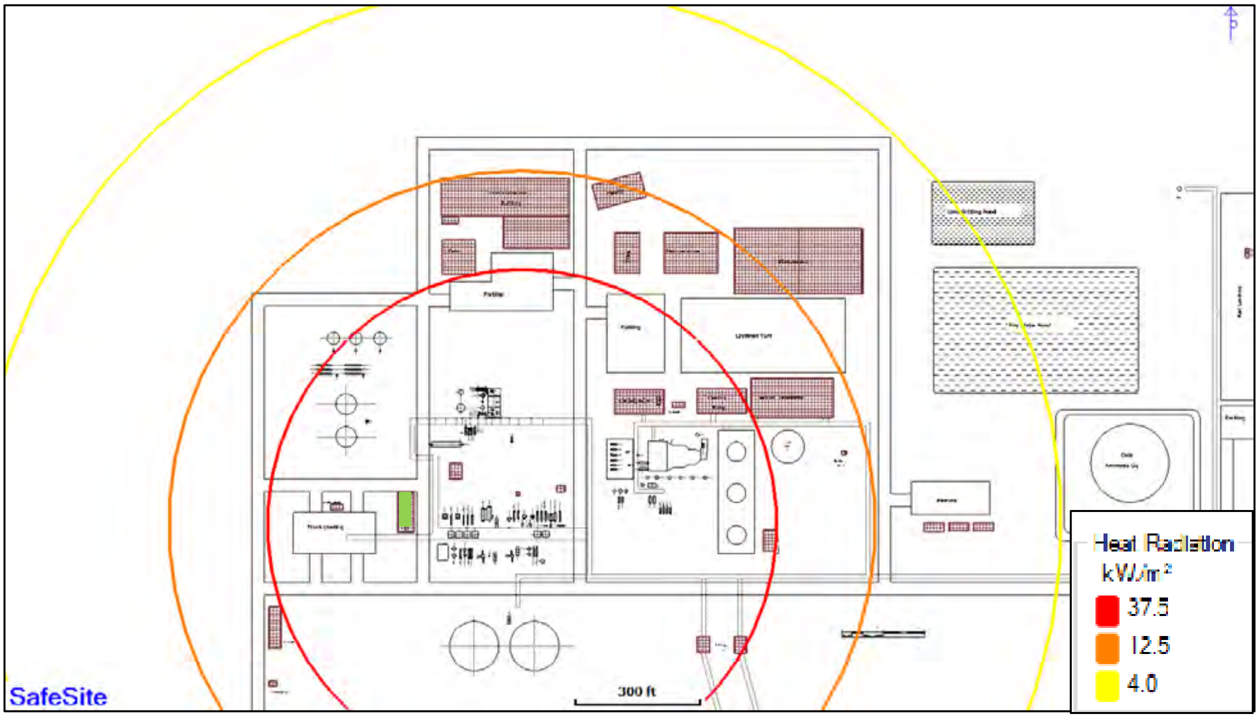


Figure 4. Thermal Contours for Facility

Overcoming biases that may lead one to think that VCE is the maximum potential exposure for an exposed population has led the client, in this example, away from the choice of an off-the-shelf BRM and towards a safer solution for building occupants. At this point, cognitive biases could again rise to the forefront: *confirmation bias* may lead a facility team to determine that a structure designed to prevent heat rise with thermal seals and no windows is certainly good for toxic protection and the *availability heuristic* may lead to a belief that a toxic event resulting in death is rare and may be considered non-credible. The definition of credible is nebulous, at best, and this belief may be justified by the language in the API Recommended Practices. Regardless, due diligence should lead the facility internal or external consequence modeler to also review potential acute toxic hazards.

Figure 5 shows the site toxic consequence profile, which indicates that the desired building location is within the 90% lethality threshold for 10-minute toxic exposure (low pressure chlorine release). From a consequence standpoint, personnel housed in this building for a release duration for 10-minutes or longer would need a significant level of toxic protection. This again rules out the wood trailer and standard BRM options. In addition, while a BRM can be retrofitted with a robust HVAC shutdown system upon gas detection and air tightness can be greatly improved, it is unlikely a standard BRM can be improved enough to provide long duration exposure without supplied breathing air or escape protection. Any building intended to serve as a toxic shelter also needs to be maintained as one. Door gaskets and active protection like HVAC shutdown, alarms, etc. need to be maintained and tested as safety critical systems to ensure the performance on demand. Air tightness cannot be presumed, and structures should be tested regularly to ensure they provide the necessary protection.

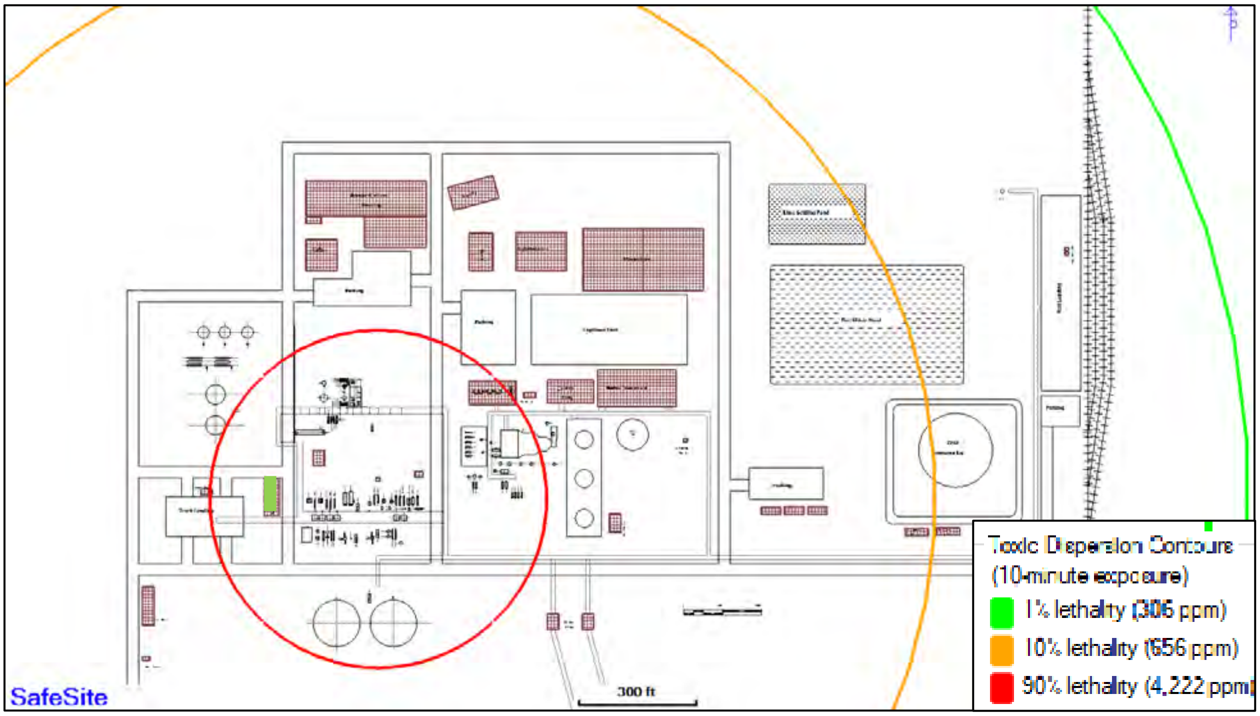


Figure 5. Toxic Contours for Facility

An air-tight, purpose-built structure described in the concrete option may be constructed such that it can provide highly effective personnel protection. While no structure can claim to be 100% effective against toxic gas ingress, a combination of the following can significantly reduce the likely impact to personnel:

- Building should be leak tight, with robust seals around potential leak points and no windows. Leak points should also be minimized, with limited wall and roof penetrations.
- A vestibule to help minimize air exchange with the outside and personnel enter and leave the structure.
- Designated interior SIP location (i.e., conference room or similar designated space) with separate air handling unit and sealed penetrations to main building volume. The air handling unit should condition the air for occupant comfort, but not have any fresh air make up.

- Automatic shutdown on air intake as well as a manual shutdown back-up. The system should trip into 100% circulation mode where the air handling system for the SIP is independent of the overall building air system.
- Slight fresh air flow into internal SIP room volume, with supplied air and escape masks for the maximum predicted occupancy.
- Toxic gas detection outside the building as well as inside the building in the door / vestibule area. Additionally, internal room SIP should have gas detection that alerts when that location approaches the predefined uninhabitable threshold, providing occupants time to implement the evacuation plan.
- A robust communication, training, and fall-back plan addressing an integrated emergency response that covers both sheltering and eventual evacuation if the building becomes a lethally toxic environment.

For a purpose-built structure meeting these minimum requirements, a case may be made that both the retrofitted BRM and the stick-built concrete structure are designed for safe occupancy at the given location based on the criteria and requirements of API RP 752/753. However, at this point, the internal or external consequence modeler should consider progressing the analysis to a risk-based facility siting analysis to determine the risk profile for building occupants. There are two reasons for this: first, to bring in the frequency of MCE events as well as the average exposed population, and second, to determine relative risk reduction vs. cost increase for the available structural options.

For this case study example, a hypothetical risk profile comparison for the four options considered is shown in **Figure *6***. From a review of hazards on a consequence basis, the wood trailer and standard BRM do not appear to be viable options for the desired building location. However, both the retrofitted BRM and the stick-built concrete options would meet the corporate risk criteria. With either construction type a viable option, a cost analysis (***Figure** 7*) can provide further feedback and guidance on which option to select for construction.

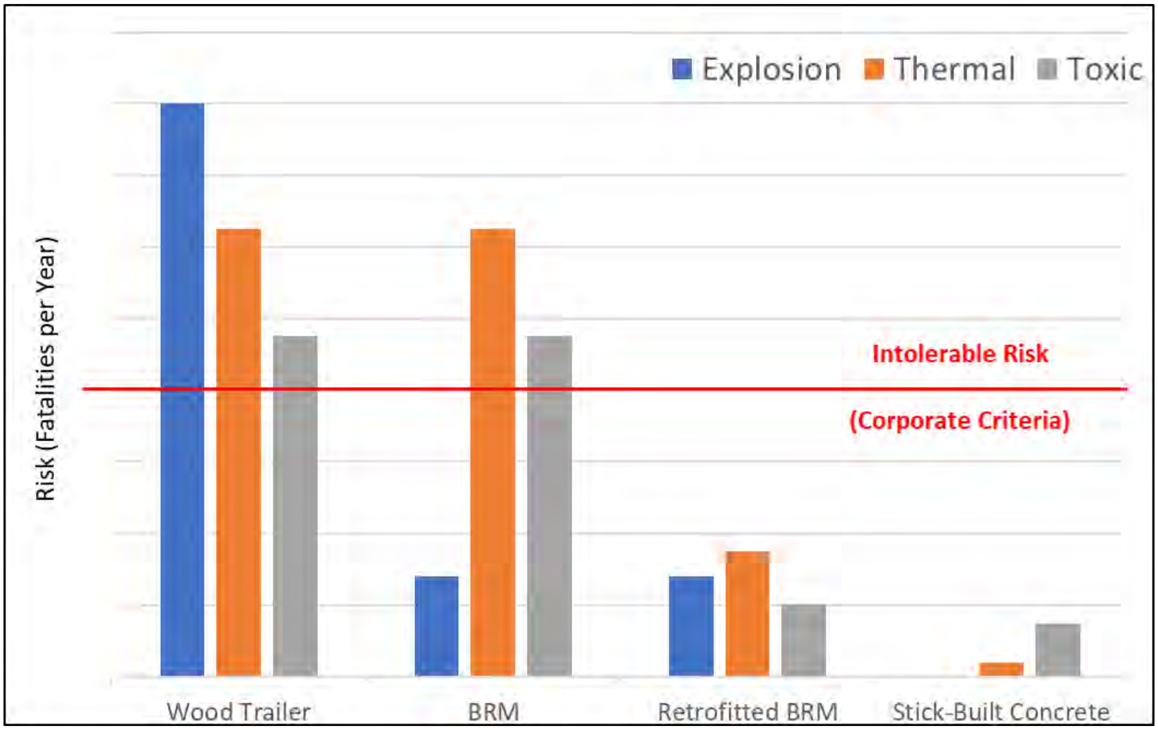


Figure 6. Risk for Each Option Considered

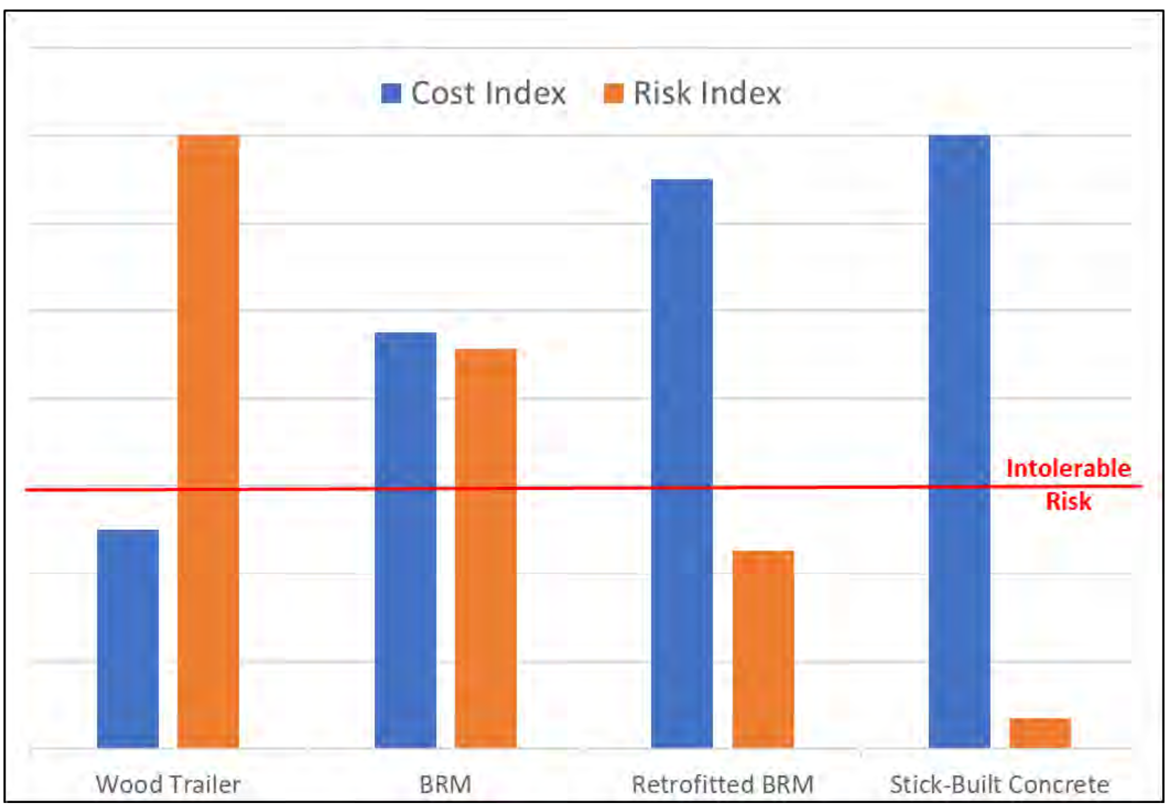


Figure 7. Cost and Risk Indices for Each Option Considered

With either the retrofitted BRM or stick-built concrete structure viable options, it becomes a business decision on which to select. In this example, a minimal increase in cost results in a significant reduction in the overall risk profile. The increased risk protection provides flexibility for future business decisions such as adding hazardous assets (i.e., increasing the frequency of exposure) as well as adding future occupancy. It is important to remember that protection systems require maintenance and upkeep, or they lose the ability to provide protection. It is, therefore, preferable to choose construction types that provide the necessary protection with the lowest level of required maintenance.

Conclusion

Cognitive biases are essential for humans to quickly process the world around us. Through the mental simplification process, both individuals as well as groups often put aside our objective and logical selves in favor of the information that reinforces our beliefs and recent history. Due in part to cognitive biases in combination with the ease at which high impact VCEs can be called to mind, the author proposes that there is a tendency in process safety to focus on blast hazards and occupant exposure when conducting facility siting.

The case study in this paper is an example of the potential consequences of this shortcut in mental calculations, which would have resulted in an increased exposure to thermal and toxic hazards due to the available of a blast resistant structure. To limit the impact of cognitive biases on individuals and teams, care must be taken in the facility siting MOC process to follow a standard procedure designed to limit the effect of mental shortcuts on decision making for safety. Once the full consequence and risk profiles are available, business decisions can be made that balance exposure with cost implications.

References

American Petroleum Institute, 2007. *Management of Hazards Associated with Location of Process Plant Portable Buildings,* Washington DC: API.

American Petroleum Institute, 2009. *Management of Hazards Associated with Process Plant Permanent Buildings,* Washington DC: API.

Baker, Q. a. B. R., 2011. Revisions to API RP-752 for Siting of Permanent Buildings. *BIC Magazine*, March, p. 97.

Cherry, K., 2019. *How Cognitive Biases Influence How You Think and Act.* [Online] Available at: https://www.verywellmind.com/what-is-a-cognitive-bias-2794963 [Accessed 23 August 2019].

Fitzgerald, G., Accessed August 2019. *Evaluation and Compliance with Faiclity Siting Regulations in the US,* San Antonio, TX: ABS Group.

Maitland, G., 2015. *Instituite of Chemical Engineers (IChemE) Blog.* [Online]
Available at: https://ichemeblog.org/2015/05/15/the-wisdom-of-trevor-kletz-the-founding-father-of-inherent-safety-day-353/
[Accessed 23 August 2019].

Psychology Resource and Reference, 2019. *Availability Heuristic Definition.* [Online]
Available at: http://psychology.iresearchnet.com/social-psychology/social-cognition/availability-heuristic/
[Accessed 23 August 2019].

Safety+Health: The Official magazine of the NSC Congress & Expo, 2015. *10 years after BP Texas City explosion, CSB and OSHA say more must be done.* [Online]
Available at: https://www.safetyandhealthmagazine.com/articles/print/12077-years-after-bp-texas-city-explosion-csb-and-osha-say-more-must-be-done
[Accessed 19 08 2019].

U.S. Chemical Safety and Hazard Investigation Board, 2007. *API R2 Text of Recommendation.* [Online]
Available at: https://www.csb.gov/assets/recommendation/api_r2_text_of_recommendation.pdf
[Accessed 19 August 2019].

Union Carbide Corporation, 2018. *Bhopal Gas Tragedy Information.* [Online]
Available at: http://www.bhopal.com/
[Accessed 30 August 2019].

Wikipedia, 2019. *Texas City Refinery Explosion.* [Online]
Available at:
https://en.wikipedia.org/w/index.php?title=Special:CiteThisPage&page=Texas_City_Refinery_explosion&id=903176231
[Accessed 19 August 2019].

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

The Importance of Misalignment to Reduce Risk and Prevent Disasters

Mark Galley*
ThinkReliability
Pearland, Texas 77584, USA (Houston)
*Presenter E-mail: mark.galley@thinkreliability.com

Abstract

Large incidents are a combination of different factors. Any of those factors on their own would not have produced the incident, but together can be catastrophic. This unfortunate alignment is the nature of all disasters. Understanding how each piece came together to produce that incident provides important insight for reducing risk and preventing future incidents from occurring. Some organizations within the energy, aviation and healthcare industries cite James Reason's Swiss cheese model of accident causation to explain this confluence of events. The holes in each slice align just right for the incident to occur. Moving just one of the slices can prevent a negative outcome. If more than one slice is misaligned, the risk can be made even lower. This is also known as defense in depth and layers of protection—approaches used across high-risk industries.

The straight-line slices of cheese overlook the important interconnections within complex issues. An incident consists of multiple cause-and-effect relationships that all come together in a particular way. Digging into these causes provides opportunities to misalign an incident, reducing the risk of the system in the future. Highly reliable organizations dissect their operations to pinpoint where simple verifications and checks can make the likelihood of an incident significantly lower.

This presentation uses a few historical disasters, including the 2005 Texas City refinery explosion, to explain how a complex incident can be analyzed starting with just a few basic cause-and-effect relationships. That simple analysis can then be expanded into a much more detailed explanation revealing how simple miscommunications like shift change, were causally related to the disaster. Changing one item would have changed that incident. Improving the way people communicate details within an incident improves the way they mitigate risk and prevent incidents going forward.
Keywords: Incident Investigation, Risk Management, Risk Assessment, Process Safety Information and Knowledge, Operational Integrity, Human Factors and Errors

1 Introduction

The way problems are explained affects the way they're solved. An accurate and thorough representation of an issue is essential for understanding the different ways risk can be reduced. There can be disconnects in the way people discuss problems depending on the tool or model people use. These miscommunications can distort the analysis and obscure the solutions. Avoiding communication roadblocks doesn't require adding another tool, but rather going back to the basics—a first principles approach.

2 Right-Answer Versus System Problems

From our earliest school years, we learn that solving problems is about finding the right answer. Twelve or more years in school focused on providing the right answer on homework, tests and college entrance exams has an effect—it creates a bias for the one, right answer. That right-answer approach from school becomes our default model for all problems. It reinforces the idea that there is a silver bullet, cure-all, panacea or root cause to solve whatever the problem might be.

But there are two fundamentally different types of problems with your operation. There are *right-answer problems* that have one answer and there are *system problems* that have a range of different solutions. Many of the daily problems people encounter in their jobs have one right answer. In these cases, the right-answer approach works well. How many people were on the crew? What's the volume of the tank? What's the flash point of that product? What is the planned start date? Which valves need to be closed to isolate this system? All these questions have a one right answer.

System problems, on the other hand, don't have a right-answer. A system problems naturally break down into parts. Because they're multifaceted there is a range of solutions. Different people working on the same problem can propose completely different ways to solve it. Solutions to a system problem vary by complexity as well as effectiveness. Some solutions are better than others. There are also trade-offs and constraints. Sometimes a high risk, potentially catastrophic problem can have a solution that is simple, yet extremely effective.

Just as risk and reliability are probabilistic, system problems are too. The concepts of a cumulative reduction in risk, layers of protection and defense in depth are based on the *degree* to which the probability and consequence can be lowered. Like the concept of six-sigma, preventing a system problem is also a matter of degree. There's not one right answer. Safety within a company, whether it's for personnel or process, strives for zero incidents by making the risk extremely low. Operations and equipment issues are system problems—as are all issues related to human performance and human error. Improving training and procedures to prevent errors also has a spectrum of solutions, instead of a right answer.

Distinguishing between right-answer and system problems is important because the approach and language for solving them is different. Right-answer problems have one right answer. The words *right* and *wrong* apply. This question, "What is 3 x 5?," has one answer: 15. Someone may believe it's 18, but their answer is wrong. It's appropriate discuss these types of problems in terms of right and wrong.

Questions like, "Why did the equipment fail?," "Why did the tank overfill?," and "Why did that injury occur?" require some digging. There is not one answer to those questions. The explanation of why something happened naturally uncovers more and more questions. The same question may be answered differently by different people. Each person may explain a different part of the overall problem since they see the incident from their different points of view. Engineering, operations and maintenance don't see problems the same way, but that doesn't mean there's necessarily a conflict either. With a system problem, different people can provide different answers to the same question, yet both can be telling the truth. This point is demonstrated in the case studies in this paper (see Section 6).

3 How the Search for the Root Cause Distorts Problems

One of the most common mistakes people make when investigating a problem is trying to apply right-answer thinking to a system problem. This right-answer bias leads people to mistakenly attribute an incident to a special cause, commonly referred to as the "root cause." A root cause is usually defined as the one factor that if removed would have prevented the incident from occurring. This model assumes that some causes are more important than other causes. The less important causes, those that cannot produce the issue on their own, are known as contributing factors. In this model, the identification of the root cause is key to eliminating the problem.

This mental model is appealing to those who think in terms of right-answer, but it is evidence of how people are biased to their own points of view. People select and emphasize the information that supports their agenda and ignore what doesn't. For an incident to have occurred, every cause of that incident had to happen. The fire triangle is one example of this. Changing any one of the causes changes the incident. Those who believe a root cause is a special type of cause, use the same argument: if the root cause wouldn't have occurred the incident never would have happened. This point may be true. But right-answer thinkers fail to recognize that same point applies to all the other causes of the incident in the same way. When a right-answer thinker tests one of the causes, they can mistakenly conclude that they're right without testing other causes. Their argument for that cause is accurate, valid and true, but it is not "right." It's not the cause. It's one of the causes. This is a known as confirmation bias. People test their root cause to confirm they're correct. If they tested their argument on any of the other causes, they would notice each of those causes satisfies the same argument. This is confirmation bias because people only test their preferred cause to confirm they are correct. It reflects how strong right-answer bias can be.

These are perceived less important causes are typically labelled as contributing causes or secondary causes and may not even be considered for solutions. By differentiating causes organizations can be missing opportunities to find better solutions. Focusing only on root causes artificially restricts the analysis, thereby limiting the set of available solutions. Ideas and insights from others can inadvertently be stifled if the group is mandated to focus only on the important causes – the root causes. Another unfortunate characteristic of root cause logic is it inadvertently aligns with a blame mentality. By looking for just one cause, blamers want to know the person or group who caused the problem. They don't want to look at the system. Blamers want to know the person or group responsible. The right-answer model of root cause analysis often mistakenly reinforces the language of blame.

Understanding that the root is a system of causes that branch out in different causal paths, all of which had to occur to produce the incident, provides an accurate and thorough explanation of an incident. The concept of conducting a root cause analysis to identify that system is based on simple cause-and-effect, and so is the Swiss cheese model.

4 How the Slices of Swiss Cheese Align

The Swiss cheese model (see Figure 1) of accident causation developed by James Reason provides an easy way to visualize how multiple breakdowns result in a problem. The Swiss cheese model has become popular across industries from refining to healthcare. It provides a conceptual framework that a problem is consists of multiple factors that all came together and aligned in the right way to produce the unwanted incident. Reason uses latent and active failures. He says the latent failures are built into the system, whereas the active failures are behaviors of individuals.

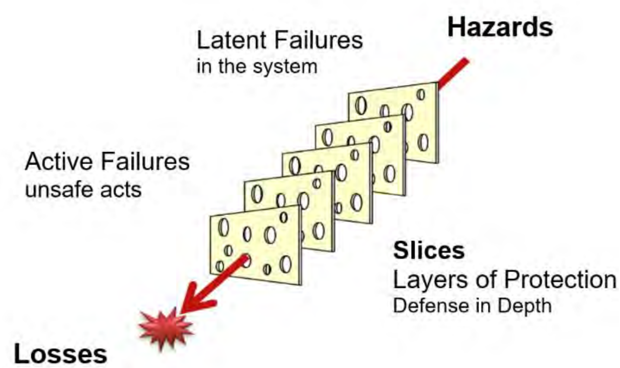


Figure 1 – James Reason's Swiss cheese model

Within the model, each slice of cheese is meant to represent an organizational defense. The holes in a slice are weaknesses where the defense can be breached. The model demonstrates that organizations put systems and processes in place that are designed to prevent a problem. When all the slices align in such a way that there's straight line passing all the way through the negative event happens. All the breakdowns are required.

The point is multiple items must align for the incident to happen. Meaning, if we misaligned just one slice the problem is avoided. Misaligning more than one slice makes the likelihood of occurrence even lower. This is the layers of protection logic that helps reduce risk in many organizations.

When a problem does occur, an investigation identifies all the different slices–the systems that broke down. For the incident to have occurred, all the slices had to align in a particular way. In retrospect, it can seem incredible how everything came together the way it did. But they had to come together in that specific way, or the incident wouldn't have happened.

What people sometimes don't realize about their organization is that multiple slices are aligning every day. Every day 2 of 5, 3 of 5 or 4 of 5 slices are lining up, but because they don't all align, there hasn't been a major problem. Everything within the company's operations look fine because there are not big problems, but there are several little problems occurring. These little problems may be considered minor because they have low consequences. But in reality, these low consequence items are essential pieces of the large problems that haven't happened yet. Improving the way an organization works the seemingly small, low consequence items lowers the risk of larger incidents. Concerns like, "Why are we even spending time on this issue, nothing happened," may happen. We're spending time on it because there's an inherent value of prevention.

This point of misaligning one slice isn't a unique insight, it's simply the nature of cause-and-effect. It is the same lesson for root cause analysis logic. All the causes must happen for the incident to occur. Changing or misaligning any one of the slices changes the issue. The lesson from the Swiss cheese model is a lesson in basic cause-and-effect.

Because the individual slices of Swiss cheese are always shown in a straight line, it leads people to believe that the breakdowns are linear. Because the model is linear people often conclude the incident is linear. Incidents, also known as a system problems, are nonlinear. The incident is nonlinear, but the cause-and-effect relationships between the different breakdowns (slices) can be linear or nonlinear. The Swiss cheese model provides no information about the cause-and-effect relationships within the incident. Conceptually, the lesson of misalignment within the Swiss Cheese model is valuable and it works well to introduce the idea. But the Swiss cheese model ignores important cause-and-effect relationships within the incident that are essential for revealing different options to lower risk. A problem analysis starts linearly, but it expands to be nonlinear in order to provide a complete explanation of what happened.

Rather than considering the slices of Swiss cheese to be inadequate defences, they can simply be thought of as causes. This provides a more thorough explanation because it includes what Reason called "conditions." He differentiated between causes and conditions in his explanation of the Swiss cheese. The distinction between types of factors that produce an issue is not necessary. The active and latent factors are causes. One isn't more causally related to an incident than the other. The latent failures occur along the same causal path as active, but farther upstream. For example, how the equipment was designed occurred before how it was operated. One is not more or less important than the other because both are required for the incident to occur. The valuable insights people share using the Swiss cheese model regarding breakdowns and alignment are simply lessons of cause-and-effect.

Cause-and-effect is not a problem-solving technique, it's a fundamental principle of the different techniques. The repeatability requirement of science is simply producing the same effects with the same causes regardless of who performs the experiment. There is no secret method to explaining how or why something occurred. Cause-and-effect is how things work on the farm, in the mechanic's garage, in the refinery, in the hospital and at an airline. People who know a particular discipline, field or hobby well can describe the detailed cause-and-effect relationships within the function. Those who don't understand a task or process can't explain its causes and effects. To them, it just happens.

Cause-and-effect may seem too simple for complex problems. But it only seems simple because it's fundamental. Cause-and-effect applies equally to small, large, simple and complex problems in safety, operations, equipment and human performance. It's works the same for explaining why something went badly as it does for explaining why something went well. It doesn't change from incident to incident. The case studies below show how the analysis of a problem can begin basically, then expand as necessary. Cause-and-effect thinking *is* the critical thinking and troubleshooting skills that so many organizations aspire to develop among their team members.

Each of the case studies in this paper show how a bias for a right answer can inadvertently confuse the way people explain a problem. But these miscommunications have no bearing on the incident. They don't change the incident in any way. If an investigation remains focused on identifying cause-and-effect relationships supported with evidence, a complete explanation of the incident will emerge. The cause-and-effect analyses in these examples begin as simple linear 3-to 5-Whys. They then expand into as much detail as needed to thoroughly explain the issue. By taking a first principles approach, people's biases will be flushed out to provide a clear, accurate and thorough explanation of the issue.

6 Texas City Refinery Explosion 2005

On March 23, 2005, a massive explosion at the Texas City, Texas, refinery 40 miles southeast of Houston resulted in a catastrophic disaster with 15 fatalities and more than 180 injuries. A simple summary of the incident is that too much liquid was added to a tower resulting in a release to atmosphere that ignited.

The incident can be explained many ways. Some of the different points of view of why the disaster happened are:

- The level instrument on the tower displayed the wrong level. The instrument indicated a lower level of 9 feet and dropping. The 165-feet-tall tower should not have been filled above 10 feet. The liquid level in the tower ultimately reached 158 feet without operations realizing it. (Instrument)

- The valve on the bottom of the tower was in the closed position. The standard operating procedure (SOP) for startup of that system states that the bottom valve should be 50% open. That procedure was not followed. (Procedure)

- The experience of the control room operator was inadequate. During startup of this isomerization unit, a qualified operator must be on the board in the control room. In cases where a less experienced operator is on the board, a senior technical representative must accompany them. Due to an unplanned family emergency, the senior technician badged out of the facility at 10:47 a.m. The less experienced operator on the board continued with the startup. (Experience)

- The blowdown drum, D-20, that the overfill of the tower flowed into was vented to atmosphere. Once the large volume of liquid left the raffinate tower, it overwhelmed the capacity of the blowdown drum, which was vented out a stack instead of a flare that could have handled the excess flow more effectively. (Design)

- There was a miscommunication on shift change that morning. One of the day supervisors missed the shift change meeting after the night crew had already filled the bottom of the tower to the required level. The plan discussed in that meeting was to not add any more liquid to the tower. (Miscommunication)

Each one of the explanations above is accurate. But none of them are individually the right answer. None of them are *the root cause* of the issue. But all are causes. The next question to ask for each one of these arguments is, “Why?”

The cause-and-effect relationships in the five bullets need to be diagrammed. The last word in each of the bullets shows how that information would typically be labeled. Organizations frequently use broad terms to categorize an incident. The intent is to provide a simple summary of what happened, but it can oversimplify and distort the issue. A thorough explanation requires an incident to be broken down into parts.

Figure 2 a simple cause-and-effect analysis for the Texas City refinery disaster. This 1-Why is accurate, but it is not a complete explanation of the incident. There are many cause-and-effect relationships that need to be added.

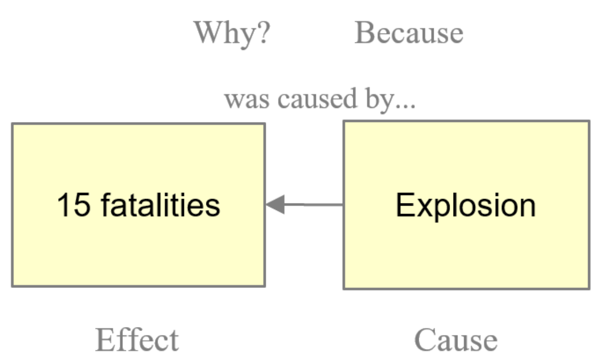


Figure 2 – A 1-Why analysis of the Texas City refinery explosion investigation.

Here's a 5-Why for the first bulleted item–instrument failure (Figure 2). This cause-and-effect analysis is linear.

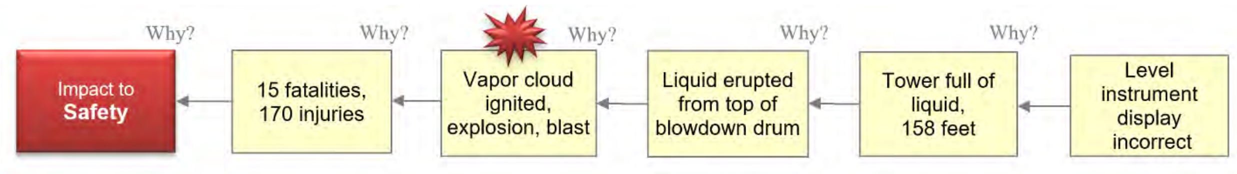


Figure 2 – An accurate, 5-Why to begin the Texas City refinery explosion investigation.

But the different perspectives listed in the bullet points allow for multiple 5-Whys. See the different 5-Whys in Figure 3 below.

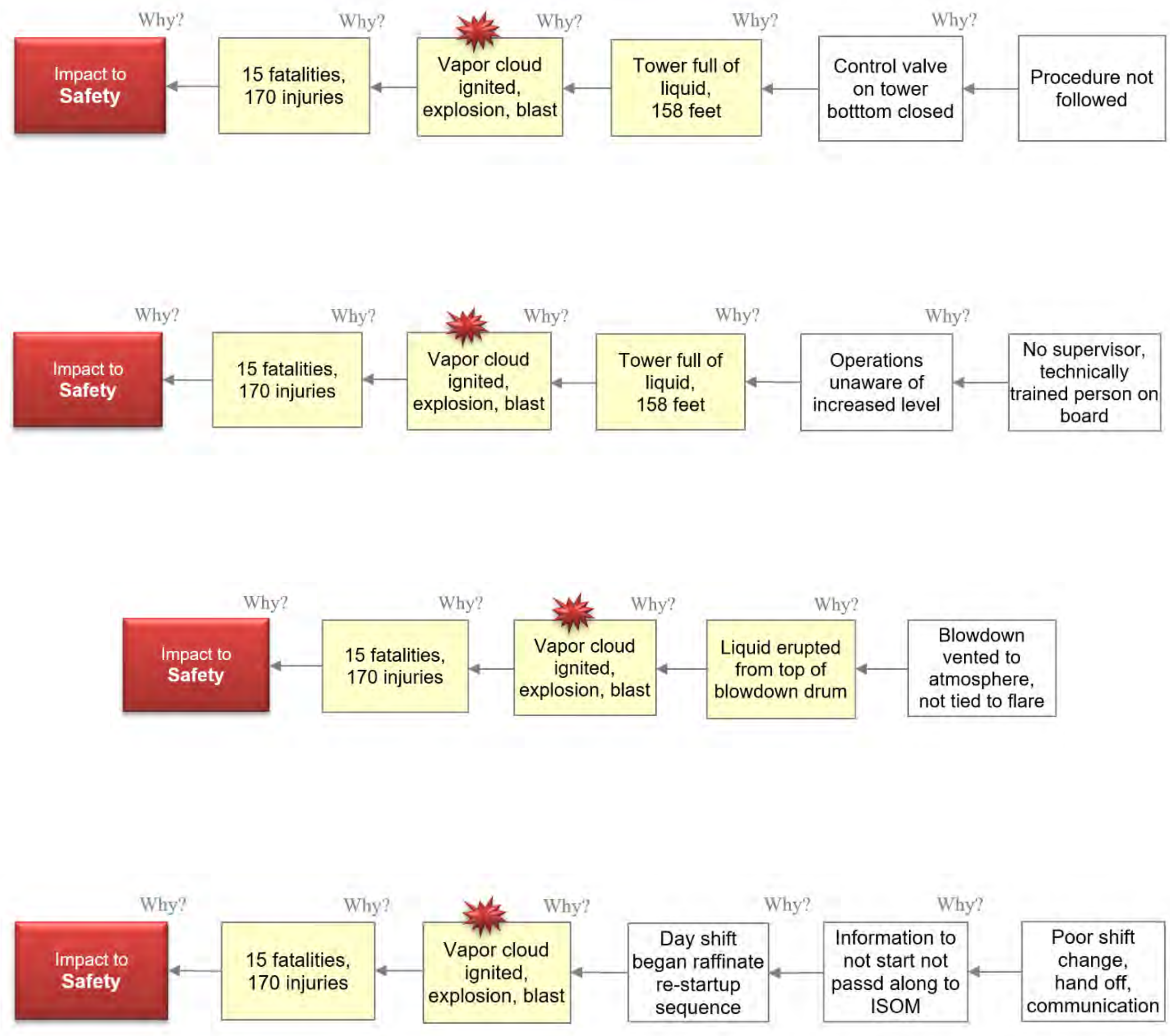


Figure 3 – Different 5-Whys. Each is accurate and can be used to start the investigation.

The 17-Why below (See Figure 4) shows how the five different linear analyses can combine into one more complete explanation with parallel cause-and-effect relationships. This is the nonlinear nature of incidents that the Swiss cheese model doesn't reflect.

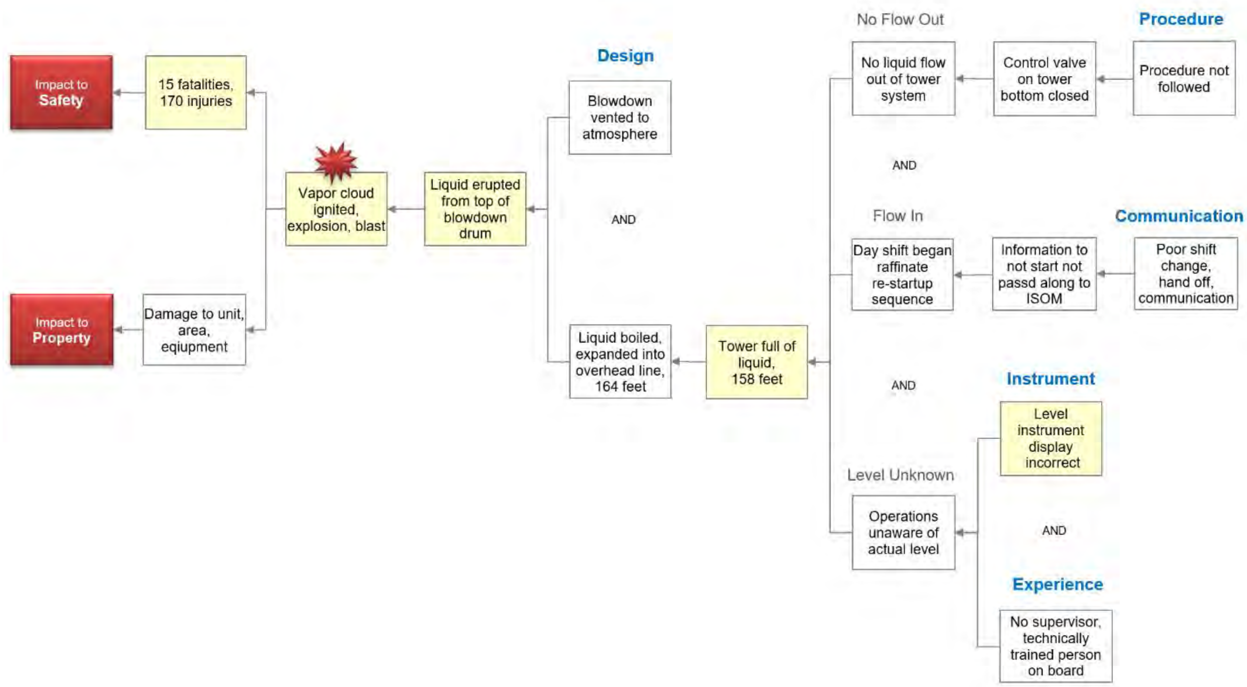


Figure 4 – The 17-Why shows how multiple 5-Whys can combine into one analysis.

All the causes in this analysis had to occur for this incident to happen. This is analogous to the multi-layered breakdowns of the Swiss cheese model that all must align for the negative outcome to occur. Each causal path in the diagram reveals an independent, linear chain of events that results in the loss of life and impact to property. Reviewing a single path can make it seem as though that path alone caused the incident. People usually believe their particular linear explanation is the right one. This is the flaw in linear, right-answer, root cause thinking. All the different paths are the root of this incident.

The Texas City disaster is shown below as a 125-Why (included in Figure 5 to show how the structure develops). An incident contains all its causes. The investigation can reveal a 1-Why, 5-Why, 17-Why or more Whys. The level of detail depends on how much the organization wants to know about the incident. Executive summaries show one level of an investigation, but they can exclude important details. The intent of root cause analysis is to dig into those details to an appropriate level to find the best solutions.

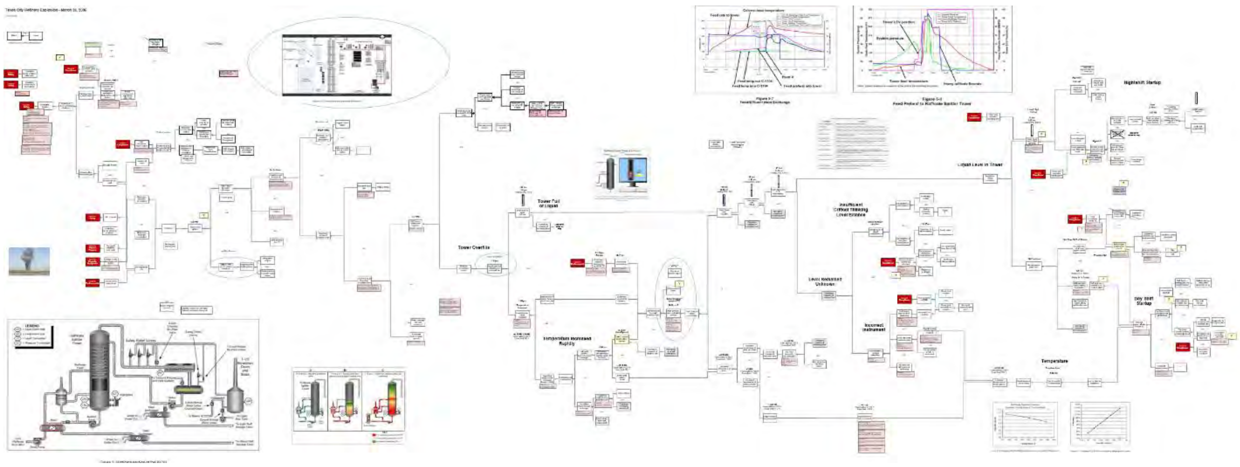


Figure 5 – The structure of the expanded 125-Why Texas City refinery explosion investigation.

Making a cause-and-effect diagram improves the way people communicate the details of what they know. The right-answer bias of conventional root cause analysis becomes difficult to support with this diagram. Verbally, root cause logic seems to make sense, but visually, its flawed logic is easier to see. Controlling (or misaligning) any one of the causes reduces the risk of a similar incident occurring. By controlling multiple causes, the risk can be reduced significantly. This basic-to-detailed approach of cause-and-effect analysis can be applied to any issue to improve communication and reduce risk.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Reverend Bayes, Meet Process Safety: Use Bayes' Theorem to establish site specific confidence in your LOPA calculation

Keith Brumbaugh, Dave Grattan*
10375 Richmond Ave. Suite 800
Houston, TX 77042
*Presenter E-mail: dave.grattan@aesolns.com

Abstract

The Process Industry has an established practice of crediting IPLs (Independent Protection Layers) to meet risk reduction targets as part of LOPA (Layer of Protection Analysis) studies. Often the risk targets are calculated to be on the order of 1E-4 per year or lower. Achieving the risk target on paper is one thing, but what is missing from the LOPA calculation is a statement of the confidence in the result. LOPA is an order-of-magnitude method, however, this only reflects the tolerance of error, not the tolerance of uncertainty. It is often stated that LOPA uses generic credits that are conservative, thereby implying the LOPA result should be conservative. By itself this statement is dubious because the generic data used in LOPA did not originate from the facility for which the statistical inferences are being made (which for frequentist-based statistics makes the inference invalid). Worse, when conservative credits are multiplied together to produce a rare-event number, does the conservative property emerge from the combination?

There is no way to answer this question without performing IPL Validation (i.e., ensuring the IPL will function when needed). However, IPL Validation and related Safety Life-cycle methods (e.g. functional safety assessments and cyber-security audits related to barrier integrity) are purely qualitative and have no apparent relation to the quantitative risk target. There is a need therefore, to bridge the qualitative results of IPL validation with the quantitative result of the associated LOPA calculation, as a way to establish a site-specific confidence level in the risk target we are trying to achieve.

This is where Bayes' Theorem comes in. Bayes' Theorem is an epistemological statement of knowledge, versus a statement of proportions and relative frequencies. It is therefore a method that can bridge qualitative knowledge with the rare-event numbers that are intended to represent that knowledge.

Bayes' Theorem is sorely missing from the toolbox of Process Safety practitioners. This paper will introduce Bayes' Theorem to the reader and discuss the reasons and applications for using

Bayes in Process Safety related to IPLs and LOPA. While intended to be introductory (to not discourage potential users), this paper will describe simple Excel^{TM} based Bayesian calculations that the practitioner can begin to use immediately to address issues such as uncertainty, establishing confidence intervals, properly evaluating LOPA gaps, and incorporating site specific data, all related to IPLs and barriers used to meet LOPA targets.

Keywords: Bayes' Theorem, IPL Validation, Uncertainty, Risk Analysis, Tolerance

Disclaimer

1 Introduction

If probability is a measure of uncertainty, then inference is used to make a statement of how accurate that probability is. Statistics is the tool by which we make inferences. Of course, an inference itself is subject to the same kind of analysis concerning its accuracy. And this is how we arrive at different kinds of statistics, namely, Frequentist and Bayesian.

That there exist different kinds of statistics may come as a surprise to many Process Safety practitioners, as most of us have never given much thought to the inferences implied in the numbers we use. We excel as Probability Calculators. This paper is asking you to become a Probability Thinker, which is much more important.

We use many numbers in Process Safety associated with predicting the likelihood of catastrophic events (e.g., failure rates, demand rates, incident rates, probability of failure, probability of ignition, etc.). Very rarely do we think about how good (i.e., trustworthy) the numbers are.

The LOPA calculation presents a unique case in statistical inference. It is neither practical nor ethical to determine rare event frequencies of catastrophic accidents by experiment [1]. Instead, the rare event frequency must be inferred. And it is actually worse than this, because several inferences must be made to arrive at the calculated LOPA number (i.e., each of the individual probabilities of failure are themselves an inference). And it is actually still worse than this, because the data I am using for the inferences are not from my plant. In this paper, I am interested in my own situation, not everyone else's.

This paper takes the position that Bayesian inference is the correct statistical tool to use for making process safety decisions regarding catastrophic rare events in my plant. It is the most consistent and rational method to update current beliefs about safe operation, as new data and evidence trickles in. It is the best we can do in a complex changing operating environment, where we can't afford to wait even 10 years to gather enough data to use Frequentist based methods.

There is one more question to answer before we get started. Does any of this matter? In other words, why do we need a different type of statistics to describe the rare event frequency? There is a simple answer. An inference on the LOPA number for a given rare event is one of the most (arguably *the* most) important Leading Indicator in your plant. On paper, calculated with generic data, the LOPA calculation is "*only the starting point"* (as someone once brilliantly but unwittingly said). Paired with Bayes' methods, the LOPA inference is *the best* plant-specific statement of how safely you are operating with respect to that potential hazard.

2 Frequentist vs. Bayesians. Why Process Safety Practitioners should be Bayesians.

Most of us reading this paper have been educated in Frequentist based statistics, learning concepts such as the Law of Large Numbers, Maximum Likelihood Estimate, hypothesis testing, etc. Frequentist based statistics assumes that the relative frequency of an event (i.e., how many times an event occurs over the sample space) is the same as the probability of the event occurring. Unfortunately, this assumption only applies to situations where many identical trials can be repeated (mathematically defined as infinity, but colloquially known as "in the long run"), with well-defined outcomes (think games of chance where the odds are known *in advance*), and where a "true" fixed parameter value can be assumed to exist in the population (e.g., average height of males versus females taking Calculus 101 for Fall 2019, at Texas A&M).

For reasons to be discussed, these concepts are not useful to the Process Safety practitioner attempting to quantify rare event frequencies. Ultimately this affects our ability to make good decisions regarding risk reduction allocation, as well as having confidence that we are truly operating safely. At a more basic level, Frequentist based statistics is the wrong math to use when making inferences about rare events that haven't happened yet in my plant.

First, a rare event is a one-off (i.e., a single-case probability). There is no meaningful interpretation of a rare event occurring many times in my plant "in the long run" (one event is too many). Second, in Process Safety, the odds of the rare event outcome are not known in advance. A common gimmick sometimes seen at trade shows is to roll several 10-sided dice ("LOPA dice") to make an analogy to the probability of all barriers failing (or being failed) at the same time. This is misleading, because in Process Safety we do not know *in advance* what dice we are gambling with! Third, the Frequentist concept of "identical" trials is not valid to Process Safety, because of the complexity of our systems (e.g., human and organizational) that change with time. Related to this is the Frequentist notion of a "true" or fixed parameter value (e.g., probability of failure, initiating event frequency, rare event frequency, etc.) describing the population. These parameters are not fixed (because over time the population changes). For example, there is not a "true" average probability of failure on demand for a safety interlock (because the systematic interactions of these safety interlocks are constantly in flux, resulting in the total PFD of the system never remaining constant, meaning you can never have a true fixed average). Process Safety parameters are not point values, they are random variables that change with time. Bayesian statistics provides the correct interpretation for this.

Contrast the Frequentist interpretation of probability to that of the Bayesians. Bayes' Theorem (also known as Bayes' Rule) provides the likelihood of occurrence for one-off events (e.g., the first roll of the dice with unknown bias, the next task, the next operation, the next demand). Bayes' probability is not defined by long-run averages. In Bayes' Rule, qualitative Knowledge (e.g., validation) of a process can be used to quantify the uncertainty of our assumptions about said process (e.g., the reliability of a barrier). It helps us quantify the odds of the safety dice *before* we throw them. The mechanism to do this is the Bayesian Prior. Bayes' Rule works with sparse data, treats parameters as random variables (not fixed point values), and provides a way to update a parameter as new evidence (data) is gathered (as opposed to waiting ad infinitum to pool enough data to make a valid Frequentist inference). Bayes' rule is also able to account for information that may not be showing up in your data.

I don't think there is much controversy is stating that Process Safety practitioners should be Bayesians. That said, a traditional Hardware Reliability person (e.g., Safety Instrumented System purists) may be resistant to accepting Bayesian thinking. I suppose if you could strip the human element from and focus purely on the hardware widget, if you could doggedly collect data on said widget from your plant over several decades, ignoring the fact that the samples separated in time may not be "identical" (a requirement of Frequentist methods), then eventually you could use Frequentist methods to calculate whatever parameter you need. However, this is *not* what you need. You need the parameter *now*. And this is just one parameter of many that you need to reliably infer the rare event frequency for your plant. Bayesian methods are the only logical and rational way to get there.

Another way to describe the difference between Frequentists and Bayesians is to look at what they mean when they use the word "Uncertainty" (a qualitative English word) [2].

To the Frequentist, uncertainty is due to the underlying randomness (i.e., aleatory) of a known but indeterminate outcome. Think of a gaming die, precision manufactured, with equal probability of landing on each of 6 sides (i.e., unbiased). When rolled with sufficient force in open space (a necessary qualifier because there are tricksters that can deterministically flip coins and roll die to a desired outcome), you don't know which side it will land on, but you know the odds in advance, or you could determine the odds by rolling the die unlimited times (assuming the edges of the die do not wear which would change the outcome). This interpretation has very limited application in process safety for the reasons discussed above.

To a Bayesian, uncertainty is associated with our degree of ignorance. The more we know about a process, the less uncertainty there is. Take the die example above. Instead of being handed an unopened package labelled "gaming die," say you found a die on the sidewalk leading to a Bingo gaming room, and you had no knowledge of its inherent bias. Further suppose you forgot to bring your lucky die with you, and so you needed to quickly and reliably estimate the bias of the die by rolling it a few times (think periodic proof-test) on the sidewalk, and that if you used a noticeably biased die in the game room, you would be thrown out (or worse). This, is Process Safety.

Figure 1 attempts to compare Frequentist and Bayesian interpretations of Uncertainty on a scale representing typical Process Safety systems and processes related to quantification of Barrier performance.

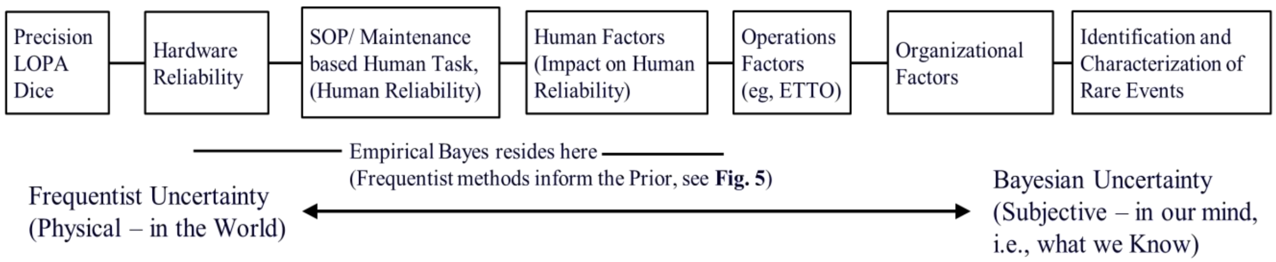


Figure 1. Frequentist vs. Bayesian Interpretation of Uncertainty related to systems and processes that affect parameters used to calculate Barrier performance. A significant part of Barrier performance resides in the Subjective Uncertainty portion of the scale. ETTO = Efficiency Thoroughness Trade-offs [3] (e.g., "unknown knows", i.e., things we should know but don't, or things we know but refuse to acknowledge may be a problem).

3 How Bayes' Rule works

Bayes' Theorem (also known as Bayes' Rule) is a simple formula for updating current beliefs based on new evidence (data, quantitative and qualitative) as it trickles in. Contrast this to Frequentist methods, which require a large pool of data all at once, to make a valid inference. Depending on the parameter of interest (e.g., initiating event frequency) this could take decades to collect enough data to be "statistically significant" (i.e., 95% confidence level), using Frequentist methods. (A corollary issue is how Frequentist methods update the "true" parameter value when new data/ evidence is collected. This is the Frequentist "magic" alluded to in **Fig. 2**.)

Knowledge is "belief justified." So when we talk about "beliefs" in this context, we are describing a degree of knowledge.

What are the "beliefs" we are trying to validate. Those related to LOPA include for example,

> "I believe the initiating event frequency is x."
>
> "I believe the probability of failure on demand is x."
>
> "I believe the frequency of this rare event occurring is x."

In each case the belief is typically the parameter of interest we are making an inference on. You could also call the belief the hypothesis.

The genius of Bayes' Rule comes in two ideas.

1. Use of a Prior probability (or probability distribution) representing our initial belief "prior to" the collection of evidence (data). Frequentists do not use a Prior.

2. Inference in the correct direction, that is, of the parameter given (that we know) the data. Frequentists make the opposite inference, that is, of the data given (that we know) the parameter. But we don't know the parameter, that is what we are trying to find!

Section 5 will develop these two ideas more fully.

Bayesian inference infers probability directly from data (via the Prior). Frequentist inference assumes the (long-run) relative frequency *is* probability. Firstly, a specific plant/ facility often doesn't have long-run frequency data related to process safety events (or, it would take decades to gather). Second, to make the assumption valid (i.e., that relative frequency *is* probability), complex techniques are needed, that often remain hidden to the user. Which leads to the potential for abuse of the methods. **Figure 2** shows this schematically.

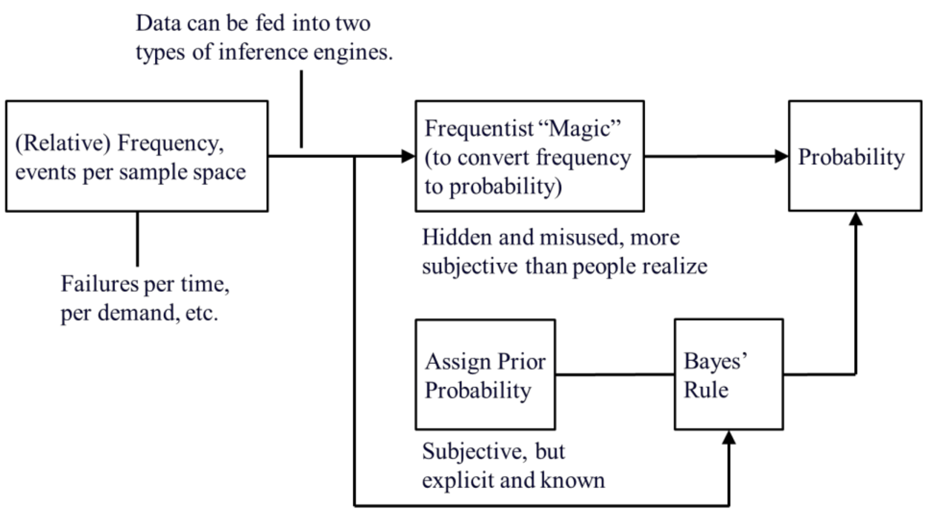


Figure 2. Bayesian inference is superior to Frequentist inference because it infers probability directly, versus Frequentist inference which requires tests and comparisons to hypothetical samples that may not be real. Because of the hidden complexity, Frequentist methods are open to abuse, as recently cited by the American Statistical Association [4].

A theorem is a mathematical statement that has been proven to be true. The mechanics of computing probabilities using Bayes' Theorem are described in **Figures 3 and 4** [5].

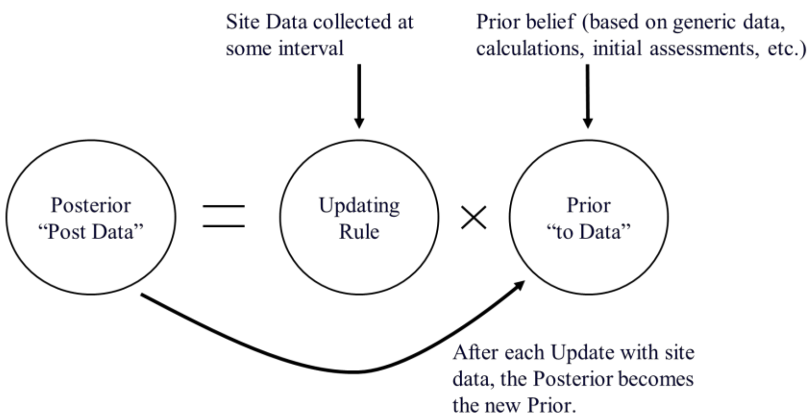


Figure 3. A Bayesian engine in simplified form. Prior belief is the starting point typically based on calculations using generic data and initial audits and assessments. As the Bayes engine runs, the confidence in the Posterior result increases. The Posterior is an inference on the future, i.e., between the Prior and the next update.

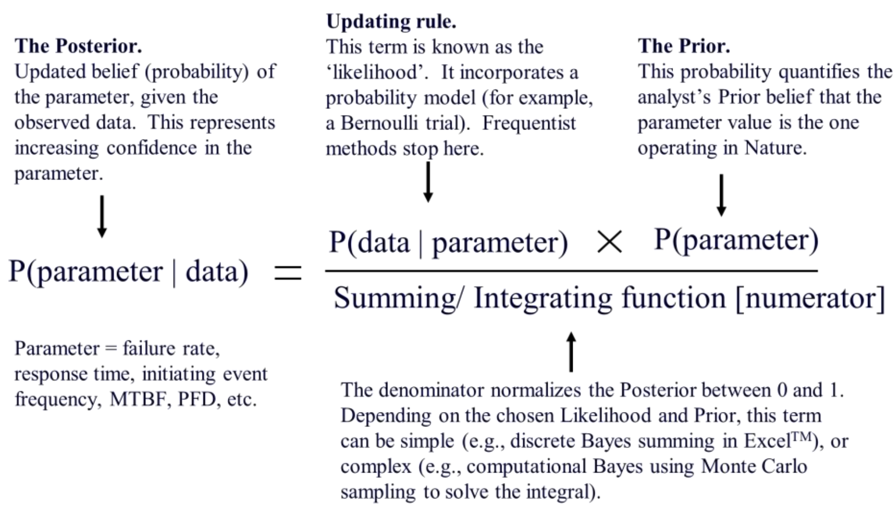


Figure 4. Bayes' Rule. Bayes' Rule works with both probabilities or probability distributions. Frequentist methods stop at the Likelihood term and then subject it to a "p-value" test *on the data* assuming the parameter is true. This is the opposite inference we need. Calculating the value of the denominator determines the complexity of implementing Bayes, ranging from Excel^{TM} based discrete methods, to Markov Chain Monte Carlo (MCMC) computational methods.

4 Process Safety, Bayes, and the Problem of Induction

Little is known about Thomas Bayes. He was a Presbyterian minister trained in theology and mathematics at the University of Edinburgh. As a Presbyterian, he was an English Dissenter (from the Church of England) and as such faced persecution. His intertwining of theology and mathematics to answer big theological questions based in mathematics such as, "what is the conditional probability Jesus rose from the dead given eyewitness testimony?" helped lead him to his famous rule, which was published a few years after his death (c. 1761). [6]

Although Bayes never could definitively prove that "God exists," or that "Jesus rose from the dead," Bayes' rule was seen at the time (and today) as a credible challenge to answer David Hume's famous Problem of Induction (i.e., the Future is only knowable when it occurs, at which time it has already become the Past). The Problem of Induction even today is still unsolved. Bayes' Posterior is an attempt to glimpse the Future. Frequentist methods have no ability to do this, relying solely on looking at the Past (data).

A lot of Process Safety practice involves trying to glimpse the Future. Think about *Leading* Indicators. They are not intended to be backward looking (we already know the Past), rather what we need is an indication of where we are today and where we are headed tomorrow. In this way too, Leading Indicators are an answer to the Problem of Induction.

Similarly, the probabilistic calculations we make to infer a rare event frequency are meant to be forward looking. What good would it be to make a statement only on the Past (data)? We care about tomorrow. Don't confuse inductive inference as being a prediction. It is a statement of how trustworthy a prediction is.

All that said, the Bayesian Prior is a key component to making the inference.

Diaconis and Skyrms say it best [7],

> "…if you were going to risk a lot on the next few trials, it would be prudent for you to devote some thought to putting whatever you Know into your Prior."

For process safety, the next "few trials" is referring to the next "day's" Operation, task, or demand on a safety critical function. And this is the basis of Empirical Bayes. Using Frequentist methods to inform the Bayesian Prior. **Figure 5** shows this graphically.

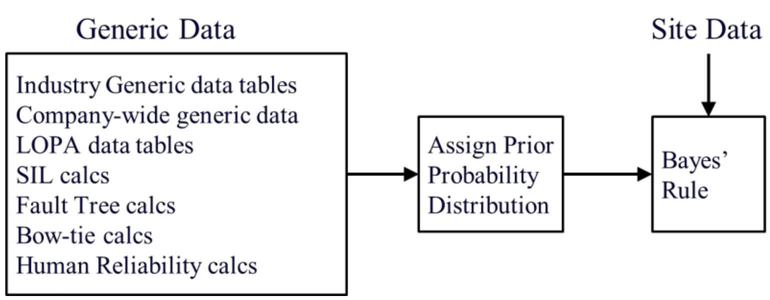


Figure 5. Empirical Bayes. The front-end engineering work becomes an important part of selecting the Prior Uncertainty distribution. Depending on the site data update rate for the function, task or operation (i.e., of the inferred parameter), the Prior can dominate for years, or be quickly over-taken by the updates.

5 How to Think like a Bayesian

Human beings are not good probability calculators. We have not evolved a probability sense organ. And our use of heuristics (mental short-cuts and other rules-of-thumb applied incorrectly) results in systematic bias when making probabilistic estimates. The Literature is replete with examples [8, 9]. The judgements we make in **Figure 7** are susceptible to the same.

Humans are good at collecting relative frequency data on the past (e.g., this event occurred 5 times out of 20). Converting this to a probability of occurrence for the next trial (i.e., the 21^{st}) is what Bayes' rule does [10].

Bayes' rule uses two concepts that can help Process Safety practitioners become better Probability Thinkers, apart from using the rule itself. They are:

1. Making sure you're using conditional probability, *in the correct direction*.
2. Don't neglect the Prior, also known as the Base Rate.

Figure 4 shows that the concept of conditional probability is a key part of Bayes' rule. Further, **Figure 4** shows two conditional probabilities, in opposite directions. First thing to note is, the probabilities are not the same. It depends on what direction you are looking. Four examples will be given.

Example 1 is from Bayes' Rule itself.

P(data | parameter). "The probability of getting the data given that I know the parameter". This is the conditional probability used by Frequentists. It's in the wrong direction! You don't know the parameter, that is what you're trying to find! Also, Frequentists don't use a Prior, they neglect it.

Example 2 is from Pop Culture.

In Season 1 Episode 17 of the Cosby Show (1984), titled "Theo and the Joint," Cliff and Claire find a marijuana cigarette in one of Theo's text books from school. They get in a discussion of whether or not it is *his cigarette*, and being in *his* text book, Claire (the lawyer) is ready to convict. But she is getting her conditional probability wrong.

P(Joint being in Theo's text book | It's his Joint). This is the conditional probability Claire was calculating, notice, *assuming it's his joint*. This conditional probability is near 100%.

P(It's his Joint | Joint being in Theo's textbook). This is the conditional probability Claire should have been calculating. Which is much lower. As it turns out, it was not Theo's joint. A classmate had hidden it there when the teacher walked in the classroom. What Claire was also missing was the Prior (her belief before seeing the joint in Theo's text book, that Theo was a pot smoker).

This example is typical of many problems seen in the Justice System (answering the wrong conditional probability). Ref [11] gives several good examples.

Example 3 is from Process Safety. This one is notorious. Suppose I have a data trend that shows the number of incident or accidents, is trending down-ward. We are operating safer, right! Not so fast.

P(Data trend downward | We are operating safer). This is the conditional probability most people answer in this type of situation, which is in the wrong direction.

P(We are operating safer | Data trend downward). This is the correct conditional probability, and depends on many factors (e.g. the Prior being one), that may not be reflected in the data.

Example 4 is whimsical, but one of my favorite. Study **Figure 6**.

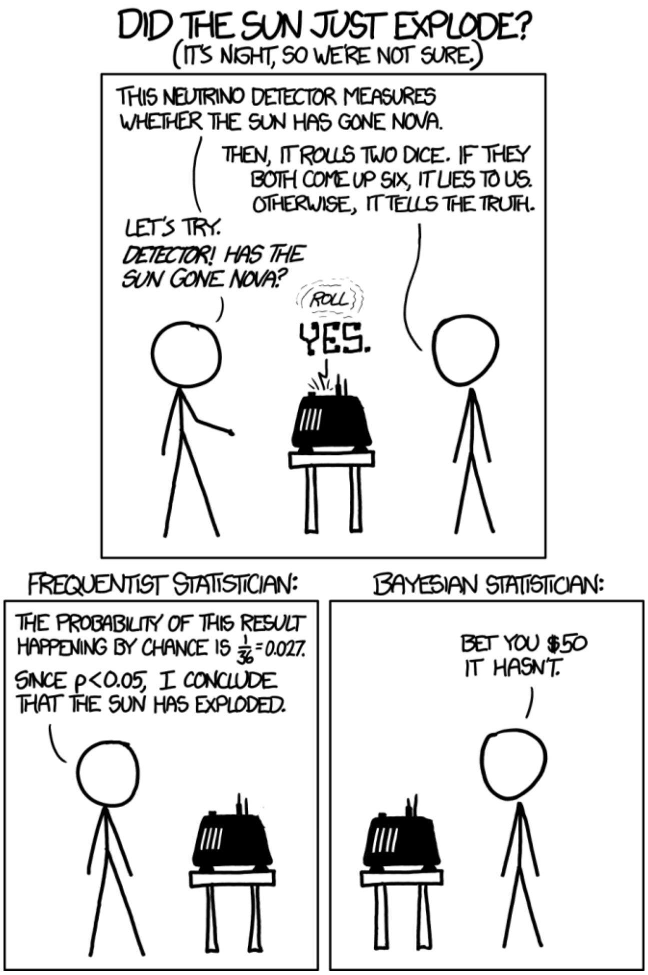


Figure 6. A Twist on the Sunrise Problem from Philosophy. Source: xkcd: A webcomic of romance,
sarcasm, math, and language. https://xkcd.com/1132/

P('getting' the data | the sun has exploded). Similar to **Example 1**.

P(the sun has exploded | the data). This is the conditional probability you want, and the Bayesian knows it! And again, accounting for the Prior (i.e., a billion+ previous sunrises) should not be neglected!

6 Converting Qualitative Knowledge (Subjective Belief) to a Prior Confidence Level

Figure 5 shows how it is possible to use quantitative Frequentist methods to inform the Prior distribution. This is possible, because the Frequentist methods themselves incorporate a statement of confidence. For example, SIL Calc standards (i.e., S84/ 61511) require a 70% single-sided confidence on the failure rate data used (i.e., 70% confident that the True value falls within the upper bound, i.e., equal to or lower than the value used). Of course, the problem with this is, the data is *generic*, it did not come from my plant. So with no further information, the actual confidence in the number (in my application) is *unknown*. Think about that! Enter the qualitative life-cycle methods (i.e., Validation, Assessments, audits, etc.).

But how do we convert purely qualitative Knowledge (i.e., from Validation, Assessments, audits, etc.) into a number that can inform the Prior distribution? That is the subject of this section.

Of all the content in this paper, this is the most subjective. From **Figure 1**, we are on the far right side of the scale, into Operational and Organizational factors for which there is no generic data tables to calculate a parameter (as a Prior). That said, there are factors (or multipliers) from Human Reliability science that can offer guidance to scale a parameter off of some base rate. See for example Refs [12, 13, 14, 15, 16]. Still, many operational and organizational factors don't have even a scaling rate, and therefore are purely qualitative.

The good news is the Bayesian Prior is completely transparent (see **Figure 2**), such that if you don't agree with my numbers, one, you know it, and two, you can come up with your own that you think are better. Conceptually what we are trying to do is shown in **Figure 7**.

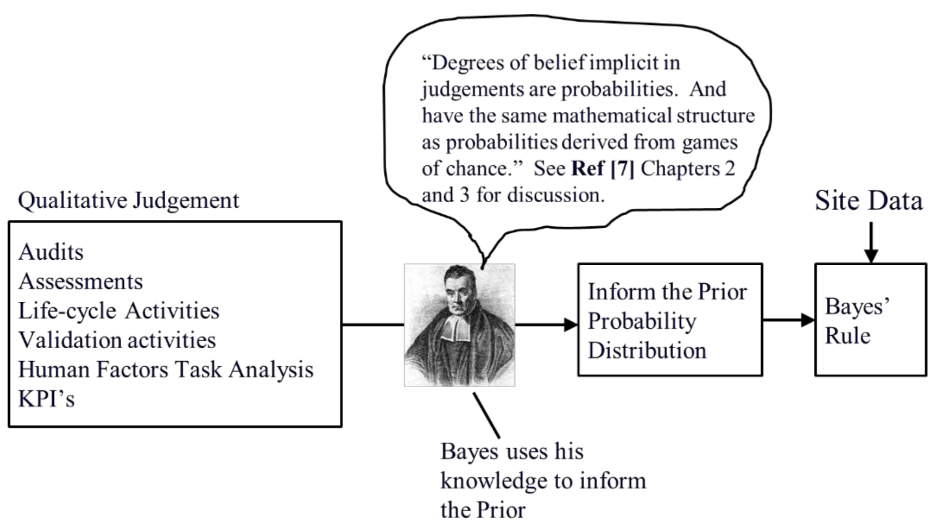


Figure 7. Converting Knowledge into a number is an exercise in Subjective Probability. Site data which is quantitative will soon dominate the Prior if the parameter you are making the inference on can be easily measured.

Frequentist Statistics says my confidence increases as the square root of 'n' times increase in the sample size, e.g., after 4 samples, my confidence level increases by a factor of 2 [9]. If each sample is a Bernoulli trial (success/ fail), by the 4th sample my confidence has gone from (for example) 50% to 75% (see **Figure 8**).

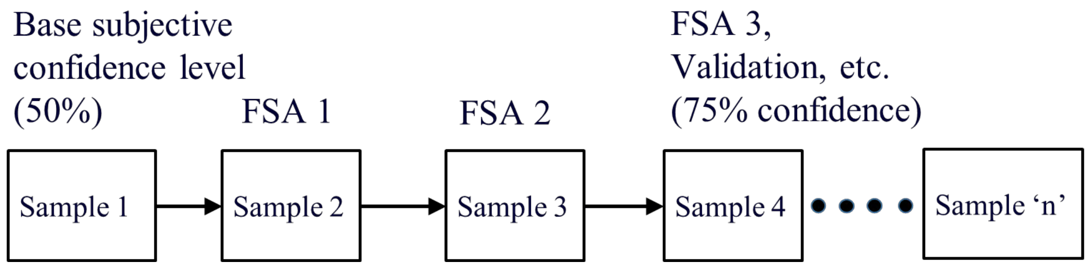


Figure 8. An attempt to quantify qualitative Knowledge. A 50% base confidence represents a site's attempt to meet industry best practices related to PSM including Barrier management, derived from lessons learned of high-profile catastrophic accidents. The number 50% is a purely subjective assignment of probability. It is meant to approximate the confidence in an average. If a site were missing a particular segment of best practice, the initial subjective confidence would be lower. Each sample represents an assessment or audit, increasing knowledge about the parameter of interest. After 4 samples I've reached 75% confidence in the parameter, this assuming each sample represents a Bernoulli trial (success/ fail). FSA = Functional Safety Assessment.

The caveat of **Figure 8** is the confidence is increasing for the "knowns" i.e., what you find during an assessment. The same square root of 'n' rule does not apply to "unknowns" i.e., what you're not sampling. Here, confidence increases much more slowly for the absence of findings. This is contributory to the Black Swan problem. For this reason, the Prior uncertainty distribution should always allow for unknowns. This is a qualitative judgement. There is no failure data that will contain information on a Black Swan event (until it happens, then it's too late!).

7 Bayes' Rule and LOPA Inference, an Overview.

Figure 9 and 10 show how we are and are not using the Bayes' engine to infer the population parameter. Recall from **Figure 4** the types of parameters we are interested in for LOPA. In each case, we are concerned with the "right tail" of the distribution, which corresponds to high initiating frequency, high probability of failure on demand, etc. We use a cumulative distribution to make a statement that we are equal to or less than a certain value (that corresponds to the confidence we want). In this way, we move decision making from "Pass/ Fail" (as is practiced today), to a degree of confidence. Think of the implications. The following list represents a potential FAIL of the risk target in each case. Decision making would be improved if we instead looked at how the confidence in the desired parameter value has been affected.

1. I'm off my risk target by a factor of 3.
   Bayes says: "We don't need to do anything because my confidence level at that increased factor hasn't changed."
2. My risk targets changed an order of magnitude more conservative.

Bayes says: "Before we go trigger a massive capital spend to close gaps, let's evaluate how the confidence in meeting the rare event freq. has changed for each scenario."

3. My generic SIL calc shows I have a residual gap.
   Bayes says: "Before I go spend money, I want site specific quantification of said gap. Assess and collect data over the year and run a Bayes' engine. Then make a decision"
4. My initiating frequency is higher than assumed in my calculation, but Operations is making changes to fix it.
   Bayes says: "Lower the confidence level in the (assumed) initiating event frequency and monitor next year's operation closely. Update Bayes' engine with new data and see where we are."
5. My Stage 4 FSA (functional safety assessment) found I can't test this safety function as often as I initially assumed.
   Bayes says: "Redo the SIL calc and input to the Prior. How has the confidence level in the target changed?"

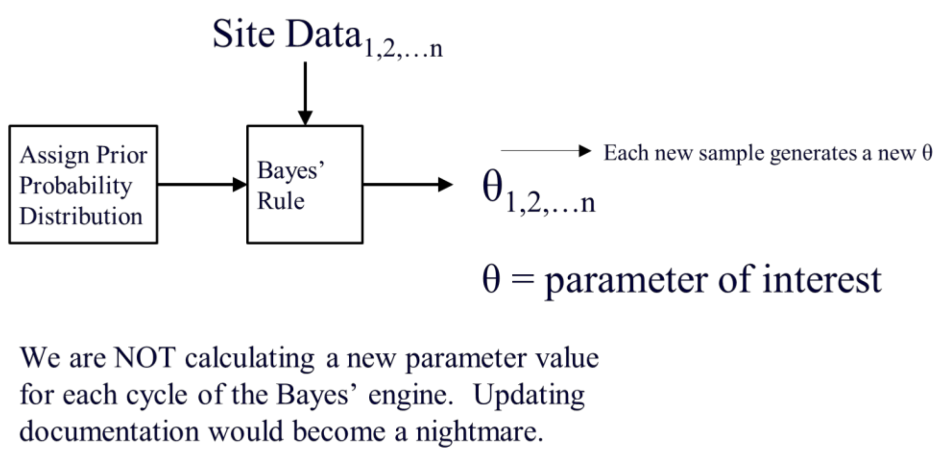


Figure 9. What we are NOT doing with Bayes (but you could do).

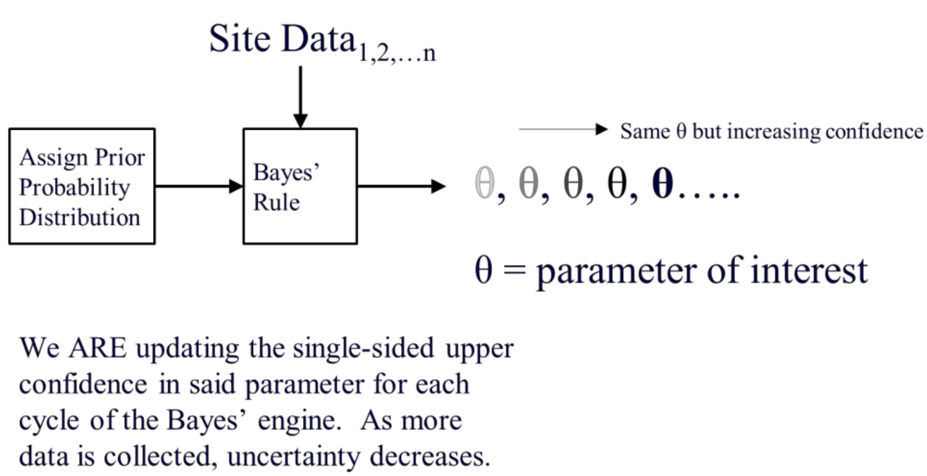


Figure 10. What we ARE doing with Bayes.

Figure 11 is intended to show the big picture of how all this would look. For each IPL (independent protection layer) as well as the initiating event frequency, a Bayes engine can be built to perform what we show in **Figure 10**. An obvious and easy place to begin is with inferring the initiating event frequency. Generic initiating event frequency data typically used in LOPA is wildly inaccurate in many cases. Often times initiating event rates are much greater than the generic 1/10 years. In other cases, certain demands have never been seen in the history of the plant. You may object by saying, "what's wrong with using a generic Frequentist based average?" Answer: because you can't demonstrate you are operating safely based on generic averages. Also, in each case, there are important qualitative insights to be derived from a closer quantitative look at the initiating event frequency. For example, for events happening more frequent than assumed, the risk is increased. Instead of say, once per 10 years, think of rolling the LOPA dice once per year instead (add in the element of unknown bias and the situation is worse). For a more rare initiating event, the qualitative take-away is operation's lack of actual practice with the event, decreased situation awareness, and decreased ability to respond when things don't go as planned (e.g., the automated trip doesn't activate).

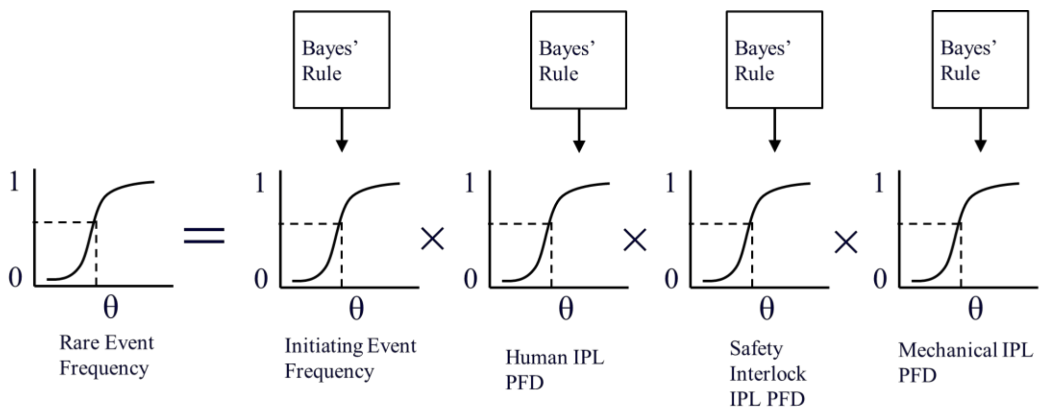


Figure 11. Putting it all together. Each parameter of the LOPA equation can be inferred using a Bayes' engine. The result is a cumulative distribution of the rare event frequency, from which the single-sided upper confidence limit in the LOPA target can be determined. This provides a better decision making tool than using a single point value with unknown confidence for the site application. As data is gathered and the Bayes' engines run, confidence in meeting the target will increase. Using Bayesian inference is the most consistent and rational way to incorporate site data to update our belief in meeting rare event targets. This method can be easily implemented in Excel™ (see **NUREG-6823** Chapter 6 for details).

8 Conclusion

Process Safety practitioners have the choice of using either Frequentist or Bayesian based inference methods. This paper has laid out the case for Bayes. Ultimately it is about making better decisions related to managing rare event scenarios. The Bayesian interpretation is where we start with a Prior informed by engineering design, assessments, and audits, and then update to a Posterior when periodic proof-tests, incident reports, continuing audits, etc. are evaluated, and is the only rational and consistent way to build confidence as a degree of belief that we are operating safely.

9 References

1. Hans Pasman and William Rogers, "How trustworthy are risk assessment results, and what can be done about the uncertainties they are plagued with?" Journal of Loss Prevention in the Process Industries, 55 (2018) 162-177.
2. Kristin Lennox, "All About that Bayes: Probability, Statistics, and the Quest to Quantify Uncertainty" https://www.youtube.com/watch?v=eDMGDhyDxuY
3. Hollnagel, E., Safety – I and Safety II The Past and Future of Safety Management, Ashgate, 2014.
4. Ronald L.Wasserstein, "ASA Statement on Statistical Significance and P-Values", The American Statistician, 70:2, 129-133
5. Ben Lambert, "A student's Guide to Bayesian Statistics", Sage Publishing, 2018.
6. Judea Pearl, "The Book of Why – The New Science of Cause and Effect", Basic Books, New York, 2018.
7. Persi Diaconis and Brian Skyrms, "Ten Great Ideas about Chance", Princeton University Press, 2018.
8. Daniel Kahneman, "Thinking Fast and Slow", Farrar, Straus & Giroux, New York, 2011.
9. Nassim Nicholas Taleb, "Fooled by Randomness – The Hidden Role of Chance in Life and in the Markets", Random House, New York, 2004.
10. James R. Henderson, "Bayesian Meets Frequentist: A Marriage Made in California", published in "Probability is the Very Guide of Life", Ed. Henry Kyburg. 2003.
11. Leonard Mlodinow, "The Drunkard's Walk – How Randomness Rules our Lives", Pantheon Books, New York, 2008.
12. Robert Taylor, "Human Error in Process Plant Design and Operations – A Practitioner's Guide", CRC Press, Taylor & Francis Group, Boca Raton, 2016.
13. Barry Kirwan, "A Guide to Practical Human Reliability Assessment", CRC Press, Taylor & Francis Group, Boca Raton, 1994.
14. Swain and Guttmann. NUREG/ CR – 1278. "Handbook of Human Reliability Analysis." 1983.
15. James Reason, "Organizational Accidents Revisited", CRC Press, 2016.
16. Institute for Energy Technology, "The Petro-HRA Guideline." Report IFE/HR/E-2017/001, 2017.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Confidence Level Assessment in Enterprise Risk Management: Case Study with Focus on Oil & Gas Operational Incidents

Henrique Martini Paula*, Magdalena Soto Ogaz*
ABS Group, Spring, TX
*Presenters' E-mails: hpaula@abs-group.com, msotoo@enap.cl

Abstract

Risk assessment and risk management are widely used in a variety of sectors and industries, particularly with the advent of Enterprise Risk Management (ERM) in the last two decades or so. Because it covers most types of risks and applies to most types and sizes of organizations, including private and Government, ERM has significantly expanded the application of risk concepts in the decision-making process worldwide. However, one aspect of risk assessment has not gained traction in practical applications. Specifically, although there are exceptions, typical ERM assessments and some other types of risk assessments do not include the evaluation of the confidence level associated with the risk estimates. This article presents a methodology for the assessment of the confidence level in ERMs with a case study that emphasizes operational incidents at Oil & Gas facilities. It also scrutinizes these risks with respect to risks of different nature considered in a typical ERM (corruption, less demand due to increased competition, lower earnings due to increased operational costs, inadequate insurance coverage etc.)

Keywords: Enterprise Risk Management, ERM, Confidence Level, Confidence Level Assessment, Girth Factor, Uncertainty, Cost Benefit, COSO, ISO 31010, Oil & Gas.

1.0 *Introduction*

The assessment of the confidence level in ERM has not gained traction in practical applications. In fact, although several mention the importance of considering and communicating the confidence in the determination of the level of risk, the major ERM standards do not offer methodologies for doing so (ISO 31000:2009(E) 2009) (ISO 31010-2009(E) 2009) (COSO 2004) (COSO 2012) (OMB 2016) (CFOC/PIC 2016) (Perera 2011). Decision makers may presume that the information given to them is all at the same level of confidence or may assume that it is all high confidence, unless the assessors provide indication otherwise.

This article presents the application of a methodology to evaluate confidence levels in ERM assessments, and it may be useful in other types of risk applications as well. The methodology has qualitative (H. M. Paula 2019a) and quantitative (H. M. Paula 2019b) parts. The qualitative evaluation may be all that is needed to account for the confidence level in some ERM efforts. The quantitative evaluation is based on the qualitative evaluation, and it provides additional insight to support and facilitate decision making.

The methodology adopts Johnson's definition of confidence level:

> *"The degree of certainty (assigned by the risk assessor) that the likelihood or severity scores reflect reality"* (Johnson 2008, ii)

In this article, the "assessor" is the analyst or a team of analysts who are leading the ERM study, and the "confidence assessment" should include the knowledge and experience of all who contributed to the evaluation. "Scores" can be point-estimates of the frequency or severity of a risk scenario. If the score comes from a risk matrix with logarithmic vertical and horizontal axes, the point estimate is typically the geometric mean[1] of the limits of the assessed category. This practice that goes back to at least the 1980s (Casada, Kirkman and Paula 1990).

There are a multitude of factors related to the confidence level, including several sources of "lack of confidence" and several control/mitigation measures to improve confidence in the risk results (H. M. Paula 2019a) (Johnson 2008). Some are directly associated with data and data relevance, which focus on the quantity and quality of the data. Others relate to the depth of analysis, including analysis methodology and model quality/fidelity. Several emphasize subject matter expertise (SME), e.g., specialist, expert judgments and subjectivism. Additionally, there is a fourth group of factors that has great influence in the level of confidence: assumptions. As shown in the next section, these four groupings of factors constitute the foundation of the methodology.

2.0 ***Step-by-step Procedures***

This section presents the six steps for conducting the confidence level assessment. It illustrates the application of the methodology with an analysis of eight risk scenarios (RSs) from a multi-national, integrated oil & gas (O&G) company. Table 1 presents the RSs, and Figure 1 shows them in the Company's risk matrix.[2, 3] The six steps are:

1. ***Identify and characterize the risk scenarios of interest.*** This involves a thorough understanding of the scenario's consequence types and severity because the frequency of a scenario depends on these definitions. For example, the frequency of a labor strike

[1] *The square root of the product of the two limit values.*
[2] These are some of the dominant risk scenarios for the Company. As typical in O&G ERM applications, there were hundreds of other risk scenarios for this company. We present only eight dominant risk scenarios to keep it simple, and they are enough to illustrate the methodology.
[3] All figures and tables are at the end of the article.

that lasts a few hours/days is typically different from the frequency of a strike that lasts weeks or months. To further illustrate this step, the next section describes three of the RSs related to operational incidents (RS1, RS5 and RS8) in more detail

2. ***Evaluate the <u>qualitative</u> confidence level for the <u>severity</u> and for the <u>frequency</u> associated with each risk scenario.*** For each scenario, consider the severity and frequency separately using the Paula-Guthrie (P-G) chart from Figure 2 or the extended P-G chart from Figure 3.[4] For the severity:[5]
    a. If the assessor has an estimate of the Girth Factor (GF),[6] the P-G chart provides a direct assessment of the level of confidence (e.g., **High** for GF = 10). In this case, the assessor can move straight to Item "f." Otherwise, go through Items b, c, d and e[7]
    b. Review the data strength and select a category (**Very Strong**, **Strong**, **Medium** etc.). The P-G chart provides guidance to make this selection, depending on the nature and amount of the available data. This is the <u>final category</u> assignation for the data strength
    c. Review the analytical strength and select an initial category (**Very Strong**, **Strong**, **Medium** etc.) without accounting for SME or depth of analysis. Note that the guidance for the selection of the analytical strength is less explicit than the guidance for the data strength. If in doubt, start by assigning the same category selected for the data strength, and then adjust, depending on the assessor's evaluation of the assumptions that are involved. This is the <u>initial category</u> for the analytical strength
    d. Still for the analytical strength, move the initial category none, one or two cells to the left, based on the benefits from relevant SME and/or relevant depth of analysis, as applicable. This is the <u>final category</u> assignation for the analytical strength
    e. Using the final category assignations for the data strength and analytical strength, use the P-G chart to select the confidence level for the severity (or frequency – see Item 2f)
    f. Repeat Steps 2a, 2b, 2c, 2d and 2e for the frequency

    Table 2 presents the results of Step 2 for the eight risk scenarios (fourth and seventh columns for the severity and frequency, respectively). For illustration of this step

[4] The P-G chart considers the four groupings of factors mentioned earlier. Two of them appear explicitly on the vertical axis (<u>data and data relevance</u> under data strength) and horizontal axis (<u>assumptions</u> under analytical strength). Data strength refers to the amount and nature of the data. Analytical strength refers to assumptions, including modeling assumptions and the assumptions about the relevance of the data. Because they are key to making and addressing assumptions, the P-G chart considers both "*<u>SME</u>*" and "*<u>depth of analysis</u>*" as modifiers to the analytical strength.

[5] The assessor can start with either the severity or the frequency evaluation. We find it more efficient to start with the severity because the frequency assessed value is often tied to the definition of the consequence, as mentioned in Step 1.

[6] The ratio of the upper bound value (95th percentile) to the lower bound value (5th percentile) of a variable of interest.

[7] Even when GFs are available and the assessor can move straight to Item f, we suggest proceeding through Items b, c, d and e. It provides a second option for estimating the confidence level. The second option may confirm the assignment from the first option, which is reassuring. Otherwise, it gives the assessor the opportunity to reflect on the reasons for the discrepancy and to select the most reasonable option.

and the use of the P-G chart, the next section presents the rationale used in Step 2 for RS1, RS5 and RS8

3. ***Evaluate the qualitative confidence level for the risk scenario.*** Using the severity and frequency assignments from Step 2, evaluate the confidence level for the risk scenario from Figure 4. The last column in Table 2 and Figure 5 show these results for each of the eight risk scenarios
4. If proceeding to the quantitative confidence level analysis***, start with the qualitative confidence levels determined for the severity and frequency in Step 2***. For easy reference, Table 3 repeats these evaluations for the eight dominant risk scenarios (third and fourth columns, respectively). Note that this first step of the quantitative analysis is just looking up the results of Step 2. It is presented as a step to highlight that the inputs to the quantitative analysis come from Step 2 and not Step 3
5. ***Use Figure 6 to get the multiplier for each risk scenario***. This is a simple look up of the multiplier based on the confidence level for the severity and for the frequency. The sixth column in Table 3 shows the multipliers for each of the eight risk scenarios
6. ***Apply the applicable multiplier to estimate the scenario's risk accounting for the impact of the confidence level*** – see Table 3:
    a. For each risk scenario, multiply the frequency by the severity to estimate risk
    b. Normalize the results by dividing the risk for each scenario by the highest risk (RS3 in Table 3). This is useful to focus on the relative level of risk for the scenarios. The second column in Table 3 shows the normalized risk results
    c. Multiply each normalized risk by its respective multiplier from Step 5. This is the revised risk, which considers the confidence level assessment (seventh column in Table 3)
    d. Renormalize the risk estimates (last column in Table 3)

3.0 *Details of the Qualitative Methodology for Selected Risk Scenarios*

This section illustrates the details of the qualitative methodology for three of the risk scenarios considered in the previous section. We selected these scenarios to focus the article on O&G operational incidents. Other publications provide details about the other types of risk scenarios (Paula and Soto Ogaz 2019a) (Paula and Soto Ogaz 2019b). For each risk scenario, we will follow Steps 1, 2 and 3 from the previous section:

- RS1 – Operational Hazards Resulting in Fatality
- RS5 – Loss of Containment in the Marketing Infrastructure
- RS8 – Environmental Restrictions and Regulations

One final observation before proceeding with this section is that the main objective of the confidence level analysis is not to ratify the assignments of the severity or frequency categories in the risk matrix. It focuses on the evaluation of the ***confidence level*** (or "certainty") associated with these assignments. But since the assessor will be reviewing the severity and frequency assignments during the confidence level assessment, this analysis can generate questions and suggestions for modifying some of these assignments.

3.1.1. RS1 – Operational Hazards Resulting in Fatality

Step 1 – The Company operates at many sites in multiple countries, and it has upstream, midstream and downstream activities. Thus, its employees and contractors are exposed to several types of hazards typical of these operations, including work at elevated heights, around sources of energy (electricity, steam etc.), in confined spaces, in excavations and near heavy load lifting. Also, workers are exposed to hazards during transportation (vehicles, helicopters, marine etc.). At this Company, most of the incidents associated with these hazards resulted in a single fatality per incident, which is a Severity Category 4 in the Company's risk matrix (RS1).[8]

To estimate the frequency for this risk scenario, the ERM team considered the Company experience over a period of 16 years. Figure 7 shows the 3-year rolling average of the number of fatal incidents.[9] The trend line shows an increasing incident rate. This was due to an increase in the number of such incidents in year 6 and then again in years 10-12. These in turn, were the result of an expansion of the company's businesses. More operating sites entail more activities, which results in more personnel exposure to hazardous conditions. In response to the increase in the total incident rate, the company instituted several additional and improved controls. The new or improved controls had a positive impact, as indicated by the downward trend in years 11 through 14.

Step 2 – Consider the severity first. Since the risk scenario is, by definition, an event that involves one fatality, it could be argued that the level of confidence for the severity assignment is 100%. In this case, the burden on the assessor would be to evaluate the confidence level for the frequency assignment that best matches the "perfectly-defined" severity level. However, it is unrealistic to assume that we can pinpoint "one fatality" with certainty. Traffic accidents, for example, may involve one or several people within the vehicle. Thus, if historically the number of fatalities has been 1 for this type of event for one company, there is no guarantee that it will always be this way. In general, we suggest that the confidence level for well-defined consequences is **Very High** (or possibly **High to Very High**), which would be the case for RS1. The data strength and the analytical strength are "**Strong**" in the P-G chart.

Regarding the frequency, one way to evaluate the frequency (and the associated confidence level) is to consider the data for the last 16 years. There have been 19 fatal incidents in the last 16 years, which for the evaluation of the confidence level is statistically **Very Strong**[10] (see Figure 3). Per Step 2c, the initial analytical strength is also **Very Strong**. However, many of the activities associated with the hazards mentioned in Step 1 have changed. For example, there were changes in the number of employees and contractors commuting in one or more of the operating regions. Also, as mentioned previously, the Company implemented new and improved controls. Thus, the assessor must adjust the frequency estimate to account for these changes. It can be argued that the analytical strength has dropped to **Medium** because there

[8] The assessors can define other risk scenarios to reflect incidents that result in different severity levels, either more severe or less severe than RS1. For example, one risk scenario could represent multiple fatalities, and others could represent severe injuries, minor injuries etc.

[9] The figure shows 14 (instead of 16) years because it considers the three-year rolling average, which cannot be evaluated for the first two years of data.

[10] Specific event data with at least 9 occurrences.

are several or somewhat material assumptions. In the P-G chart, a **Very Strong** data strength with **Medium** analytical strength result is a **High** confidence level.

A second way of evaluating the frequency is to limit the period to the more recent data (e.g., the last 5 years). There were 4 fatalities in this period, thereby for the evaluation of the confidence level, the data strength would be **Strong**. Since the time period is more recent, the data are more appropriate or "relevant." The analytical strength is better than in the previous paragraph because there are fewer or less immaterial assumptions; it is considered **Strong**. These assignments for the data and analytical strengths result is a **High** confidence level.

In this case, the confidence level for the frequency score is **High** in both ways of evaluation. This is not unusual in risk evaluations: if we broaden the time period to have more data, the data strength increases but the analytical strength decreases and vice versa. That is, changing the time period moves the confidence level ***along*** a diagonal in the P-G chart but not necessarily to a ***different*** level, as illustrated in Figure 8. In fact, the goal of the confidence level analysis is to identify the best diagonal in the P-G chart to represent the level of confidence. This comment applies to the severity and to the frequency. During the evaluation of the confidence level, the assessor may consider using different time periods to either confirm the assessment or to identify discrepancies. The former confirms that the assessor found the "best" diagonal, and the latter indicates the need for further considerations. [11]

Step 3 – This step is always simple. The confidence assignment for the severity is **Very High** and the confidence assignment for the frequency is **High**. Figure 4 shows that the confidence level for the risk scenario is **High**.

3.1.2. RS5 – Loss of Containment in Marketing Infrastructure

Step 1 – This risk scenario addresses loss of containment from one of the Company's pipelines, and it represents a loss of containment that results in multiple fatalities. This type of incident has not happened in the 50 years of operation of this pipeline. However, similar events have occurred involving other companies (NTSB 2002).

Step 2 – Similar to previous discussions, we assume that the confidence level for this well-defined consequence is **Very High**. For the frequency, there have been many incidents

[11] When there are two or more ways of evaluating the severity or frequency score, the level of confidence should be the one associated with the way the assessor chose to assign the score.

Source: (NTSB 2002)

involving loss of containment from this pipeline in the last two decades. However, none of them were catastrophic in the sense of the severity considered for RS5. Thus, for the purpose of using the P-G chart, there are no occurrences with the severity of RS5, and the data strength and initial analytical strength are **Very Weak**. The assessors evaluated this risk scenario using the available data and a Monte Carlo risk simulator. Thus, if we give credit to depth of analysis, the analytical strength becomes **Weak**, and the confidence level for the frequency is **Very Low to Low**.

Step 3 – With confidence levels of **Very High** for the consequence and **Very Low to Low** for the frequency, Figure 4 suggests that the confidence level for the risk scenario is **Very Low to Low**.

3.1.3. RS8 – Environmental Restrictions and Regulations

Step 1 – The Company is routinely audited by the environmental agencies in the countries/regions where it operates. Additionally, these agencies require that the Company investigates incidents, including near misses that have or could have caused environmental impacts. As a result of these internal and external investigations, the Company receives several notifications of potential non-compliances. In most cases, these issues are addressed and resolved to the satisfaction of all parties. However, in some cases the issue can escalate, resulting in penalties, temporary suspensions and even overturning of the license to operate. RS8 considers these potential incidents resulting from environmental issues.

Step 2 – The Company has extensive experience with previous and current non-compliance issues, including sanctions at its operating sites. This provides extensive background to evaluate the severity, thereby the confidence level is **Very High** (**Very Strong** data strength and analytical strength).

The extensive experience applies to the frequency estimate as well, but there are probably more assumptions because RS8 involves uncertainties about the actions of the regulatory agencies. The latter may have political influences in some countries, and is generally more unpredictable (i.e., requires more analysis <u>assumptions</u>.) Thus, the data strength is **Very Strong** for the frequency, but the analytical strength may be **Strong** to **Very Weak**, depending on the level of assumptions. The assessor assumed **Weak** based on our level of knowledge for this risk scenario. With **Very Strong** data strength and **Weak** analytical strength, the confidence level for the frequency is **Medium to High** per the P-G chart.

Step 3 – With **Very High** confidence on the consequence assignment and **Medium to High** confidence on the frequency assignment, the confidence level for RS8 is **Medium to High** (Figure 4).

4.0 ***Results***

Figure 9 shows the risk scenarios with the confidence level analysis excluded (vertical axis) and included (horizontal axis). These are the normalized and renormalized risks from Table 3, respectively. Note that RS1, RS6 and RS8 are ranked the same by normalized risk in Table 3 and in the vertical axis in Figure 10. The dash line in Figure 11 shows this more visibly. And they appear in the same risk cell in the Company's risk matrix shown in Figure 1. That is, they seem to pose the same level of risk to the Company. However, the renormalized risk shows that they are different (see dash-dot lines in Figure 11). In fact, RS6 poses twice the risk posed by RS1. Without the extra "dimension' provided by the confidence level evaluation, all 3 risk scenarios seem to pose the same level of risk because they project on the same point in the vertical axis in Figure 11. With the added "dimension" provided by the confidence level evaluation, they project into distinct points in the horizontal axis.

The impact of the confidence level is even more evident for RS2 and RS7, which are more dominant than operational risks in this case study. Note that RS2 and RS7 are ranked the same in the second column in Table 3 and on the vertical axis in Figure 9. Also, they appear in the same risk cell in the Company's risk matrix (Figure 1). That is, without the confidence level analysis, both the qualitative and the quantitative risk assessments suggest that RS2 and RS7 pose similar risk to the Company. However, RS2 poses 8 times more risk than RS7 when we account for the confidence level. This can be seen in the last column in Table 3 or in the horizontal axis in Figure 9. The reason is that the GF for RS2 is higher, indicating less confidence. Because there is less confidence on the risk estimate for RS2, it is ranked higher.

The impact of "lack of confidence" can even reverse the order of the risk scenarios on the risk scale. RS4, for example, is 2.5 times higher risk than RS5 in the normalized risk in Table 3. However, RS4 represents only 60% of the risk from RS5 in the renormalized risk ranking.

The insights just presented are not available without the confidence level analysis. We get a hint of these insights from the qualitative analysis of the confidence level. For example, Figure 5 shows RS1, RS6 and RS8 in the same risk cell, but it indicates **High** confidence for RS1, **Low** confidence for RS6 and **Medium to High** confidence for RS8. Therefore, both the qualitative and the quantitative analyses provide useful and consistent insights. The supplemental value of the quantitative analysis is that it provides a measure that helps the Company ***rank*** the different risk scenarios. This ranking is useful in risk reduction decisions, including cost-benefit analysis, where the decision makers focus first on the elements with the highest rank (Paula, Lorenzo and Costa Jr. 2015). And this ranking is generally different from the ranking provided without the confidence level analysis.

Another angle to consider in the confidence level analysis is the focus of the decision making. If the risk is high and the confidence is high, the resources would focus on risk reduction. If the risk is high and the confidence is low, the resources would focus on first improving the confidence and then on reducing the risk. Figure 14 shows this concept in a graphical format (Guthrie 2018).

5.0 Concluding Remarks

The analysis of the confidence level presented in this article contributes to key aspects for the successful completion of a risk assessment (Cross and Ballesio 2003) (ABS Consulting 2003). By adding the evaluation of the confidence level, it enhances completeness and comprehensiveness of ERM studies. Because it offers a systematic approach, it helps improve consistency, tractability and documentation of the analysis. And since it uses categories to express the level of confidence, it is straightforward and consistent with the concept of risk matrixes so widely used in ERM and other types of risk assessments. By considering the key factors/sources of lack of confidence, the methodology brings more credibility and realism to the evaluation. And finally, it is simple enough to be efficient in ERM applications, particularly if using the criteria from Figure 2.

One important observation is that the quantitative analysis can be performed very quickly and straightforwardly once the qualitative analysis is completed – just apply a multiplier to the normalized risk estimates and renormalize them. Thus, it is a simple, powerful tool to supplement the qualitative analysis. Another important observation is that the quantitative confidence level evaluation can have a significant impact on the ranking of risk scenarios. The examples from a multi-national, integrated O&G company shows this very clearly.

Finally, some analysts argue that there is so much uncertainty in some of the quantitative results that quantification may not be useful. The insights provided in Figures 9 and 10 show quite the opposite. The extra "dimension" in the horizontal axis in the figures refine the ranking of the risk scenarios. This is useful regardless of the level of confidence (or lack of).

The existence of uncertainty or variability is no excuse for skipping the quantitative analysis of the confidence level or the quantitative ERM altogether. They are ingrained in the decision-making process and ***ignoring uncertainty or variability will not make them go away.***

6.0 Acknowledgements

The authors appreciate the several discussions with Vernon H. Guthrie, which helped shape the objectives and the foundation of the methodology. Several colleagues from ABS Group provided extensive reviews and comments during the different stages of this work: Vernon Guthrie (Knoxville, TN), David Montague (Irvine, CA), Andres Vargas (Viña del Mar, Chile), and Benjamin Roberts (Knoxville, TN).

7.0 References

ABS Consulting. 2003. *Oil Tanker Quantitative Risk Assessment - Final Report, Rev. 1.* Technical Report, ABS Consulting, an ABS Group Company.

Casada, Myron L., John Q. Kirkman, and Henrique M. Paula. 1990. "Facility Risk Review as an Approach to Prioritize Loss Prevention Efforts." *Plant/Operations Progress* 9 (4): 213-219.

CFOC/PIC. 2016. *Playbook: Enterprise Risk Management for the U.S. Federal Government.* Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC).

COSO. 2004. *Enterprise Risk Management Framework.* The Committee of Sponsoring Organizations of the Treadway Commission.

COSO. 2012. *Risk Assessment in Practice.* Committee of Sponsoring Organizations of the Treadway Commission.

Cross, Robert B., and Jorge E. Ballesio. 2003. "A Quantitative Risk Assessment Model for Oil Tankers." *SNAME Conference.* Society of Naval Architects and Marine Engineers (SNAME). 343-357.

Guthrie, Vernon H. 2018. "Risk-Confidence Chart." *e-mails sent to the author.* Knoxville, TN, October 10-11.

ISO 31000:2009(E). 2009. "Risk Management -- Principles and Guidelines."

ISO 31010-2009(E). 2009. "Risk Management -- Risk Assessment Techniques."

Johnson, Gary. 2008. *Defininig Risk Assessment Confidence Levels for Use in Project Management Communications.* Department of Industrial Engineering and Management Systems, Orlando: University of Central Florida. http://stars.library.ucf.edu/cgi/viewcontent.cgi?article=4651&context=etd.

NTSB. 2002. *Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999.* Pipeline Accident Report, National Transportation Safety Board, Washington, D.C.: National Transportation Safety Board. Accessed 03 19, 2019. https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.

OMB. 2016. *OMB Circular No. A-123, Management's Responsibilities for Enterprise Risk Management and Internal Control.* Office of Management and Budget (OMB).

Paula, Henrique M., Donald K. Lorenzo, and Marcelo Costa Jr. 2015. "An Efficient and Effective Approach for Performing Cost Benefit Analysis." *ABRISCO Congresso 2015 & PSAM Topical Meeting.* Rio de Janeiro: ABRISCO.

Paula, Henrique Martini. 2019a. "A Qualitative Methodology to Evaluate the Confidence Level in Entreprise Risk Management." *To be submitted for publication in Risk Analysis* (The Society for Risk Analysis).

Paula, Henrique Martini. 2019. "A Qualitative Methodology to Evaluate the Confidence Level in Entreprise Risk Management." *Submitted for publication in Risk Analysis* (The Society for Risk Analysis).

Paula, Henrique Martini. 2019b. "A Quantitative Methodology to Evaluate the Confidence Level in Entreprise Risk Management." *To be submitted for publication in Risk Analysis* (The Society for Risk Analysis).

Paula, Henrique Martini, and Magdalena Soto Ogaz. 2019b. "Confidence Level Assessment in Enterprise Risk Management: Case Study with Focus on Financial Risks." *To be submitted for publication in the Journal of Applied Corporate Finance.*

Paula, Henrique Martini, and Magdalena Soto Ogaz. 2019a. "Confidence Level Assessment in Enterprise Risk Management: Case Study with Focus on Risk Transfer and and Illegitimate Acts." *To be submitted for publication in the International Journal of Disclosure and Governance.*

Perera, Jeevan S. 2011. "NASA's Enterprise Risk Management System." *2011 Risk and Compliance Conference.* Valley Forge, PA: The Vanguard Group.

Table 1 — Eight Dominant Risk Scenarios

- Risk Scenario 1 (RS1) – Operational Hazards Resulting in Fatality
- Risk Scenario 2 (RS2) – Carelessness or Illegitimate Acts
- Risk Scenario 3 (RS3) – Less Demand Due to Increased Competition
- Risk Scenario 4 (RS4) – Lower Earnings Due to Increased Operational Costs
- Risk Scenario 5 (RS5) – Loss of Containment in the Marketing Infrastructure
- Risk Scenario 6 (RS6) – Inadequate Insurance Coverage
- Risk Scenario 7 (RS7) – Inadequate Project Management
- Risk Scenario 8 (RS8) – Environmental Restrictions and Regulations

		Severity Category					
		1	**2**	**3**	**4**	**5**	**6**
Frequency Category	6				**RS5**		**RS3**
	5					**RS4**	**RS2** **RS7**
	4						**RS1** **RS6** **RS8**
	3						
	2						
	1						

Figure 1 — The Eight Risk Scenarios in the Company's Risk Matrix

Paula-Guthrie Confidence Criteria

P-G Chart with Girth Factors within Parenthesis			Analytical Strength		
			Strong (S)	**Medium (M)**	**Weak (W)**
			• Few or mostly immaterial assumptions	• Several or somewhat material assumptions	• Numerous or fairly material assumptions
			<-- Consider moving one cell to the left when benefiting from relevant "SME"† knowledge and experience **or** relevant "depth of analysis" <-- Consider moving two cells to the left when benefiting from both relevant "SME" knowledge and experience **and** relevant "depth of analysis"		
Data Strength	**Strong(S)**	• Specific event data with at least 4 occurrences	High (10)	Medium to High (18)	Medium (32)
	Medium(M)	• Specific event data with 3 occurrences or • Plentyful generic data or • Well-thought-out pseudo data	Medium to High (18)	Medium (32)	Low to Medium (56)
	Weak(W)	• Specific event data with 2 or fewer occurrences or • Limited generic data or • Pseudo data	Medium (32)	Low to Medium (56)	Low (100)

† Subject Matter Expertise

Figure 2 — Confidence Criteria

Expanded Paula-Guthrie Confidence Criteria

P-G Chart with Girth Factors within Parenthesis

Data Strength		Analytical Strength: Very Strong (VS)	Strong (S)	Medium (M)	Weak (W)	Very Weak (VW)
		• No or only immaterial assumptions	• Few or mostly immaterial assumptions	• Several or somewhat material assumptions	• Numerous or fairly material assumptions	Numerous or highly material assumptions
Very Strong (VS)	• Specific event data with at least 9 occurrences	Very High (3.2)	High to Very High (5.6)	High (10)	Medium to High (18)	Medium (32)
Strong (S)	• Specific event data with at least 4 occurrences	High to Very High (5.6)	High (10)	Medium to High (18)	Medium (32)	Low to Medium (56)
Medium (M)	• Specific event data with 3 occurrences or • Plentyful generic data or • Well-thought-out pseudo data	High (10)	Medium to High (18)	Medium (32)	Low to Medium (56)	Low (100)
Weak (W)	• Specific event data with 2 occurrences or • Limited generic data or • Pseudo data	Medium to High (18)	Medium (32)	Low to Medium (56)	Low (100)	Very Low to Low (320)
Very Weak (VW)	• Specific event data with 1 or no occurrences or • Sparse generic data or • Mostly judgement	Medium (32)	Low to Medium (56)	Low (100)	Very Low to Low (320)	Very Low (1,000)

<-- Consider moving one cell to the left when benefiting from relevant "SME"† knowledge and experience **or** relevant "depth of analysis"
<-- Consider moving two cells to the left when benefiting from both relevant "SME" knowledge and experience **and** relevant "depth of analysis"

† Subject Matter Expertise

Figure 3 — Expanded Confidence Criteria

Table 2 — Summary of the Results from the Qualitative Analysis

Risk Scenario	Severity			Frequency			Confidence for the Risk Scenario
	Strength		Confidence Level for the Severity	Strength		Confidence Level for the Frequency	
	Data	Analytical		Data	Analytical		
RS1	Very Strong	Very Strong	Very High	Very Strong	Medium	High	High
				Strong	Strong		
				Medium	Very Strong		
RS2	Very Strong	Very Strong	Very High	Very Weak	Very Weak	Very Low	Very Low
RS3	Very Strong	Very Strong	Very High	Very Weak	Weak	Very Low to Low	Very Low to Low
RS4	Very Strong	Very Strong	Very High	Very Strong	Strong	High to Very High	High
RS5	Very Strong	Very Strong	Very High	Very Weak	Weak	Very Low to Low	Very Low to Low
RS6	Very Strong	Very Strong	Very High	Very Weak	Medium	Low	Low
RS7	Very Strong	Very Strong	Very High	Very Strong	Very Strong	Very High	High to Very High
RS8	Very Strong	Very Strong	Very High	Very Strong	Weak	Medium to High	Medium to High

Confidence Level for Risk Scenario										
		Confidence Level for the Frequency								
		Very High	High to Very High	High	Medium to High	Medium	Low to Medium	Low	Very Low to Low	Very Low
Confidence Level for the Severity	Very High	High to Very High	High	High	Medium to High	Medium	Low to Medium	Low	Very Low to Low	Very Low
	High to Very High	High	High	Medium to High	Medium	Low to Medium	Low	Low	Very Low to Low	Very Low
	High	High	Medium to High	Medium	Medium	Low to Medium	Low	Low	Very Low to Low	Very Low
	Medium to High	Medium to High	Medium	Medium	Low to Medium	Low	Low	Very Low to Low	Very Low	Very Low
	Medium	Medium	Low to Medium	Low to Medium	Low	Low	Very Low to Low	Very Low to Low	Very Low	Very Low
	Low to Medium	Low to Medium	Low	Low	Low	Very Low to Low	Very Low to Low	Very Low to Low	Very Low	Very Low
	Low	Low	Low	Low	Very Low to Low	Very Low to Low	Very Low to Low	Very Low	Very Low	Very Low
	Very Low to Low	Very Low to Low	Very Low to Low	Very Low to Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Figure 4 — Confidence Level for the Risk Scenario

Frequency Category	Severity Category 1	Severity Category 2	Severity Category 3	Severity Category 4	Severity Category 5	Severity Category 6
6				RS5^{VL-L}		RS3^{VL-L}
5					RS4^{H}	RS2^{VL} RS7^{H-VH}
4						RS1^{H} RS6^{L} RS8^{M-H}
3						
2						
1						

H-VH - High to Very High
M-H - Medium to High
H - High
L - Low
VL- L - Very Low to Low
VL - Very Low

Figure 5 — Qualitative Confidence Levels for the Eight Risk Scenarios

Table 3 — Quantitative Confidence Level Analysis for the Eight Dominant Risk Scenarios							
Risk Scenario (RS)	**Normalized Risk**	**Confidence Level**		**GF for RS**	**Multiplier for RS**	**Revised Risk**	**Renormalized Risk**
		Severity	**Frequency**				
RS3	1.00	**VH**	**VL-L**	354	4.9	4.91	1.00
RS7	0.25	**VH**	**VH**	5.1	1.1	0.28	0.058
RS2	0.25	**VH**	**VL**	1,100	9.6	2.41	0.49
RS6	0.10	**VH**	**L**	115	2.8	0.28	0.058
RS8	0.10	**VH**	**M-H**	22	1.6	0.16	0.032
RS1	0.10	**VH**	**H**	13	1.4	0.14	0.028
RS4	0.025	**VH**	**H-VH**	8	1.2	0.03	0.006
RS5	0.010	**VH**	**VL-L**	354	4.9	0.049	0.010
VH − Very High **H-VH** High to Very High		**H** − High **M-H** − Median to High		**L** − Low **VL-L** − Very Low to Low			**VL** − Very Low

Confidence Level Multiplier										
		Confidence Level for the Frequency								
		Very High	High to Very High	High	Medium to High	Medium	Low to Medium	Low	Very Low to Low	Very Low
Confidence Level for the Severity	Very High	1.1	1.2	1.4	1.6	1.8	2.3	2.8	4.9	9.6
	High to Very High	1.2	1.3	1.5	1.7	2.0	2.4	3.1	5.3	10
	High	1.4	1.5	1.6	1.9	2.2	2.7	3.4	5.9	12
	Medium to High	1.6	1.7	1.9	2.1	2.5	3.1	3.9	6.8	13
	Medium	1.8	2.0	2.2	2.5	3.0	3.7	4.6	8.0	16
	Low to Medium	2.3	2.4	2.7	3.1	3.7	4.5	5.6	9.8	19
	Low	2.8	3.1	3.4	3.9	4.6	5.6	7.1	12	24
	Very Low to Low	4.9	5.3	5.9	6.8	8.0	9.8	12	21	42
	Very Low	9.6	10	12	13	16	19	24	42	82

Figure 6 — The Confidence Level Multiplier

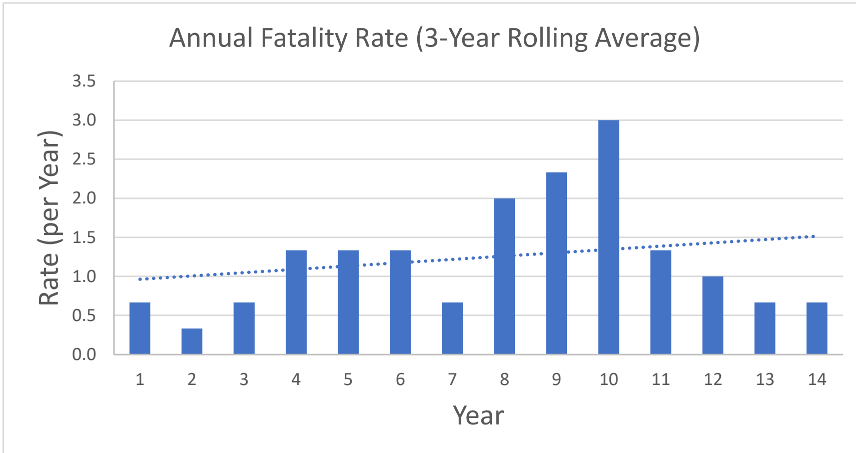


Figure 7 — Historical Experience Related to RS1

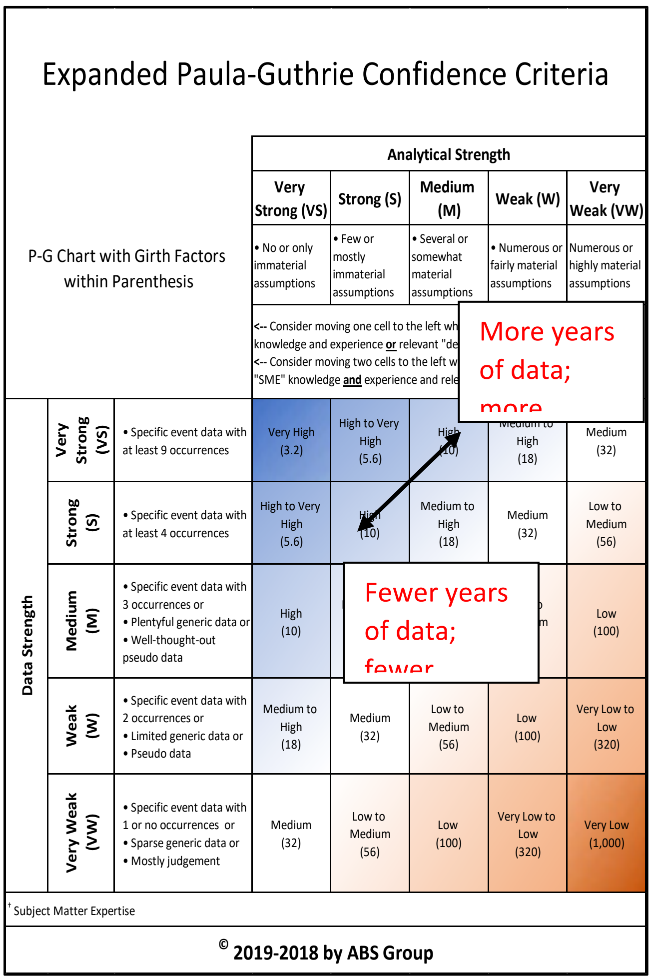


Figure 8 — Impact of Time Period

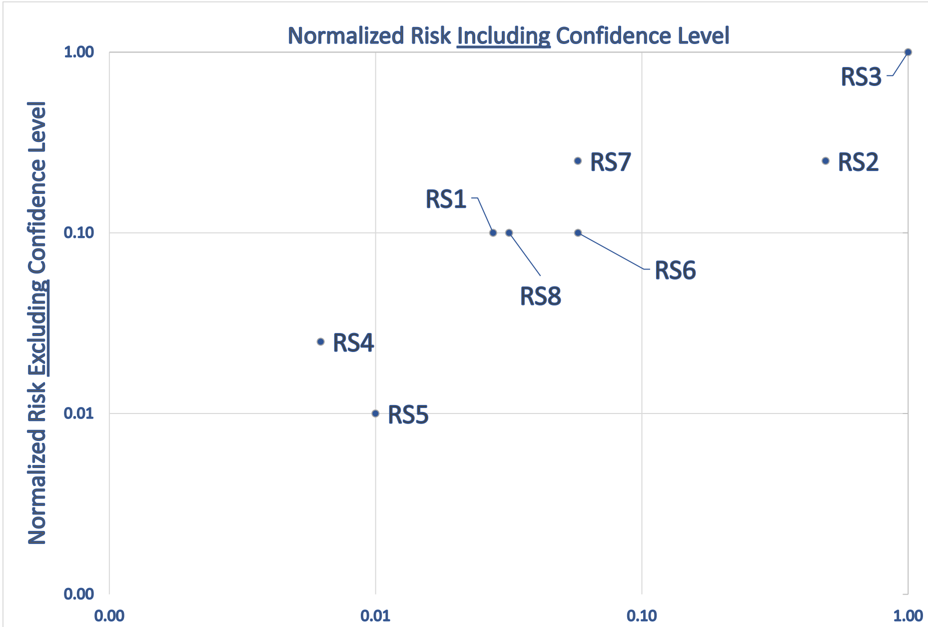


Figure 9 — Risk Estimates with and without the Confidence Level Analysis

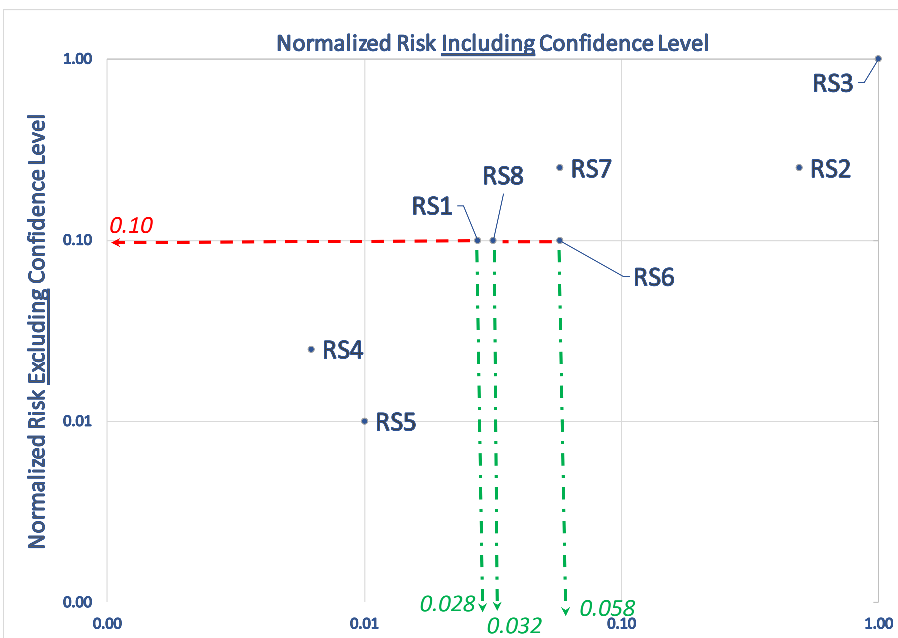


Figure 10 — RS1, RS6 and RS8 with and without the Confidence Level Analysis

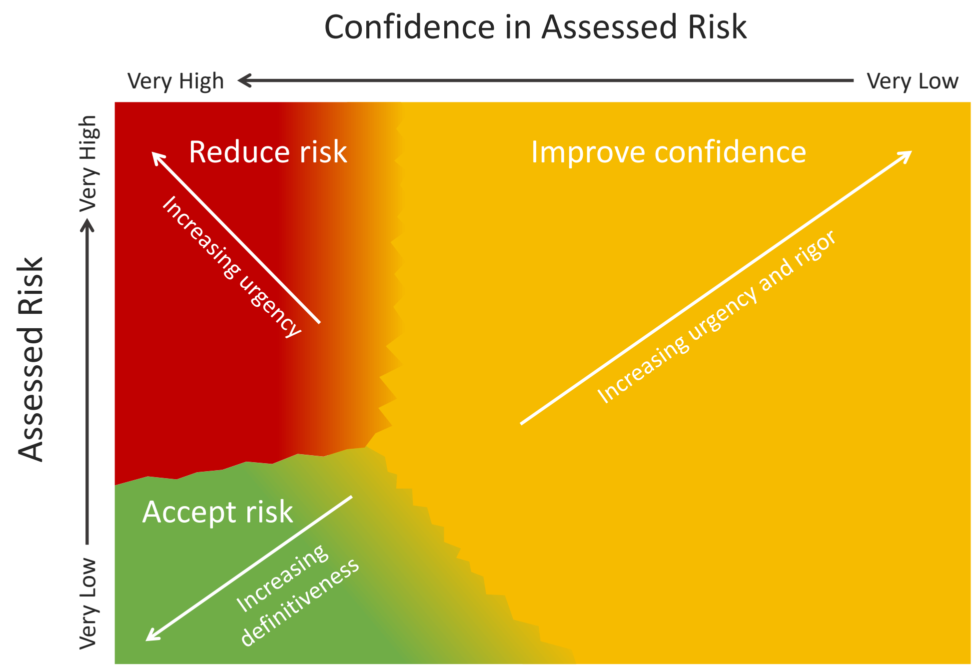


Figure 11 — Guthrie's Assessed Risk and Confidence

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

A New Look at Release Event Frequencies

Benjamin R. Ishii, Jeffrey D. Marx*
Quest Consultants Inc.
Norman, Oklahoma
*Presenter E-mail: jdm@questconsult.com

Abstract

Within the context of a quantitative risk analysis (QRA), the two main constituents used to describe petrochemical risks are, and have always been, consequence and probability. The consequences of hazardous material accidents are easy to apprehend – if a hazard is realized it can injure people or cause fatalities, damage equipment or other assets, or cause environmental damage. Frequencies for these consequences, on the other hand, are not as easy to understand. Process safety professionals develop event frequencies by evaluating historical data and calculating incident rates, which represent, in the QRA context, how often a release of a hazardous material has occurred. Incident rates are further modified by probabilities for various hole sizes, release orientations, weather conditions, ignition timing, and other factors, to arrive at unique event probabilities that are applied in the QRA. This paper describes the development of incident rates from historical database information for various equipment types, as well as defining a methodology for assigning hole size probabilities from the same data, such that a hole size distribution can be assigned within each QRA study. The combination of total incident rates and a hole size distribution relationship can then serve as a foundation within the frequency side of many QRA studies.

Keywords: Probability, Frequency, Quantitative Risk Analysis, QRA

1 Historical Context

The use of quantitative risk analysis (QRA) within the realm of petrochemical process safety has its roots in the risk assessments of the 1950s and 1960s nuclear industry, as well as the probabilistic risk analysis of the 1960's aerospace programs. It was not until the 1980s, however, that computing power made a fully numeric and sufficiently detailed QRA possible. In the decades since then, QRA has progressed to be more sophisticated, more comprehensive [1], and more adept at providing sensitivity and validation studies with an analysis.

During the early days of QRA, the consequence analysis portion was viewed as the weak link – the models were simplistic and overly conservative, but necessarily so due to the computational resources that were available. As computing power increased over the years, and the consequence models were improved with new techniques and field-scale validations, the frequency assessment became the weaker of the two. A general realization was made by risk analysts that many of the incident rates in published data were nothing more than engineering estimates (guesstimates) and often came with uncertainties that were measured in orders of magnitude (for example, see the "Purple Book" from TNO[2] or the data presented by the International Association of Oil and Gas Producers[3]).

While it is rare to find properly documented data from which incident rates can be developed, there have been some attempts at petrochemical incident rate data collection stretching several decades. These, of course, come out of regulatory systems that mandate detailed incident reporting, as well as data collection about the equipment in service within a given system. Examples of such systems include the federally-regulated pipeline industry in the United States [4] and the offshore industry in the United Kingdom (UK).

The UK system, founded after the Piper Alpha incident, mandates incident reporting for all hydrocarbon releases from offshore systems, as well as recording of the equipment populations of all installations. This hydrocarbons release database (HCRD) is maintained by the Health and Safety Executive (HSE), and has collected data since 1992[5], continuing under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) since 2013. It has become the chosen database for petrochemical QRA applications due to its comprehensive nature, where all hydrocarbon releases, and the populations of equipment from which releases could happen (and have happened), are captured by the data gathering requirements.

2 Risk Criteria

There are, effectively, two ways to use QRA results. The first is in a comparative way. In a comparative QRA, two or more options are evaluated and the outcome of the analysis provides the basis for the risk assessment in the end. In this situation, the various results (associated with the various options) are compared to each other to see which option creates a lower risk. This approach does not typically concern itself with the absolute value of calculated risk, just the risk relative to the other options. In taking this viewpoint, the uncertainties of the analysis can be ignored (as they are deemed equal) and the insufficiencies of either the frequency data or the consequence analysis may be overlooked – provided that the same methodology and assumptions were applied to each option.

In contrast to comparative QRA, most studies are done so that their results can be compared to some criterion in the risk assessment stage (after the analysis is complete) to determine if the calculated risk is acceptable or not. In this case, a criterion or criteria are needed to evaluate the risk. It is this application for which many governmental or industry (and some corporate) criteria have been developed. These criteria allow risk analysts to compare calculated risk to a standard to evaluate whether or not the level of risk is acceptable.

When developing measures of risk, there needs to be some baseline time frame on which the risk is calculated. For comparative risk, this is perhaps open to the analyst, as the only item of importance in the end is the comparison itself. With published risk criteria, the basis is virtually always one (calendar) year. In this way, the calculated risk has a time constraint and can be compared to other measures with the same time constraint. In most cases, published risk criteria are based on fatalities for members of the public. Thus, the risk criteria sets an acceptable limit for the public's exposure to a potentially fatal event within a one year period. This common basis also allows for comparison to other modes of potential fatality, which are often expressed on an annual basis.

3 Frequency vs. Probability

Within the context of conducting QRAs, there is often debate on the exact definitions (and meaning of) frequency and probability. While mathematicians may have very precise definitions for these terms, they become blurred when put into the context of a petrochemical QRA. So, for the purposes of this paper, the following definitions will apply [6]:

Frequency: The number of occurrences of an event per unit of time.
Probability: The likelihood of an event or event sequence during an interval of time; expressed as a number ranging from 0 to 1.

Using these concepts, it is possible to establish the basis for a QRA in both terminology and the numerical formulation of frequencies and probabilities. The QRA then proceeds with the following steps:

- Historical data is gathered for the events of concern. In this case, each incident is some type of loss of containment (LOC) that results in a hydrocarbon (or other chemical) release.
- Using the number of incidents over a given number of years, as well as the population count for the equipment that could have had an LOC, an incident rate is developed. This incident rate is expressed as the number of incidents per year, for a given equipment type.
- Incident rates are applied as LOC event frequencies to evaluate specific hazardous events.
- Frequencies may be modified by conditional probabilities, which are a value between zero and one, addressing the occurrence of some specific condition, provided that an initiating even has occurred. Examples include the probability of given hole size when there is a release event, the probability of certain weather conditions among the many site-specific possibilities, or the probability of ignition of the flammable vapor cloud that is generated.
- The LOC frequency (as modified by several probabilities) is mathematically transformed into the probability of the unique event in a one-year period for use in the risk calculations. While probabilities do not by definition carry units of time, it is necessary to address the probability values with a specific time period (i.e., one year) due to the basis of the incident rates, as well as the basis for risk assessment through comparison to established criteria.

With the above process outlined, it can be seen that it is necessary to use historical frequencies, expressed as incident rates, to define probabilities that are then used in QRA calculations. The remainder of this paper focuses on the development of frequencies associated with petrochemical processing equipment incidents that represent a LOC event.

The first use of a database is to develop a total incident rate for each type of equipment. This rate is independent of the specifics of each incident (such as release magnitude or release hole size) as it is only concerned with the number of incidents experienced by a given type of equipment. The total incident rate (TIR) can be easily expressed as:

$$TIR = \frac{number\ of\ incidents}{Population, equipment{\cdot}years} \tag{1}$$

Consider the following example. In a given installation, there are 200 incidents involving LOC events from pumps during a ten-year span that data is gathered. If the population of pumps is 1,000 for every year over the same span of 10 years, then there are 10,000 pump-years in the data set. Application of Equation 1 then provides the total incident rate:

$$TIR\ (pumps) = \frac{200\ incidents}{10{,}000\ pump{-}years} = 2.0\ x\ 10^{-2}\ incidents\ per\ year, per\ pump \tag{2}$$

In this example, pumps would be found to have a historical incident rate of 0.02 per year, or 2.0 x 10^{-2} per year. This incident rate can then be used for probability calculations in a QRA. The calculated frequency, or incident rate, can be transformed into a probability using the following formula:

$$P = 1 - e^{(-\lambda \cdot t)} \tag{3}$$

Where:

P = annual probability of occurrence (dimensionless)
λ = annual incident frequency (LOC events per year)
t = time period (one year)

This transformation provides the probability that a given event will occur within a specified time period. When dealing with incident rates for QRA and subsequent comparison to published standards, the time period is always set at one year. Because of this, the incident rates must be expressed as LOC events per year. While probabilities are dimensionless, we attach the word 'annual' to the probability to signify that it is the probability of the event happening in the period of one year.

For our example above, the incident rate for pumps, per year, was found to be 2.0 x 10^{-2}. This results in an annual probability of 1.98013 x 10^{-2}. This means that if the historical data are taken to be applicable to future pump events, in any given year there is a one in 50.5 chance of any individual pump experiencing an LOC event. Note that, numerically, the incident rate is nearly identical to the probability. This is true for frequencies less than about 1.0 x 10^{-2}, but diverges as the frequency approaches one. For events with a frequency of once per year, the annual probability is about 0.632. For the typical frequencies (incident rates) used in a QRA, the frequency and probability values are often close enough such that they are effectively interchangeable.

4 HCRD

As discussed above, the most comprehensive database for LOC events is the HSE's HCRD. Each incident recorded in the database is a release of hydrocarbon, without regard to the cause of that event. Additionally, there is a full count of the equipment from which LOC events could occur, broken down by equipment types. The reporting for both events and population is mandatory, overseen by regulators in the UK. Reporting began in 1992 and has continued consistently since then. As of the writing of this paper, the data through 2016 was the latest available [7].

The HCRD is effectively two databases: (1) a recording of equipment populations, and (2) a reporting log for incidents. The equipment population data is reported annually, and includes classification by one of 53 systems and by equipment in one of 120 categories or subcategories. Incidents include any unintended release of hydrocarbons, and each incident is reported with a set of information including the time, date, place, and other circumstances associated with the release event, the material released, the amount released, pressure at the time of the release, the hole size, the cause of the release, and many other parameters. The database includes a total of 4,756 incident entries for 1995 through 2016.

There have been previous attempts to provide LOC event data. In 2013, Det Norske Veritas (DNV) published a guidelines document that provided frequency data for use in QRAs[8]. The data, extracted from the HCRD, was presented for a range of equipment sizes within the various equipment types, for a fixed set of hole size ranges. Then recently, Lloyd's Register published a revision for the Process leak for offshore installations frequency assessment model – PLOFAM(2)[9], which is based on the offshore Norwegian Continental Shelf facilities that are similar to the UK's offshore facilities. Both of these publications present LOC event data, but the former is somewhat cumbersome, and the latter is a complicated system whose results are geared more toward mass release rates than incident rates. Thus, this paper strives to provide a more streamlined and flexible system for event probability determination.

5 Calculating Equipment Incident Rates

The HCRD provides a recording of all hydrocarbon release incidents from the population of equipment within its scope of influence. Each release event is reported under the HSE's system, and data is gathered concerning the release. Of the many data fields in the database, this analysis was concerned with the following entries for each recorded incident:

- HCRD ID (a unique identification number)
- The HSE-ranked incident severity (*minor, major, significant*)
- Equipment codes (general, primary, secondary, and tertiary classifications)
- Estimated quantity released [kg]
- Equivalent hole diameter [mm]
- Pressure at the time of release [bar]

Of the 4,756 recorded release events in the database, there were several that did not have an entry (often "BLANK" is found), or had a bad entry, in the equipment code field(s). Without a valid equipment code, these incidents were not able to be categorized, and were excluded from the analysis.

The core consideration in this analysis was that each incident be of sufficient magnitude such that the event is capable of harming people or damaging equipment. Many of the incidents are reported to have occurred at very low pressures or to have released very little hydrocarbon. So, while such events have been reported as LOCs, they are not considered to be a hazardous incident for the purposes of incident rates applied to a QRA. These are often referred to as "maintenance events" where certain maintenance tasks result in hydrocarbon release even after the system has been depressurized or partially drained/vented. The following criteria were applied to the data:

- Remove incidents where a valid equipment code is not provided (326 incidents removed)
- Remove incidents whose reported release pressure was less than 0.5 bar, **unless** that incident was labeled by the HSE as *major* or *significant* (267 incidents removed)
- Remove incidents whose reported released mass was less than 1.0 kg, **unless** that incident was labeled by the HSE as *major* or *significant* (461 incidents removed)

The labeling of 728 incidents as maintenance events represents the removal of about 15% of the incidents from consideration. While the pressure and released mass filtering values are somewhat arbitrary, they are deemed appropriate due to the concerns listed above. Figure 1 demonstrates the independent distributions of mass released and release pressure within the HCRD.

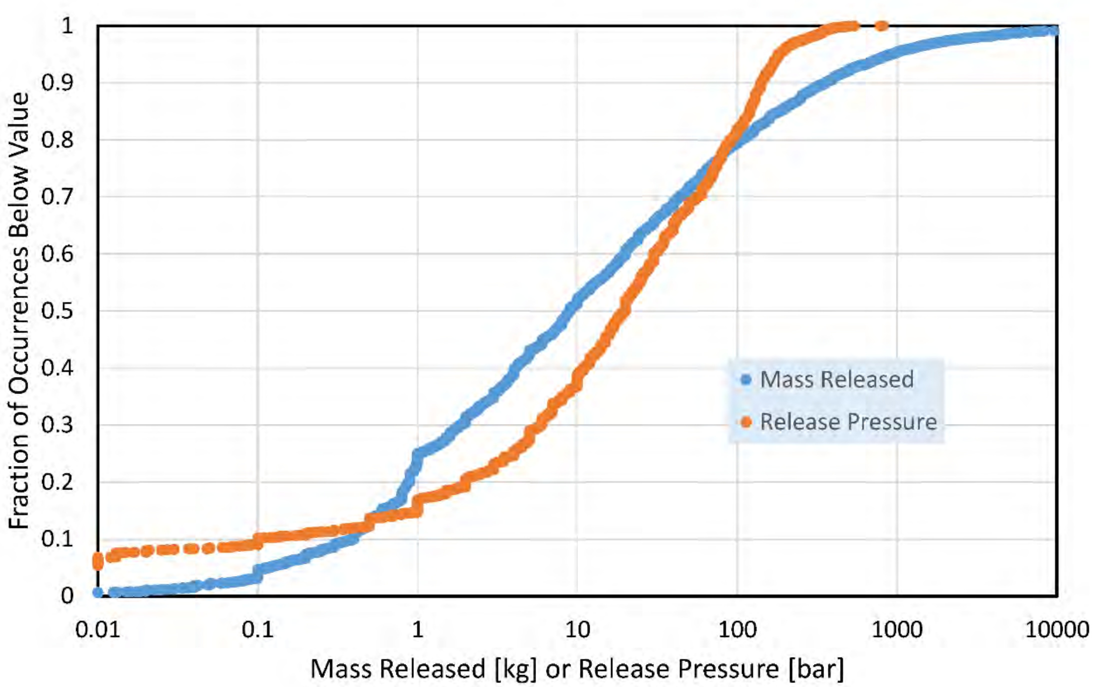


Figure 1
Cumulative Distribution of Mass Released and Release Pressure Data

Of the 120 categories and sub-categories of equipment types, there are about 30 classifications or equipment groups that are of general interest to QRAs. In many cases, multiple equipment types are grouped to develop a more general incident rate. For example, the HCRD includes 38 classifications for valves, based on various classifications by valve size (diameter), whether they are manual or actuated, or whether the valve is a blowdown, choke, emergency shut down, relief, or bleed valve. From these 38 categories, a user could determine an incident rate for a very specific valve type (if there were sufficient incidents with that type; sometimes there are none), but it is more statistically meaningful to group valves into larger categories. In this work, valves are divided into classifications of manual or actuated. All valve characteristics or service types are lumped into these two categories.

The results for the total incident rate calculation are given in Table 1, based on a selection of equipment types that is generally useful to QRA application for hydrocarbon processing systems.

Table 1
Calculated Equipment Incident Rates

Equipment Type or Group	HCRD Number of Equipment-Years	Number of Incidents (Filtered)	Calculated Total LOC Rate per Year
Compressors	8,661	106	1.224×10^{-2}
Crude Oil Storage	8,733.5	59	6.756×10^{-3}
Filters	19,435.6	59	3.036×10^{-3}
Flanged Connections	13,747,657	379	2.575×10^{-5}
Flexible Connections	1,787,286.3†	135	7.553×10^{-5}†
Shell & Tube Heat Exchangers	20,630.2	47	2.278×10^{-3}
Plate Heat Exchangers	6,690	47	7.025×10^{-3}
All Heat Exchangers	29,329.1	102	3.478×10^{-3}
Instruments (Small Connections)	1,629,769	641	3.933×10^{-4}
Pig Traps	8,160	36	4.412×10^{-3}
Piping $D \leq 3$ inches	3,600,856†	512	1.422×10^{-4}†
Piping $3 < D < 11$ inches	6,093,607†	245	4.021×10^{-5}†
Piping $D \geq 11$ inches	1,918,542†	69	3.596×10^{-5}†
Pressure Vessels	44,715.6	82	1.834×10^{-3}
Pumps	28,246.7	176	6.231×10^{-3}
Turbines	3,222.4	121	3.755×10^{-2}
Actuated Valves	724,192	375	5.178×10^{-4}
Manual Valves	3,744,845	277	7.397×10^{-5}
All Valves	4,469,037	644	1.441×10^{-4}

† Reported count by meters of piping; incident rate per meter per year

While the HCRD offers data on many equipment types, there are some that are not included and must be referenced in outside databases. Incident frequency data for items such as large floating roof storage tanks, LPG transfer hoses, LNG marine transfer hard arms, and others do not appear in the HCRD. The methodologies presented in this paper could be applied to these other items, but they are not discussed further here.

6 Hole Size Distribution

While the development of total incident rate is important, it does not fully describe the frequency of an LOC event. When applied to a properly constructed QRA, incident rate data must include a relationship between event hole size and the total incident rate. This is generally realized as large, high consequence events having small frequencies (or probabilities) and small, low consequence events having larger frequencies, such that within the total incident rate, there is a probabilistic distribution of hole sizes that create the range of consequences.

To develop a hole size distribution from the HCRD, the analysis began with the set of incidents used for the total incident rate. A second filtering was applied on the reported hole size so that a numerical evaluation of hole sizes could be done. All incident entries that had no hole size identified (listed as “BLANK”) or a hole size of “999” mm were removed from the analysis. This filtering reduces the data set, but only in the sense that incidents with undefined hole sizes are not used to describe the hole size distribution. The “999” values are a database placeholder where a real hole size was not recorded, and thus are not discarding holes of nearly one meter in diameter.

If the data remaining in the analysis are grouped by equipment type, then any one group can be evaluated on the range of hole sizes that were reported in the HCRD. At this level of analysis, no other variables are important to the analysis – only the individual hole sizes and how any one relates to the distribution of hole sizes within the full set are of interest. Distilling the data to this level leaves a list of hole sizes and a total number of incidents for that equipment type. The most useful way to characterize this data set is a cumulative distribution, which describes the fraction of total incidents as a function of hole size. Such a relationship can then be applied to the various hole sizes modeled in a QRA to calculate the probability of a given hole size range, which is then represented by a single hole size and matched with the appropriate consequence modeling set. Analysis of the data found that a two-variable log-logistic equation was able to sufficiently describe the fraction of incidents as a function of hole size. The log-logistic cumulative distribution function (CDF) can be expressed as:

$$C = \frac{1}{1+\left(\frac{d}{\alpha}\right)^{-\beta}} \tag{4}$$

Where:

C = Fraction of occurrences for hole sizes up to hole size *d*
d = hole diameter, mm
α = alpha parameter for log-logistic equation
β = beta parameter for log-logistic equation

In this application, for a given hole size, *d*, the CDF represents the fraction of all LOC events that will have a hole size of that diameter or smaller. When combined with the total incident rate (as calculated above) the CDF can be used to describe the frequency of LOC events in a given hole size range:

$$f_{d_2-d_1} = TIR \cdot (C_2 - C_1) \qquad (5)$$

Where:

C_1	=	Fraction of occurrences for hole sizes up to hole size d_1
C_2	=	Fraction of occurrences for hole sizes up to hole size d_2
TIR	=	Total incident rate for the equipment type
$f_{d_2-d_1}$	=	LOC event frequency for hole size range between d_1 and d_2

To implement Equation 5, the analyst must first have the alpha and beta parameters that best fit the data for a given type of processing equipment. An example plot for pump LOC events from the HCRD is shown in Figure 2, with the hole size axis show in log-scale. The graph in Figure 2 demonstrates the hole size distribution for multiple pump types, as well as the distribution of all pump incidents as a single data set, and how a log-logistic curve fits this data.

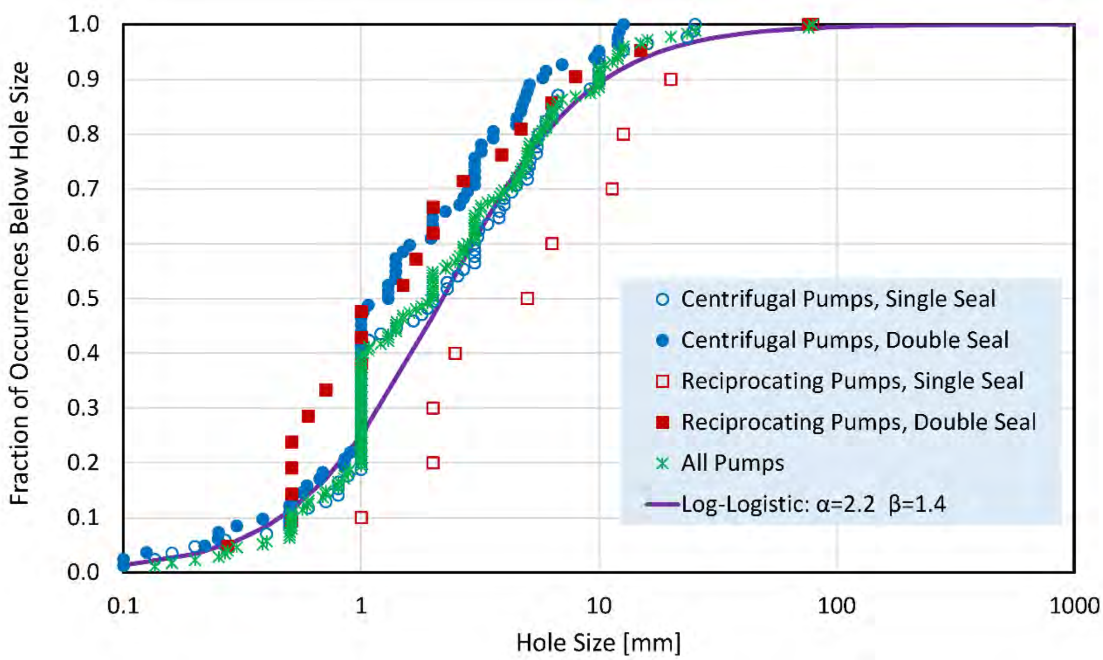


Figure 2
Cumulative Distribution of Hole Size and Log-Logistic Curve Fit for Pumps

A review of Figure 2 shows that the four types of pumps for which data is collected in the HCRD each have a unique distribution. This data could be used to create a log-logistic fit for each pump classification in the database. The problem that occurs is that some data sets are not large enough to be reliably used. For example, as seen in Figure 2, the single seal reciprocating pumps only have ten recorded incidents, and are not statistically significant for their own curve fit. It is better to merge these pumps with the double seal reciprocating pumps (21 incidents) or create a group that is all pumps (175 incidents), as shown in Figure 2. While there is a discernable difference between each of the four pump types, and between single or double seals, a combined group is a reasonable representation of all pump types.

The implementation of a log-logistic curve fit has specific implications when the results are interpreted. As an example, consider the log-logistic fit in Figure 2, where 25% of the occurrences are predicted to be 1 mm or smaller holes, 50% are predicted to be 2 mm or smaller, and about 90% are predicted to be 10 mm or smaller. This indicates that 90% of the total incident rate is attributed to the smaller hole sizes. The fit to one curve for multiple equipment classifications also shows the potential imprecision of the method. Considering the single seal reciprocating pumps, the 50% value for is about 5 mm, and the 90% value at 20 mm. If there were sufficient data to develop an independent curve fit for single seal reciprocating pumps, and that expanded data followed the same trend indicated in Figure 2, it may be warranted to have a separate curve.

7 Application to QRA

The system described here is implemented by having a table of values, by equipment type, listing the total incident rate and the alpha and beta parameters for the hole size distribution. To select incident rates for the various hole sizes that apply to a type of equipment, a risk analyst can follow these steps:

- Define a set of hole sizes to be implemented in the QRA where
    - Each chosen hole size defines a ranges of incident hole sizes;
    - For the smallest hole size range, the d_1 value is taken to be zero; and
    - The largest range is categorized as a rupture and ends with a very large hole (e.g., 1 m)
- Select the equipment type.
- For each hole size range, use Equations 4 and 5 above to assign an LOC frequency for the hole size range, using the total incident rate for that type of equipment, the alpha and beta parameters, and the bounding hole sizes.
- Where there is a maximum hole size for a type of equipment (e.g., instrument connections) the hole size range representing the maximum hole size should be assigned a frequency that is the sum of the calculated one for that range and all larger hole sizes. All larger hole size ranges being applied in the QRA should then be assigned a frequency of zero.
- Select the consequence modeling hole size associated with the specified hole size range (e.g., a range of 15-25 mm can be modeled with a 25 mm diameter hole). The hole size at the top of a range is often applied as a conservative assumption, but a hole size in the middle of the range may also be selected.

A set of values that can be used with the above methodology is given in Table 2, including the alpha and beta parameters for the various equipment types.

8 Concluding Remarks

The system presented in this paper represents a portable and flexible tool that can be applied to various QRA studies. It offers the comprehensive basis of the HCRD, plus a simplified methodology for application with a QRA. Table 2 can be applied to various QRA studies where the hole sizes selected for analysis are varied. This offers consistency in the applied incident rate data, as well as consistency in the hole size distribution.

This methodology can be followed with a different set of assumptions applied to HCRD, or alternatively, the methodology can be applied to other databases that have the same quality of data. The latter option would certainly be necessary for equipment types not found in the HCRD.

Table 2
Incident Rates and Cumulative Distribution Factors

Equipment Type or Group	**Calculated Total Incident Rate per Year**	**Log-Logistic Curve Fit Parameters**	
		α	**β**
Compressors	1.224×10^{-2}	2	1.3
Crude Oil Storage	6.756×10^{-3}	18	1.2
Filters	3.036×10^{-3}	16	1.1
Flanged Connections	2.575×10^{-5}	1.5	0.9
Flexible Connections	7.553×10^{-5}†	5.5	1.2
Shell & Tube Heat Exchangers	2.278×10^{-3}	1.3	1
Plate Heat Exchangers	7.025×10^{-3}	3	1.7
All Heat Exchangers	3.478×10^{-3}	2	1.3
Instruments (Small Connections)	3.933×10^{-4}	3.5	1.9
Pig Traps	4.412×10^{-3}	2	0.9
Piping $D \leq 3$ inches	1.422×10^{-4}†	2	1.2
Piping $3 < D < 11$ inches	4.021×10^{-5}†	1.8	0.8
Piping $D \geq 11$ inches	3.596×10^{-5}†	2	0.7
Pressure Vessels	1.834×10^{-3}	8	1
Pumps	6.231×10^{-3}	2.2	1.4
Turbines	3.755×10^{-2}	2	1.2
Actuated Valves	5.178×10^{-4}	1.3	0.9
Manual Valves	7.397×10^{-5}	2	0.9
All Valves	1.441×10^{-4}	1.7	0.9

† Incident rate per meter per year

9 References

[1] Marx, J.D. and J.B. Cornwell (2008), "*The Importance of Weather Variations in a Quantitative Risk Analysis.*" Presented at Mary Kay O'Connor Process Safety Center Annual Symposium, College Station, Texas, October 28-29, 2008.

[2] TNO (2005), *Guidelines for Quantitative Risk Assessment*, the Purple Book. CPR 18E, the Netherlands Organization for Applied Scientific Research, Committee for the Prevention of Disasters, the Hague, Netherlands, December 2005.

[3] OGP (2010), *Occupational Risk Assessment Data Directory*, Report No. 434-1. Process release frequencies. The International Association of Oil & Gas Producers. March 2010.

[4] PHMSA (2019), *Distribution, Transmission & Gathering, LNG, and Liquid Accident and Incident Data*. Pipeline and Hazardous Materials Safety Administration, Washington, DC, Updated March 7, 2019.
https://www.phmsa.dot.gov/data-and-statistics/pipeline/distribution-transmission-gathering-lng-and-liquid-accident-and-incident-data (accessed September 2019)

[5] HSE (2019), *Hydrocarbon Releases System*. Health and Safety Executive, United Kingdom.
http://www.hse.gov.uk/offshore/hydrocarbon.htm (accessed September 2019)

[6] CCPS (2000), *Guidelines for Chemical Process Quantitative Risk Analysis - Second Edition*. Center for Chemical Process Safety of the American Institute of Chemical Engineers, 3 Park Avenue, New York, New York, 10016. (ISBN 0-8169-0720-X)

[7] HSE (2019), *Statistics*. Health and Safety Executive, United Kingdom.
http://www.hse.gov.uk/offshore/statistics.htm (accessed September 2019)

[8] DNV (2013), *Failure Frequency Guidance - Process Equipment Leak Frequency Data for Use in QRA*. Det Norske Veritas AS, Norway, www.dnv.com.

[9] PLOFAM (2018), *Process Leak for Offshore Installations Frequency Assessment Model – PLOFAM(2)*, Lloyds' Register Group Limited, Report No. 107566/R1, December 6, 2018. (https://www.norskoljeoggass.no/contentassets/9972d6e9f1b74f158931aac3b462770e/107566_r1_final.pdf)

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Fault Tree Uncertainty Analysis

Raymond "Randy" Freeman*
S&PP Consulting
12303 Lake Shore Ridge
Houston, TX 77041
*Presenter E-mail: Rafree@yahoo.com

Abstract

Fault tree analysis (FTA) is a widely used methodology in the process industries. FTA is used for the development of failure mechanisms, computation of failure frequencies and the determination of the probability of failure on demand of safety systems. Much of the data used in a FTA study are uncertain. For example, the failure rate of a pump is often not known with great precision. Likewise the failure rates of instrumentation are often known only within some defined limits. The common practice, used by analysts in the quantification of a fault tree, is to use the most likely or best guess as to the needed failure rate data. The use of best guess values as data inputs to the quantification of a fault tree creates uncertainty in the computed results.

This paper presents a general methodology for the determination of the impact of uncertainty on the results of a fault tree study. The general methodology is based on the mathematics of propagation of error and variance contribution analysis. An example is presented to illustrate the application of the fault tree uncertainty analysis methodology to a real world problem.

Keywords: Quantitative Risk Assessment, Fault Tree Analysis, Uncertainty Analysis

1. Background

Fault tree analysis is a widely used method for representation of failure mechanisms in chemical plants. The methodology is described in the CCPS CPQRA guideline book [Ref. 1] and is extensively discussed in Chapter 9 of Lees [Ref. 2]. Lacking in these discussions is a systematic method to quantify the uncertainty of the results of the fault tree calculations.

Fault tree analysis has also been used in the aircraft and aerospace industries, nuclear power plant review and is recognized by the OSHA Process Safety Management (PSM) standard [Ref. 3] as a method for process hazards analysis.

2. Review of Error Propagation and Variance Contribution Analysis (VCA) Methodology

The mean and variance of a function of random variables can be approximated using the method described by Haugen [Ref. 4] and applied by Freeman [Ref. 5, 6, 7]. Define an arbitrary function of a set of random variables, x_i, as:

Let

$$Y = F(x_i) \qquad \text{(Eq 1)}$$

The mean of Y can be estimated using the following approximation:

$$E(Y) = F[\ E(x_i)] \qquad \text{(Eq 2)}$$

Where:

E(Y) = expected value of random variable Y = mean of Y

$E(x_i)$ = expected value of random variable x_i = mean of x_i

The variance of Y can likewise be estimated as:

$$V(Y) = \sum_{i=1}^{n}\left[\frac{\partial Y}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq 3)}$$

Where:

V(Y) = variance of random variable Y as defined above in Equation 1

$V(x_i)$ = variance of random variable x_i as defined above in Equation 1

Note that the variance is simply the square of the standard deviation. Using the variance will simplify the mathematics that is described below. The contribution of each independent random variable to the overall variance in the function is:

$$V(Y \text{ from } x_i) = \left[\frac{\partial Y}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq 4)}$$

The relative contribution of each term to the overall variance V(Y) is a measure of the importance in the uncertainty in the particular random variable, x_i. In effect, this is a sensitivity analysis combined with a uncertainty evaluation. The variance contribution combines the sensitivity in the answer to changes in the uncertain random variable, x_i, with a measure of the uncertainty in the random variable, x_i. The overall variance in Y is found by summing the sensitivity weighted variances from each random variable.

Numerical Estimate of the Sensitivity

Let us return to the fundamental definition of the derivative.

As before, set y = F(xi)

$$\frac{\partial y}{\partial x} = \lim_{\Delta xi \to 0} \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi}\right] \quad \text{(Eq 5)}$$

We are interested in a numerical estimate of the derivative. Therefore, we will make the following approximation.

$$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi}\right] \quad \text{(Eq 6)}$$

Linear Functions

Let us examine the approximation for a simple linear function.

Let Y = AX + B (Eq 7)

What is the sensitivity of Y to a change in variable X? By simple calculus:

$$\frac{\partial y}{\partial x} = A \quad \text{(Eq 8)}$$

We can also find the sensitivity using the numerical approximation as:

$$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi}\right] \quad \text{(Eq 9)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi + \Delta xi) + B) - (A(xi) + B)}{\Delta xi}\right] \quad \text{(Eq 10)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi + \Delta xi)) - (A(xi))}{\Delta xi}\right] \quad \text{(Eq 11)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{((A\,xi + A\,\Delta xi)) - (A(xi))}{\Delta xi}\right] \quad \text{(Eq 12)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{A\,\Delta xi}{\Delta xi}\right] \quad \text{(Eq 13)}$$

$$\frac{\partial y}{\partial x} = A \quad \text{(Eq 14)}$$

Note that for a simple linear equation the numerical result for the sensitivity is exactly the same as the analytical expression. There is no restriction on the size of the perturbation (Δxi) used in the calculations. Previously, Freeman [Ref 7] has suggested using a 10% perturbation in xi to do the sensitivity calculations. However any size of perturbation will work and generate the correct sensitivity.

This is a general result. As long as the function can be expressed as a linear function of a number of variables, xi, the sensitivity can be directly calculated by a simple perturbation of the function. The resulting sensitivity will be exactly the same as would be obtained using analytical methods.

Non-Linear Expressions

In the quantification of a fault tree, the top event frequency is computed using failure rates of the component devices and time that measures the interval between system validations. In a minimal cut set of two or more basic events, the time variable may be the same. For example the test interval for a valve may be the same for a pressure transmitter. A minimal cut set involving both the valve and the pressure transmitter would create a 2rd order term in the test interval. If the test interval is uncertain, how do we compute the sensitivity of the top event frequency with respect to the test interval? We will now explore how to deal with this type of problem when completing the uncertainty analysis.

As before, let

$$y = F(xi) = Axi^n + B \qquad \text{(Eq 15)}$$

What is the sensitivity of Y to a change in variable X? By simple calculus:

$$\frac{\partial y}{\partial x} = nAxi^{n-1} \qquad \text{(Eq 16)}$$

Let us evaluate the numerical approximation for this case. If n=2, the function of interest is:

$$y = F(xi) = Axi^2 + B \qquad \text{(Eq 17)}$$

From basic calculus, the exact analytical expression for the sensitivity is:

$$\frac{\partial y}{\partial x} = 2\ A(xi) \qquad \text{(Eq 18)}$$

If xi = 1

$$\frac{\partial y}{\partial x} = 2\ A \qquad \text{(Eq 19)}$$

Again the approximation of the derivative is:

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi+\Delta xi)^2+B)-(Axi+B)}{\Delta xi}\right] \qquad \text{(Eq 20)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi+\Delta xi)-F(xi)}{\Delta xi}\right] \qquad \text{(Eq 21)}$$

Inserting the equation for F(xi) we obtain:

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi+\Delta xi)^2+B)-(Axi+B)}{\Delta xi}\right] \qquad \text{(Eq 22)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A\,(xi^2+2\Delta xi+\,\Delta xi^2)\,+B)-(Axi+B)}{\Delta xi}\right] \quad \text{(Eq 23)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{A\,(xi^2+2\Delta xi+\,\Delta xi^2)\,-Axi}{\Delta xi}\right] \quad \text{(Eq 24)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(xi^2+2\Delta xi\,+\,\Delta xi^2)\,-xi}{\Delta xi}\right] \quad \text{(Eq 25)}$$

Setting xi =1, and using a 10% perturbation as $\Delta xi = 0.1\ xi = 0.1$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(1^2+(2)(0.1)1+0.1^2\,)\,-1}{0.1\,(1)}\right] \quad \text{(Eq 26)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(2)(0.1)+\,0.01}{0.1}\right] \quad \text{(Eq 27)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{0.21}{0.1}\right] \quad \text{(Eq 28)}$$

$$\frac{\partial y}{\partial x} = 2.1\ \mathrm{A} \quad \text{(Eq 29)}$$

Note that the numerical estimate (Eq 29) is approximately 5% greater than the analytical value (Eq 19). As shown in Table 1, for higher order equations the error will increase as the size of the perturbation becomes more important. Table 2 shows the impact of reducing the perturbation size to 1%. For 10^{th} order variables (say a minimal cut set with 10 basic events) the error is 5%. For almost all engineering evaluations, a maximum error of 5% should be adequate.

For cases where the test frequency, repair time, or mission time appears in a minimal cut set 3 or more times, I suggest that the following perturbation in time be used to compute the sensitivity of the top event:

$$\Delta time = 0.01\ time \quad \text{(Eq 30)}$$

The sensitivity of the top event frequency to all uncertain variables can be computed using a perturbation of 1%.

$$\Delta xi = 0.01\ xi \quad \text{(Eq 31)}$$

3. Fault Tree Analysis

Fault trees are often used to analyze potential failures of an engineered system. A fault tree is a failure logic diagram that shows the relationship of device or system failures leading to an accident. Fault tree analysis is covered in detail in the CCPS CPQRA book [Ref. 1]. A fault tree is constructed by starting with a top event or condition and asking the question:

What conditions lead to this outcome?

Each condition in the next layer down is then analyzed by asking the same question. What conditions lead to this outcome? The logic of how these intermediate conditions (termed intermediate events) are related is expressed using AND and OR logic gates. An AND gate output is true if and only if (iff) all of the inputs to the AND gate are all true simultaneously. An OR gate output is true iff one of the inputs to the OR gate is true.

Once the fault tree logic structure is created, numerical data can be used to calculate the frequency or probability of the top event of concern occurring. For fault trees where a basic event is found in multiple branches of the tree, such as power failure, the logic structure of the tree must be simplified to remove the impact of the repeated events on the top event of concern. This simplification is done using Boolean Algebra. Each resulting grouping of basic events can cause the top event to occur. These groupings of basic events are called minimal cut sets. As a simple example consider the the Boolean Algebra representation of a fault tree :

$$T = BE11 + BE1 \cdot BE2 + BE1 \cdot BE3 + BE2 \cdot BE9 + BE3 \cdot BE7 \qquad \text{(Eq 32)}$$

Where:

T = Fault Tree Top Event

BE11 = Basic Event 11

BE1 = Basic Event 1

BE2 = Basic Event 2

BE3 = Basic Event 3

BE7 = Basic Event 7

BE9 = Basic Event 9

+ = Boolean Algebra Addition Symbol

• = Boolean Algebra Multiplication Symbol

For this example the top event T, the minimal cut sets are:

BE11

BE1 BE2

BE1 BE3

BE2 BE9

BE3 BE7

For example the existence of basic events BE1 and BE3 guarantees that the top event T will occur. Publically available standard computer software such as SAPHIRE [Ref. 8] may be used to find the minimal cut sets of a large fault tree.

The representation of the top event in equation 32 can now be used to compute the probability or frequency of occurrence of the top event. If the devices describe by the basic events are non-repairable and are tested after a period of time TI, the probability of top event, T, may be calculated as:

$$\text{Prob}(T) = \lambda_{11}\, TI/2 + (\lambda_1\, TI/2)(\lambda_2\, TI/2) + (\lambda_1\, TI/2)(\lambda_3\, TI/2) + (\lambda_2\, TI/2)(\lambda_9\, TI/2) + (\lambda_3\, TI/2)(\lambda_7\, TI/2) \qquad \text{(Eq 33)}$$

Where:

λ_{11} = failure rate of device 11 in basic event BE11, failures per unit time

λ_1 = failure rate of device 1 in basic event BE1, failures per unit time

λ_2 = failure rate of device 2 in basic event BE5, failures per unit time

λ_3 = failure rate of device 3 in basic event BE3, failures per unit time

λ_7 = failure rate of device 7 in basic event BE7, failures per unit time

λ_9 = failure rate of device 9 in basic event BE9, failures per unit time

TI = test interval, time

Equation 33 assumes that the device failure rates are small and the product λ TI < 0.1. The other major assumption is that the values of all of the failure rates and test intervals are known. In reality the failure rate data are not known exactly with only a range or probability distribution representing the state of knowledge.

4. Example Problem

The following example is taken from the ISA technical report on fault tree analysis [Ref. 9]. This example should not be considered as a recommendation by either ISA or AIChE. The example is presented to allow for the demonstration of the methods that can be used in a fault tree study to quantify the uncertainty in the resulting calculated failure frequency or failure probability.

Consider the interlock on the intermediate storage tank T101 shown on Piping and Instrument Diagram in Figure 1. The interlock block diagram is shown in Figure 2. The interlock is intended to prevent an abnormal condition in the tank which could lead to a uncontrolled release of the tank contents. The process hazards analysis team has recommended that the interlock be designed to safety integrity level 2 (SIL 2) with a target probability of failure on demand (PFD) of no greater than 1E-2 or a risk reduction factor (RRF) of 100. Does the proposed interlock shown on Figure 1 meet the SIL 2 target? What is the uncertainty in the predicted PFD of the interlock?

A fault tree for the failure of this interlock is shown in Figure 3. A minimal cut set analysis has been completed and the resulting minimal cut sets are presented in Table 3. We can now write the Boolean Algebra equation that represents this fault tree as:

$$T = PE + TS1 \bullet TS2 + LS1 \bullet LS2 + FT1 \bullet FT2 + FT2 \bullet FT3 + FT1 \bullet FT3 + BV1 \bullet BV2 + BV1 \bullet SOL1 + BV2 \bullet SOL2 + SOL1 \bullet SOL2 + PT1 \bullet PT2 \qquad \text{(Eq 34)}$$

Assuming that the interlock is non-repairable until tested at time TI and using lamda-time (λT) approximation of the failure rate, the Boolean representation of the fault tree may now be converted to a failure probability model as:

$$\begin{aligned}\text{Prob (T)} = {} & \text{Prob(PE)} + (\lambda_{TS1}\, TI/2)(\lambda_{TS2}\, TI/2) + (\lambda_{LS1}\, TI/2)(\lambda_{LS2}\, TI/2) + (\lambda_{FT1}\, TI/2)(\lambda_{FT2}\, TI/2) + \\ & (\lambda_{FT2}\, TI/2)(\lambda_{FT3} TI/2) + (\lambda_{FT1}\, TI/2)(\lambda_{FT3}\, TI/2) + (\lambda_{BV1}\, TI/2)(\lambda_{BV2}\, TI/2) + \\ & (\lambda_{BV1}\, TI/2)(\lambda_{SOL1} TI/2) + (\lambda_{BV2}\, TI/2)(\lambda_{SOL2}\, TI/2) + \\ & (\lambda_{SOL1}\, TI/2)(\lambda_{SOL2}\, TI/2) + (\lambda_{PT1}\, TI/2)(\lambda_{PT2}\, TI/2) \qquad \text{(Eq 35)}\end{aligned}$$

Where:

Prob(PE) = failure probability of electronic logic solver, assumed to be constant at 5E-3.

λ_{TS1} = failure rate of temperature switch 1, failures per unit time

λ_{TS2} = failure rate of temperature switch 2, failures per unit time

λ_{LS1} = failure rate of level switch 1, failures per unit time

λ_{LS2} = failure rate of level switch 2, failures per unit time

λ_{FT1} = failure rate of flow transmitter 1, failures per unit time

λ_{FT2} = failure rate of flow transmitter 2, failures per unit time

λ_{FT3} = failure rate of flow transmitter 3, failures per unit time

λ_{BV1} = failure rate of block valve 1, failures per unit time

λ_{BV2} = failure rate of block valve 2, failures per unit time

λ_{SOL1} = failure rate of solenoid valve 1, failures per unit time

λ_{SOL2} = failure rate of solenoid valve 2, failures per unit time

λ_{PT1} = failure rate of pressure transmitter 1, failures per unit time

λ_{PT2} = failure rate of pressure transmitter 2, failures per unit time

TI = test interval, time

The electronic logic solver PE is assumed to have a constant failure probability of 5E-3.

Failure rate data for the other devices are present in Table 4. The mode (most likely value) of the failure rate is set equal to the point value taken from the ISA example [Ref. 9]. The triangular probability distribution (Appendix A) was assumed to represent the failure rate data for the equipment items. The upper and lower limits are based on the failure rate data of Appendix 4 of Smith [Ref. 10].

Using the device failure rates represented by the Table 4 column labeled as the mode and the minimal cut sets presented in Table 3, the ISA technical report [Ref.9, page 35] computes an interlock PFD as 7.5E-3 (RRF of 133). This would satisfy the requirement for a SIL 2 interlock {PFD of 1E-2 or a RRF of 100}. Now what is the uncertainty in the interlock PFD?

The first thing to remember is that the PFD should be calculated based on the mean value of the failure rate lambda (λ), not the mode of the failure rate. For a data set, the mean is the best single point representation of the data set. Table 5 presents the PFD of each minimal cut set using the mean of the device failure rate lambda (λ). The total of the PFD becomes 1.47E-2 (RRF of 68). This would not satisfy a SIL 2 interlock requirement.

Now we will compute the variance of the predicted probability of top event, T. To compute the variance of the probability of the top event, T, we will need to compute the sensitivity of the top event to each of the variables.

Sensitivity Using Numerical Perturbation Calculation

We will use the ISA interlock example previously analyzed by Freeman (Ref. 7). Using public data sources Freeman found that the probability of failure on demand (PFD) was 1.49E-2. To use the perturbation method for the evaluation of the sensitivities requires evaluating the impact of small changes in the uncertain input parameters. To enable these calculations to be completed numbers using 8 significant digits were used. The calculations were completed using Microsoft Excel which uses double-precision floating-point arithmetic compliant with IEEE 754 specification. Excel nominally carries 15 significant figures in calculations. We will complete the calculations with Excel displaying 5 significant digits and round the result at the end of the calculations to 4 significant digits. We will illustrate the calculations by looking at the Flow Transmitter, FT1.

a. First we recalculate the PFD of the example and find it to be 1.4594E-02. This is the base number that we will use in the perturbation calculations.
b. We now make a small change in mean failure rate of FT1. The mean failure rate is 8E-6 failures/hour. A 1% perturbation is used or an increase of 0.08E-6 failures/hour.
c. The perturbed value of the failure rate of FT1 becomes
(8 + 0.08) * 1E-6 failures/hour or 8.08E-6 failures/hour.
d. The perturbed value of the failure rate of FT1 is now used to re-calculate the PFD of the interlock. The resulting re-calculation finds that the PFD is 1.4618E-02
e. The change in the PFD from the base number due to the perturbation of the failure rate of FT1 is now computed as:

    delta PFD = 1.4618E-02 - 1.4594E-02 = 2.4556E-05

f. The sensitivity of the PFD to a change in the failure rate of FT1 is now computed by dividing the change in the PFD by the change FT1 failure rate as:

    sensitivity = (2.4556E-05)/(0.08E-6 failures/hour) = 307.0 hours
    Result is rounded to 4 significant digits.

We now note that in the paper by Freeman (Ref. 7) that equation 32 presents the sensitivity for FT1 as:

$$\frac{\partial Prob(T)}{\partial \lambda \mathrm{FT1}} = 307.0 \text{ hr} \qquad \text{(Eq 32 of Ref 7)}$$

The answers are exactly the same. The sensitivity calculations for all of the devices are presented in Table 6. Note that in every case the sensitivity found using the analytical expression and the numerical estimate are the same. This is a general result which will be true for all basic event equipment failure rates found in a fault tree minimal cut set.

Once found, the sensitivities can now be used to compute the variance contribution of each particular device to the overall variance of the top event PFD in the same manner as Freeman previously presented.

The sensitivities of the top event probability are summarized in Table 6. We may now compute the variance contribution of each uncertain variable using Equations 1 – 4 in the methodology section of this paper. The relative variance contribution is expressed as a percent of the total variance of the top event probability. The top event variance is found to be 8.24E-6 (failures per hour)^2 or equivalently the top event standard deviation is 2.78E-3 failures per hour.

In this example the variance (measure of uncertainty) is dominated by the flow transmitters. The flow transmitters account for almost 2/3 of the uncertainty in the top event probability. Failures of the flow transmitters appear in 3 of the minimal cut sets. Since the uncertainty in the transmitter failure rates is large, the flow transmitters should contribute a significant amount to the variance of the fault tree top event.

We can use the variance in the top event to define the likelihood of achieving SIL 2 performance of the interlock. The calculations are done using the normal probability distribution. The normal distribution is tabulated as the standard normal distribution using a normalization factor Z.

The standard normal factor, Z, [Ref. 11] is defined as:

$$Z = \left[\frac{xi - E(x)}{\sigma}\right] \qquad \text{(Eq 36)}$$

Where:

σ = standard deviation. Note that the variance of a random variable is the square of the standard deviation of the random variable.

E(x) = Expected value of the random variable x_i

For the example, the expected value of the probability of the top event of concern was calculated as

E[Prob(T)] =1.47E-2 (Eq 37)

From Table 4, the standard deviation in the probability of the top event is

σ_T = 2.78E-3 (Eq 38)

The target PFD for a SIL 2 interlock must not be worse than 1E-2 (RRF of 100).

We compute the normal distribution Z factor at the SIL 2 target value as

Z = (0.01 – 0.0147)/2.78E-3 (Eq 39)

Z = -1.69065 (Eq 40)

Tabulations of standard normal distribution are presented in most statistics books such as Meyer [Ref. 11]. For this value of Z, the corresponding probability that the interlock will achieve SIL 2 performance is 4.55 percent. We can also compute the risk reduction that the proposed interlock design will achieve.

What is the interlock probability of failure on demand (PFD) that we can be 95% certain that the interlock will provide? At the 95% level, the corresponding Z factor is 1.65 [Ref 11]. We now compute the corresponding PFD of the interlock that corresponds to this Z factor.

$$Z = \left[\frac{\mathrm{x95\%} - \mathrm{E[Prob(T)]}}{\sigma}\right] \qquad \text{(Eq 41)}$$

In this case:

$x_{95\%}$ = the PFD that we can be confident that the interlock will achieve

σ_T =2.78E-3 (Eq 42)

E[Prob(T)] =1.47E-2 (Eq 43)

Z= 1.65 (Eq 44)

Rearranging equation 40 to find $x_{95\%}$we obtain:

$x_{95\%} = E[Prob(T)] + Z\ \sigma_T$ (Eq 45)

$x_{95\%} = 1.47E\text{-}2 + (1.65)\ (2.78E\text{-}3) = 0.0193$ (Eq 46)

or a 95% certain risk reduction factor of

RRF = 1/PFD = 1/0.0193 = 52 (Eq 47)

By the same logic there is 5% chance that the risk reduction is a PFD of 0.01 or an RRF of 99. In summary, this interlock is likely to perform as a mid-range SIL 1 interlock, not the SIL 2 interlock desired by process hazards analysis team.

5. Methodology for Fault Tree Uncertainty Analysis

We can now generalize the methods used in the above example to a proposed method for the evaluation of the uncertainty in a fault tree. The following step-by-step procedure is modified from that that previously published by Freeman (Ref 7) to indicate the use of numerical methods to compute the sensitivity. Step 8 shown in *italics* indicates the modification..

1. Create the fault tree using standard methods outline in the CPQRA book [Ref 1].
2. Determine minimal cut sets by hand or using standard computer software such as SAPHIRE [Ref 12].
3. Define the needed failure rate data for each basic event.
4. Define those basic events that are considered to be uncertain.
5. For the basic events that are uncertain, define the probability distribution and associated parameters needed to numerically define the probability distribution. Appendix B of this paper presents the needed description of 4 commonly used probability distributions. In many cases the triangular distribution will be selected. The minimum, maximum and mode (most likely) parameters will be needed for the triangular distribution.
6. Compute the mean of each of the uncertain variable
7. Compute the probability or frequency of the fault tree top event of interest using the mean value for each uncertain variable.
8. *Compute the sensitivity of the top event probability or frequency using the numerical methods outlined in this paper.*
9. Compute the variance of each of the uncertain variables
10. Compute the variance contribution of for each of the uncertain variables to the top event probability or frequency using equation 6.
11. Compute the total variance of the top event of interest probability or frequency by summing all of the contributions determined in Step 10.
12. Compute the variance contribution percent of each uncertain variable by dividing the variable contribution (Step 10) by the total variance of the top event of interest (Step 11).
13. Define the level of risk the project is willing to take. What chance will the project management accept for potential failure of the interlock to achieve the desired risk reduction? In the above example, I have used a 5% risk of failure or a 95% certainty that the interlock will achieve a risk reduction factor of 52. In the example, there is a very low probability that the interlock will achieve a SIL 2 PFD of 0.01 or an RRF of 100.

Alternately you can report the 90% range for the top event of interest. For the example the 90% range starts at the 5% RRF of 99 and there is a 95% certainty that that an RRF of at least 52 will be achieved. The expected risk reduction for this interlock is an RRF of 68.

6. Conclusions

A general procedure has been presented to quantify the uncertainty in calculations of failure frequencies using the fault tree methodology. The uncertainty analysis procedure is based on the application of propagation of error and variance contribution analysis techniques to the minimal cut sets created during a fault tree study. The procedure is simple and can be incorporated into standard fault tree analysis programs such as SAPHIRE [Ref 8]. This procedure is based on perturbation calculation of the frequency of the top event from changes in the uncertain variables. Incorporation of a numerical perturbation method into standard fault tree software such as SAPHIRE would be easy to implement and would provide the means for evaluation of the uncertainty in the quantified fault tree results.

For the example interlock presented in this paper, the uncertainty in the device failure rates degrades the predicted interlock SIL from meeting SIL 2 requirements to becoming a mid range SIL 1 interlock. This is a general result. Uncertainty in design parameters will reduce the likelihood that the equipment will achieve desired results. The design engineer has two choices:

- Accept the conclusion that the interlock will not perform as SIL 2
- Re-design the interlock using more reliable components to achieve the SIL 2 target

The variance contribution analysis shown in Table 7 indicates that the major contributor to the uncertainty in the interlock performance is the Flow Transmitters. Flow transmitters certified to SIL-2 or SIL-3 performance with lower failure rates could improve the calculated PFD of the interlock.

7. References

1. Center for Chemical Process Safety , *Guidelines for Chemical Process Quantitative Risk Analysis – 2rd edition*, American Institute of Chemical Engineers, New York, 2000.
2. Frank P Lees, Loss Prevention in the Process Industries – 2rd Edition, Butterworth, ISBN 0-7506-1547-8, Oxford, UK, 1996
3. US Department of Labor, Occupational Safety and Health Administration, CFR 1910.119 - Process Safety Management of Highly Hazardous Chemicals, 1910.119(e)(2)(vi).
4. Edward B. Haugen, *Probabilistic Approaches to Design*, John Wiley, New York, 1968
5. Raymond. Freeman and Angela Summers, "Evaluation of Uncertainty in Safety Integrity Level Calculations," *Process Safety Progress,* Published online in Wiley Online Library (wileyonlinelibrary.com) DOI 10.1002/prs. 11805, 2016
6. Raymond. Freeman, "General Method for Uncertainty Evaluation of Safety Integrity Level Calculations – Part 2 Analytical Methods," *Process Safety Process*, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI 10.1002/prs 111915, October 2017

7. Raymond. Freeman ,“Error Propagation and Uncertainty Analysis: Application to Fault Tree Analysis”, Process Safety Progress, Published Wiley Online Library (wileyonlinelibrary.com/journal/prs) DOI: https://doi.org/10.1002/prs.12080, June 29, 2019
8. US Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) – Version 8,” NUREG/CR-7039, Vol 3, June 2011.
9. ISA, “Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of a SIF via Fault Tree Analysis, ISA Technical Report ISA-TR-84.00.02-2002 – Part 3, Approved 17 June 2002.
10. David J. Smith, *Reliability Maintainability and Risk – 8th Edition*, ISBN 978-0-08-096902-2, Elsevier, London, 2011
11. Paul L. Meyer, Introductory Probability and Statistical Applications, John Wiley, New York, 1972

Table 1. Comparison of Analytical Sensitivity with Numerical Approximation with Perturbation of 10% in xi for the equation: $y = F(xi) = Axi^n + B$

Order of Equation n	Equation for Analytical Sensitivity $\frac{\partial y}{\partial x} = nAxi^{n-1}$	Sensitivity with xi = 1 and A=1	Numerical Sensitivity with $\Delta xi = 0.1\ xi$	Error %
1	$\frac{\partial y}{\partial x} = 1A(xi)^0$	1	1	0
2	$\frac{\partial y}{\partial x} = 2A(xi)^1$	2	2.1	5
3	$\frac{\partial y}{\partial x} = 3A(xi)^2$	3	3.31	-10%
4	$\frac{\partial y}{\partial x} = 4A(xi)^3$	4	4.64	-16%
5	$\frac{\partial y}{\partial x} = 5A(xi)^4$	5	6.11	-22%
6	$\frac{\partial y}{\partial x} = 6A(xi)^5$	6	7.72	-29%
7	$\frac{\partial y}{\partial x} = 7A(xi)^6$	7	9.49	-36%
8	$\frac{\partial y}{\partial x} = 8A(xi)^7$	8	11.44	-43%
9	$\frac{\partial y}{\partial x} = 9A(xi)^8$	9	13.58	-51%
10	$\frac{\partial y}{\partial x} = 10A(xi)^9$	10	15.94	-59%

Error = (Analytical- Numerical)/Analytical

Table 2. Comparison of Analytical Sensitivity with Numerical Approximation with Perturbation of 1% in xi for the equation: y = F(xi) = $Axi^n + B$

Order of Equation n	Equation for Analytical Sensitivity $\frac{\partial y}{\partial x}$ = $nAxi^{n-1}$	Sensitivity with xi = 1 and A=1	Numerical Sensitivity with $\Delta xi = 0.1\, xi$	Error %
1	$\frac{\partial y}{\partial x} = 1A(xi)^0$	1	1	0
2	$\frac{\partial y}{\partial x} = 2A(xi)^1$	2	2.01	-1%
3	$\frac{\partial y}{\partial x} = 3A(xi)^2$	3	3.03	-1%
4	$\frac{\partial y}{\partial x} = 4A(xi)^3$	4	4.06	-2%
5	$\frac{\partial y}{\partial x} = 5A(xi)^4$	5	5.10	-2%
6	$\frac{\partial y}{\partial x} = 6A(xi)^5$	6	6.15	-3%
7	$\frac{\partial y}{\partial x} = 7A(xi)^6$	7	7.21	-3%
8	$\frac{\partial y}{\partial x} = 8A(xi)^7$	8	8.29	-4%
9	$\frac{\partial y}{\partial x} = 9A(xi)^8$	9	9.37	-4%
10	$\frac{\partial y}{\partial x} = 10A(xi)^9$	10	10.46	-5%

Error = (Analytical- Numerical)/Analytical

Table 3. Basic Events in Minimal Cut Sets For Example

Cut Set No	BE 1	BE 2
1	PE	-
2	TS1	TS2
3	LS1	LS2
4*	FT1	FT2
5*	FT2	FT3
6*	FT1	FT3
7*	BV1	BV2
8*	BV1	SOL1
9*	BV2	SOL2
10*	SOL1	SOL2
11	PT1	PT2

* Minimal cut Set with same basic event as another cut set

Table 4. Lamda (λ) Failure Rate Data With Uncertainty Limits

Device	Minimum Failures per 1E6 Hours	Mode Failures per 1E6 Hours	Maximum Failures per 1E6 Hours	Mean Failures per 1E6 Hours	Lamda Variance (Failures per 1E6 Hours)^2
Flow Transmitters FT1, FT2 and FT3	1.0	2.9	20.0	8.0	18.3
Pressure Transmitters PT1 and PT2	1.0	2.3	20.0	7.8	18.8
Temperature Switch TS1 and TS2	3.0	7.6	20.0	10.2	12.9
Level Switch LS1 and LS2	2.0	4.6	20.0	8.9	15.8
Block Valves BV1 and BV2	0.2	2.3	10.0	4.2	4.4
Solenoid Valves SOL1 and SOL2	1.0	2.3	8.0	3.8	2.3

Table 5. Probability of Minimal Cut Sets Based on Mean Failure Rates

Cut Set No	BE 1	BE 2	PFD based on mean λ
1	PE	-	5.00E-03
2	TS1	TS2	2.00E-03
3	LS1	LS2	1.52E-03
4	FT1	FT2	1.23E-03
5	FT2	FT3	1.23E-03
6	FT1	FT3	1.23E-03
7	BV1	BV2	3.38E-04
8	BV1	SOL1	3.38E-04
9	BV2	SOL2	3.38E-04
10	SOL1	SOL2	2.77E-04
11	PT1	PT2	1.17E-03

Table 6. Sensitivity of Example System PFD to Basic Event Failure Rates Based on a 1% Perturbation

Basic Event Label	Device Type	Mean Failures per 1E6 Hours	Failure Perturbation of 1% of Mean Failures per 1E6 Hours	Perturbed Failure Rate Failures per 1E6 Hours	Total System PFD Using Peturbed Failure Rate of Basic Event	Change in Total System PFD	Sensitivity of PFD to Change in Failure Rate Hours
FT1	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
FT2	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
FT3	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
PT1	Pressure Transmitter	7.8	0.078	7.878	1.460560E-02	1.167179E-05	149.6
PT2	Pressure Transmitter	7.8	0.078	7.878	1.460560E-02	1.167179E-05	149.6
TS1	Temperature Switch	10.2	0.102	10.302	1.461389E-02	1.995945E-05	195.7
TS2	Temperature Switch	10.2	0.102	10.302	1.461389E-02	1.995945E-05	195.7
LS1	Level Switch	8.9	0.089	8.989	1.460912E-02	1.519596E-05	170.7
LS2	Level Switch	8.9	0.089	8.989	1.460912E-02	1.519596E-05	170.7
BV1	Block Valves	4.2	0.042	4.242	1.460037E-02	6.445958E-06	153.5
BV2	Block Valves	4.2	0.042	4.242	1.460037E-02	6.445958E-06	153.5
SOL1	Solenoid Valves	3.8	0.038	3.838	1.459976E-02	5.832058E-06	153.5
SOL2	Solenoid Valves	3.8	0.038	3.838	1.459976E-02	5.832058E-06	153.5

Table 7. Variance of Top Event Probability Due to Uncertain Device Failure Rates

Device No	Device Type	Label	Sensitivity of Top Event Probability to Device Failure Rate Hour^{-1}	Variance of Device Failure Rate (Failures per 1E6 Hour)^2	Variance Contribution to Top Event Variance	Contribution to Top Event Variance %
1	Logic Solver	PE	-	0	0.00E+00	0%
2	Temperature Switch	TS1	195.7	12.9	4.94E-07	6%
3	Temperature Switch	TS2	195.7	12.9	4.94E-07	6%
4	Level Switch	LS1	170.7	15.8	4.60E-07	6%
5	Level Switch	LS2	170.7	15.8	4.60E-07	6%
6	Flow Transmitter	FT1	307	18.3	1.72E-06	21%
7	Flow Transmitter	FT2	307	18.3	1.72E-06	21%
8	Flow Transmitter	FT3	307	18.3	1.72E-06	21%
9	Block Valve	BV1	153.5	4.4	1.04E-07	1%
10	Block Valve	BV2	153.5	4.4	1.04E-07	1%
11	Pressure Transmitter	PT1	149.6	18.8	4.21E-07	5%
12	Pressure Transmitter	PT2	149.6	18.8	4.21E-07	5%
13	Solenoid valve	SOL1	153.5	2.3	5.42E-08	1%
14	Solenoid valve	SOL2	153.5	2.3	5.42E-08	1%

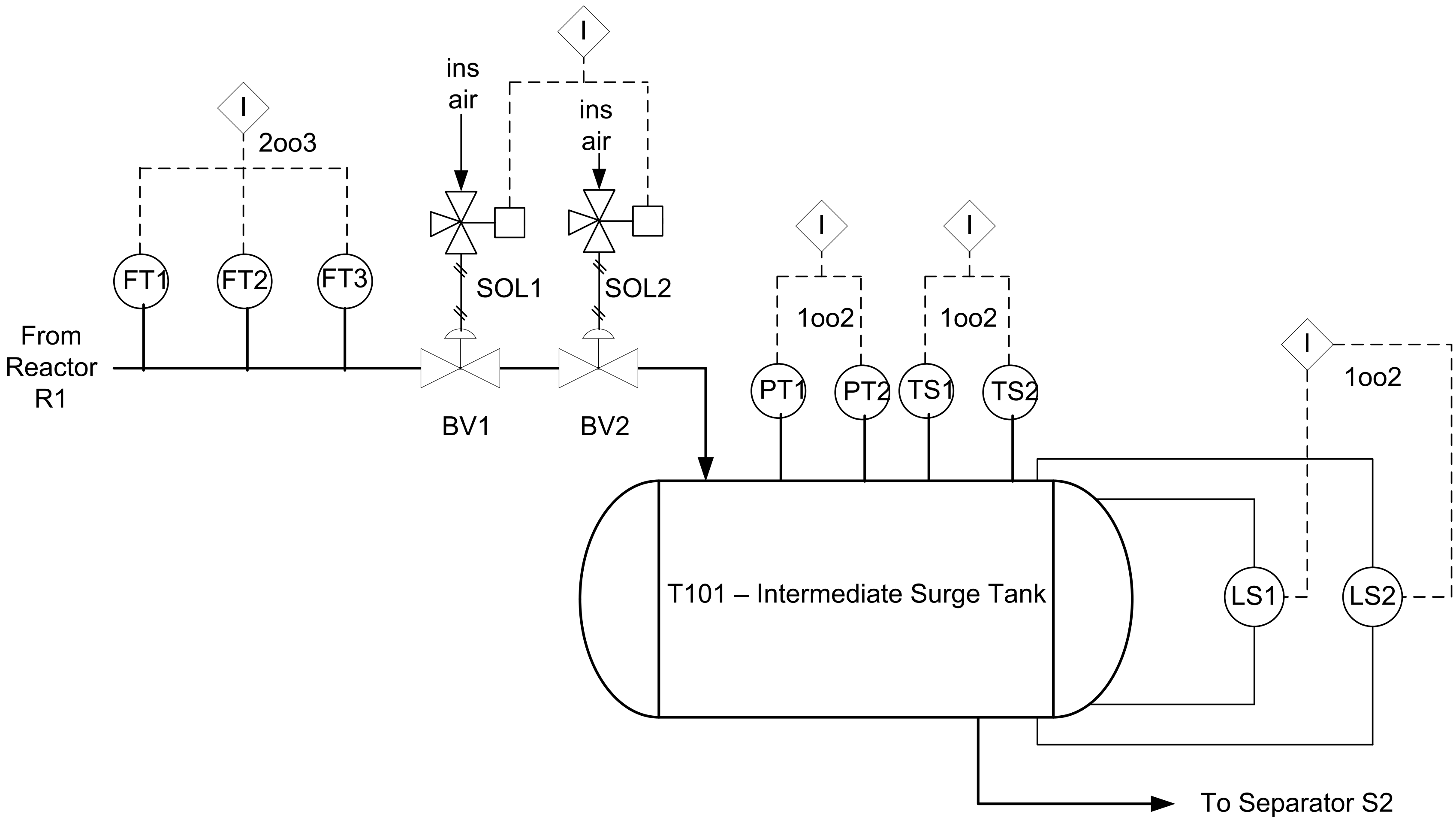


Figure 1. P&ID Diagram for Example

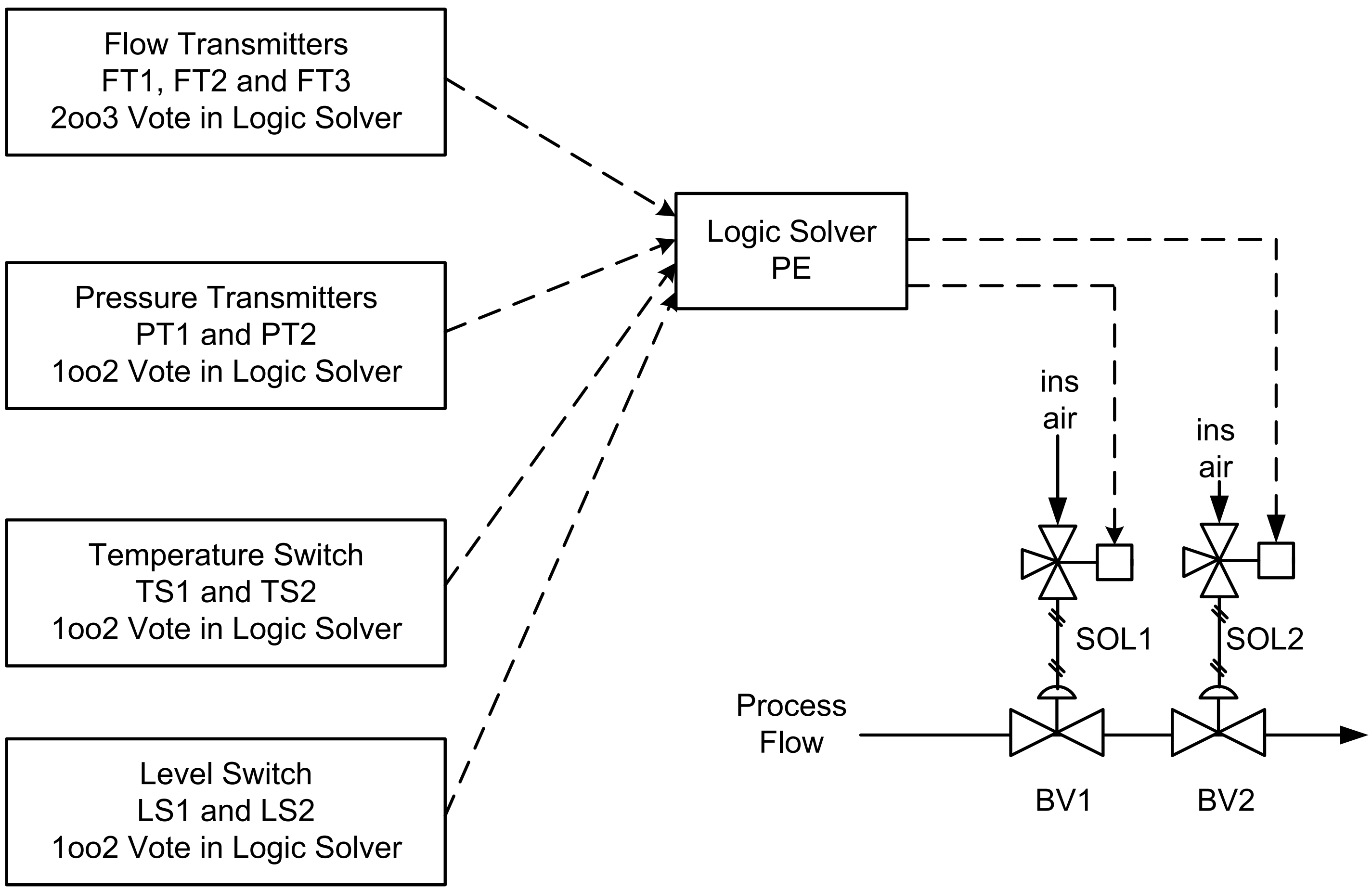


Figure 2. Interlock Block Diagram

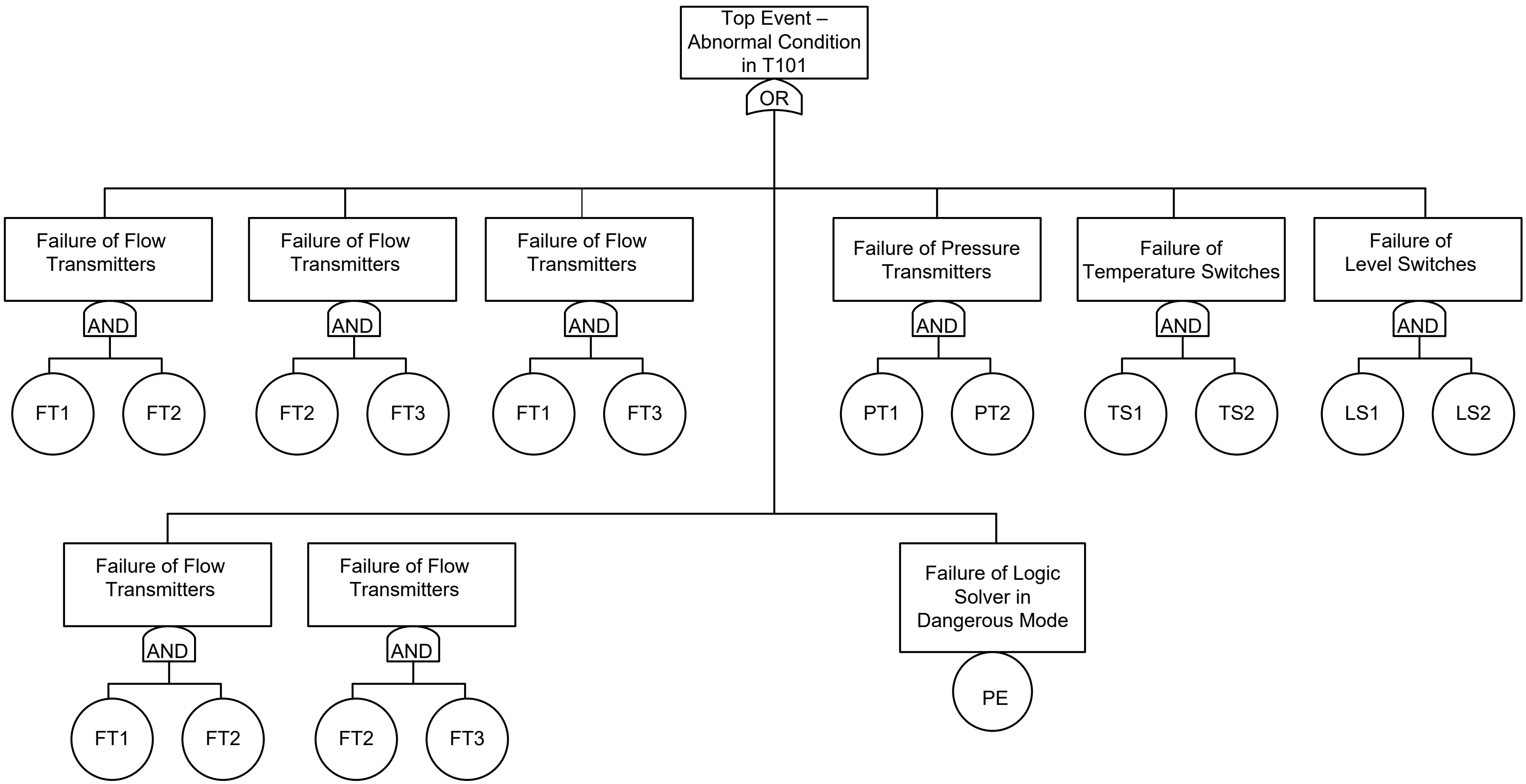


Figure 3. Fault Tree for Example Interlock

Appendix A – Commonly Encounter Probability Distributions

There are four probability distributions used to represent the failure rate of equipment items. These are:

1. Uniform Distribution
2. Triangular Distribution
3. Normal Distribution
4. Log-Normal Distribution

This appendix reviews the properties of these four probability distributions.

1. Uniform Distribution

The uniform distribution [Ref. A-1, pg 74; A-2, pg 687-688] is used when a variable is only known within a defined range. Figure A-1 presents a plot of the probability density function (pdf) for the uniform distribution. The distribution is defined using two parameters, A and B.

Where:

A = minimum value of the random variable

B = maximum value of the random variable

The mean or expected value of a random variable, x, that follows the uniform distribution is:

Mean = Expected Value – $E(x) = (A+B)/2$ (Eq A-1)

The variance of a random variable, x, that follows the uniform distribution is:

Variance = $V(x) = (B-A)^2/12$ (Eq A-2)

The standard deviation of a random variable, x, that follows the uniform distribution is:

Standard Deviation = $(\text{Variance})^{1/2} = (B-A)/(12)^{1/2}$ (Eq A-3)

2. Triangular Distribution

The triangular distribution [Ref. A-2, pg 686-687] is used when a variable is known to lie within a defined range and a "best guess" or estimate can be made as to the most likely value to the variable. Figure A-2 presents a plot of the probability density function (pdf) for the triangular distribution. The distribution is defined using three parameters, A. B and C.

Where:

A = minimum value of the random variable

B = maximum value of the random variable

C = most likely (mode) of the random variable

The mean or expected value of a random variable, x, that follows the triangular distribution is:

Mean = Expected Value – $E(x) = (A+B+C)/3$ (Eq A-4)

The variance of a random variable, x, that follows the triangular distribution is:

$\text{Variance} = V(x) = [A^2 + B^2 + C^2 - AB - AC - BC]/18$ (Eq A-5)

The standard deviation of a random variable, x, that follows the triangular distribution is:

$\text{Standard Deviation} = (\text{Variance})^{1/2} = \{[A^2 + B^2 + C^2 - AB - AC - BC]/18\}^{1/2}$ (Eq A-6)

3. Normal distribution

The normal distribution [Ref A-2, pg 665-666] is used when a variable when data analysis finds the normal distribution is the best model to describe the spread in the measured variable. Figure A-3 presents a plot of the probability density function (pdf) for the normal distribution. The distribution is defined using two parameters, μ and σ.

Where:

μ = mean of the measured data for variable

σ = standard deviation of the measured data for variable

The expected value of a random variable, x, that follows the normal distribution is:

$\text{Expected value} = \text{mean} = E(x) = \mu$ (Eq A-7)

The variance of a random variable, x, that follows the normal distribution is:

$\text{Variance} = \text{square of standard deviation} = V(x) = \sigma^2$ (Eq A-8)

The standard deviation of a random variable, x, that follows the normal distribution is:

$\text{Standard deviation} = \sigma$ (Eq A-9)

4. Lognormal Distribution

The lognormal distribution [Ref. A- 2, pg 658-659] is used when a variable when data analysis finds the lognormal distribution is the best model to describe the spread in the measured variable. Figure A-4 presents a plot of the probability density function (pdf) for the lognormal distribution. Many variables in nature are lognormally distributed (for example the height of people). The log normal distribution is used when the variable of interest has a known physical lower limit of zero. A variable, x, is lognormally distributed if ln(x) is normally distributed. The lognormal distribution is defined using two parameters, μ_y and σ_y.

Let the original data be defined by the variable x with mean and standard deviation as:

μ_x = mean of the measured data for variable x

σ_x = standard deviation of the measured data for variable x

Define a new variable y as:

$y = \text{Ln}(x)$ (Eq A-10)

Then variable x is said to be lognormally distributed if y is normally distributed. We can now write the mean and standard deviation of y (μ_y and σ_y.) [Ref. A-3, A-4 and A-5] as

$\mu_y = Ln[\mu_x^2 /((\sigma_x^2 + \mu_x^2)^{½})]$ (Eq A-11)

$\sigma_y = [Ln(\sigma_x^2 / \mu_x^2 + 1)]^{½}$ (Eq A-12)

Where:

Ln is the natural logarithm (base e) of the argument

Appendix A References:

A-1. P. L. Meyer, *Introductory Probability and Statistical Applications*, 2nd Edition, Addison-Wesley, Reading Mass, Library of Congress Catalog no. 75-104971, 1972, pp. 74

A-2. D. Vose, *Risk Analysis–A Quantitative Guide*, 3rd edition, Wiley, Chichester, West Sussex, England, ISBN 978-0-470-51284-5, 2008, pp. 686-687

A-3. "Lognormal mean and variance - MATLAB lognstat". www.mathworks.com. Retrieved 27 December 2018

A-4. M. Mood, F. A. Graybill, and D. C. Boes. *Introduction to the Theory of Statistics.* 3rd ed., New York: McGraw-Hill, ISBN 0-07-042864-6, 1974. pp. 117.

A-5. E.L. Crow and K. Shimizu, Lognormal Distributions – Theory and Applications, Marcel Dekker, New York, ISBN 0-8247-7803-0, 1988, pp. 9

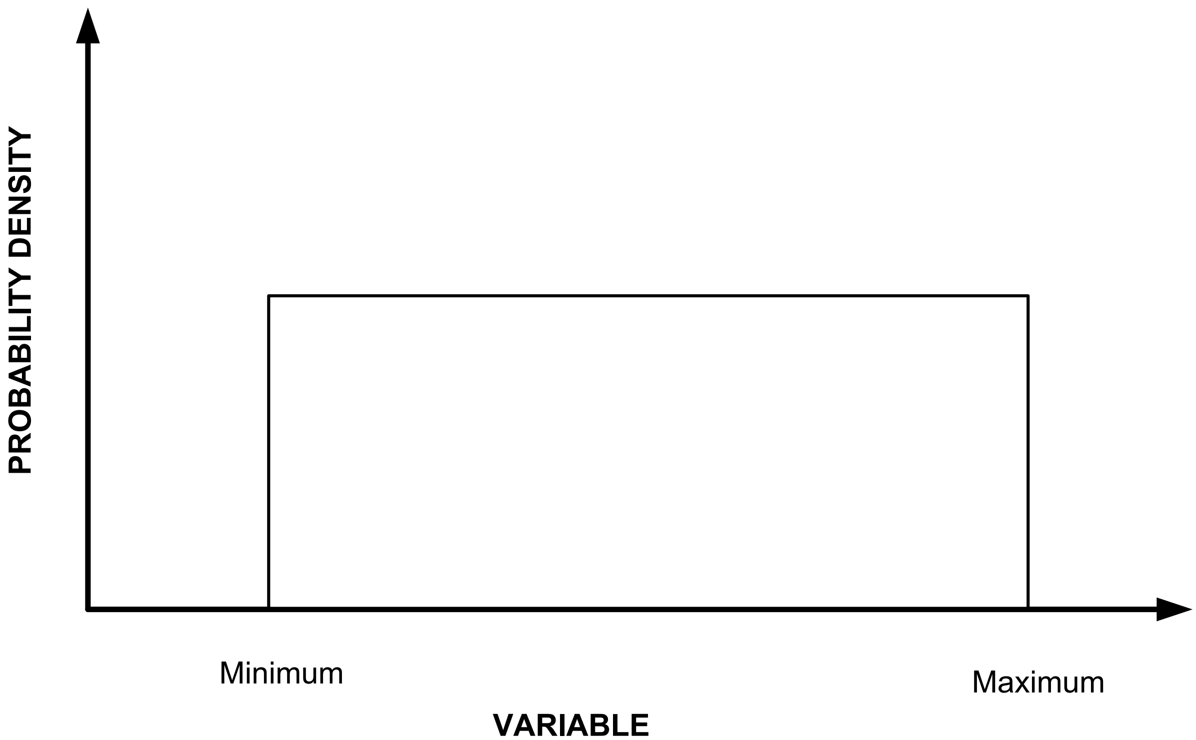


Figure A-1. Uniform Probability Distribution

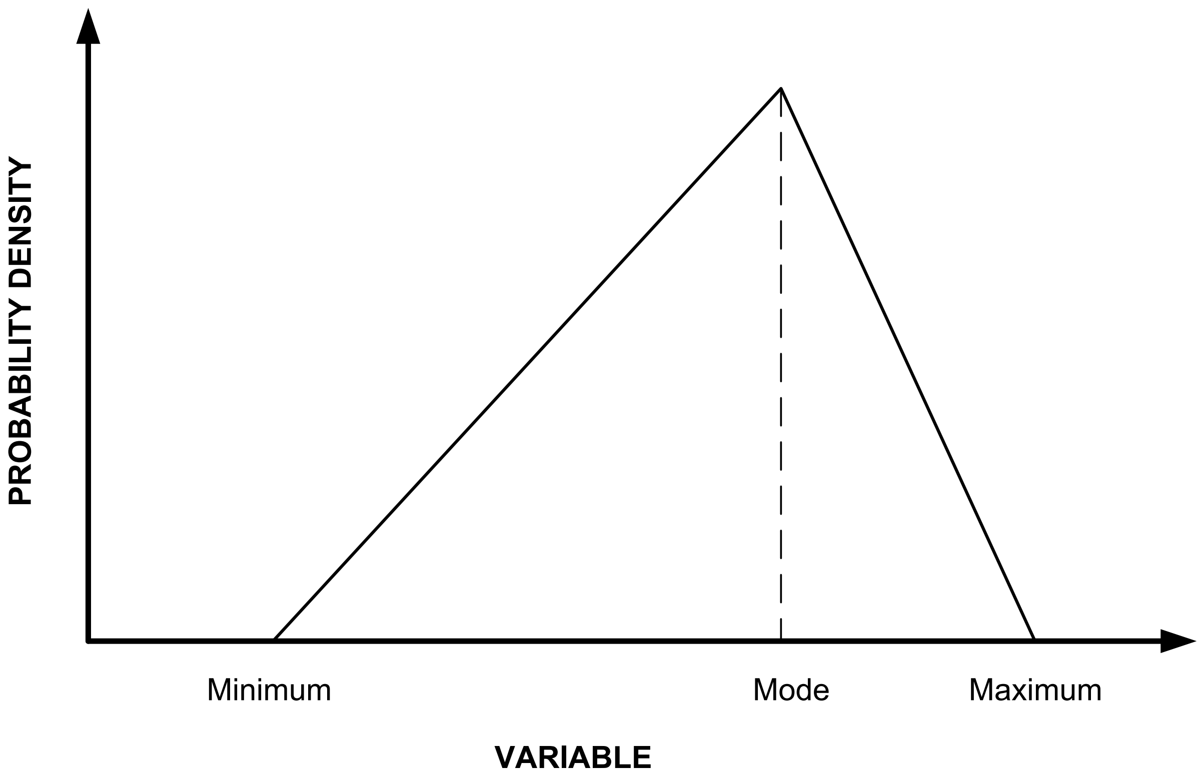


Figure A-2. Triangular Probability Distribution

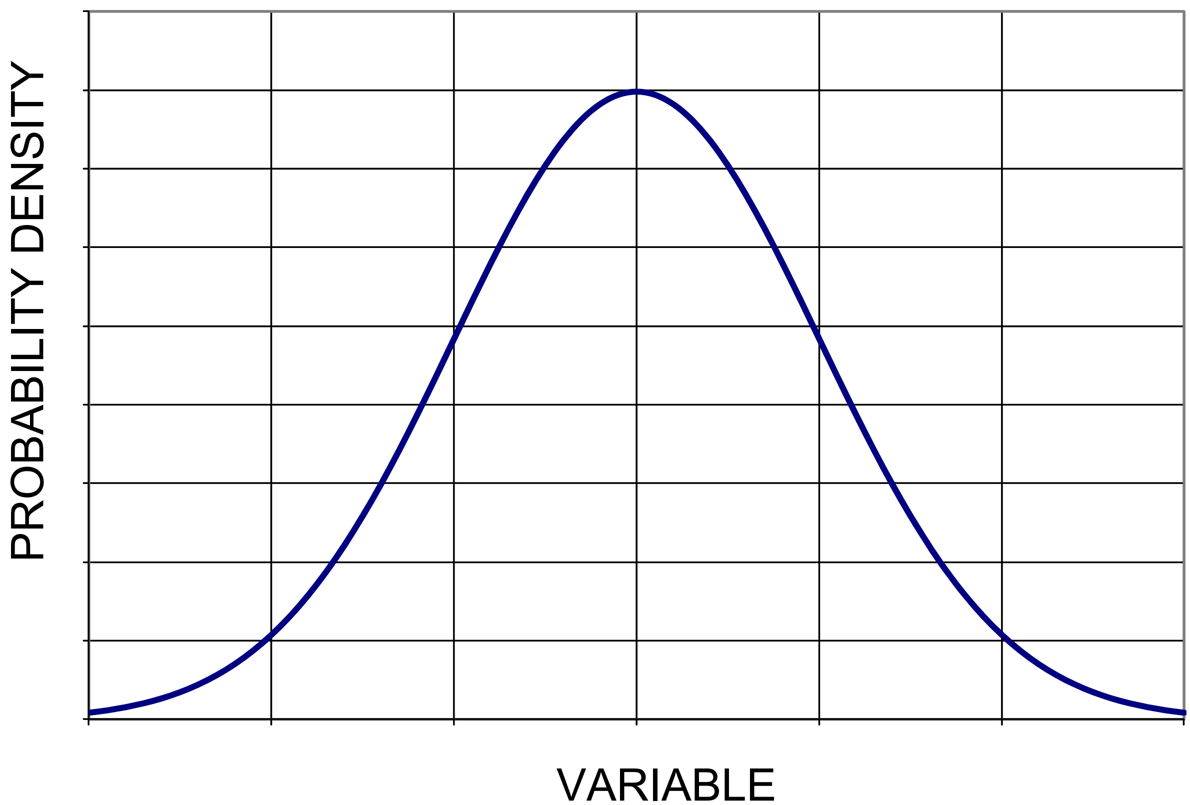


Figure A-3. Normal Probability Distribution

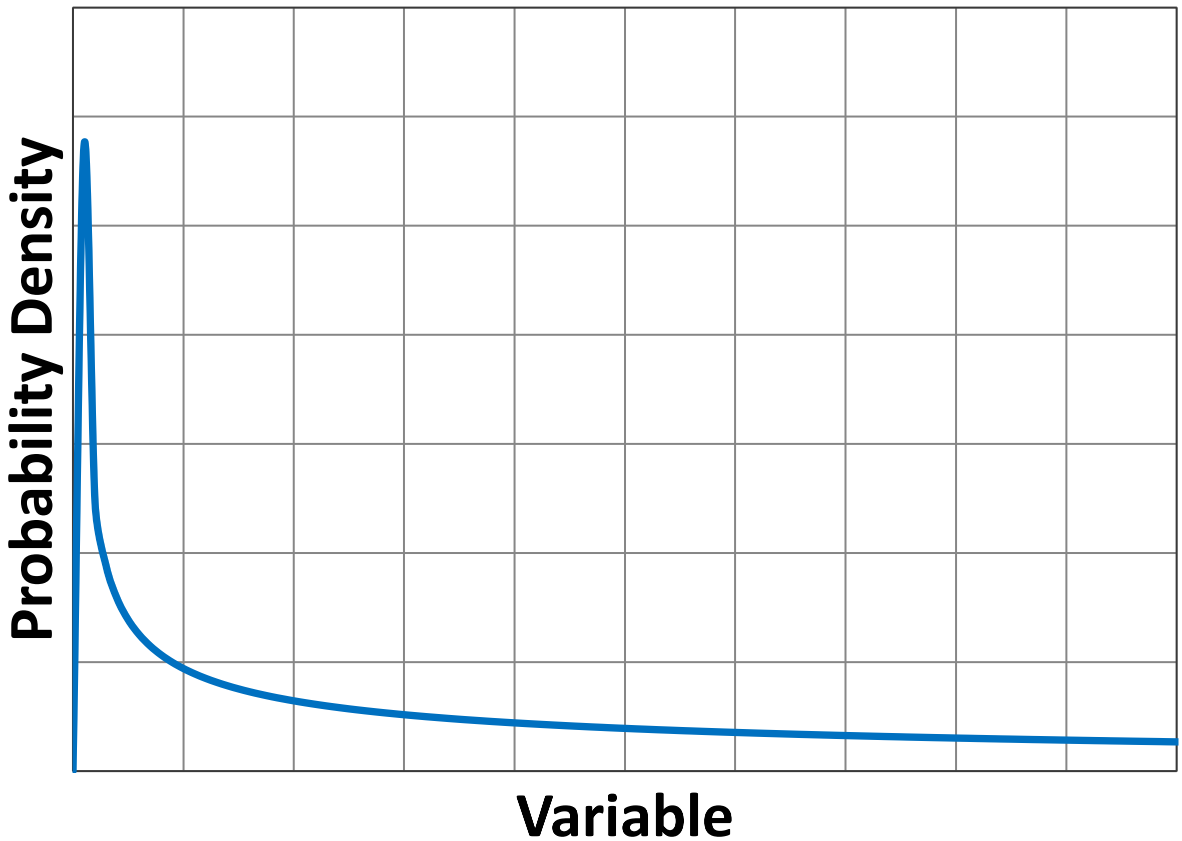


Figure A-4. Lognormal Probability Distribution

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Assessment of Hazard Analysis and Implementation of STPA in Process Industry

Parveen Chahal, Javeed I Mohammed
Fluor Canada Ltd.
*Presenters E-mails: *christina.ng@fluor.com, javeed.mohammed@fluor.com, parveen.chahal@fluor.com,

Abstract

High-performance computing has changed the world on its head with capabilities of image processing and artificial intelligence. The world of Energy and chemical has also changed with the adoption of these highly complex computing power and software capabilities of the modern processors by adoption of smart measurement technology (in sensors and final elements) and development of complex software algorithms. The modern technology has helped to put the plants to optimum level of operation and close to design margins to maximize profitability, which resulted in adding to the complexity of process control strategies.

With the advent of complex software capabilities the understanding the flaws in the specification and hazard identification process is not well understood.

Process Industry uses many available tools / techniques for HAZARD identification but many of these techniques predate to the advent of these advancement being made in the computer technology. Industry uses international performance based standards viz. IEC 61508/61511 which do provide guidelines to eliminate the "systematic errors" that may propagate through the design of the safety systems life cycle and render the safety system useless in certain modes of operation. Still there have been many incidents /near misses that have the potential to cause hazard to the People, Asset and environment which highlights that there is a plank missing which can help and reduce the number of incidents by designing more robust safety systems.

STAMP model address these concerns which indicate that "the safety related incidents can be related to flaws in requirement specification" (Prof. Nancy Leveson)

1. Introduction

The concept of process safety has come to the forefront of Energy and Chemical industry due to various incidents like Flixborough, Piper Alfa, BP Texas city and has become norm for operating companies, being required by legislation as well as by industry standards. The industrial standards, rather than being prescriptive, are performance based. The industry however still adheres to proven safety codes like NFPA-85 for boiler and combustion safety.

In Energy and chemical industry the process safety is managed as follows

- Structured study for the Identification of Hazards (eg. HAZOP)
- Allocation of safety function to protection layers viz. Quantitative / qualitative risk analysis (eg. FTA, Risk Matrix, LOPA etc.)
- Design and Engineering of Safety System: SIL level design verification including verification of systematic capability to address interactions within different components of the subsystem.
- Installation, commissioning and validation of the safety system for continued reliability of operation
- Management of changes in design and impact analysis of the changes

The backdrop to this view of process safety has been implementation of high-performance computing which changed the world on its head with capabilities of image processing and artificial intelligence. The world of Energy and chemical has also changed with the adoption of these highly complex computing power and software capabilities of the modern processors by adoption of smart measurement technology (in sensors and final elements) and development of complex software algorithms. The modern technology has helped to put the plants to optimum level of operation and close to design margins to maximize profitability, which resulted in adding to the complexity of process control strategies.

With the advent of complex software capabilities the understanding the flaws in the specification and hazard identification process is not well understood.

Process Industry uses many available tools / techniques for HAZARD identification but many of these techniques predate to the advent of these advancement being made in the computer technology. Industry uses international performance based standards viz. IEC 61508/61511 which do provide guidelines to eliminate the "systematic errors" that may propagate through the design of the safety systems life cycle and render the safety system useless in certain modes of operation. Still there have been many incidents /near misses that have the potential to cause hazard to the People, Asset and environment which highlights that there is a plank missing which can help and reduce the number of incidents by designing more robust safety systems.

1.1 Present state of the industry in Hazard Analysis and Identification

Hazard identification is first and most important activity of the safety life cycle and lays the foundation stone of the Safety System. Hazard & Operability study (HAZOP) has been an integral part of identifying the Hazard in process plants. This HAZARD identification or design verification process have been adopted in response to various disaster in process industry which involved significant plant damage, environmental damage and worse of them all being loss of lives.

So application of Hazard identification in process industry has almost been a knee jerk reaction. It is seen as one the critical (and payment) milestone on the project schedule. The HAZOP ToR(term of reference) is a key document which is developed by HSE, Process Engineering and Safety Engineering department. The final outcome of this painstaking, multidisciplinary brain-storming exercise is to identify the risks in the process and also identify (or design) the safeguards that are appropriate for risk as determined by risk ranking of the Hazards. Due to the sheer nature and process of HAZOP, it is generally done on mature designs. However there are various other analytical methods which can be implemented in Hazard Identification like

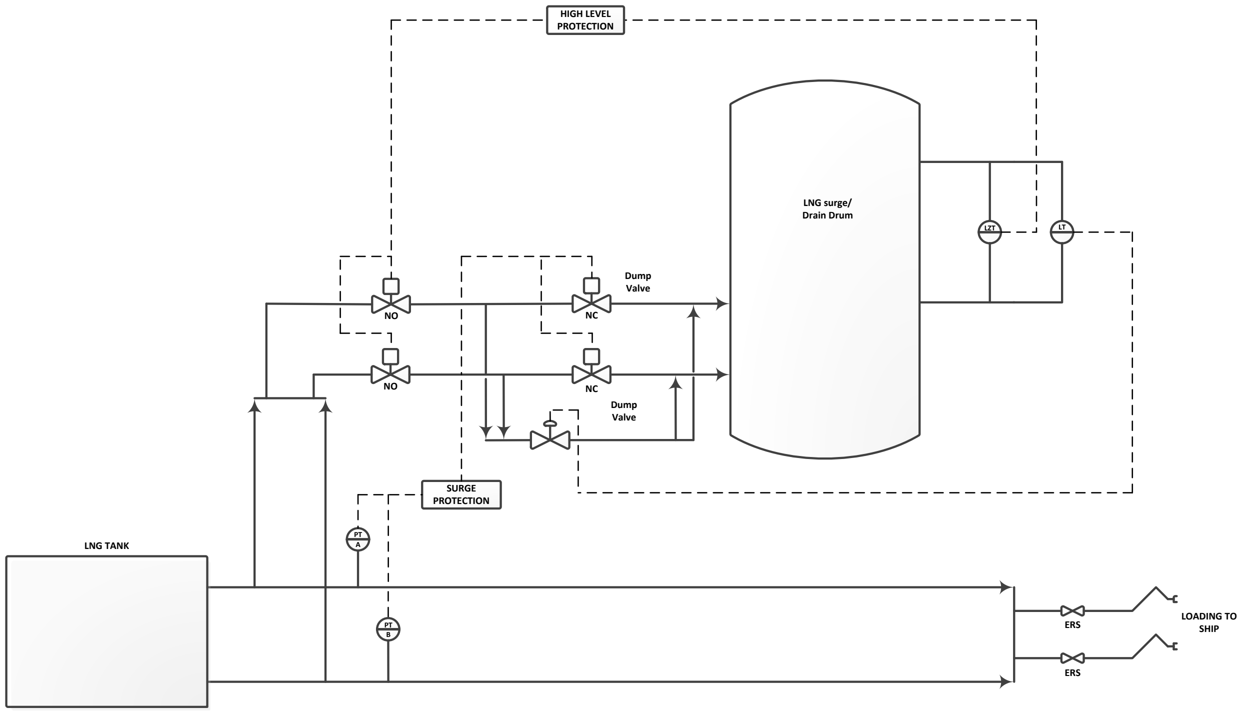
- What-If Analysis
- Failure Modes and Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Bow-tie analysis

From traditional execution point of view, HAZOP can be seen as a formal audit, or design verification tool of an essentially mature design. So HAZOP relies on the overall design process to properly consider hazards, risk and safeguards. The next step in the life cycle is to conduct Layer of Protection Analysis (LOPA) which identifies the independent protection layers to guard against the hazard. The safeguards shall being identified during the LOPA analysis shall be Specific, Independent, Dependable and Auditable.

1.2 Case Study – LNG Tank Loading

LNG storage tank continuously receives rundown LNG from the LNG trains. LNG is stored in storage tank and is shipped to the Jetty via 2 redundant lines (approx. 1.5 km away). There are 2 modes of operation:

- Holding Mode – In this mode the LNG is circulated to the Jetty for cold keeping and to prevent vapor accumulation in loading line. The LNG goes through one header and returned through the other. Only 1 LNG loading pump (inside the LNG tank) is running during this mode.
- Loading Mode – In this mode LNG is pumped from the LNG storage tank and loaded into an LNG carrier through redundant loading lines.



LNG Loading

During normal operation a small fraction of LNG is also routed to the LNG drain / Surge Drum to maintain the drum at the operating temperature. The level inside the drum is maintained by level controller via control valve which is located on the bypass line of the Normally Closed Dump Valves.

During loading mode the if there is an emergency at the Jetty, Loading arm or at the ship the Emergency Release System (ERS) valves are closed within 5 seconds to prevent damage to the loading arms. Some of the safeguards are as follows:

Excessive movement of the loading arm will close the ERS valves and open the normally closed Dump Valves within 5 second matching the closing time of the ERS valves.

Emergency shutdown at the ship will also initiate the closure of ERS and also opens the dump valve within 5 seconds

Activation of ERS will result in high pressure on the LNG loading lines, which will be detected by the pressure transmitters which in turn will activate the surge protection and open the dump valve in 5 seconds.

High-high level inside the Drain / Surge Drum will initiate high high level protections and close the valves upstream of the dump valves and also trip the LNG pumps.

1.3 Incident

In case of activation of ESD from ship the ERS valves closed in 5 seconds and activated the surge protection which opened the dump valve in 5 seconds. The level inside the Drain/

Surge vessel rises instantaneously to high-high level and initiated the high-high level protection. This protective function closed the valves upstream of the dump valve which conflicted with the design intent of the surge protective function and resulted in aborting the surge protection.

In the above example all the functions performed as designed but there was a systematic error in the design which could not be identified by conventional HAZOP technique due to the inherent nature of how HAZOP is conducted.

2. Missing link and expert analysis

There is no substitute for expert thought; providing that thought, however, is easy to say, but hard to do.

Some barriers to the kind of careful, expert thought; which is needed for effective systems theoretic implementation that are addressed in the paper are:

- Time constraint, lack of skills and retiring of experts
- Risk and the problem of scale
- Countervailing effect of advancements in engineering

2.1 Time constraint, lack of skills and retiring of experts

Not very long ago majority of the big Oil and Gas operating companies had quite a large number of experts who were engaged in projects and were available for resolving complex problems. Majority of these groups are now dismantled or dissolved due to restructuring within the organizations and/or cost reasons and/or retiring of the experts in task force. The current situation is that fairly inexpert personnel in the organization are trying to solve these problems by applying complex – typically performance based -standards that they understand fairly poorly. As a result many of the big operating companies prepared heavily prescriptive engineering specifications. But even the best standards require a considerable level of understanding and cannot be used as a replacement of the experience. Many of the personnel in the projects are new to the organization and do not completely understand the intent behind these specifications. Lack of understanding of specifications coupled with fast paced schedules has made the situation even worse.

2.2 Risk and the problem of scale

Risk appetite is function of organizational scale. For a big multinational Oil and Gas organization, operating plants at multiple plants across the globe, the impact of releasing a hazard or catastrophe is quite high, but for a small operating company the impact of a Hazard is not huge. Hence smaller companies do not have much of an incentive to carefully evaluate the risk in their plants.

The risk matrices perform poorly at the edges which reflect frequent-but-trivial and catastrophic-but-rare. So using these matrices at the extremes can provide either highly over rated systems (more CAPEX and OPEX) or under specified systems. Big operating companies generally use more sophisticated and quantitative analysis for such high consequence e scenario to properly asses the Hazard in the process and optimizes the design. Smaller organization on the other hand does not see potential benefits out of it.

So these two considerations indicate that large organizations are likely to see more potential benefits of systems theoretic approach.

2.3 Countervailing effect of advancements in engineering and corporate policies

It might seem that the large organizations have higher incentives in implementing the Systems theoretic implementation but – Don't count your chickens before they hatch.

Large organizations have technical experts who work with more stringent safety standards which provide proven guidance on implementation of these standards with proven outcomes.

Also bigger organizations have corporate safety policies which place onus on safety first and value safety more than the production. These policies are part of corporate safety culture and have been proven by test of time.

As a result, surprisingly, big organizations also have less incentive to adopt new approaches.

3. Traditional process safety and systems theoretic approach

Highly sophisticated and new hazard analysis technique like Systems Theoretic Process Analysis (STPA) and Causal Accident Systems Theoretic (CAST) which are based on an extended model of accident causation are widely applied in aerospace and automobile sector and can be applied to process industry but the focus here is on how to apply the systems theoretic approach on the already available methods in process industry.

3.1 Opportunities in quantitative and semi-quantitative methods

There are various quantitative and semi-quantitative techniques available but the most commonly used techniques are LOPA and Bow-tie. LOPA is a semi-quantitative analysis and is a simplified method of risk assessment that provides much needed middle ground between qualitative hazard analysis and traditional, quantitative analysis.

LOPA provides a chain of event leading to the Hazard and may not be the best tool for analyzing all the hazardous event outcomes but these this tool can be used a starting point which can combine the simplicity with a meaningful level of analysis. LOPA can be used to change the perception of risk that one evaluates in qualitative reviews like HAZOP to a more scientific approach like STPA. It can be used a first step towards such a transition.

Bow-tie on the other hand is not being currently used many organization in process industry. The ones who use this technique do not the understand power of this tool and merely use it as verification tool to count the barriers leading to a hazard. Bow-tie can analyze multiple initiating scenarios and multiple consequences at same time which can be the tool used to analyze more complex scenarios and transition from traditional approach to scientific approach.

3.2 Alarm objective Analysis

With the advent of sophisticated control systems and advance computing capabilities more complex logic can be implemented but this also resulted in unnecessary complexities and operability issues.

More and more alarms are being added sometimes even when not necessary which subsequently results in unnecessary nuisance and overwhelming the operator and diverting attention from important issues during an emergency or shutdown. Majority of the alarms are recommended during the HAZOPs as the team assessing the design thinks it as a good to have feature. Later in the project during the Alarm rationalization workshops majority of these alarms are deleted. This is a clear indication that the team involved in providing these kinds of recommendation does not understand the implications of adding so many alarms and fully understand the process.

The process of alarm rationalization itself is an activity which can help in understanding the operation of the plant from a system engineering approach rather than the conventional approach used during the conventional methods lie HAZOP and can be viewed as a step in transitioning towards systems model.

4. Implementation in Energy & Chemicals

Hazards present in Energy & Chemicals are different from other industries where STAMP model have been implemented. The following factors are unique to process sector.

4.1 Multiple failures and Global Acceptance

Majority of failures in process industry are not due to a single component failures but are a result of multiple component failures which interact with each other and loss of containment being at the center of the multi-casualty incidents. As a result the professional believe that reliability and availability model are best models for identification of hazards especially with limited expertise with in the industry. Many NoBo (Notified bodies) and standards like IEC 61511 ask for a functional safety assessment (FSA) complying with the local regulations or with international standards before the startup. Convincing the end users and these regulators to accept a new technique like STPA will take some time.

4.2 Designers and Operators

EPC companies are involved in the designing of the plants are not involved in the operation of the plant. They can provide guidance and provide recommendation to the end user to operate the plant within safe design criteria. So once the plant is handed over to the end-user they have no control or ability to prevent the system to migrate to higher risk state or beyond the safe design limits

5. Conclusion

Looking into the kind of techniques currently used in process industry it does represent an advance in the opinion on how the risk is assessed and managed. Over time the there is a potential to insert more rigorous technologies like STAMP models to identify the Hazards. Adapting to these new models will guide the operating companies on how to operate the plants within the constraints identified in the design.

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Quantitative Review of Storage Tank Performance in Extreme Weather Events (Hurricanes, Flooding, Rainfall)

Philip E. Myers*, P.E., George Woodworth, Ph.D.
PEMY Consulting, LLC
*Presenter E-mail: phil@pemyconsulting.com

Table of Contents

Organization

This paper is divided into 4 parts:

1. Abstract and Introduction
2. Water and Wind
3. Estimating Water Loads on Floating Roofs
4. Summary and Conclusions

Part 1: Abstract and Introduction

Severe natural disasters can trigger disasters or "domino events". These natural events are initiators called Natech events (Natural Hazard Triggering Technological disasters) and certainly hurricanes represent such events. Consider the threat of hurricane exposure on petroleum storage facilities located in the US Gulf Coastal and eastern seaboard regions. Figures 1 and 2 make it clear that both hurricanes and petroleum facilities have a high potential to interact.

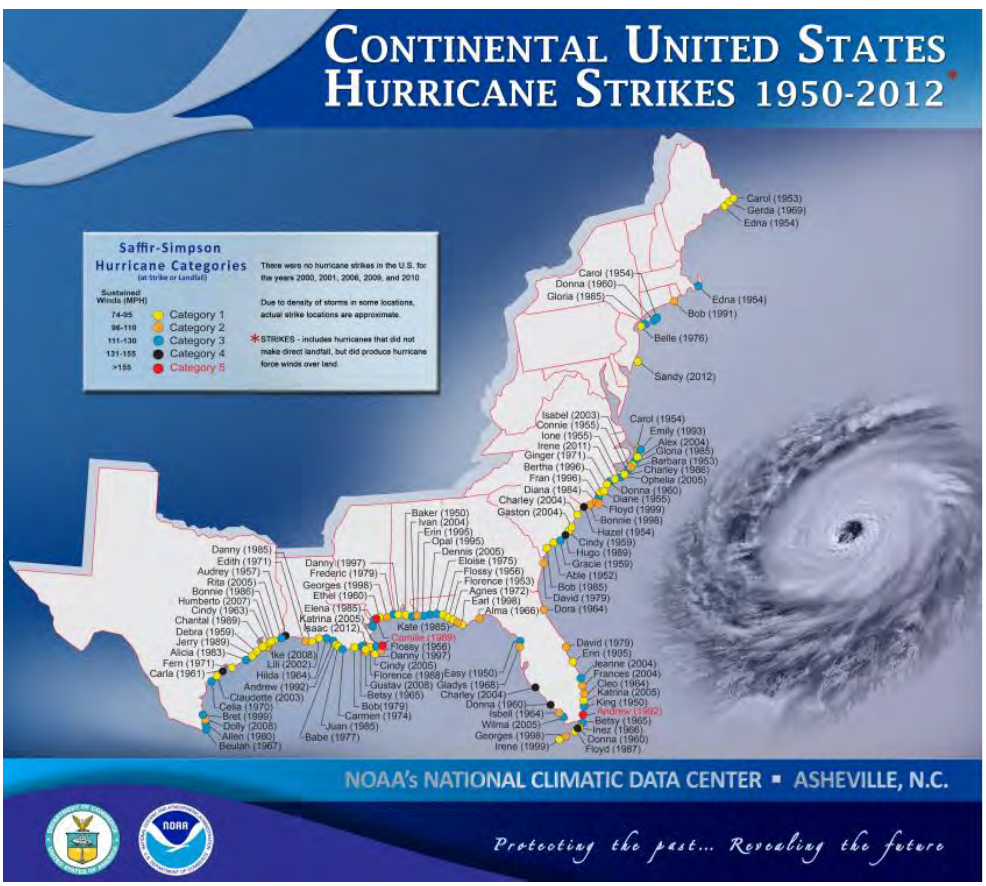


Figure 1 - Hurricane strike locations source https://data.nodc.noaa.gov/cgi-bin/iso?id=gov.noaa.ncdc:C00538

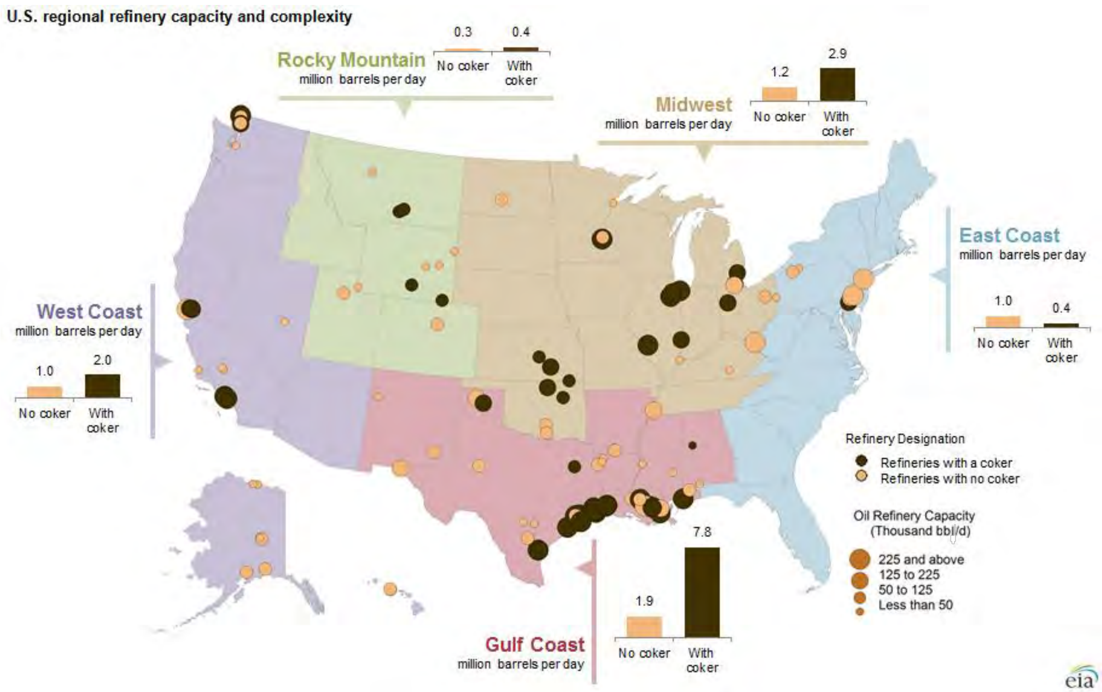


Figure 2 - Petroleum Refining Capacity source https://www.eia.gov/todayinenergy/images/2015.01.15/mainlarge.png

Hurricane Harvey was a grim reminder of the threat that hurricanes expose inhabitants along the Gulf Coast, but also the impacts on the coastal oil infrastructure as shown in Figure 3.

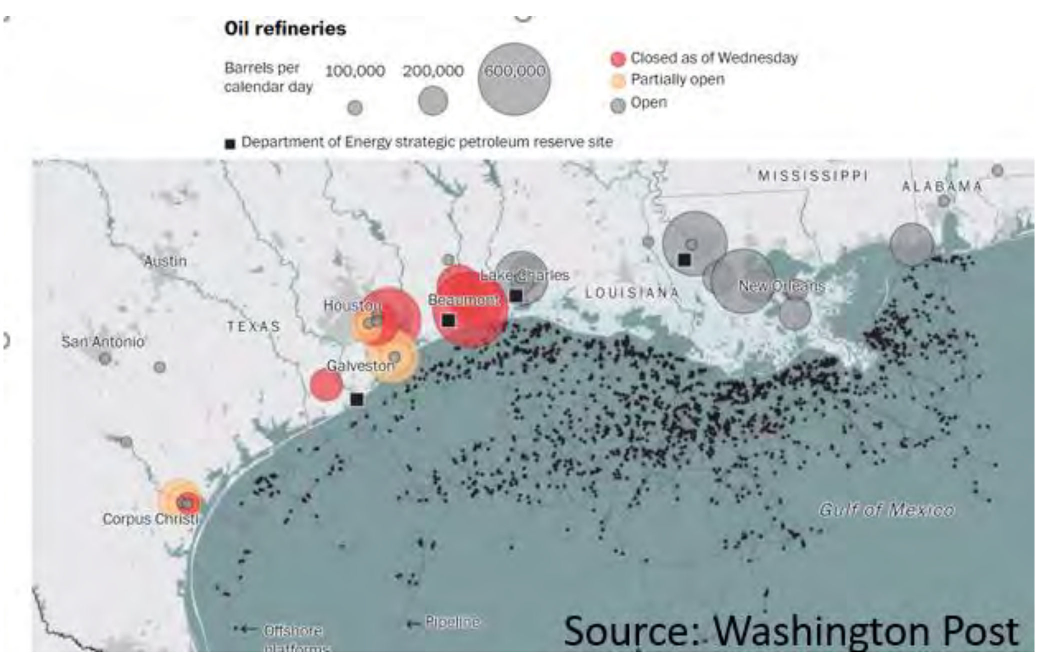


Figure 3 - 18 oil refinery closures and more than one million gallons of oil spilled

But, in fact, the devastation of Category 3 through 5 hurricanes is evident from Figure 4.

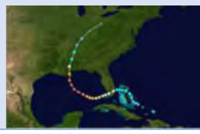
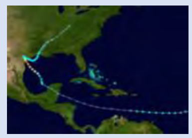
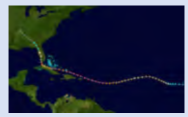
	Katrina	Sandy	Harvey	Irma	Maria
Year	2005	2012	2017	2017	2017
Date Range	8/23/05-8/31/05	10/22/12-11/2/12	8/17/17-9/2/17	8/30/17-9/13/17	9/16/17-10/2/17
Location	Bahamas, South and Central Florida, Louisiana, Mississippi, Alabama, Florida Panhandle, Eastern US 	Greater Antilles, Bahamas, most of the eastern United States (especially the coastal Mid-Atlantic States), Bermuda, eastern Canada 	Windward Islands, Suriname, Guyana, Nicaragua, Honduras, Belize, Cayman Islands, Yucatán, Southern and Eastern United States, Texas, Louisiana 	Greater Antilles (Cuba and Puerto Rico), Turks and Caicos Islands, The Bahamas, Eastern United States (especially Florida) 	Lesser Antilles, U.S. Virgin Islands, Puerto Rico, Dominican Republic, Haiti, Turks and Caicos Islands, The Bahamas, Southeastern United States, Mid-Atlantic States, Ireland, United Kingdom, France, Spain 
Max Wind Speed	175 mph	115 mph	130 mph	185 mph	175 mph
Estimated Cost	$161 Billion	$70 Billion	$134 Billion	$65 Billion	$91.6 Billion
Storm Category	Cat 5	Cat 3	Cat 4	Cat 5	Cat 5
Storm Casualties	1833	233	68-120	33-138	112-1133

Figure 4 - Consequences of Hurricanes

The focus of this paper is on how high winds and floods can impact the potential for damage to oil storage tanks and what kinds of preparations can be taken to reduce risks. The focus is on the engineering considerations which are rarely discussed or promoted. Although there are many other typical resources[1] for dealing and preparing for hurricanes this paper focuses directly on the impacts of these storms on petroleum and chemical storage tanks from a technical perspective. This paper provides a way to assess vulnerability at petroleum storage facilities.

Putting politics aside, science clearly shows that the global weather patterns are changing. In a paper written by Emanuel[2] 3700 simulated events at the single point of Houston, Texas, from each of six global climate models over the period 1981–2000 from historical simulations (blue), and 2081–2100 from RCP.

- [1] Ready.gov
- https://www.nhc.noaa.gov/outreach/
- https://www.fda.gov/NewsEvents/PublicHealthFocus/ucm317232.htm
- https://www.nsc.org
- https://www.fema.gov
- SSPEED severe storm prediction, education, and evacuation from disasters. http://sspeed.rice.edu
- https://nebula.wsimg.com/a1d6859382e7f333261a56bd692f2988?AccessKeyId=B38FF36BAC7128384C74&disposition=0&alloworigin=1
- pemyconsulting.com

[2] Kerry Emanuel, Lorenz Center, Massachusetts Institute of Technology, Cambridge, MA 02139 www.pnas.org/cgi/doi/10.1073/pnas.1716222114

8.5 simulations (red) showed that in the future the return period for these events decreases by about an order of magnitude for rainfall up to 500 mm.

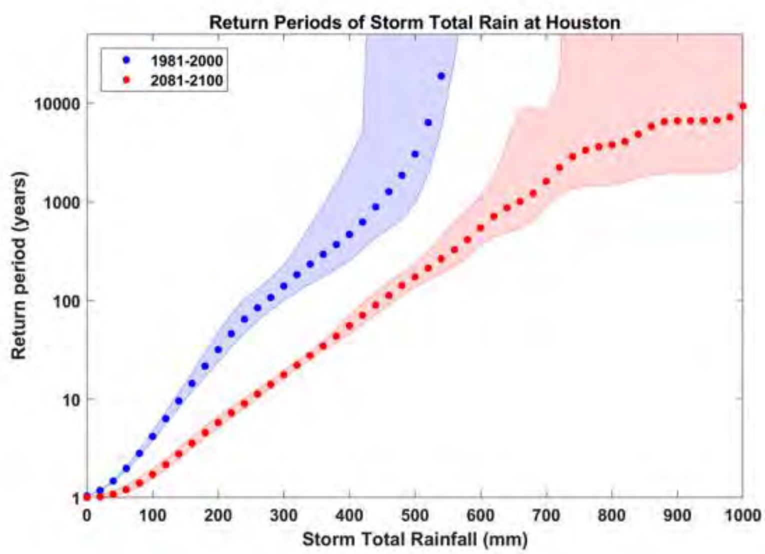


Figure 5 – Return periods of hurricane total rainfall (millimeters) at the single point of Houston, Texas, based on 3,700 simulated events each from six global climate models over the period 1981-2000 from historical simulations (blue) and 2091-2100 from RCP 8.5 simulations (red). The dots show the six climate-set mean and the shading shows 1 SD in storm frequency, remapped into return periods.

Storage Tank Failure Mechanisms

There are at least 4 fundamental and distinct modes of tank failure that are caused by high winds and storms typical for hurricanes:

1. Overturning: results when a tank is "knocked over" and spillage through the top or from punctures can occur.
2. Shell buckling: wind pressure causes the cylindrical shell buckles and may result in a tank dent. While this failure does not usually result in lost product it puts the tank out of commission until repairs can be enacted.
3. Sliding: movement of the tank along the ground without tipping over. This mechanism can break connected piping and cause major spills.
4. Roof Failure: Floating roof sinks potentially puncturing the tank bottom and putting the tank out of commission

The photos in Figure 6 show overturning failures

Figure 6 -Overturning Failures

An example of a dent caused by a tornado is shown in Figure 7.

Figure 7 - Tank dent caused by high winds (Tornado)

Some tanks which have slid off their foundations are shown in Figure

Figure 8 – Sliding tank failures

Figure 9 illustrates a floating roof typically used in storage tanks that may fail as shown in Figure 10.

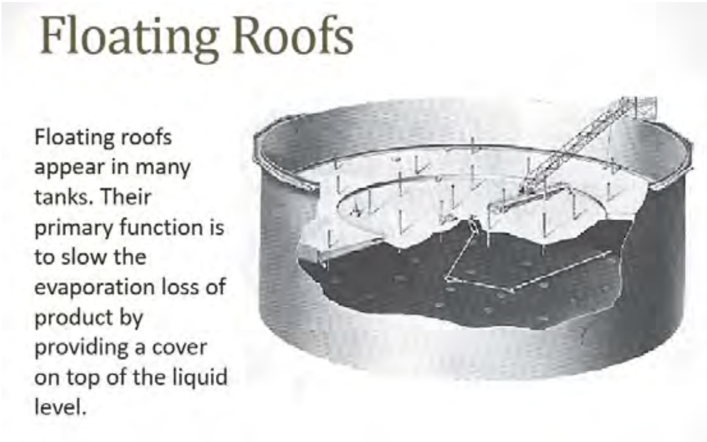


Figure 9 -Open top floating roof typical for crude oil or volatile organic compounds

Figure 10 - Floating roof sunk by Texas storm Alison. Roof under diesel but tops of floating roof rolling ladder and tops of landing legs visible as white points just under surface

The balance of this paper addresses the nature of the risks, the quantification of the hazards, and an approach to planning for high winds and rainfall.

Part 2: Water and Wind

Overview

Several pieces of legislation have helped to establish guidelines for water and wind loads for structures. In 1968 Congress established the National Flood Insurance Program (NFIP) and passed the National Flood Insurance Act of 1968. In order to identify the locations and manage floodplains prone to flooding the NFIP provides incentives and insurance programs for flood losses to property owners, local governments, and state governments. Participation in the NFIP is based on an agreement between communities and the Federal Government. Later, in 1987 the Federal Emergency Management Agency (FEMA) produced a Flood Insurance Study (FIS) and provided Flood Insurance Rate Maps (FIRMs). Areas subject to flooding are called 100-year floodplains and are shown on the Special Flood Hazard Area (SFHA) maps. This work is periodically updated and provides critical information about flood elevations at both new and existing infrastructure. These programs are used to establish the Base Flood Elevation (BFE) and is incorporated into ASCE 7-16, the engineering standard that governs loads for buildings and other structures. Explicitly, the BFE is defined in ASCE 7-16 as the "elevation of flooding, including wave height, having a 1% chance of being equaled or exceeded in any given".

Some areas near coastal regions that are defined as a Special Hazard Area include risks from flowing water and breaking waves. For example, VE Zones, known as coast high hazard areas, are subject to flooding phenomena and can have a BFE concurrent with wave effects of 3 feet or greater. The hazard zone is mapped with base flood elevations (BFEs) that reflect the combined influence of stillwater flood elevations, primary frontal dunes, and wave effects 3 feet or greater. There are many other designations such as AO, AH, Z, etc. Any facility considering flooding should check with the local regulatory and government agencies to obtain data specific to their location. FEMA websites can be used to provide information about the flood zone data for a location.

Designing new facilities with tanks at the recommended requirements is no guarantee that significant damage may not occur. For example, the probability that the 100-year storm flood levels will be exceeded in the design life of a facility (e.g. Let us say that it is 20 years) is approximately 20%. Probability of exceedance plots are provided in Figure 11.

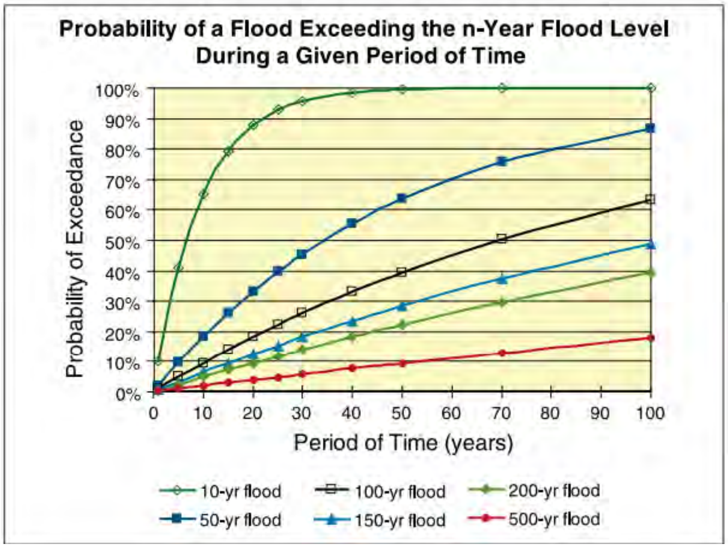


Figure 11 - FEMA Designing for Flood Levels Above the BFE Technical Fact Sheet No. 1.6

Also note that the exceedance probabilities do not consider the changing weather (i.e. BFEs and Storm Surge changes).

Damage Mechanisms

The impact of storms wind and water on tanks arises from:

- Buoyancy effects: Any standing water around a tank results in a reduced effective weight. In turn this makes overturning and sliding more likely. The primary starting point for assessing buoyancy is establishing the tank weight. This can prove difficult as tanks have many components. Consultation with tank vendors can help to establish approximate weights or algorithms based on tank design can be applied to establish tank weights[3].
- Flooding over berms: When water exceeds the berm height or penetrates the berm, then flowing water is then possible and it creates lateral forces on the tank shell which can be significant. This was seen in Hurricane Harvey (2017). In addition, if the facility is in a coastal region subject to breaking waves then the force of the breaking waves is very significant in terms of lateral forces imposed on the tank.

Figure 12 below shows the critical components to consider in assessing risks for a specific petroleum storage facility.

[3] PEMY Consulting, LLC as developed tank weight algorithms for use in estimating tank weights for cone roof tanks, dome roof tanks and open top tanks which is available on request (pemyconsulting.com).

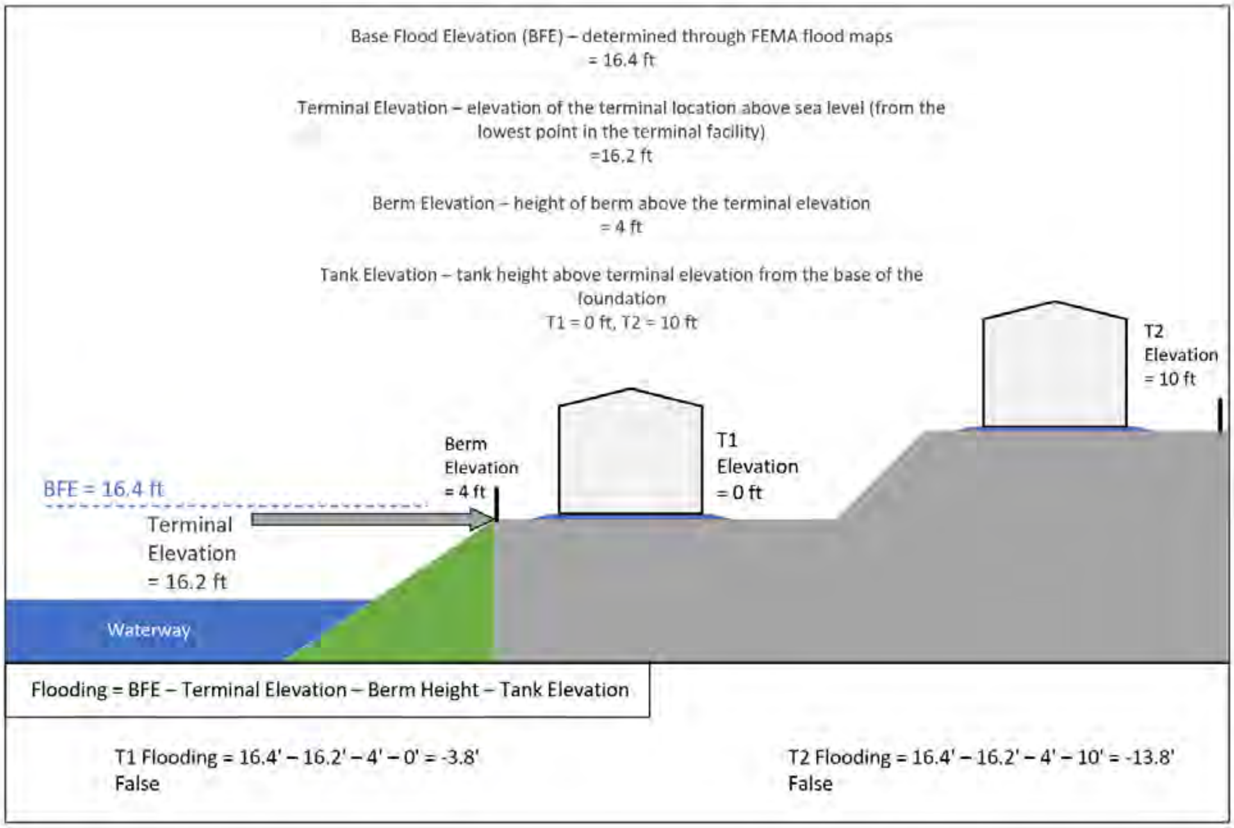


Figure 12 - Important elevations for assessing storm risk. Diagram does not show flowing water or breaking waves in coastal regions.

If there is any way that the flood level can exceed or breech the secondary containment the risks increase dramatically[4], Figure 13. For example, a 50 ft diameter cone roof tank with a height of 48 ft and 10 inches of rain surrounding the base requires only 3.7 ft of water to keep it safe from both 120-mph wind and buoyancy effects (i.e. sliding and overturning). However, the same tank with a breeched secondary containment 5 ft above the tank base requires 21.5 ft of product to keep it safe. Additionally, if the tank had a dome roof, then the product level required would be 31.5 ft as dome roofs have a much higher uplift than cone roofs due to the airfoil effects.

[4] PEMY Consulting, LLC. created a model using the rules of ASCE7-16 to determine vulnerability of storage tanks to wind and flooding. Copies of the spreadsheet are available from PEMY Consulting, LLC.

A range of tank sizes and required product levels required to save the tank against wind and flooding is given in **Error! Not a valid bookmark self-reference.**.

Table 1 Water or Product Needed to Survive Flooding

Diameter	Height	Water enters secondary containment	Breaking waves	Failure Mode	Recommended Product level	Recommended water level	Height of product for buoyancy	Height of water for buoyancy
ft	ft						ft	ft
15	48	No	No	Overturning	3.7	2.6	0.0	0.0
15	48	Yes	No	Sliding	30.5	21.3	9.7	6.8
15	48	Yes	Yes	Sliding	**64.2**	44.9	9.7	6.8
50	48	No	No	Sliding	1.5	1.1	0.3	0.2
50	48	Yes	No	Sliding	21.5	15.0	10.3	7.2
50	48	Yes	Yes	Sliding	31.6	22.1	10.3	7.2
100	48	No	No	Sliding	1.1	0.8	0.4	0.3
100	48	Yes	No	Sliding	19.4	13.6	10.4	7.3
100	48	Yes	Yes	Sliding	24.5	17.1	10.4	7.3
200	48	No	No	Sliding	28.1	19.6	15.9	11.2
200	48	Yes	No	Sliding	18.1	12.6	10.2	7.2
200	48	Yes	Yes	Sliding	20.6	14.4	10.2	7.2
250	29.75	No	No	Sliding	0.6	0.4	0.4	0.2
250	80	Yes	No	Sliding	17.1	12.0	9.7	6.8
250	48	Yes	Yes	Sliding	19.8	13.9	10.2	7.1

Assumes a cone roof for each tank
Assumes a wind speed of 120 mph (approximately 11 psf on projected vertical area of tank and 18 psf uplift on dome roof tanks)
Assumes a specific gravity of stored product of 0.7 and 1.0 (water)
Assumes an ASCE 7-16 Risk Category III Facility
Assumes 10 inches of rainfall surrounding tank
Pink cells show that completely filling tanks with water or product will not prevent failure

Flooding Insights

Despite the highly restricted condition set, some fundamental conclusions can be derived from this table:

- If the BFE exceeds the top of the secondary containment, then the required product or water to stabilize the tank is drastically increased. This increase is necessary if the secondary containment is not able to withstand the external hydraulic pressure of the floodwaters or if the operations does not close the secondary containment drainage valves.
- If breaking waves are present a significantly greater product or water loading.
- Some tanks simply cannot be stabilized no matter how much product or water is put in because the stabilizing weight required exceeds the height of the tank. This condition can occur for tanks that are 50 ft or less in diameter and which are subject to breaking waves.
- Sliding is by far the most common failure mechanism as opposed to overturning. Sliding can cause appurtenances and piping to tear or break away from the tank which would result in complete loss of containment.

Wind Forces

It should be recognized that the wind forces interact with the buoyancy forces to cause problems in tank facilities. To clarify the interaction between the two forces a word about estimating wind forces is in order. At first glance the various editions of API 650 published throughout the years would seem to create a multitude of different factors and results that would be applicable to establishing wind pressure on tanks. In 2010, ASCE 7 wind speeds were revised upwards from a 100 year mean recurrence interval (MRI) to a 1700-year MRI for Category III structures, while the factor on wind loads for allowable strength design (used in API 650) was reduced from 1 to 0.6. The net effect of these changes on wind pressures was slight if both changes were recognized. ASCE 7-16, the current edition as of 2019, maintained this approach, made some revisions to the wind speed maps to reflect better data, and added provisions that better address wind loads on API 650 tanks. Ballots for API 650 revisions are currently underway to recognize these changes in ASCE 7-16 which represents the best knowledge available today and which should be used in assessing risk from hurricanes.

API 650's requirements for tank components that resist wind loads (e.g., wind girder size and unstiffened shell height) have the wind pressure embedded in them rather than showing the wind pressure explicitly. To reflect different wind loads at different sites, API 650 factors its requirements by the design wind speed. Wind pressures are proportional to the wind speed squared. API 650's current wind roof pressure for a design wind speed of 120 mph is 0.6*(31 psf) = 18.6 psf on all roofs. These current wind pressures are approximated as uniform over projected areas, and don't include variations in factors such as site exposure, topographic factor, site elevation, and tank height, as these usually do not affect pressures enough to warrant the additional complexity. Furthermore, API 650's current design requirements for wind loads are factored by the square of the ratio of the design wind speed for a given site to the reference wind speed $(V/120)^2$. The adjustment factor is 1 if the design wind speed is the same as the reference wind speed of 120 mph. The 120 mph is arbitrary, and API 650 could potentially have used any reference wind speed if the API 650 requirements for components designed for wind are based on the wind pressure produced by that same reference wind speed.

As a rule of thumb where accurate calculations are not needed (as for example in risk screening tanks for hurricane impacts) the following should enable the tank facility owner/operator to perform the wind calculations. For the effective wind pressure acting on the tank shells, multiply the project area (height times diameter) by the effective wind for of 11 psf. This number should be scaled by $V^2/120$ for wind speeds that are different than 120 mph. For tank roofs, multiply the area of the tank projected roof area by 18.6 psf and scale this by $V^2/120$ for wind speeds that are different than 120 mph. It should also be noted that in this paper we have not considered buckling effects since they do not generally lead to loss of contents.

Part 3: Estimating Water Loads on Floating Roofs

External Floating Roofs

The basic concept of a floating roof is shown in Figure 14. The floating roof is like a swimming pool cover that floats on the hydrocarbon surface to prevent evaporation. It rides up and down as the liquid level increases or decreases. By regulation, they are required in order to control volatile organic compounds from evaporating and polluting the air.

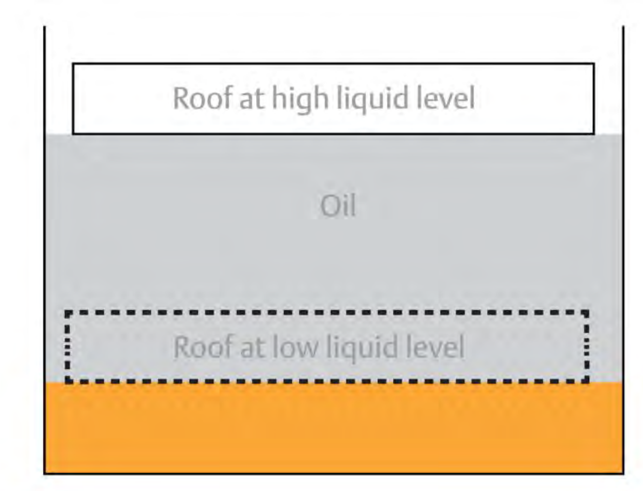


Figure 54 - Floating Roofs are used to reduce evaporation of volatile organic liquids such as gasoline and crude oil

There are many different designs and the materials may be constructed of steel, aluminum or composite materials (see Figure for a steel floating roof).

One very important matter that a floating roof in an open top tanks that it must deal with is drainage of rainwater from the deck since there is no “cover” for an open top floating roof, Figure 15. It should be noted that a large percentage of all petroleum storage is contained by open top floating roofs.

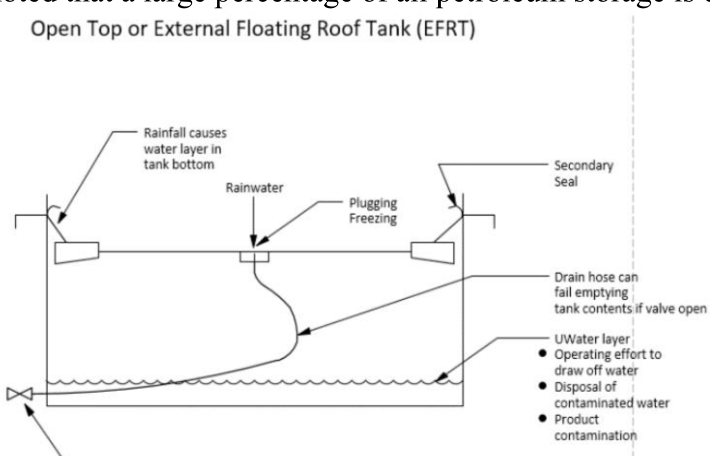


Figure 15 -6 Schematic showing floating roof rainfall drainage system

Because rainfall is free to enter the tank and accumulate on the floating roof a drainage system is required. This is done by have a sump at the center of the floating roof or at multiple locations and collecting the rainwater and draining it through flexible hoses or articulating pipe to the base of the tank as shown in Figure and 16. It is important to acknowledge that API specifies that the roof must be able to capture 10 inches of rainfall without failing of the floating roof. This failure method is discussed later in the section on standing water events.

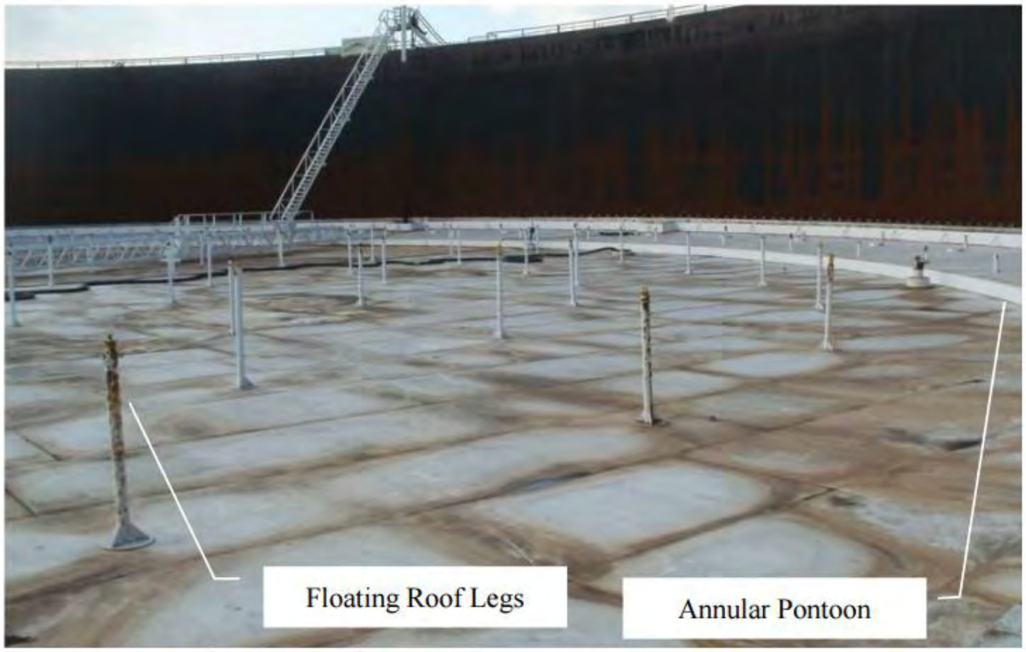


Figure 16 - Steel annular pontoon floating roof in large crude oil tank

Establishing Standing Water on Floating Roofs

It was reported that during Hurricane Harvey, there were more than 15 incidents of floating roofs failing atop oil storage tanks. In this paper we describe a method of using historical rain gauge data to estimate the statistical frequency (return time) of roof flooding to various depths. We present a way to approximate roof flooding risk from widely available hydrological intensity-duration-frequency (IDF) tables and demonstrate the accuracy of our approximation using data from the Harris County, TX, Flood Warning System (HCFWS) rain-gauge network.

Terminology

IDF	Intensity Duration Frequency table
DDF	Depth Drawdown Frequency table
iph	inches per hour
ddr	drawdown rate (expressed in iph)
HCFWS	Harris County, TX Flood Warning Service
Intensity	Rate of rainfall (expressed in iph)

The best conditions for a floating roof during a heavy rainfall event include a high product level, open drain valve, no obstructions within the hose, and no standing water at the discharge location (see **Error! Reference source not found.**). High product level is an important characteristic because that provides the potential energy necessary to transfer water from the roof to the ground.

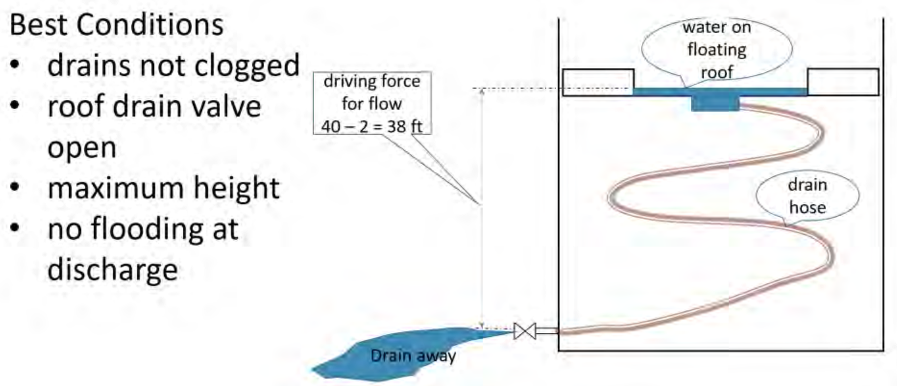


Figure 7 Best Conditions for Floating Roof

The worst conditions exist when the opposite of those cases exist: when the roof is in a low position, the drain valve is closed, the hose has obstructions, or the secondary containment are is flooded (see Figure 8).

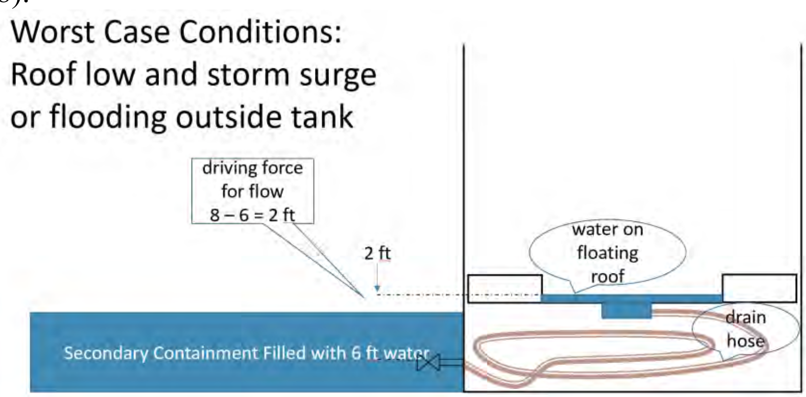


Figure 8 Worst Condition for Floating Roof

Standing-water events

The space above a floating roof is a broad, shallow, open-topped cylinder with a drain at bottom-center. Standing water will build up if rainfall intensity exceeds roof-drain drawdown rate (ddr) both expressed in inches per hour. Roof-drain flow rate is generally expressed as volume per time unit; for example, gravity flow through 4" pipe is about 15,000 gallons per hour. Our forecasting system requires re-expressing drain rate (volume per hour) as drawdown rate (DDR) expressed as inches of water depth per hour. Thus, for example, a 124-foot diameter tank contains 7528 gallons per vertical inch ($7.48 \cdot \pi \cdot 62^2/12$) so the drawdown rate would be 2 inches per hour (iph) (15,000 /7528).

Floating roofs are required by API Standard 650 to withstand 10 inches of rainfall over 24 hours *with primary drains inoperative*. The standard is hard to interpret; 10 inches of water accumulated due to *partly inoperative* drains exposes a roof to the same stress, as does 10 inches accumulated over a longer or shorter time interval. For that reason, we have developed statistical tables to predict the depth and frequency of standing water events for fully operational as well as impaired roof drains.

For our hypothetical 124-foot tank with 2 iph nominal drawdown, rain would have to fall at an average rate of 12 inches per hour (iph) for at least one hour to exceed the 10-inch limit. As of August 28, 2017, the US one-hour rainfall record was 13.5 inches per hour (Burnsville, WV, 1943-08-04), so 10 inches of standing water is possible but very unlikely for properly sized, fully operative roof drains. See also International Plumbing Code[5].In fact, Hurricane Harvey's 60-minute maximum near the Exxon storage terminal at Baytown, TX was about 4.12 inches per hour, Figure 17.

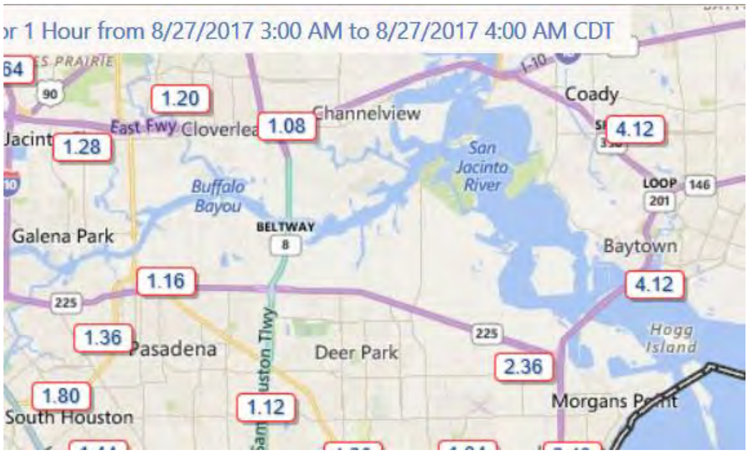


Figure17 -. One hour of rainfall data during Hurricane Harvey, Harris Co. TX.

At that rate, our hypothetical tank would have accumulated a little over 4 inches of standing water, as shown in Figure 9.

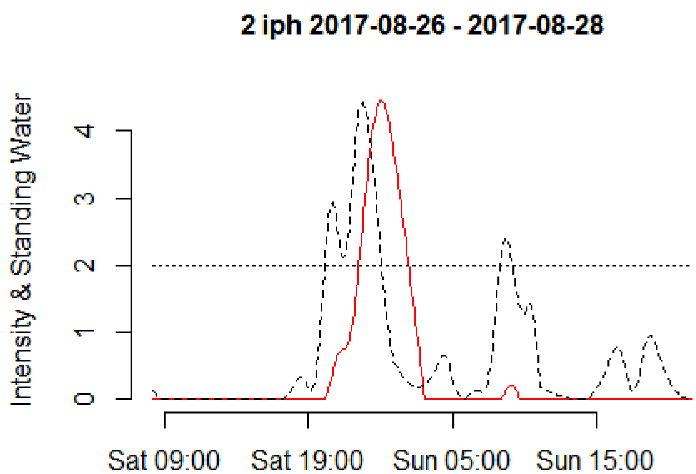


Figure 98 -. Gage 1540 Harvey Rain Event dotted: drawdown rate (in/hr), dashed: rain intensity (in/hr), solid: standing water level (in).

Why Do Roofs Sink?

It appears that a well-maintained floating roof with a drain operating at full capacity is very unlikely to experience 10 inches of standing water. So why did fifteen floating roofs fail in Harris County, TX during Harvey? Based on the few published analyses of roof failures we have found, it seems that either the drain was partially clogged, or one or more pontoons were sufficiently corroded to take on water. Other failure modes are referenced in an endnote[6].

[5] International Plumbing Code, Roof Drains
[6] Maintenance & Reliability of Floating Roofs https://onestopndt.com/blog/storage-tanks-maintenance-reliability-of-floating-roofs/

In this paper we quantify how a compromised roof drain raises the probability of high levels of standing water. Since standing water adds extra stresses to a roof it will raise the probability of failure; however, engineering analysis is needed to quantify how standing-water-induced stress influences the probability of roof failure by each of the possible failure modes.

Rain Gauge Data

The rain gauge in Figure 9 is part of a grid of 133 rain gauges maintained by the Harris County, TX, Flood Warning System (HCFWS). Continuous 5-minute data for years 1986 to the present are available for 61 of the gauges.

Identifying Standing Water Events

Standing water accumulates when rainfall intensity (in/hr) exceeds the (possibly compromised) drawdown rate (in/hr). We define a Standing Water Event as a continuous period of positive standing water beginning and ending with a dry roof (zero inches of standing water). Figure 10 shows the history of a standing water event in a hypothetical tank located near HCFWS gauge 1540. The event began at 22:00 on Wednesday, Jan 21, 1998 and ended just after 03:00 on Jan 22. We assumed that the roof drain was compromised to the extent that the drawdown rate was only 1 in/hr. The dashed line is a hyetograph: a graph of rainfall intensity in inches per hour (iph). Note that standing water increases only when intensity exceeds draw down rate.

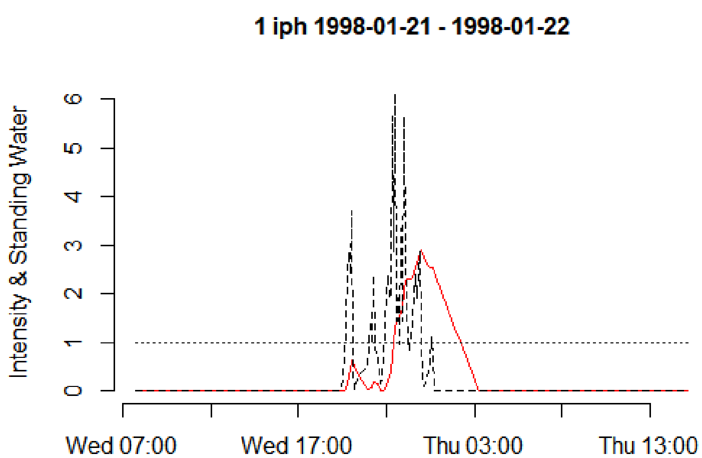


Figure 10 - Rainfall Hyetograph and resulting standing water assuming 1 iph drawdown.

Depth-Drawdown-Frequency (DDF)

We summarize the statistical risk of various depths of standing water in a Depth-Drawdown-Frequency (DDF) table, analogous to Intensity-Duration-Frequency (IDF) tables used in infrastructure planning[7].

Table 2 shows estimated maximum standing water at various drawdown rates and return periods based on pre-Harvey data. For example, a partly clogged drain with 1.5 in/hr drawdown rate (DDR) would experience 1.88 or more inches of standing water once in 10 years. Tabled values are percentiles of Generalized Extreme Value distributions fitted to annual standing water maxima at each draw down rate.

DDR (in)	0.25	0.5	1	2	3
RP (yrs)	Maximum Standing Water (in)				
2	2.34	1.71	1.14	0.62	0.32
5	3.12	2.35	1.63	0.91	0.51
10	3.89	2.99	2.14	1.21	0.73
25	5.20	4.10	3.07	1.77	1.16
50	6.48	5.21	4.03	2.36	1.65
100	8.08	6.62	5.29	3.14	2.35
1000	16.78	14.69	13.05	8.11	7.56

Table 2 - Gauge 1540 max. standing water by return period (RP) and drawdown rate (DDR).

Figure is a plot of the fitted standing water values in Table 2.

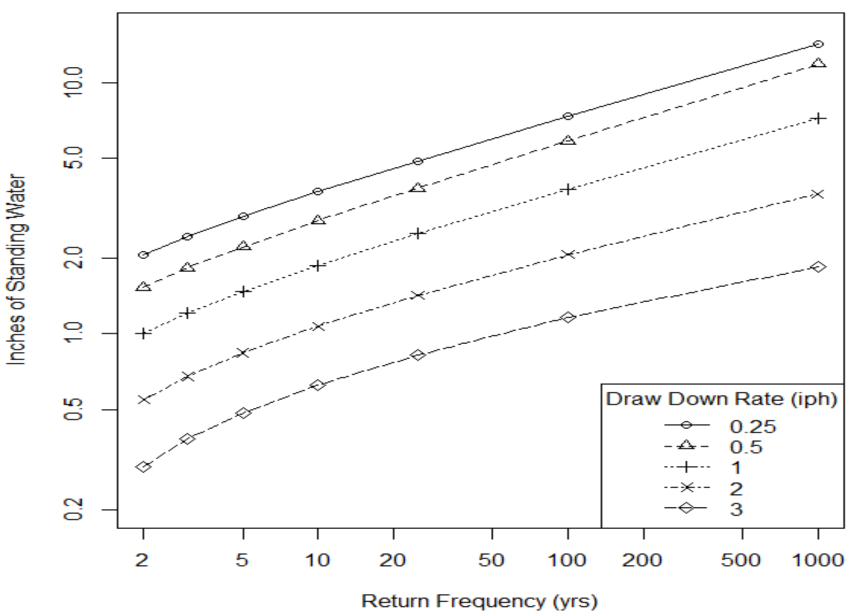


*Figure 20 -. DDF: Max Standing Water **D**epth by **D**raw down Rate and Return **F**requency.*

[7] API 650 C.3.4.1 "Floating roofs shall have sufficient buoyancy to remain afloat on liquid with a specific gravity of the lower of the product specific gravity or 0.7 and with primary drains inoperative for the following conditions: 250 mm (10 in.) of rainfall in a 24-hour period over the full horizontal tank area with the roofs intact. "

IDF Approximation of DDF.

It is difficult to find the three decades of high quality 15-minute rainfall data needed to compute a DDF table for a given location. For that reason, we investigated using rainfall Intensity-Duration-Frequency (IDF) tables from NOAA's Precipitation Frequency Data Server[8] to approximate standing water DDF tables.

NOAA Precipitation Frequency Server

NOAA has IDF tables for 43 of the lower 48 states[8] computed from rainfall data through April 2017 over a grid of rain gauges in each state. Table 3 is an excerpt of the IDF table for NOAA's Goose Creek gauging station near Baytown terminal in Houston, TX. Rain gauge data underlying this table included Hurricane Harvey.

	Return period (years)						
	2	5	10	25	50	100	1000
Duration	Inches of Rain						
5-m	0.61	0.76	0.89	1.08	1.22	1.37	1.96
10-m	0.96	1.21	1.42	1.72	1.95	2.19	3.05
15-m	1.22	1.53	1.79	2.15	2.43	2.73	3.88
30-m	1.75	2.18	2.54	3.05	3.43	3.83	5.56
1-h	2.33	2.93	3.44	4.14	4.68	5.27	7.90
2-h	2.92	3.77	4.53	5.66	6.58	7.61	12.0
3-h	3.27	4.30	5.26	6.71	7.95	9.35	15.2
6-h	3.90	5.24	6.55	8.56	10.3	12.4	20.9
12-h	4.59	6.23	7.85	10.3	12.6	15.1	26.7
24-h	5.32	7.29	9.24	12.3	14.9	18.1	32.5

Table 3. IDF Table for Goose Creek Station, TX

Given the wide availability of up-to-date IDF tables, it would be useful to be able to approximate tank roof flooding risk from IDF data.

How our approximation works

To illustrate how our approximation works one should consider a tank that can drain 1.5 inches of water per hour (ddr = 1.5). We can approximate the 25-year standing water event for that tank from the 25-year rainfall maxima in Table 3. For example, the 3-hour 25-year maximum is 6.71 inches of rain. In 3 hours, 4.5 inches of that accumulation would drain off leaving 2.21 inches of standing water.

This may be acceptable if the 25-year standing water event happened to last 3 hours from dry to maximum. In general, we need to do the same calculation for other durations and take the maximum of those. Table 4 repeats this calculation at each duration. Maximum standing water is 2.66 inches at two hours. So, we know that about once in 25 years there will be a two-hour interval in which 2.66 inches of standing water are added to any existing standing water; consequently the 25-year standing water maximum must be at least 2.66 inches.

[8] NOAA Atlas 14, point precipitation server. https://hdsc.nws.noaa.gov/hdsc/pfds/pfds_map_cont.html

Duration	Hours	25 year Rainfall	Drawdown ddr x hours	Net standing water
5-m	0.08	1.08	-0.13	0.96
10-m	0.17	1.72	-0.25	1.47
15-m	0.25	2.15	-0.38	1.78
30-m	0.50	3.05	-0.75	2.30
1-h	1.00	4.14	-1.50	2.64
2-h	2.00	5.66	-3.00	**2.66**
3-h	3.00	6.71	-4.50	2.21
6-h	6.00	8.56	-9.00	0.00
12-h	12.00	10.3	-18.00	0.00
24-h	14.00	12.3	-21.00	0.00

Figure 21 -. Approximate 25 year standing water is 2.66 inches when ddr=1.5 iph.

Figure 2 is the approximate DDF table computed by this method; the nominal drawdown rate is 1.5 inches per hour. The table shows standing water risk at full capacity as well as 75, 50, 25, and 10% capacity. If the drain is operating at 0.15 inches per hour (10% capacity), ten inches of standing water is a 25 to 50-year event.

Draw down rate	Return period (years)						
	2	5	10	25	50	100	1000
	Inches of Standing Water						
1.500	1.00	1.43	1.94	**2.66**	3.58	4.85	11.9
1.125	1.21	1.81	2.32	3.41	4.58	5.98	14.2
0.750	1.58	2.27	3.03	4.46	5.80	7.90	17.7
0.375	2.17	3.18	4.30	6.31	8.10	10.6	23.5
0.150	3.00	4.43	6.05	8.70	11.3	14.5	30.7

Figure 22 - Approximate maximum standing water by drawdown rate and return period, Goose Creek.

Potential Accuracy of the Approximation

Figure 23 shows a standing water event at HCFWS gauge 1540 assuming drawdown rate (DDR) 1.0 inches per hour. Maximum standing water was 2.92 inches at 00:05 on 1/22/1998 starting from no standing water at 21:55 on the previous day, an interval of 2 hours.

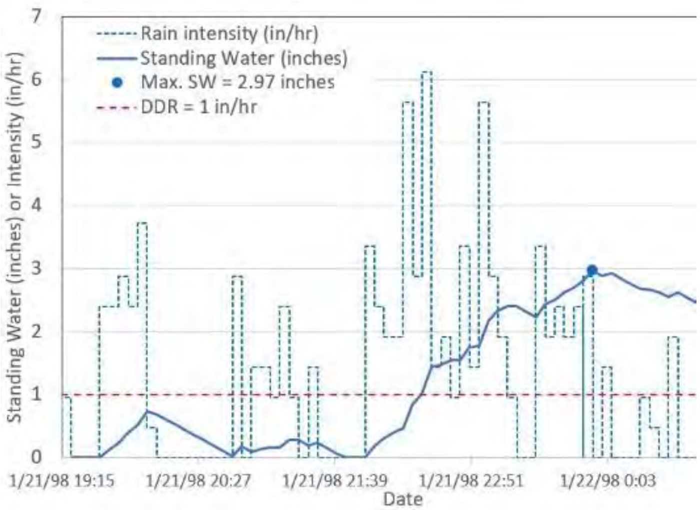


Figure 23 - Rain event of 21-Jan-1998.

The dashed line in Figure is the 3-hour interval with maximum average rainfall intensity (ARI), 1.9 inches per hour. The diagonal line shows theoretical standing water assuming constant intensity 1.9 iph.

Total accumulation, is (ARI-DDR) x Duration = (1.9 – 1) x 3 = 2.7 in. Actual maximum standing water is 2.97 inches, so the approximation is 9% lower than the measured value. There are two reasons for the error. First, during the circled interval on the time axis there was no standing water and therefore no drawdown; however, the approximation assumes constant rainfall intensity and therefore continuous drawdown. Second, there happened to be positive standing water at the beginning of the 3-hour window which is not included in the estimate.

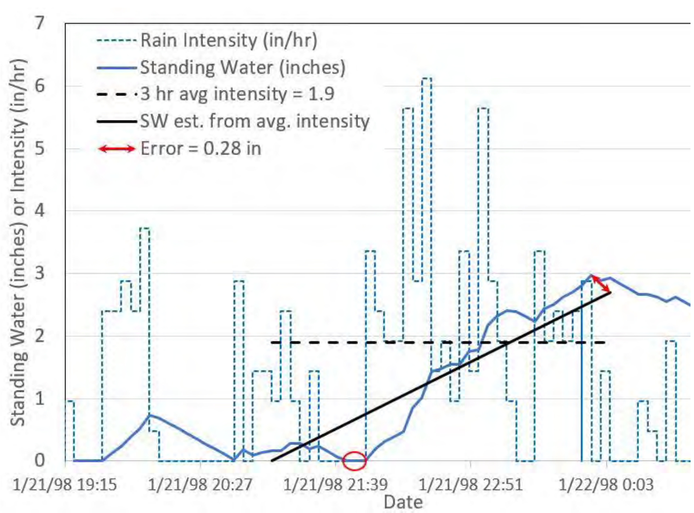


Figure 24 - Max standing water approximated by 3-hour average intensity.

Figure 24 shows that it is possible for the estimate to be perfect when the interval of maximum constant intensity starts with zero standing water and includes no intermediate stretches of zero standing water. Unfortunately, without access to raw data there is no way to know if or when this is true.

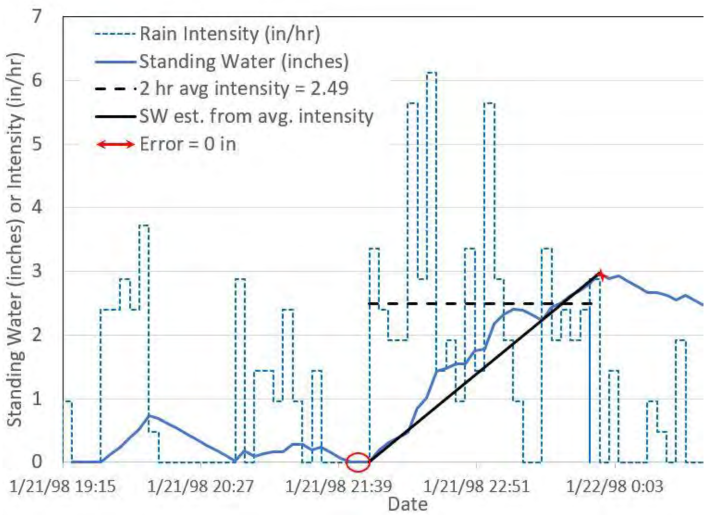


Figure 25 - Max standing water approximated by 2-hour average intensity.

Error analysis of the IDF approximation.

While it is true that for any standing water maximum there is a corresponding maximum average rain intensity interval that produces a perfect approximation, another source of error emerges when estimating standing water percentiles from rain intensity percentiles. This component of error can be computed at a given site from raw 5-minute data or it could be estimated using simulated 5-minute data, generated with a Poisson cluster stochastic rainfall generator[9].

We illustrate the raw-data method with 5-minute data from the average of Harris County, TX. Our error analysis used the average 5-minute rain accumulation of HCFWS gauges 1540 and 1520, north and south of Baytown in Figure17 -. We computed annual maximum rain accumulation for years 1986 – 2013 at durations 5 minutes through 4 days and fit Gumbel distributions to each duration to produce the IDF table graphed in Figure . We estimated the approximate DDF table from the IDF table via the method described prior.

[9] A Poisson Cluster Stochastic Rainfall Generator That Accounts for the Interannual Variability of Rainfall Statistics: Validation at Various Geographic Locations across the United States, https://www.hindawi.com/journals/jam/2014/560390/

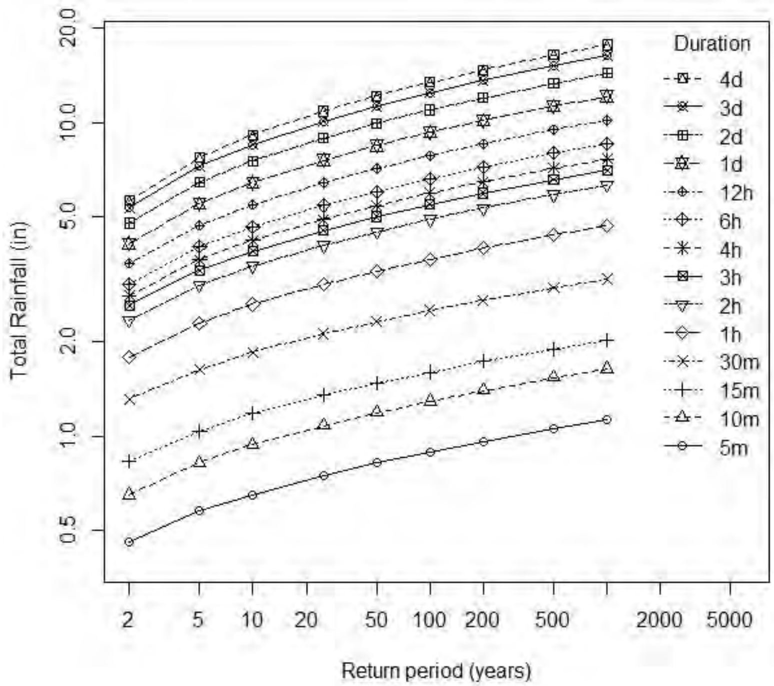


Figure 26 - Baytown IDF, Gumbel-smoothed annual maximum rain accumulation

Next, we computed, directly from raw rainfall date, annual maximum standing water at drawdown rates from .1 to 4 inches per hour and fit Gumbel distributions to each drawdown to produce the true DDF table. Approximate (symbol) and exact (curve) DDF values are in Figure 27.

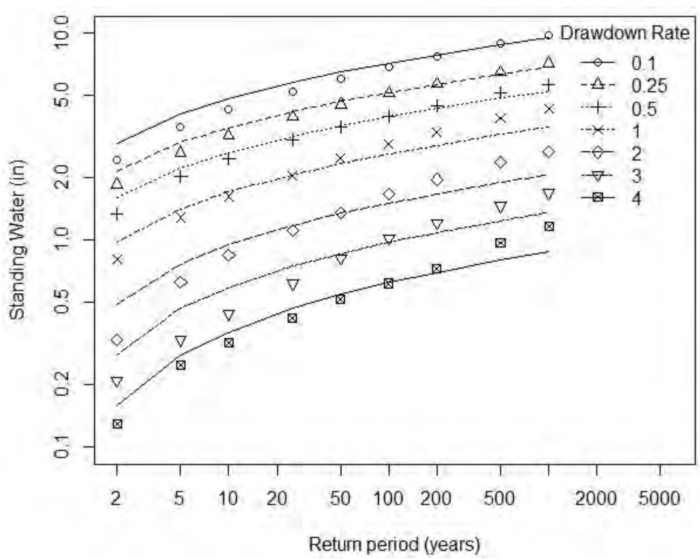


Figure 27 - Approximate and Gumbel-smoothed Exact DDF at Baytown.

Approximation errors for Figure 27 are listed in Table 4. Errors for extreme standing water events (5 or more inches of standing water) are highlighted; for extreme events, absolute errors are less than ± 0.55 inches and percent errors are less than ± 7%.

Draw-down (in/hr)		Return Period (years)								
		2	5	10	25	50	100	200	500	1000
0.1	%	.19	.16	.13	.11	.7	.4	.2	1	2
	in	.47	.56	.55	.55	.44	.28	.13	.07	.22
.25	%	.16	.12	.9	.6	.3	.1	1	2	5
	in	.29	.31	.28	.23	.15	.06	.04	.15	.33
.5	%	.19	.10	.7	.4	.2	1	3	6	7
	in	.26	.20	.17	.12	.06	.02	.12	.29	.42
1	%	.21	.10	.5	0	6	11	14	17	19
	in	.17	.13	.08	.01	.14	.31	.46	.66	.82
2	%	.48	.21	.12	.4	1	10	15	20	23
	in	.16	.13	.10	.05	.01	.16	.29	.47	.62
3	in	.33	.42	.34	.21	.5	4	10	16	20
	in	.07	.14	.15	.13	.04	.04	.12	.23	.33
4	%	.23	.12	.13	.12	.6	.2	4	18	25
	in	.03	.03	.04	.05	.03	.01	.03	.17	.29

Table 4. DDR approximation errors. Highlighted: standing water events of 5 or more inches

Conclusion for Part 3

Easily computed, approximate standing water depths can be computed from NOAA IDF tables. The estimates, accurate to a half inch, are a guide to sizing tank drains. These calculations can be applied to a wide variety of tanks as well as various failure modes to allow for improved tank design. It has also been clearly shown that there is a serious need to clear drain intakes regularly to maintain adequate drawdown rates in order to prevent tank failure and possible product loss.

Appendix to Part 3

DDR [in/hr]						
	Elevation Diff [ft]					
Diameter [ft]	40	30	20	10	5	2.5
50	8.362765	7.215703	5.852955	4.082853	2.838242	1.96471
100	2.090691	1.803926	1.463239	1.020713	0.70956	0.491178
150	0.929196	0.801745	0.650328	0.45365	0.31536	0.218301
200	0.522673	0.450981	0.36581	0.255178	0.17739	0.122794
250	0.334511	0.288628	0.234118	0.163314	0.11353	0.078588
300	0.232299	0.200436	0.162582	0.113413	0.07884	0.054575
L	80	80	80	80	80	80

2" Pipe Drawdown Rate (various Diameter and Elevation, constant Pipe Length)

DDR [in/hr]						
	Elevation Diff [ft]					
Diameter	40	30	20	10	5	2.5
50	23.46574	20.25495	16.45592	11.50493	8.019627	5.573542
100	5.866435	5.063737	4.11398	2.876232	2.004907	1.393386
150	2.607305	2.25055	1.828436	1.278325	0.89107	0.619282
200	1.466609	1.265934	1.028495	0.719058	0.501227	0.348346
250	0.93863	0.810198	0.658237	0.460197	0.320785	0.222942
300	0.651826	0.562637	0.457109	0.319581	0.222767	0.154821
L	80	80	80	80	80	80

3" Pipe Drawdown Rate (various Diameter and Elevation, constant Pipe Length)

DDR [in/hr]						
	Elevation Diff [ft]					
Diameter	40	30	20	10	5	2.5
50	47.53442	41.05402	33.36773	23.3726	16.32357	11.36277
100	11.88361	10.2635	8.341931	5.843151	4.080892	2.840693
150	5.281603	4.561558	3.707525	2.596956	1.81373	1.26253
200	2.970902	2.565876	2.085483	1.460788	1.020223	0.710173
250	1.901377	1.642161	1.334709	0.934904	0.652943	0.454511
300	1.320401	1.140389	0.926881	0.649239	0.453432	0.315633
L	80	80	80	80	80	80

4" Pipe Drawdown Rate (various Diameter and Elevation, constant Pipe Length)

DDR [in/hr]						
	Elevation Diff [ft]					
Diameter	40	30	20	10	5	2.5
50	136.8631	118.2846	96.22572	67.50016	47.26972	33.00008
100	34.21577	29.57115	24.05643	16.87504	11.81743	8.250019
150	15.20701	13.14273	10.69175	7.500018	5.252191	3.666675
200	8.553942	7.392787	6.014107	4.21876	2.954357	2.062505
250	5.474523	4.731384	3.849029	2.700006	1.890789	1.320003
300	3.801752	3.285683	2.672937	1.875004	1.313048	0.916669
L	80	80	80	80	80	80

6" Pipe Drawdown Rate (various Diameter and Elevation, constant Pipe Length)

DDR [in/hr]						
	Elevation Diff [ft]					
Diameter	*40*	*30*	*20*	*10*	*5*	*2.5*
50	276.4712	238.9711	194.5593	136.667	95.83356	67.00996
100	69.11781	59.74279	48.63982	34.16675	23.95839	16.75249
150	30.71903	26.55235	21.6177	15.18522	10.64817	7.445551
200	17.27945	14.9357	12.15995	8.541687	5.989597	4.188123
250	11.05885	9.558846	7.782371	5.466679	3.833342	2.680398
300	7.679757	6.638087	5.404424	3.796305	2.662043	1.861388
L	*80*	*80*	*80*	*80*	*80*	*80*

8" Pipe Drawdown Rate (various Diameter and Elevation, constant Pipe Length)

Part 4: Summary and Conclusions

In this paper we have shown that chemical and petroleum storage tanks can be vulnerable to high rainfall and winds typical of hurricanes where most of the risk is concentrated in the US Gulf Coast and Eastern seaboard. There are several damage mechanisms that can cause complete loss of contents exposing people and the environment to chemicals and oily products.

While much of the industry simply relies on buoyancy calculations to establish how much product or water loading is necessary to stabilize the tank, this approach is completely inadequate in many cases and particularly for the high-risk hurricane exposure areas. The risk of inadequate tank stability goes up dramatically when water enters the secondary containment. This may happen when the flood elevations can exceed the secondary containment heights or where secondary containment fails either physically or from operational errors.

Coastal regions which experience these conditions, and which have the potential for breaking waves to form have the highest risk in the tank sector because the breaking wave forces are extremely high. Smaller tanks subject to these conditions in some cases may not be capable of being stabilized and will fail despite best efforts.

Another basic problem during storm conditions is sunk floating roofs. We have shown that the typical design conditions governing floating roof drainage in open top tanks should be adequate to provide sufficient drainage. However, roof drain flow is impeded by either clogging with debris, failure of operations to open drains, or by low floating roof levels which reduced the gravity drainage flow. When floating roofs sink, there is a possibility of the bottom being punctured as well as evaporation of volatile organic materials which pollute the air but also are a significant fire hazard.

Most tank owners have difficulty determining the amount of water or the methods of computing the drainage. In this paper we have show how to establish the design criteria for floating roofs no matter where they are located. We have shown how to size them even if the percent occlusion is known or established as a design basis.

We have established computational tools that provide a way to establish standing water levels on floating roofs based on location and predicted rainfall intensities by return period[10].

[10] See PEMY Consulting, LLC rainfall intensity app www.pemyconsulting.com

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Analysis Oxygen Piping Layout to Eliminate High Consequences Risk

Suprayudi S. Kadir*
Jubail United Petrochemical Company, SABIC affiliate
Al-Jubail, Saudi Arabia
*Presenter E-mail: kadirss@united.sabic.com

Abstract

During detail engineering project for EG3 (Ethylene Glycol Plant no.3) for Jubail United Petrochemical Company, a SABIC affiliate, the writer found oxygen feed header from Gas Plant pipeline laydown on pipe rack instead of underground as standard practice for existing plants. Currently, as the oxygen pipe passes the hydrocarbon product storage tanks, there are hydrocarbon products pipelines above it with only a 4-meter space in between.

Oxygen is an oxidizer, and in oxygen-enriched atmospheres, the reactivity of oxygen significantly increases the risk of ignition and fire. Materials that may not burn in normal air may burn vigorously in an oxygen-rich environment. Materials that burn in normal air may burn with a much hotter flame and propagate at a much greater speed. The onset of this enhancement is seen at 25% oxygen level in the atmosphere and reaches its maximum from approximately 40% oxygen concentration as per section 6.2 Oxygen Enrichment or Deficiency of Determination of Safety Distance (IGC Doc 75/07/E) published by European Industrial Gases Association AISBL.

This paper delves into three approaches which are: oxygen's effect on the surrounding area, the surrounding area's (specifically fire's) effect on the oxygen line, and a comparison to the standard.

Based on the three dimension risk analysis made, the writer concludes that the current configuration is unsafe and potential to high risk. Although the cost of construction increases significantly, rerouting the oxygen pipe is the best option because safety is more valuable.

Keywords: Consequence Analysis; Managing Process Safety; Oxygen hazard, Thermal Radiation

1 Introduction

Although we would die in minutes without the 21% oxygen within the air we breathe, if the concentration reaches more than 24%, it will be more dangerous and prone to fire and explosion. It becomes easier to start a fire, which will then burn hotter and more fiercely than in normal air; it may be almost impossible to put the fire out. Oxygen itself is not flammable, but it does support combustion. Materials that may not burn in normal air may burn vigorously with a much hotter flame and propagate at a much higher speed in an oxygen-rich environment. The fire that killed the Apollo 1 crew in a launch pad test spread so rapidly because the capsule was pressurized with pure O2 at slightly more than atmospheric pressure. Given the possibility of spontaneous combustion in oxygen piping systems, special precautions need to be taken in design, fabrication, erection, testing, and commissioning of oxygen pipelines.

The oxygen hazard can be illustrated in figure 1, which shows three main elements required for a fire to occur: an oxidizer, a fuel, and an ignition source.

Figure 1 – Oxygen Fire triangle

The oxygen itself is the oxidizer, and fire hazard increases by increasing the concentration, pressure, temperature, and flowrate. The fuels in an oxygen system are the materials of construction (metals and non-metal) or contaminants in the pipe like particulates, oils, or greases. The ignition source could be particle impacts (from improperly cleaned construction or corrosion products), compression heating, frictional heating, and others (lightning, static charge, electrical arching). For more detail, the ignition mechanism can be found in Appendix B [**1**].The method control hazard in an oxygen system, one or more elements shall be minimized or eliminate as follow:

Oxidizer: reduce oxygen pressure, temperature, or concentration as practical.

Fuel: ensuring burn-resistant alloys are used in locations where active ignition mechanism exist.

Ignition: ensuring clean the pipe to reduce particle impact and promoted combustion, elimination of adiabatic compression, and other mechanisms.

With the current project for expansion of EG3 (Ethylene Glycol plant no.3) which reduces the severity from oxidizer, an element is not possible as the process needs high purity for oxygen concentration with operating of pressure 27 barg and temperature 35 °C.

The second element that needs control is the fuel, which is selecting piping material construction according to best practice [**1**]. Based on Figure 2, the maximum velocity allowable for this project is 16 m/s to minimize particle impact ignition hazards. Accordingly, the piping selection is 12" SS-304 material with a velocity of about 4.4 m/s for the design flow rate of 44,000 kg/h.

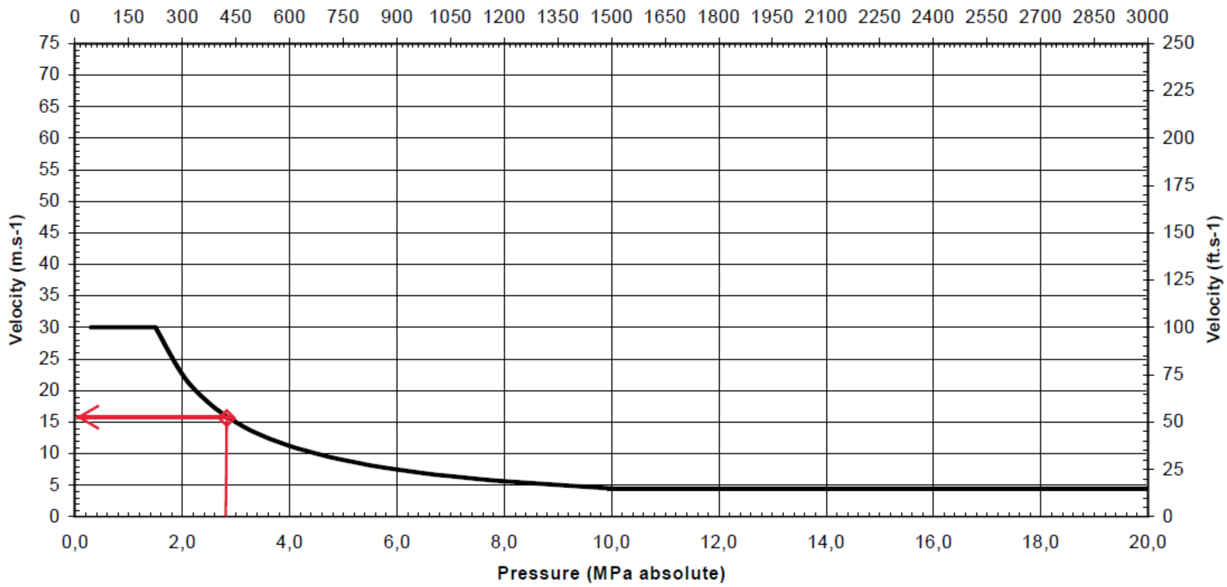


Figure 2 – Impingement velocity curve [1]

A higher grade alloy like Monel 400 or Inconel 625 is installed in someplace based on velocity, especially in a filter, venting, and downstream control valve.

Due to underground oxygen pipes having reported cases for fires in oxygen filter caused by unproperly cleaning, the contractor proposes above ground piping, as shown in Figure 3 to overcome cleanness challenged.

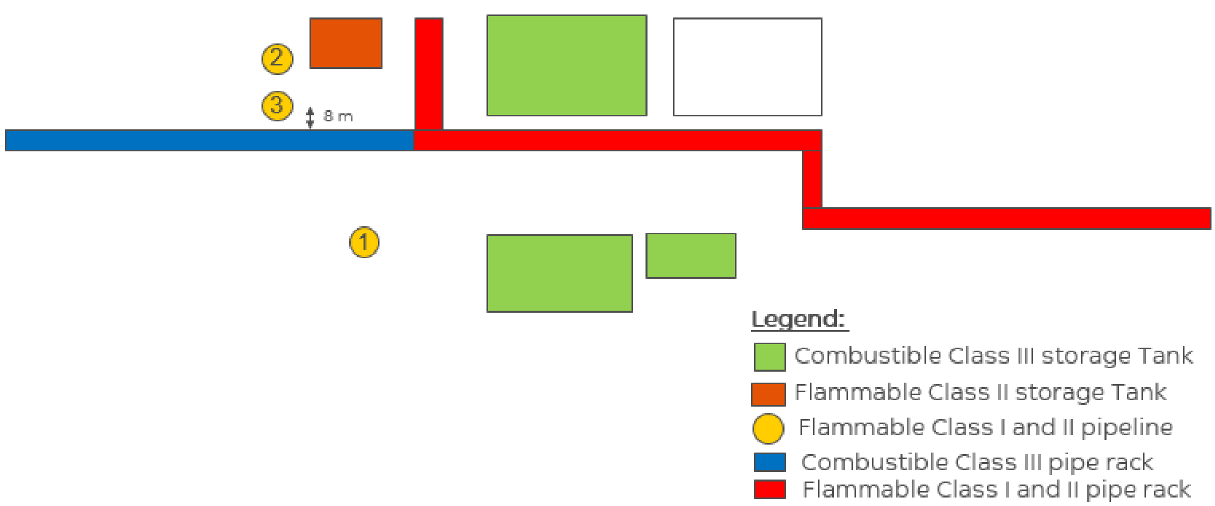


Figure 3 – Upper ground pipe lay out

2 Methodology

The new oxygen pipe will be laid down on existing utility pipe rack and hydrocarbons illustrated in figure 3, a flammable gas class I & II (indicated in red) and combustible class III (in blue). Chemical in “red” are Ethane, Ethylene, 1-Butene, 1-Hexene, Toluene, 1-Octene, and 1-Decene. In “Blue” 1-Dodecene, C14-18 mixture, 1-Eicosene, Mono Ethylene Glycol, Di-Ethylene Glycol, and Tri Ethylene Glycol.

Two consequence analysis methods were used. One method is based on the impact of thermal radiation on oxygen upper ground piping, and the other is a comparison to the standard.

The definition of safety distance is the minimum distance that the effects of an event do not cause a risk of injury to people or failure of equipment. Fires primarily cause failure or harm through direct flame contact or radiation, causing a rise in temperature leading to material failure or burning.

In this methodology, the only failing condition is if the equipment measures a value greater than or equal to 37.5 kW/m^2 (sufficient to cause damage to process equipment) [**2**]. This value is equivalent to 631 °C (which will fail the metal strength) based on the equation below [**3**]:

$$\boxed{T_s = \left[\frac{q''}{\sigma} + T_\infty^4\right]^{1/4}}$$

Where;

T_s is surface temperature of the target (K)
T_∞ is temperature of the surroundings (K)
σ is Stefan-Boltzmann constant (5.67 x 10^{-11} kW/m^{2}K^4)
q'' is incident heat flux to the target (kW/m^2)

2.1 Oxygen effect on the surrounding area

Basis calculation is 150 mm leak size for oxygen enrichment between 25% and 40%. This approach is used to identify the consequence in case of oxygen leakage or rupture affecting product storage and piping that content hydrocarbon flammable and combustible materials.

2.2 The surrounding area effect on the oxygen line

This method is used to calculate the effect from hydrocarbon pipes or tanks with a leak size of 12.5 mm based on SABIC standard [**4**] for assessment of equipment spacing. The analysis takes into account the results of three pool fires and two jet fires.

2.3 Comparison to the standard

Little information is available relating to standard spacing of oxygen piping to hydrocarbon. In this case, the reference is from the Asia Industrial Gases Association [**1**] as shown in Table 1.

Nature of exposure	Category 1 stations [3]	Category 2 stations	Category 3 stations	Category 4 stations
Aboveground pipeline (flammable fluid) without close proximity of mechanical joints (see 8.6).	15m	6m	2m	2m
Buried tank (flammable fluid)	5m	2m	2m	2m
Pressure vessel (non-flammable fluid) with P • V > 200 bar m3 water capacity (P • V >100 000 psi ft3)	5m	3m	3m	2m
Flammable product storage	8m	5m	2m	2m
Liquid hydrogen storage	15m	15m	15m	15m
Transformer station	15m	6m	3m	2m
Administrative building with openings or air conditioning intake owned by customer	10m	8m	8m	2m
Public building	15m	10m	10m	2m
Public road/railway/car park	15m	10m	6m	2m
Internal road/ railway	3m	3m	3m	2m
High tension electric cable (aboveground)	10m	6m	5m	2m
Boundary of user's property	15m	10m	2m	2m
Internal car park	15m	6m	2m	2m
Flame and/or spark producing activities. For smoking restrictions (see 8.6).	15m	8m	3m	2m

NOTES

1 Category 1 Stations: $P \bullet D^2 > 3000$, $P > 4$ bars, $D > 2.5$ cm.
Category 2 Stations: $P \bullet D^2 < 3000 > 1500$, $P > 4$ bars, $D > 2.5$ cm.
Category 3 Stations: $P \bullet D^2 < 1500$, $P > 4$ bars, $D > 2.5$ cm.
Category 4 Stations: Isolating and/or metering purposes only.

2 Oxygen stations should not be beneath high-tension cables without protection.

3 For PD^2 above 3000, a specific risk assessment should be performed to determine if safety distances greater than listed in Appendix E are necessary.

Table 1 – Minimum safety distance (without barriers) for oxygen control and isolating/metering stations

3 Results

3.1 Oxygen Effect

PHAST was used to model oxygen pipeline dispersion with wind speed 1.5 m/s and atmosphere stability "F". The worst-case scenario for meteorology conditions as per US-EPA [**5**], 1.5F, was inputted and resulted in an affected area with a radius of 16 meters (see figure 4).

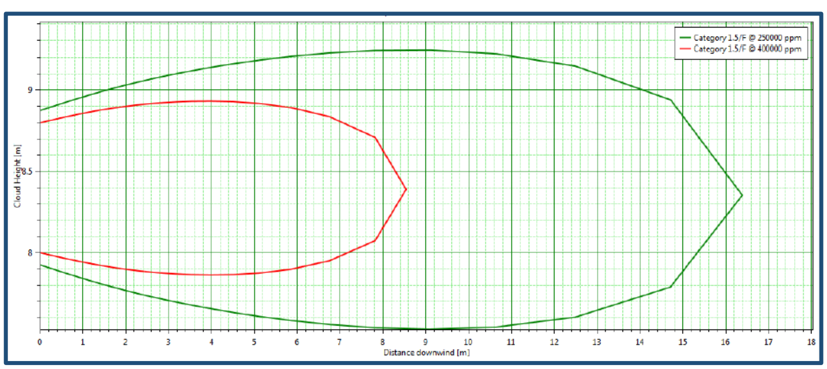


Figure 4 – Oxygen Dispersion 150-1.5F

3.2 Effect on Oxygen Line

The table below shows the result of pool fire and jet fire for some hydrocarbon pipelines that affect an oxygen line. Data is extracted from BakerRisk report on FSS/QRA study for United [**6**].

Reference	Type of Fire	Material	P (barg)/T (°C)	Distance to 37.5 kW/m2 Threshold (m)
1	Pool fire	C7 (Toluene)	12.5/35	16.3
2	Pool fire	C14-18	5/35	13.8
3	Pool fire	C12 (1-Dodecene)	12.5/35	19.9
4-Piperack	Jet Fire	C4 (1-Butene)	50/52	17.8
5-Piperack	Jet Fire	C2 (Ethylene)	41/35	12.4

Table 2 – Distance to 37.5 kW/m² threshold from surrounding oxygen line

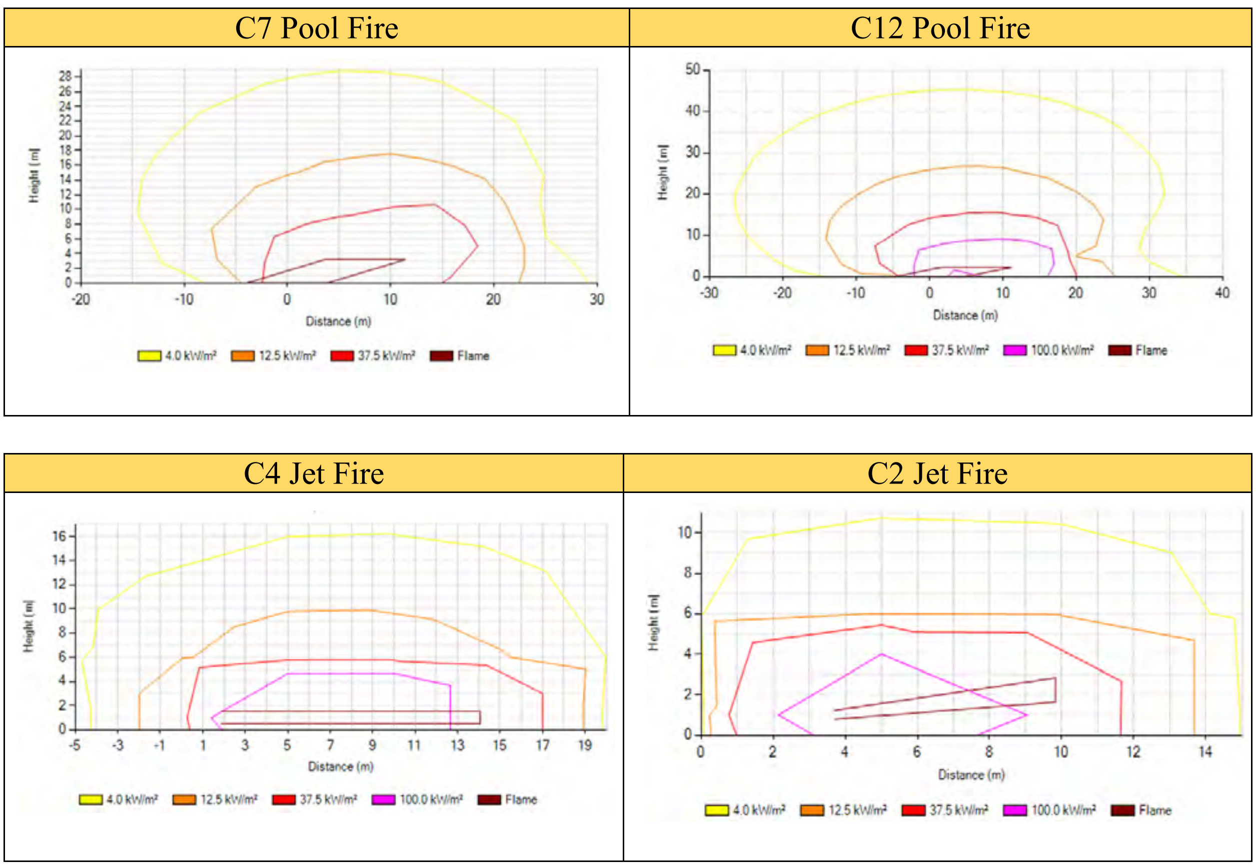


Figure 5 – Heat Radiation Side View

3.3 Referring to Standard

Three categories of energy release to appropriate safety distance expressed as $P \cdot D^2$ where P is the normal operating pressure (bar) and D the pipe diameter (cm).

- Category 1: $P \cdot D^2 > 3000$
- Category 2: $P \cdot D^2 < 3000$
- Category 3: $P \cdot D^2 < 1500$

Based on operating pressure 27 barg and 12 inches or 30.48 cm diameter of the pipe, it falls under category 1. The safety distance for the aboveground pipeline (flammable liquid) without the proximity of mechanical joints is 15 meters.

4 Discussion

Although oxygen enrichment reaches the piping content of hydrocarbon, especially C2 and C4 which is a location in the same pipe rack, the oxygen will not cause a risk without ignition source and fuel present in the atmosphere.

The proposed oxygen line passing through the storage tank and their piping are at risk of pool fire due to C12 product location within the 37.5 kW/m^2 distance.

In contrast, the jet fire effect from either C2 or C4 have very high risk as the distance to an oxygen line of 4 meters is very close compared to their flame distance of more than 10 meters.

The recommended standard requires 15 meters, while the current distance is less than that.

One technique to mitigate the risk while ensuring oxygen stays above ground is by installing a solid barrier. Barrier material could be concrete, reinforcing Masonry, or reinforcing insulation with metal structural sheets. But implementing a barrier in the long pipeline is not practical and may create other issues and need further risk analysis.

5 Conclusions

Based on all three dimensions of analysis, above ground oxygen line should be 20 meters away from hydrocarbon to avoid high risk in the case of fire, which can cause oxygen pipe failure and an increasing burning rate that creates more damage to a facility through a series of domino effects.

Underground piping for oxygen line is the best choice for managing process safety separate from hydrocarbon facilities.

Other than the cleaning issue, standard practice in handling oxygen line service shall follow such as but not limited to: avoid using grease/oil in bolt/nuts, install isolating gasket in flange between under and upper ground, grounding and bonding, cathodic protection.

The cleanness issue in an underground pipe that can be solved during construction and pre-commissioning by best practice approaching as listed below:

- Use long radius elbow instead of 90 degrees.

- Pigging with compatible material and logging each time pigs are used. Pigs should be inspected once they are removed from the receiver.
- Purging with high velocity gas of 25 m/s and inspecting the dirt by target plate to see if it meets criteria.

6 References

[**1**] AIGA, *Oxygen pipeline and piping systems*, 021/12 Globally Harmonised Document, Asia Industrial Gases Association, 2012

[**2**] EIGA, *Determination of Safety Distances*, IGC Doc 75/07/E, European Industrial Gases Association AISBL, 2007.

[**3**] CCPS, *Guidelines for Fire Protection in Chemical, Petrochemical, and Hydrocarbon Processing Facilities*, AIChE, New York, 2003.

[**4**] SES S02-E04, *Quantitative Risk Analysis*, Sabic, Jubail, 2018.

[**5**] Daniel A. Crowl, *Joseph F. Louvar, Chemical process safety: fundamentals with applications*, 2nd Edition, New Jersey, 2001.

[**6**] Mather, W, et Al-Jubail United Facility EO/EG III Project *Quantitative Risk Analysis Report*, Revison B. Issued date 5 June 2018.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Quantitative assessment and Consequence modeling of deliberately induced Domino effects in Process facilities

Priscilla Grace George*[1] and V. R. Renjith[2]
[1]Research Scholar, [2]Professor
Division of Safety and Fire Engineering
Cochin University of Science and Technology, Kerala, India
*Presenter E-mail: priscillagrace.mec@gmail.com

Abstract

Process facilities handling hazardous chemicals at elevated temperature and pressure conditions are attractive targets to external attacks. The possibility of an external attack on a critical installation with an intention of triggering escalation of primary events into secondary and tertiary events, thereby increasing the severity of consequences needs to be effectively analyzed. A prominent Petrochemical Industry located in Kerala, India was identified for induced domino effect analysis. In this study, Bayesian network is used to model the development of a domino sequence and to quantitatively determine the occurrence probabilities of domino effect. Moreover, the updating feature of Bayesian networks is used to update probabilities in the light of new evidences. Phast Process hazard analysis software and ALOHA (Areal Locations of Hazardous Atmospheres) software is used for consequence modeling of the security event to obtain the impact zones. Recommendations to manage and reduce the domino effect attractiveness by incorporating inherently safer design concepts and use of appropriate active and passive mitigating barriers are also discussed.

Keywords: Security risk; Domino effect; Process plants; Bayesian networks; Consequence modeling; Phast; ALOHA

1. Introduction

Process industries handling huge amount of hazardous chemicals can be potentially dangerous resulting in catastrophic incidents such as explosions, fire and toxic gas releases with serious adverse effects on people, property and environment. Such Industries involving the storage and transportation of hazardous chemicals are prime targets of security threats. Security risk assessment for process plants was not given serious reflection until the terrorist attack on the World Trade Centre on 11 September 2001. The possibility of inducing a chain of incidents with maximized damage potential makes complex industrial areas a very attractive target for terrorists. Hence complex industrial clusters should be protected against such deliberately induced domino effects (Reniers et al., 2008). Implementing efficient security risk management programs in process industries can help in reducing the attack likelihood and minimizing the consequences of a successful attack (Garrick et al., 2004). Security risk assessments consists of threat analyses and vulnerability analyses involving the consideration of target attractiveness, attack likelihoods and attack consequences. The API standards for security risk assessment (API, 2013) provides guidelines for performing semi-quantitative security risk assessments. (Bajpai and Gupta, 2005) introduced a semi-quantitative method of security risk assessment based on the use of a Security Risk Factor Table (SRFT) as a pre- screening tool for further assessments.

Conventionally, domino incidents are analyzed by two approaches- Event tree approach and Fault tree approach. In the Event tree approach, consequences of a given incident are increased to account for domino effects. In the Fault tree approach, domino effect is incorporated as an external event and failure frequency of a given incident is increased. (Khan and Abbasi, 2001) has developed and demonstrated the application of a computer automated tool for domino effect analysis- DOMIFFECT in an Industrial Cluster in Manali, Chennai, India.

The typical primary incidents for a domino sequence are explosions and fires. The physical effects associated with the primary incidents such as thermal radiation, overpressure and fragment effects can affect nearby units leading to secondary and tertiary incidents. The overall consequence of the domino sequence is much severe than that of the primary incident happening alone. An effective domino effect analysis should include accurate modeling of domino sequence development and a quantitative estimate of occurrence probabilities along with consequence modeling- together identifying the most vulnerable units in the industrial area. Hence, such analyses can be used to reduce the attractiveness of industrial area to external threat agents by determining the units where security measures are to be strengthened. Typically, domino effect analysis has to be performed in the initial stages of design of the industrial area for effective land use planning- thereby assigning adequate safe distances between different units to reduce escalation effects.

Bayesian networks are graphical representations consisting of nodes representing the system variables interconnected by links showing conditional dependencies between them. (Khakzad et al., 2013) has demonstrated the use of Bayesian networks in modeling the propagation sequence of domino effect and determination of domino effect probability at each level. Consequence modeling of the incidents may be performed to determine the impact zones by making use of Phast software and ALOHA software.

The objective of this paper is to analyze the possibility and consequences of a deliberately induced domino effect on a prominent petrochemical industrial area in Kerala, India. A dedicated Bayesian network is developed with nodes representing different units of the industry. The damage potential and the attractiveness of each unit to threat agents depends on the amount and type of hazardous chemicals being stored. The domino propagation sequence is effectively modeled using the Bayesian network. Consequence modeling is performed using Phast software to determine the impact zone of primary incident. Finally, recommendations to reduce the domino effect attractiveness by incorporating inherently safer design concepts and adequate safety barriers are also discussed.

The paper is organized as follows: Section 2 discusses the materials and methods. Section 3 describes the case study and Section 4 discusses the development of domino sequence using Bayesian network and consequence modeling using Phast and ALOHA. Section 5 gives the main conclusions drawn from the study.

2. Materials and Methods

The accident or primary incident in one unit propagating to neighboring units by means of escalation effects are termed as Domino effects. The escalation vectors of primary incident- such as overpressure, heat radiation and fragment effects are compared with threshold values for neighboring units to find potential secondary incidents.

2.1 Bayesian Network modeling of domino sequence

The various units in the industrial area under consideration are represented as nodes to form the Bayesian network. The primary unit for starting the domino sequence is the one most attractive to terrorists depending on its damage potential. The escalation vectors corresponding to this primary incident is determined. The threshold values of surrounding units are compared to the values of escalation vectors to determine the secondary units.

The threshold values for overpressure capable of damaging an atmospheric storage vessel and pressurized storage vessel is 23.8kPa and 42kPa respectively (Cozzani and Salzano, 2004). The threshold value for thermal radiation capable of damaging any storage vessel (both atmospheric and pressurized) is taken as $25 kW/m^2$ (Alileche et al., 2017).

The probit values and escalation probabilities of secondary units given primary incident are calculated. The probability of loss of containment at a nearby unit (P) due to an initiating event in a unit is given by (Mannan, 2012),

$$P = \left(1 - \frac{r}{r_{limit}}\right)^2 \tag{1}$$

Where r is the distance between the units and r_{limit} is the maximum distance at which the initiating event can cause damage.

The units with highest escalation probabilities becomes the secondary units. The primary unit is connected to these secondary units by arcs showing interdependency. This method is then repeated at each level to find the tertiary and further units until propagation ends.

2.2 Consequence Modeling using Phast and Aloha

ALOHA (Areal Locations of Hazardous Atmosphere) and Phast (Process Hazard Analysis Software) are efficient simulation tools for consequence modeling. ALOHA is capable of providing the threat zones corresponding to a chemical release by modeling the atmospheric conditions. The estimated impact zones can be exported and displayed on Google Earth platform. Similarly, Phast is an advanced tool for modeling the incident from release to far-field dispersion.

It also provides extensive modeling for release scenarios such as from leaks, pipelines, ruptures etc. Atmospheric and weather conditions can also be incorporated and detailed reports are available for all possible incidents corresponding to each scenario.

3. Case Study

A prominent petrochemical industry located in Central Kerala, India is selected for the study. The industrial area involves storage of hazardous chemicals such as cyclohexane, Benzene, Low Sulfur- Heavy Stock (LS-HS), Ammonia and Liquefied Petroleum Gas (LPG). Fig 1 shows the google earth image of the chemical storage area.

Figure 1 Google Earth Image of Petrochemical Plant *(Source: Google Earth)*

The quantity actually stored and threshold quantity allowed is listed in Table 1.

Chemical	Threshold Quantity (Tons)	Actual Quantity stored (Tons)
Benzene	1500	1270
Cyclohexane	1500	1150
Ammonia	60	5000
LPG	15	33

The storage of such flammable chemicals in large quantities are potential sources for explosions and fires. The loss of containment can occur by leaks, cracks or rupture in vessel or pipeline. Since the chemicals are stored in close proximity there is a great chance for domino effect if an undesirable event starts in one unit. Moreover, the industry is located in a municipality housing several industries and is one among the world’s most toxic spots. The population density is approximately 2938 people per square kilometer.

4. Results and Discussions

The petrochemical industry stores 1150 tons of cyclohexane in atmospheric conditions. Induced damage on this vessel can result in vapor cloud explosion creating overpressure effects on nearby Benzene, Ammonia, LS-HS and LPG storage tanks. TNT equivalent Vapor cloud explosion modeling (Casal and Darbra, 2013) results in overpressure values as listed in Table 2, which are then compared with threshold values to find potential secondary units.

Nearby Unit	Distance from Cyclohexane vessel (m)	Overpressure (KPa)
Benzene A	30	170
Ammonia	47	60
Benzene B	58	40
LS-HS	85	25
LPG	150	2

On comparing with the threshold value of 23.8 kPa required for damaging atmospheric vessels, it is found that Benzene tanks, Ammonia tanks and LS-HS vessels comes under domino spell and hence is considered for further analysis.

The secondary incident at Benzene Tank A (Atmospheric vessel) is pool fire due to loss of containment occurring by the impact of overpressure from primary incident. The subsequent thermal radiation at LPG tank, Ammonia tank and Benzene Tank B is estimated by Solid flame model (Casal and Darbra, 2013) and found to be 8.96 kW/m^2, 16.07 kW/m^2 and 92.5 kW/m^2 respectively. Hence, Benzene Vessel B comes under domino spell as the escalation vector value is greater than the threshold value.

The loss of containment from Benzene Tank B resulting in pool fire due to the impact from Benzene Tank A forms the tertiary event. The thermal radiation at LS-HS tank at a distance of 40 m is estimated to be 37.6 kW/m^2.

The domino sequence is modelled as a Bayesian Network using HUGIN EXPERT software and shown in Fig 2. The conditional probability tables (CPTs) are filled by using escalation probabilities calculated according to equation 1. The probability of loss of containment in Ammonia tank, LS-HS tank, Benzene Tank A and Benzene Tank B due to overpressure effects from cyclohexane tank is estimated as 0.39, 0.099, 0.58 and 0.28 respectively. The probability of loss of containment from Benzene Tank B due to thermal radiation from Benzene Tank A is calculated as 0.77. The probability of loss of containment from LS-HS Tank due to thermal effects from Benzene Tank B is 0.34. Moreover, Synergistic effects are also considered when populating the CPTs.

Development of domino sequence using Bayesian network has many advantages such as computation of domino probabilities in each level by appropriately adding logic gates in each level as discussed by (Khakzad et al., 2013). Also probability updating is possible when new information is incorporated onto the network.

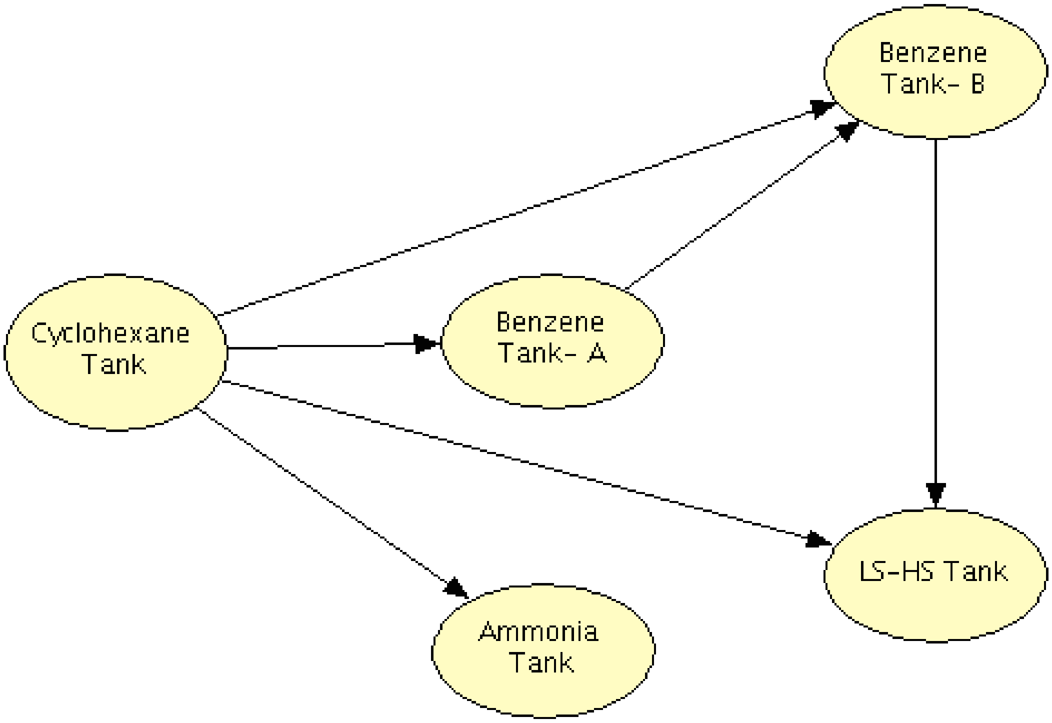


Figure 2 Bayesian Network Modeling of Domino Sequence

The consequence modeling for the above incidents are also implemented using ALOHA software and Phast software. The thermal radiation zone obtained for pool fire from Benzene Tank A is shown in Figure 3. The red zone corresponds to thermal radiation greater than 10 kW/m^2. It is observed that Benzene Tank B is being affected.

Figure 3 Thermal radiation footprint from Benzene Tank A

Phast software provides different analysis results for all possible incidents corresponding to the scenario being represented. The pool vaporization rate Vs time obtained from analysis performed in Phast software is shown in Figure 4.

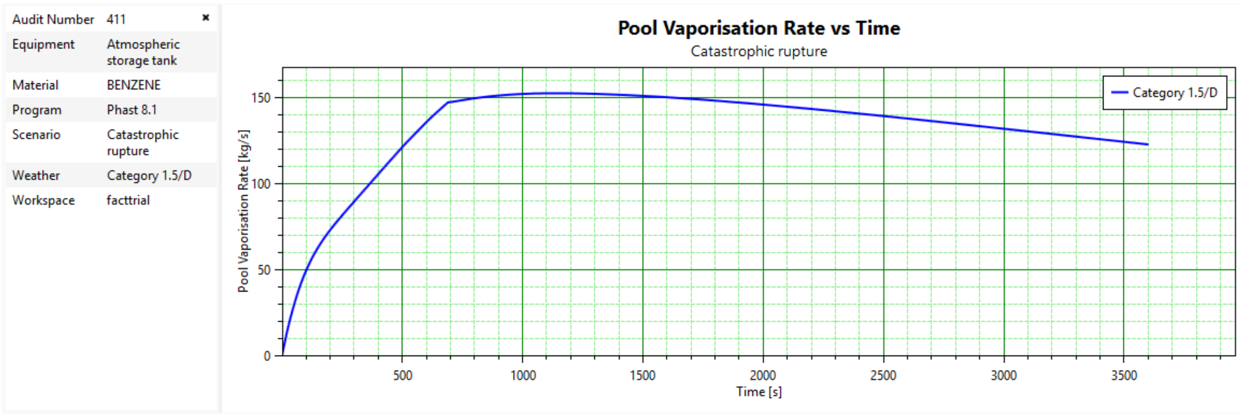


Figure 4 Pool Vaporization rate Vs time for Benzene Tank A

Phast software also provides the toxic dosage per distance corresponding to the catastrophic rupture scenario of Benzene tank A (Figure 5). The toxic dispersion footprint resulting from rupture of Benzene Tank A is shown in Figure 6.

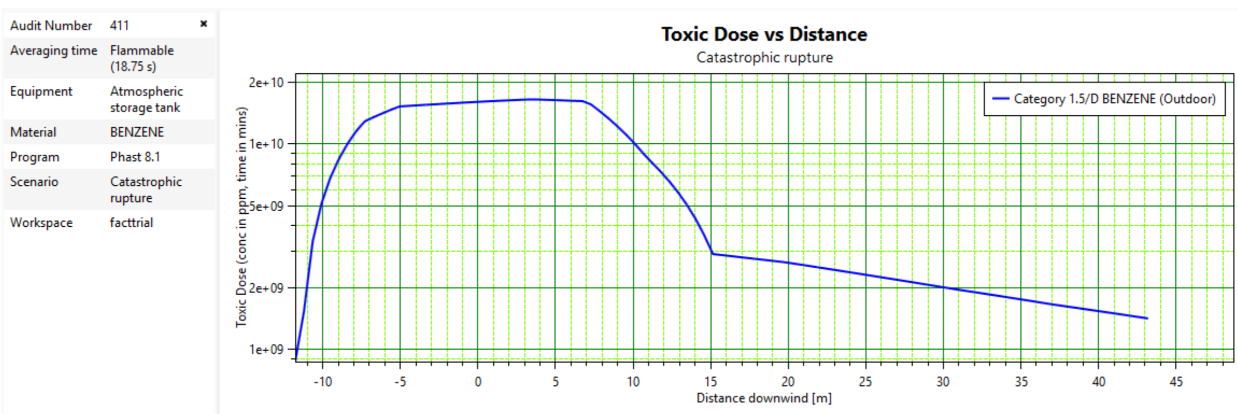


Figure 5 Toxic Dose Vs Distance for rupture of Benzene Tank

Figure 6 Toxic Dispersion Footprint for Catastrophic rupture of Benzene Tank A

The thermal radiation threat zones corresponding to pool fire incident from Benzene Tank B is shown in Figure 7. The red zone corresponds to thermal radiation greater than 10 kW/m^2. It is observed that LS-HS tank is affected.

Figure 7 Thermal radiation footprint from Benzene Tank B

5. Conclusions

In this study, the possibility of attacks on critical installations triggering domino effects with increased consequences are analyzed. A prominent Petrochemical Industry located in Kerala, India was identified for the analysis. HUGIN EXPERT software was used to model the Bayesian Network representing the domino sequence. Also detailed consequence modeling was carried out using Phast (Process hazard analysis) software and ALOHA (Areal Locations of Hazardous Atmospheres) software to obtain the impact zones. It is observed that if an undesirable event is initiated at cyclohexane tank, subsequent incidents of fire and explosions are being triggered in nearby tanks with huge consequences. This is a serious concern as this can result in fatalities to surrounding populations as well. Such studies need to be carried out in the design phase of industries to allocate safe distances between units to inhibit domino effects. The escalation vectors for all possible incidents need to be calculated and layout needs to be planned in such a way that escalation vectors do not cross the threshold values for nearby units. Thus the industry should be made inherently safer. This can reduce the attractiveness of the industry to terrorists. Also appropriate active and passive mitigating barriers such as fire extinguishing systems, active alarm systems and physical protection systems needs to be implemented and maintained properly.

References

API, 2013. Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. ANSI/API 780. American National Standards Institute/ American Petroleum Institute.

Alileche, N., Olivier, D., Estel, L., Cozzani, V., 2017. Analysis of domino effect in the process industry using the event tree method. Saf. Sci. https://doi.org/10.1016/j.ssci.2015.12.028

Bajpai, S., Gupta, J.P., 2005. Site security for chemical process industries, in: Journal of Loss Prevention in the Process Industries. https://doi.org/10.1016/j.jlp.2005.06.011

Casal, J., Darbra, R.M., 2013. Analysis of Past Accidents and Relevant Case-Histories, in: Domino Effects in the Process Industries: Modelling, Prevention and Managing. https://doi.org/10.1016/B978-0-444-54323-3.00002-6

Cozzani, V., Salzano, E., 2004. The quantitative assessment of domino effects caused by overpressure: Part I. Probit models. J. Hazard. Mater. https://doi.org/10.1016/j.jhazmat.2003.09.013

Garrick, B.J., Hall, J.E., Kilger, M., McDonald, J.C., O'Toole, T., Probst, P.S., Parker, E.R., Rosenthal, R., Trivelpiece, A.W., Van Arsdale, L.A., Zebroski, E.L., 2004. Confronting the risks of terrorism: Making the right decisions. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2004.04.003

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013. Domino Effect Analysis Using Bayesian Networks. Risk Anal. https://doi.org/10.1111/j.1539-6924.2012.01854.x

Khan, F.I., Abbasi, S.A., 2001. An assessment of the likehood of occurence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. J. Loss Prev. Process Ind. https://doi.org/10.1016/S0950-4230(00)00048-6

Mannan, S., 2012. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment And Control: Fourth Edition, Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control: Fourth Edition. https://doi.org/10.1016/C2009-0-24104-3

Reniers, G.L.L., Dullaert, W., Audenaert, A., Ale, B.J.M., Soudan, K., 2008. Managing domino effect-related security of industrial areas. J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2007.06.007

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Develop a Hazard Index Using Machine Learning Approach for the Hazard Identification of Chemical Logistic Warehouses

Qingsheng Wang, Mengxi Yu, Shuai Yuan, and Zhuoran Zhang*
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University
College Station, Texas 77843-3122
*Presenter E-mail: zhuoranzhang@tamu.edu

Abstract

With the rapid development of chemical process plants, the safe storage of hazardous chemicals become an essential topic. Several chemical warehouse incidents related to fire and explosion have been reported recently. Therefore, an accurate hazard identification method for the logistic warehouse is needed not only for the facility to develop a proper emergency response plan but also for the residents who live near the facility to have an effective hazard communication. Furthermore, the government can better allocate the resources for first responders to make fire protection strategies, and the stakeholders can lead to improved risk management. Hazard index is a helpful tool to identify and quantify the hazard in a facility or a process unit. The challenge for this research is to improve the current method with the novel technique to implement our purpose.

The first objective of this research is to develop a "Storage Hazard Factor" (SHF) to evaluate and rank the inherent hazards of chemicals stored in logistic warehouses. In the factor calculation, the inherent hazard of chemicals is determined by various parameters (*e.g.*, the NFPA rating, the flammability limit, and the protective action criteria values, *etc.*) and validated by the comparison with other indices. The current criteria for flammable hazard ratings are based on flash point, which is proved to be insufficient. Two machine learning based methods will be used for the classification of liquid flammability considering aerosolization based on DIPPR 801 database. Subsequently, SHF and other warehouse safety penalty factors (*e.g.*, the quantity of the chemicals, the distance to the nearest fire department, *etc.*) are utilized to identify the Logistic Warehouse Hazard Index (LWHI) of the facilities. In the last chapter, this method is applied to real-time data from Houston Chronicle, and several statistical analyses are used to prove the hazard index is helpful for hazard identification to emergency responders and hazard communication to the public.

Keywords: Hazard identification, Hazard index, Machine learning classification

1. Introduction

Since entering the 21st century, people enjoy the benefits of the rapid development of the industry. With the innovations of the new chemical process, process safety must also be up to date and accommodate the new chemical process.

Many industrial cities around the world are facing a dilemma between economic growth and population growth. With the blooming development of chemical process plants, the safe storage of hazardous chemicals become an essential topic. People should understand that some inherent properties of a chemical which makes it profitable to our society may be hazardous in the meantime. The researcher lived in Tianjin for five years, which is one of the economic centers in the north of China. Tianjin has developed a sub-provincial district named Binhai New Area, which is near the largest port in northern China, and where more than 1800 facilities are related to the storage of hazardous chemicals [1]. This thesis is focused on hazard identification for chemical logistics warehouses, which is inspired by the Tianjin explosion that happened on August 12, 2015 [2].

Based on the investigation reports of the storage facilities related to safety incidents, some hazardous chemicals are mentioned more than one time, such as ammonium nitrate. Former researchers in Mary Kay O'Connor Process Safety Center (MKOPSC) have investigated the thermal decomposition and runaway reaction characteristics of some hazardous chemicals [3-5] while few studies have explored the hazard identification applications.

The storage of hazardous chemicals in a warehouse is a complex problem. The potential hazards include flammability, reactivity, and interaction among different types of hazardous chemicals. Hazard index is a helpful tool to identify and quantify the hazard in a facility or a process unit. Various hazard indices are developed in history. Dow's Fire and Explosion Index is the most famous and widely used one, and others like Mond Index, Dow's Chemical Exposure Index, IFAL Index, Weighted Average Risk Rating Index, etc. are developed or modified based on different scopes and purposes [6]. The first edition of Dow's F&EI was issued in 1964 and used within Dow Chemical Company. After the development over half a century, F&EI has been widely used in Dow and outside Dow and becoming the leading hazard index recognized by the chemical industries.

The first objective of this research is to develop a "Storage Hazard Factor" (SHF) to evaluate and rank the inherent hazards of chemicals stored in logistic warehouses. In the factor calculation, the inherent hazard of chemicals is determined by various parameters (*e.g.*, the NFPA rating, the flammability limit, and the protective action criteria values, *etc.*) and validated by the comparison with other indices. Machine learning attracts much attention in recent years and has been applied in process safety in several aspects. Numerous works applied supervised learning to predict lower flammable limit (LFL), upper flammable limit (UFL), minimum ignition energy (MIE), and autoignition temperature [7-12]. Mage et al. utilized unsupervised learning to cluster the thermal stability of organic compounds into seven groups [13]. Therefore, with the lack of study in liquid flammability considering aerosolization and the tendency of the machine learning approach, it is worthful to implement machine learning algorithms to liquid flammability rating. Two machine learning based methods will be used for the classification of flammability. Subsequently, SHF and other warehouse safety penalty factors (*e.g.*, the quantity of the chemicals, the distance to the nearest fire department, *etc.*) are utilized to identify the hazard index of the facilities.

The index can be used not only for the facility to develop a proper emergency response plan but also for the residents who live near the facility to have an effective hazard communication. Furthermore, the government can better allocate the resources for first responders to make fire protection strategies, and the stakeholders can lead to improved risk management.

2. Methodology

2.1. Data collection

The Design Institute for Physical Properties (DIPPR) 801 is a project sponsored by AIChE, which provides more than 30 constant properties and nearly 50 thermophysical properties as well as molecular structure, hazard properties, physical constants for more than 2000 compounds. This database is widely used in chemical properties classification and prediction [7, 8]. After data cleaning, 823 organic compounds will be used in this research.

2.2. Storage hazard factor (SHF)

Based on the literature reviews, various hazard indices are developed or modified based on different scopes and purposes. Considering that the index will be applied to the chemical logistic warehouse, the overall index function can be represented as follows in Equation 1.

$$Logistic\ Warehouse\ Hazard\ Index\ (LWHI) = \sum F_i \times SHF \qquad (Eqn. 1)$$

where F_i represents different penalty factors such as quantity, population density, SHF represent the inherent hazard of the chemicals stored in the warehouse.

Based on the MKOPSC's PCHP project, the formula for calculating the SHF can be modified as follows in Equation 2.

$$SHF = 2^{Modified\ NF} + 2^{NR} + 2^{Modified\ NH} \qquad (Eqn. 2)$$

where NR represents the degree of reactivity, which will be determined by the original NFPA rating; NH represents the degree of health hazard, which will be modified by PAC-3 value; NF represents the degree of flammability, which will be modified by two machine learning methods using DIPPR 801 database.

2.2.1. Modified NH

Protective Action Criteria (PACs) values are an exposure limit system, and this system is commonly used as the guideline for an emergency response to the concentration of the accidental release of the hazardous chemicals.

NH represents the degree of health hazard. The original NFPA rating criteria are based on LC_{50} and LD_{50}, which is more focus on emergency conditions for the working area. Since PAC-3 is the maximum airborne exposure resulting in the most severe consequence, which is life-threatening effects, PAC-3 will be used to modify the NH value for our purpose.

The Department of Energy 's (DOE) current PAC dataset is Revision 29, published in May 2016 [14]. It provides chemical exposure limit values for 3146 chemicals.

2.2.2. Modified NF

The most widely used chemical classification method is NFPA 704, GHS, and OSHA (29 CFR 1910.106). However, both of these criteria are based on flash points only [15]. (Table 1) Evidence shows that liquid can be ignited below its flash point if it is in some particular condition, such as aerosol form [16, 17]. In this research, flash point, autoignition temperature, surface tension, and viscosity are selected to modify the classification, using K-Mean and hierarchical clustering with PCA.

Table 1. Current standards for liquid flammability rating and classification

Standard	Flammability rating and classification	Criteria
	0	Materials will not burn in air when exposed to a temperature of 1500°F for a period of 5 minutes
	1	Flash point at or above 200°F
	2	Flash point between 100 and 200 °F
	3	Flash point between 73 and 100°F
	4	Flash point below 73°F
GHS classification and labeling of chemicals	1	Flash point < 23°C and boiling point ≤ 35°C
	2	Flash point < 23°C and boiling point > 35°C
	3	Flash point ≥ 23°C and ≤ 60°C
	4	Flash point > 60°C and ≤ 93°C
OSHA (29 CFR 1910.106)	1	Flash point < 73.4°F and boiling point ≤ 95°F
	2	Flash point < 73.4°F and boiling point > 95°F
	3	Flash point ≥ 73.4°F and ≤ 140°F. When a category 3 liquid with a flash point ≥ 100°F is heated for use to within 30°F of its flashpoint, it shall be handled in accordance with the requirements for a Category 3 liquid with a flash point < 100°F.
	4	Flash point > 140°F and ≤ 199.4°F. When a category 4 liquid is heated for use to within 30°F of its flashpoint, it shall be handled in accordance with the requirements for a Category 3 liquid with a flash point < 100°F.
	5	When a liquid with a flash point > 199.4°F is heated for use to within 30°F of its flashpoint, it shall be handled in accordance with the requirements for a Category 4 flammable liquid.

In this study, the KC and HC algorithm is implemented through the Python package, Scikit-Learn [18]. The number of clusters is determined by the elbow method, which plots the within-cluster sum of square (WCSS) with respect to the number of clusters [19]. Figure 1 shows the example of the elbow plot when implementing the KC algorithm on liquid flammability clustering based on flash point and autoignition temperature. The number of clusters is 5 in this thesis.

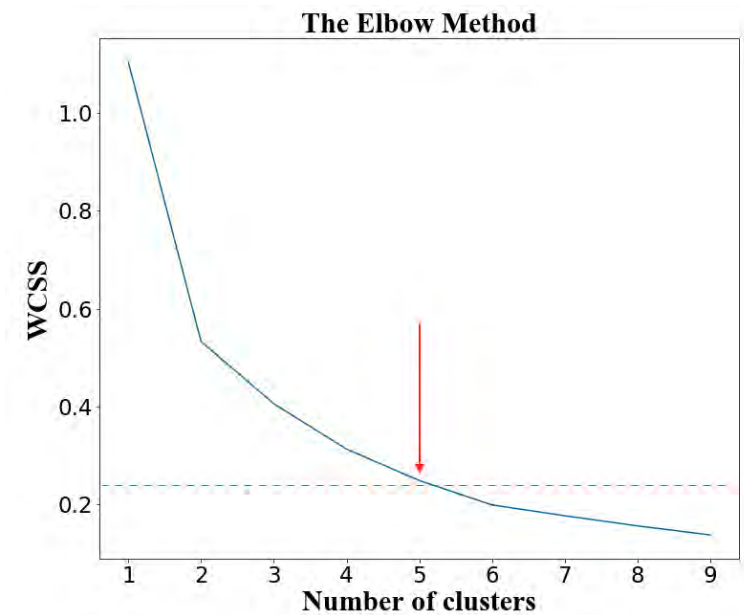


Figure 1. Within-cluster sum of square (WCSS) and the number of clusters

This modification method is reliant on the availability of the data. Despite the lack of data, the original NFPA rating with simple update (if UFL – LFL > 10%, then NF + 1 with a maximum of 4) can be used for SHF calculations.

2.3 Penalty factors

The other important part of Equation 1 is $\sum F_i$, which represents different penalty factors. In this study, quantity, population density, and distance to the nearest fire station are selected to be the penalty factors. The determination guides for each factor are described in this section.

2.3.1. Quantity

Quantity is an important factor that should be considered first when designing a hazard index. Besides the inherent hazard of a hazardous chemical, the amount of chemicals stored in the facility also reveals the level of hazardous.

The following table shows the determination guide of the quantity penalty value. (Table 2)

2.3.2. Population density

Besides the inherent hazards of a chemical and the quantity of the facility stored, another important factor is the safety impact to the public. Given the coordinate of a facility, we defined the population in a radius of two miles near the facility that can be used to represent the population density factor in Equation 1.

Population density information is retrieved on LandView 6.0, a geographic information system software. The following table shows the determination guide of population density penalty value. (Table 3)

Table 2. Penalty value of quantity determination guide

Original code	Min (Pounds)	Max (Pounds)	Penalty value
1	0	99	1.2
2	100	499	1.4
3	500	999	1.4
4	1,000	4,999	1.6
5	5,000	9,999	1.6
6	10,000	24,999	1.8
7	25,000	49,999	1.8
8	50,000	74,999	1.8
9	75,000	99,999	1.8
10	100,000	499,999	2
11	500,000	999,999	2
12	1,000,000	9,999,999	2
13	10,000,000	…	2

Table 3. Penalty value of population density determination guide

(in a radius of two miles near the facility)

Min	Max	Penalty value
10	100	1.2
100	1000	1.4
1000	10000	1.6
10000	100000	1.8
100000	…	2

2.3.3. Distance to the nearest fire station

In the previous sections, we considered the inherent hazard, quantity, and the potential impact to the public. And last but not least, we choose a factor that can reflect the mitigation process, which is an essential point for a storage facility.

Distance to the nearest fire station (FS) is retrieved from HazardHub, a provider of property-level hazard risk database [20]. The following table shows the determination guide of distance to the FS penalty value. (Table 4.)

Table 4. Penalty value of distance to FS determination Guide

Min (Miles)	Max (Miles)	Penalty value
0	1	1.2
1	2	1.4
2	3	1.6
3	4	1.8
4	…	2

3. Results and discussions

3.1 NF modification

3.1.1 Database visualization

Before conducting the liquid flammability rating with the inclusion of aerosolization, we would like to investigate the distribution of observations for each liquid property, and the scatter plots of each pair of liquid properties. The figure 2 shows the aggregated scatter plots, distribution plots, and heatmap of liquid properties. The diagonal of figure 2 shows the distribution of observations for each liquid property. For example, Figure 3 shows the distributions of flash point and surface tension are normally distributed. However, the distributions of autoignition temperature and viscosity are right-skewed.

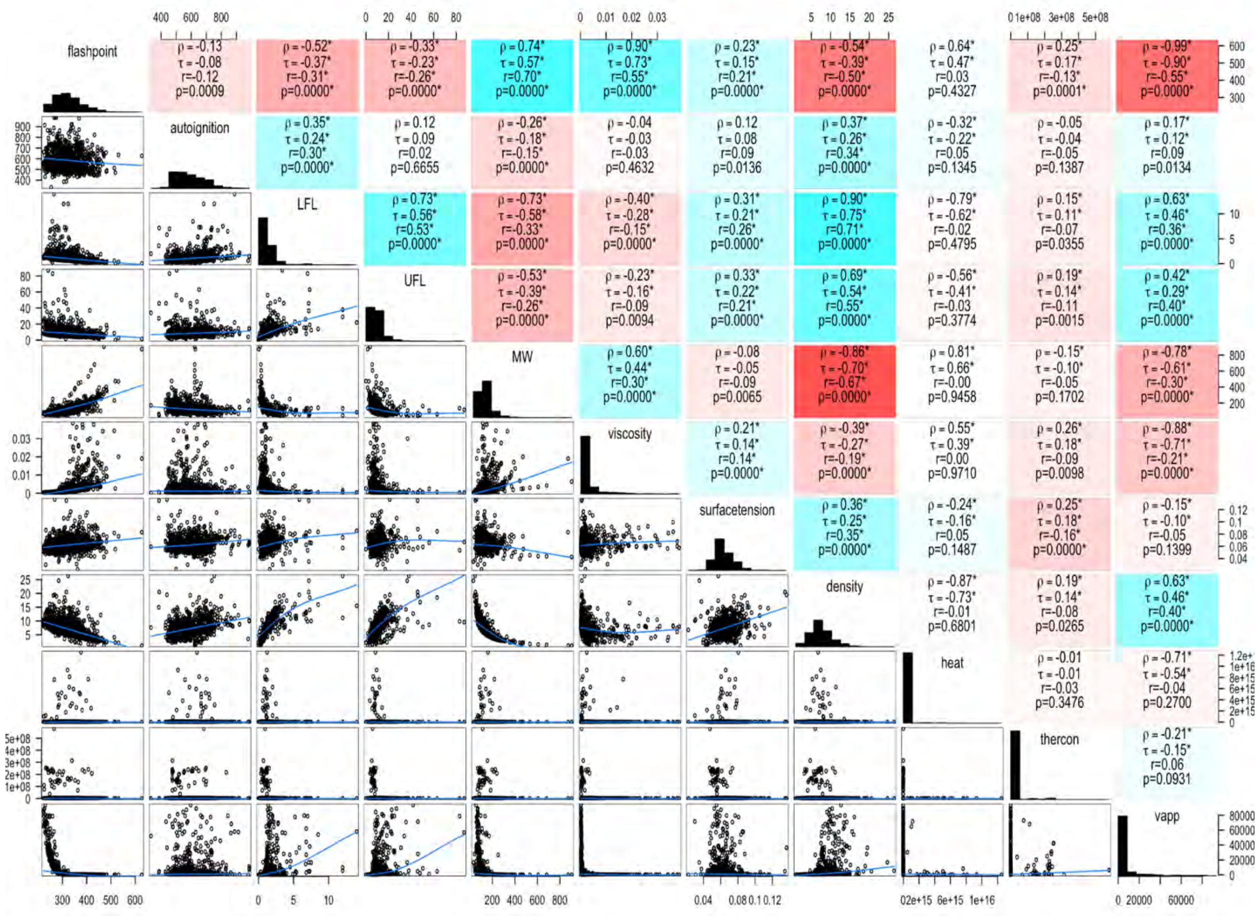


Figure 2. Scatter plots, distribution plots, and heatmap of liquid properties

The left part of figure 2 is the scatter plot of each pair of liquid properties. For example, a positive slope is plotted for the relationship between flash point and molecular weight, shown in the 5th plot from the top in the first column on the left part of figure 2, and the magnified plot in Figure 4.

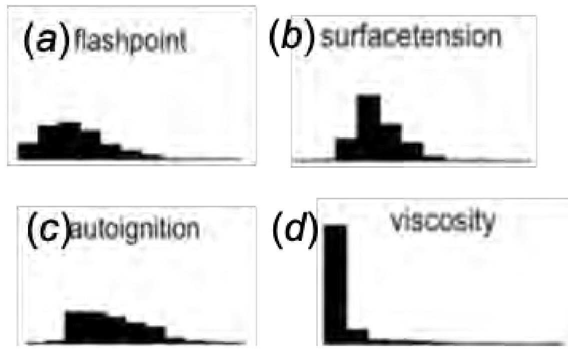


Figure 3. Distributions of liquid properties: (a) flash points; (b) surface tension; (c) autoignition temperature; (d) viscosity

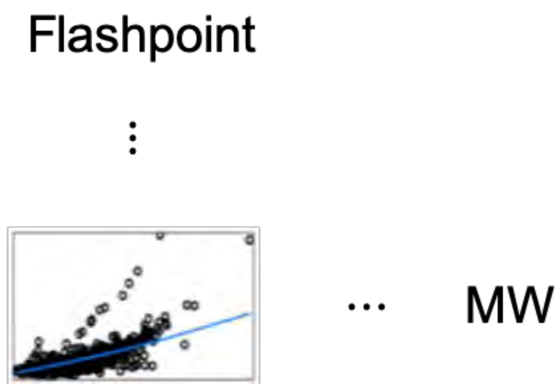


Figure 4. Scatter plot for flash point and molecular weight

The right part of figure 2 shows the statistical correlation between each pair of liquid properties, including Pearson coefficient (ρ), Kendal coefficient (τ), Spearman coefficient (r), and the P-value for Pearson coefficient (p). For example, the statistical correlation between flash point and vapor pressure is found in the upper rightmost location. The Pearson coefficient between flash point and vapor pressure is -0.99, which means a completely negative correlation.

3.1.2. KC and HC algorithm

As discussed before, the number of clusters determined by the elbow method is 5 in this thesis. Thus, the 823 organic compounds from DIPPR 801 are split into five groups and rated from 0 to 4 as in the NFPA rating. The KC clustering is based on flash point and autoignition temperature, which is different from the NFPA rating. The compounds in the group with a rating of 4 are the compounds with the highest flammability. On the other hand, compounds with a rating of 0 have the lowest flammability. Figure 5 shows the data distribution.

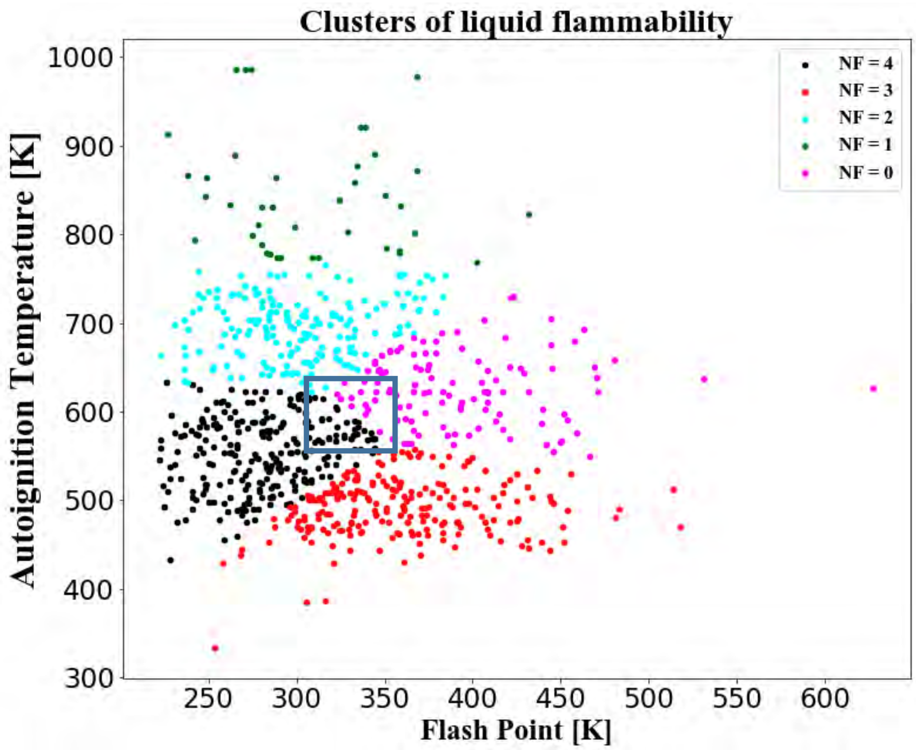


Figure 5. Clusters of liquid flammability using KC algorithm

In Figure 5, some data points labeled black have a medium flash point and medium autoignition temperature comparing to the neighbor points labeled red and cyan. Those points either have a high flash point and low autoignition temperature, or have a low flash point and high autoignition temperature. However, the black label means NF = 4, which is higher than the red (NF = 3) and cyan (NF = 2) label. Similar results and doubts show at the boundary of different clusters in the circled area.

Similarly, Figure 6 displays the dendrogram of clustering through the HC algorithm. Also, 823 organic compounds from DIPPR 801 are split into five groups and rated from 0 to 4 as the same criteria with the HC algorithm. The agglomerative clustering result will assign to each data point. Figure 7 shows the visualized plot in Cartesian coordinates.

In Figure 7, the results located in the controversial boundary between the black (NF = 4) and the red (NF = 3) regions are more reasonable. But this time, a misclassification may happen in the circled area. With a similar flash point, the black labeled data points have the medium autoignition temperature comparing to the red and magenta labeled data points. However, these data points are classified as NF = 4, which is the most hazardous material among all. On the other hand, some points with the lower autoignition temperature are classified as NF = 3, which is less dangerous than black labeled points.

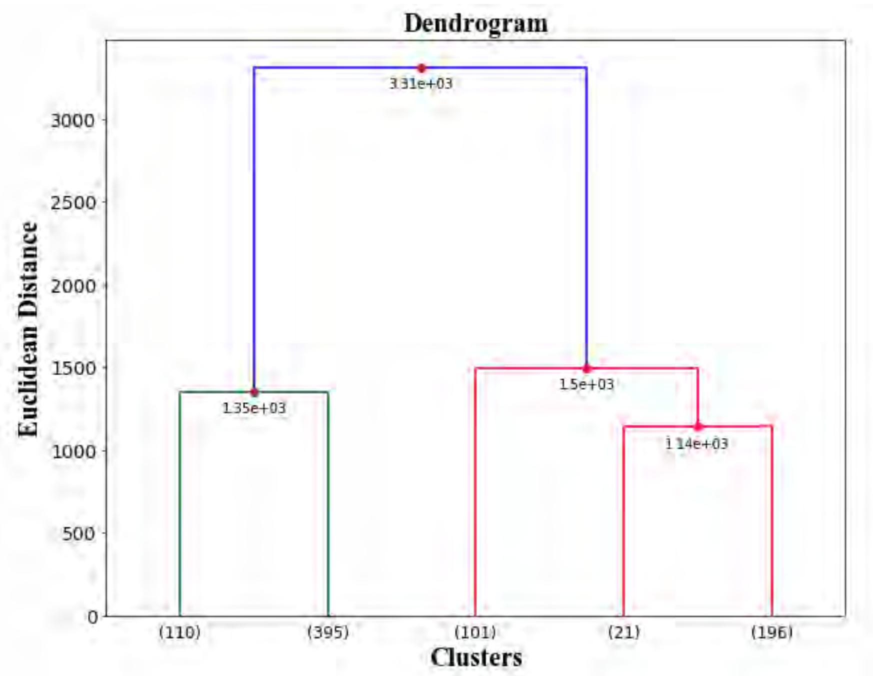


Figure 6. Truncated dendrogram of clustering of liquid flammability

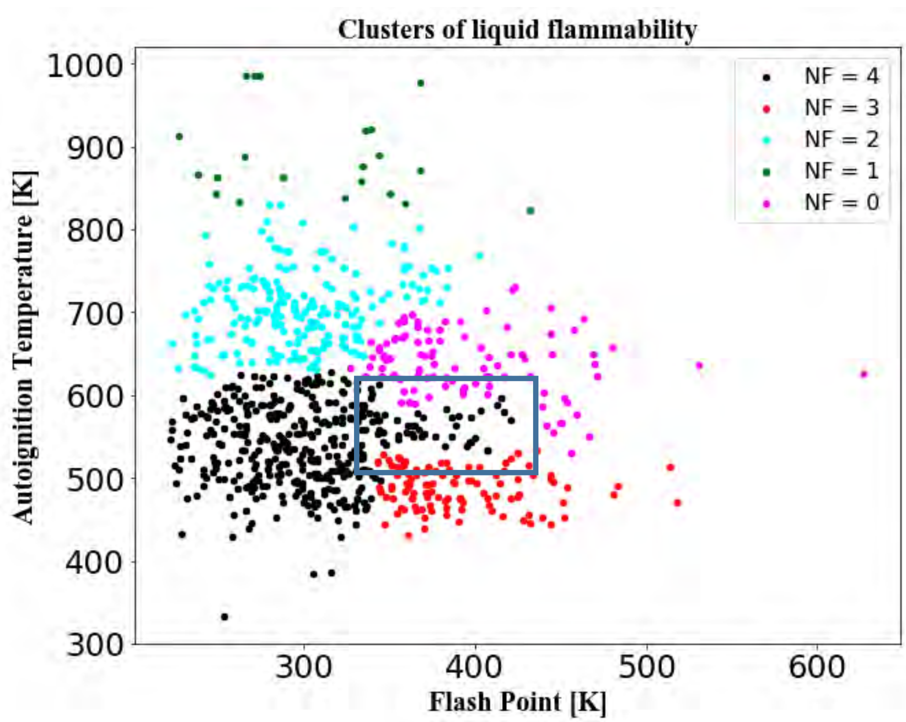


Figure 7. Clusters of liquid flammability using HC algorithm

Comparing the KC and HC algorithms, there are 653 out of 823 compounds with the same rating for liquid flammability in both algorithms. Table 5 shows the liquids with significantly different ratings between the two algorithms. Those liquids in Table 5 require more attention when conducting a risk assessment with inherent flammability.

Table 5. Liquids with significant different ratings between KC and HC algorithm

Substance name	Flammability rating (KC)	Flammability rating (HC)
o-ethylaniline	2	0
hexylene glycol	0	4
cetyl methacrylate	3	0
3-methyl-1-pentene	4	2
1-dodecanol	3	4
4-methyl-1-octanol	0	4

As a result, the KC algorithm has a more reasonable rating for the clustering of liquid flammability, because the circled area is smaller in Figure 5 compared with Figure 7. Another reason is that the misclassification in the KC algorithm is more likely to happen on the boundary of two clusters, whereas the misclassification in HC algorithm is more likely to happen in an area. These results are considering the flash point and autoignition temperature in two dimensions. Therefore, the results are highly interpretable since the X and Y axis both have physical meaning.

But if we want to consider liquid aerosolization probability at the same time, we need to reduce the features for visualization and easier calculation. The PCA method will be applied in the next section.

3.1.3. PCA with KC and HC algorithm

The main purpose of NF modification is to consider aerosolization. In the previous chapter, we conclude that viscosity and surface tension can be used as two indicators of aerosolization. To reduce the flash point, autoignition temperature, viscosity, and surface tension into two principal components (PCA1 and PCA2), we applied the RBF kernel function when reducing four features. Another advantage is that PCA does not need to specify the weight of contributions of liquid aerosolization and flammability. Figure 8 shows the clustering results by the KC and HC algorithm based on PCA1 and PCA2. Besides the advantages of PCA, one thing that needs to keep in mind is that both X and Y axes in Figure 11 have no physical meaning. This is the main disadvantage of the PCA method.

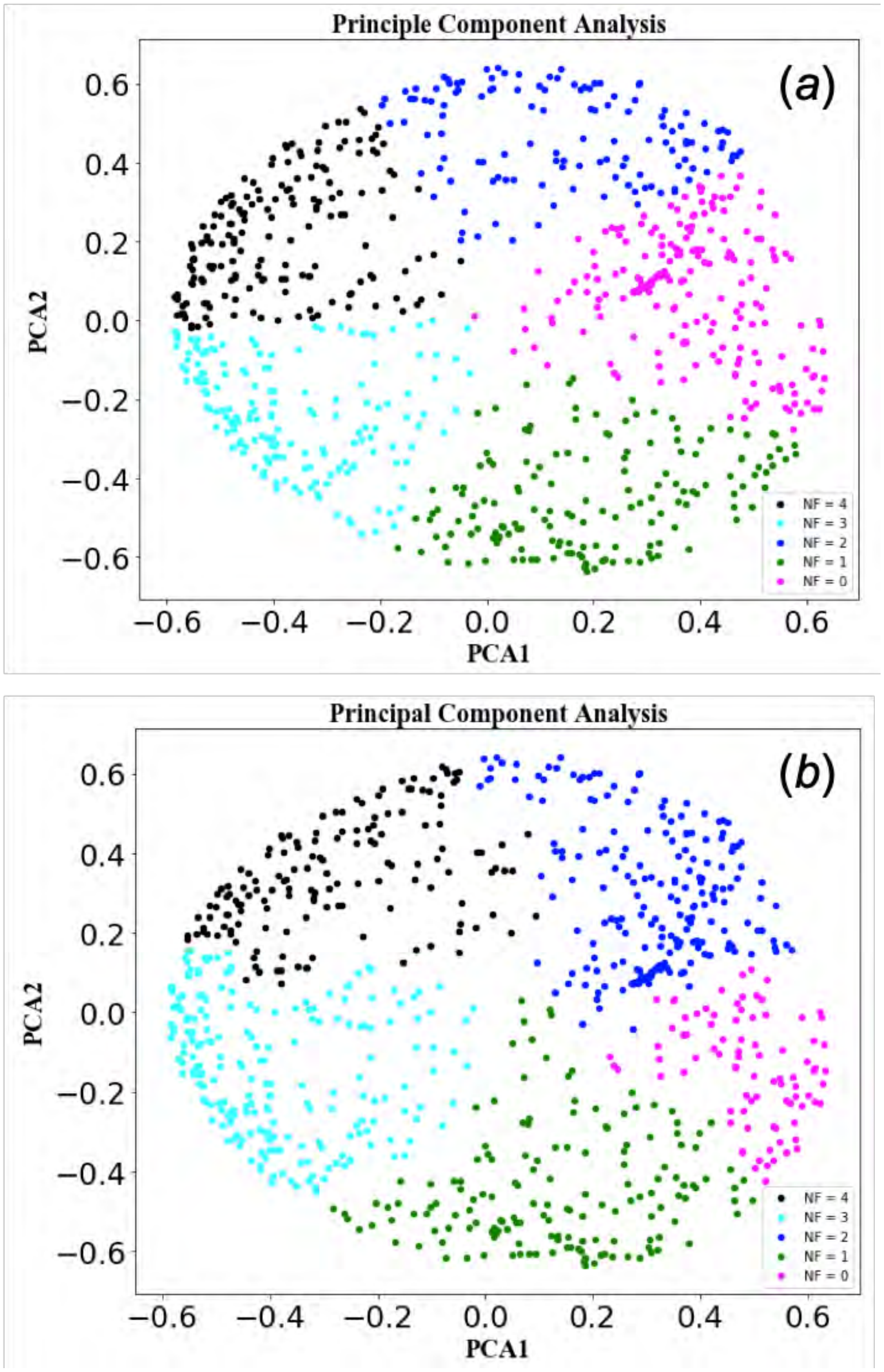


Figure 8. Principal component (PCA1 and PCA2) clusters using (a) KC algorithm (b) HC algorithm.

4. Case study

4.1 Data collection

Houston Chronicle has published a series of articles [21], aiming at exploring fatal mistakes that could have the largest consequences and probes that put the citizen in jeopardy. Houston Chronicle has collected 2581 facilities and over 18000 chemical records in the greater Houston area. The raw data is in EPA Tier II standard and shared with MKOPSC. After data cleaning, at least 33 warehouses that have more than 400 records and over 170 kinds of hazardous chemicals will be used in this research. The raw database includes company information, location information, chemical information, and storage quantity.

4.2 Sample calculation

Table 6 is the sample hazard review for 2-Butoxyethanol from DIPPR 801, DOE's PAC, and NFPA database.

Table 6. Hazard review: 2-Butoxyethanol

Parameter	Data
CAS No.	111-76-2
NFPA NR	0
NFPA NH	2
PAC-3	3400 mg/m^3
NFPA NF	2
Flash point	334.15 K
Autoignition temperature	511.15 K
LFL/UFL	1.1% / 12.7%
Viscosity	2.9 cP at 25°C
Surface tension	26.1 mN/m at 25 °C

Based on the data above, the SHF should be:

1. The original NFPA NR rating is 0, in our calculation, keep the original value.
2. The original NFPA NH rating is 2, and the PAC-3 value is 3400 mg/m^3. Based on the previous discusstion, the modified NH value is still 2.
3. The original NFPA NF rating is 2, the flash point is 334.15 K, autoignition temperature is 511.15 K, LFL / UFL are 1.1% / 12.7%, viscosity is 2.9 cP, and surface tension is 26.1 mN/m. The result of the machine learning method using KC algorithm is 3, but the result become 4 when using HC algorithm. As we discussed in the previous section, result with KC algorithm is more reasonable. So the modified NF value is 3.
4. $SHF = 2^3 + 2^0 + 2^2 = 13$

With the chemical information, we can get the SHF value using the method discussed above. Then the storage quantity information allowed us to convert it into units in pounds. Finally, the location information will help us extract information about population density and distance to FS. Continue the 2-Butoxyethanol example and calculate the LWHI. (Table 7)

Table 7. Tier II information for 2-Butoxyethanol in facility #33

Parameter	Data
CAS No.	111-76-2
SHF	13
Quantity	4 (original code)
Population density	4154 (in a radius of two miles)
Distance to FS	1.62 miles

Based on the data above, the LWHI should be:

1. SHF for 2-Butoxyethanol is 13, based on the calculation from last example.
2. For facility #33, the quantity indicator of 2-Butoxyethanol is 4, which means in (1000,5000) pounds range, and the penalty value is 1.6 based on Table 3.
3. For facility #33, the population density in a radius of two miles is 4154, and the penalty value is also 1.6 based on Table 4.
4. For facility #33, the distance to the nearest fire station is 1.62 miles, and the penalty value is 1.4 based on Table 5.
5. Therefore, the LWHI for 2-Butoxyethanol in facility #33 is: $13 \times 1.6 \times 1.6 \times 1.4 = 46.592$.

5. Conclusions

In this thesis, a hazard index for the hazard identification of chemical logistic warehouses was created and named LWHI. The aim of this index is to numerically calculate the potential hazards in a logistic facility. And the manager or the emergency reponder can use those results to develop their hazard chemicals management plan.

To reach the goal mentioned above, the SHF was introduced to the index. First, two machine learning based methods for liquid flammability rating with the consideration of aerosolization have been proposed. The first method applies KC and HC algorithms in machine learning to chemical classification. The 823 organic compounds in DIPPR 801 are clustered into 5 groups based on their flash point and autoignition temperature. Then the 5 groups regarding liquid flammability are rated from 0 to 4 based on 4 is the most hazardous rating. The advantage of the KC and HC clustering method is its high interpretability. With the analysis mention in previous, the KC algorithm has a more reasonable rating on liquid flammability clustering.

The second method presented uses PCA to reduce the four features (i.e., flash point, autoignition temperature, viscosity, and surface tension) into two principal components (PCA1 and PCA2). The advantage of the PCA rating method is that the weight of contribution of the four features is automatically considered. Admittedly, the lack of interpretability is a disadvantage of the PCA method as the principal components do not have physical significance but only statistical significance. However, compared with traditional flammability classification methods which only rely on flash point and boiling point, the two proposed methods have shown a statistical correlation with liquid flammability. Additionally, one obvious disadvantage of traditional flammability classification methods is the threshold values are determined by humans, which invariably has bias. While machine learning based methods partly eliminate this bias. Also, the boundary of traditional flammability classification methods is linear. But the boundary of the proposed machine learning based methods can be nonlinear to eliminate some misclassification cause by the linear boundary.

After the modified classification metheds and the SHF was developed, LWHI can be calculated with the proposed equation. In chapter 5, we applied real-time data from Houston Chronicle to test and verify LWHI. The results shows high level of reliability, and the distribution of LWHI is left-skewed normal distribution. With this reliable result, the LWHI can serves as a simple and effective hazard identification method that can be included in the overall PHA (Process Hazard Analysis) process of the facility.

6. References

[1] 天津市 2017 年国民经济和社会发展统计公报 / Statistical Communiqué of Tianjin on the 2017 National Economic and Social Development in, Statistical Bureau of Tianjin, 2017.

[2] G. Fu, J. Wang, M. Yan, Anatomy of Tianjin Port fire and explosion: Process and causes, Process Safety Progress, 35 (2016) 216-220.

[3] Z. Han, S. Sachdeva, M.I. Papadaki, M.S. Mannan, Ammonium nitrate thermal decomposition with additives, Journal of Loss Prevention in the Process Industries, 35 (2015) 307-315.

[4] C.-P. Lin, J.-S. Li, J.-M. Tseng, M.S. Mannan, Thermal runaway reaction for highly exothermic material in safe storage temperature, Journal of Loss Prevention in the Process Industries, 40 (2016) 259-265.

[5] Q. Wang, D. Ng, M.S. Mannan, Study on the Reaction Mechanism and Kinetics of the Thermal Decomposition of Nitroethane, Industrial & Engineering Chemistry Research, 48 (2009) 8745-8751.

[6] S. Mannan, Chapter 6 - Hazard Identification, in: Lees' Process Safety Essentials : Hazard Identification, Assessment and Control, Elsevier Science & Technology, Oxford, UNITED STATES, 2013.

[7] B. Wang, H. Yi, K. Xu, Q. Wang, Prediction of the self-accelerating decomposition temperature of organic peroxides using QSPR models, Journal of Thermal Analysis & Calorimetry, 128 (2017) 399-406.

[8] B. Wang, L. Zhou, K. Xu, Q. Wang, Prediction of Minimum Ignition Energy from Molecular Structure Using Quantitative Structure–Property Relationship (QSPR) Models, Industrial & Engineering Chemistry Research, 56 (2017) 47-51.

[9] Y. Pan, J. Jiang, R. Wang, H. Cao, Advantages of support vector machine in QSPR studies for predicting auto-ignition temperatures of organic compounds, Chemometrics and Intelligent Laboratory Systems, 92 (2008) 169-178.

[10] S. Yuan, Z. Jiao, N. Quddus, J.S. Kwon, II, C.V. Mashuga, Developing Quantitative Structure–Property Relationship Models To Predict the Upper Flammability Limit Using Machine Learning, Industrial & Engineering Chemistry Research, 58 (2019) 3531-3537.
[11] Y. Pan, J. Jiang, R. Wang, H. Cao, Y. Cui, A novel QSPR model for prediction of lower flammability limits of organic compounds based on support vector machine, Journal of Hazardous Materials, 168 (2009) 962-969.
[12] P. He, Y. Pan, J.-c. Jiang, Prediction of the self-accelerating decomposition temperature of organic peroxides based on support vector machine, Procedia Engineering, 211 (2018) 215-225.
[13] L. Mage, N. Baati, A. Nanchen, F. Stoessel, T. Meyer, A systematic approach for thermal stability predictions of chemicals and their risk assessment: Pattern recognition and compounds classification based on thermal decomposition curves, Process Safety and Environmental Protection, 110 (2017) 43-52.
[14] C.E. Baukal, The Slipcover for The John Zink Hamworthy Combustion Handbook, Boca Raton, 2013.
[15] J.F.L. Daniel A. Crowl, Chemical Process Safety: Fundamentals with Applications, Third Edition ed., 2013.
[16] R.C. Santon, Mist fires and explosions - An incident survey, Institution of Chemical Engineers Symposium Series, (2009) 370-374.
[17] M.S. Mannan, The Buncefield explosion and fire–lessons learned, Process Safety Progress, 30 (2011) 138-142.
[18] F. Pedregosa, Ga, #235, l. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, #201, d. Duchesnay, Scikit-learn: Machine Learning in Python, J. Mach. Learn. Res., 12 (2011) 2825-2830.
[19] T. Kodinariya, P.R. Makwana, Review on Determining of Cluster in K-means Clustering, International Journal of Advance Research in Computer Science and Management Studies, 1 (2013) 90-95.
[20] John, HazardHub API, in: HazardHub (Ed.), 2019.
[21] M. Collette, M. Dempsey, Chemical Breakdown, in, Houston Chronicle, 2016.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Dust Explosions and Collapsed Ductwork

Brenton L. Cox*, David C. Hietala, and Russell A. Ogle*
Exponent, Inc.
Warrenville, Illinois 60555
*Presenters E-mails: rogle@exponent.com, bcox@exponent.com

Abstract

One of the more obvious consequences of a dust deflagration inside process equipment or a structure is the mechanical damage caused by shock (compression) waves. This overpressure damage is revealed through the displacement of equipment, the outward deformation or rupture of enclosures constructed of ductile materials, or the projection of missiles. However, a different type of damage is sometimes observed in the ductwork connecting process equipment. In particular, the ductwork is collapsed as if it were subjected to an external, rather than an internal pressure. The phenomenon that causes this collapse of thin-walled conduit is a gas dynamic process called an expansion wave. When a dust deflagration travels through a conduit, it accelerates and causing a rise in pressure. When the dust deflagration is vented (say through a deflagration vent), the discharge of the high pressure combustion products causes the formation of an expansion wave that travels in the reverse direction from the vent backwards. The expansion wave causes the pressure in the ductwork to fall below atmospheric pressure. The sub-atmospheric pressure, in turn, causes the ductwork to fail by buckling. In this study, we examine the gas dynamics of the expansion wave, demonstrate how to calculate the degree of pressure drop caused by the expansion wave, and illustrate the concept with case studies of dust explosions.

Keywords: Incident Investigation, Dust Explosion

1 Introduction

Incident investigation plays an important role in process safety management. The objective of incident investigation is to prevent a recurrence of the same incident. The investigation of an accidental dust deflagration is oftentimes challenging due to the severity of both mechanical and structural damage. The dynamics of the deflagration event can be especially difficult to trace in a process unit with process lines and vents connecting multiple pieces of equipment. In a unit with interconnected equipment, it is not unusual to find evidence of overpressure damage such as bulged or ruptured process vessels. Ductwork, on the other hand, tends to exhibit less damage associated with deformation directed outwards from the duct interior. Instead, if it exhibits any damage at all, ductwork and process vents tend to exhibit a collapsed appearance.

There are two potential mechanisms for the collapse of a length of duct. One mechanism requires that the external pressure on the duct is greater than the internal pressure. In this circumstance, it is possible that the dust deflagration inside the building caused the positive overpressure on the outside of the duct. This hypothesis would lead the investigator to search for signs of a deflagration propagating through the room. The second mechanism requires that the internal pressure inside the duct is less than the ambient (atmospheric) pressure in the room. The mechanism that can cause this to occur is an expansion wave, a gas dynamic phenomenon discussed in the next section. An expansion wave is a consequence of a deflagration propagating inside the duct.

2 Flame Acceleration and Pressure Waves

If a large combustible dust cloud is ignited at its center, a flame will propagate outwards in a radial direction. This radial expansion will continue until either the flame reaches the edge of the dust cloud or it encounters a solid boundary. If the dust flame propagates inside a duct or channel, the dynamic behavior of the flame changes. The duct confines the flame and the hot combustion products thus preventing the three-dimensional expansion process. Instead, the flame and combustion products can expand in only one direction. Because the fluid medium—air—is a compressible medium, the gas velocity increases as the hot gaseous combustion products expand. The expansion process causes an acceleration of the flame speed which results in turbulence.[1] The turbulent mixing of the flow field causes the mass burning rate to increase. This leads to a positive feedback loop with flame speed, turbulent mixing, mass burning rate, and gas expansion rate all increasing. This process is illustrated in Figure 1.

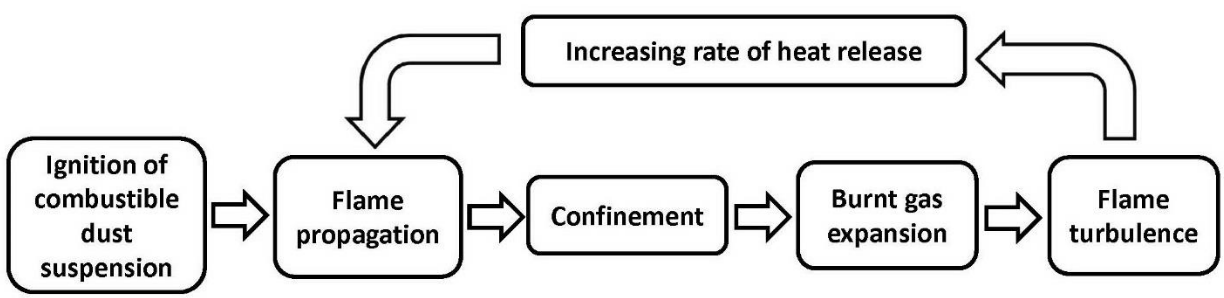


Figure 1 Flame acceleration caused by turbulence

This positive feedback loop leads to the formation of a pressure wave called a compression wave. The compression wave steepens as it travels down the duct eventually forming a shock wave. The compression wave is a pressure disturbance. It travels in the same direction as the gas

[1] The flame speed should not be confused with the burning velocity. The flame speed is the velocity of the flame as measured by an observer using a fixed, stationary coordinate system. The burning velocity is the velocity of the unburnt mixture relative to a coordinate system fixed to the flame.

flow. Figure 2 illustrates the flow field of an accelerating flame with a shock wave and the associated pressure profile for an instant in time.

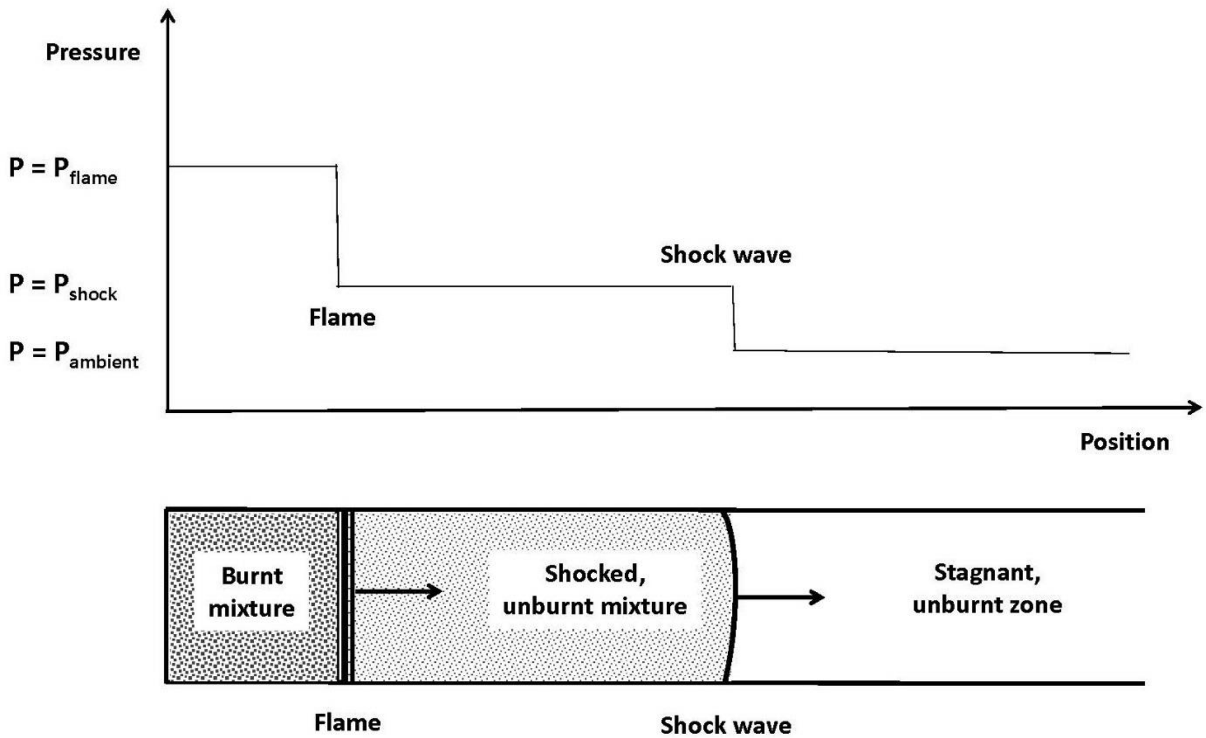


Figure 2 Illustration of a flame accelerated shock wave propagating down a tube

The positive overpressure of the shock wave, generated by flame acceleration, can damage equipment downstream of the point of ignition. Overpressure damage is the type of damage one most often associates with an explosion.

The dynamics of the compression wave process is characterized by two velocities: the speed of sound in the unburnt gas and the flame speed. The sound speed is a measure of how quickly a pressure disturbance travels in the gaseous medium. For an ideal gas, the sound speed can be calculated with the equation

$$a = \sqrt{\frac{\gamma\, R_g\, T}{\mathcal{M}}}$$

where a is the sound speed, γ is the specific heat ratio, R_g is the universal gas constant, T is the absolute temperature, and $\mathcal{M}$ is the molar mass of the gas. The significance of wave interactions depends on the acoustic time scale of the flow. The time scale for an acoustic disturbance in a conduit is the time it takes a sound wave to travel the distance of the conduit. The acoustic time scale is simply the length of the conduit divided by the sound speed. For a conduit length of 10 m and a sound speed of 350 m/s, the acoustic time scale is approximately 29 ms.

The flame speed is generally a measured quantity. The strength of the overpressure is related to the magnitude of the flame speed. This relationship can be calculated using the normal shock relations for an ideal gas.[2] However, these equations form a set of nonlinear algebraic equations which tend to obscure the relationship between flame speed and overpressure. In many cases, the overpressure can be estimated by a simpler linear equation based on an acoustic approximation.[3] The equation takes the following form:

$$\Delta P = \rho_u \, a_u \Delta v$$

In this equation ΔP is the overpressure (final minus initial) across the shock wave, ρ_u is the unburnt gas-dust mixture density, a_u is the sound speed of the unburnt gas-dust mixture, and Δv is the flame speed. This relation more clearly indicates the importance of flame speed and shock overpressure. It gives reasonable estimates of the overpressure for flame speeds up to approximately 400 m/s. Using the properties of air at an ambient pressure of 1.013 bar absolute and a temperature of 300 K, a flame speed of 100 m/s gives a shock overpressure of 0.41 bar gauge. An overpressure this large can cause the failure of non-reinforced concrete block wall panels.

A dust deflagration can travel down a duct as long as there is fuel to sustain it. If the deflagration runs out of fuel, the high pressure gas column will expand and reduce the magnitude of the overpressure behind the flame. The dissipation of the shock wave below the level of damaging overpressures will usually require a travel distance much greater than the length of conduits typically found in industrial facilities. Thus, even if it runs out of fuel, the high pressure gas formed by the deflagration will vent to the atmosphere by causing a failure of containment or by design through an explosion vent. Explosion vents are a common safeguard used to mitigate a potential dust deflagration. Venting of high pressure gas into the ambient environment can lead to an external shock wave, flames, and hot gases, all of which may cause injury or property damage. Hence, explosion venting must occur in a location that will maintain the risk of injury or damage to an acceptable level.

However, the venting of the flame and the gaseous combustion products is not the end of the story. The venting of the high pressure gases leads to the formation of another pressure wave called an expansion (or rarefaction) wave. An expansion wave is the fluid dynamic process by which the gas pressure in a vessel or conduit achieves its final pressure in hydrostatic equilibrium with the ambient pressure. In complex conduit networks with multiple lines, elbows, tees, and process equipment, a very complex set of wave interactions can occur. These complex wave interactions are beyond the scope of this paper. A key feature of an expansion wave in a long conduit is its ability to cause the formation of a partial vacuum (pressure below atmospheric pressure).

An expansion wave is a pressure disturbance that travels in the opposite direction of the gas flow. To understand how an expansion wave works, we must first distinguish between a slow leak process and a fast leak process. Consider a conduit filled with high pressure gas (i.e., the gas pressure is at least several multiples of ambient pressure). If a very small hole is formed in one

---

2 Anderson, J.D. *Modern Compressible Flow with Historical Perspective*. New York: McGraw-Hill, pp.54-63 1982.

3 Ogle, R.A. *Dust Explosion Dynamics*. Oxford, Butterworth-Heinemann, pp. 513-516, 2017.

end of the conduit, a steady leak of gas will occur. If the time to depressurize the conduit is several multiples of the acoustic time scale for the conduit, any spatial gradients are smoothed by the multiple reflections inside the conduit and the leak is considered slow. A slow leak of high pressure gas from a closed volume exhibits a gradual, spatially uniform decrease in pressure. The pressure declines monotonically and asymptotically approaches the ambient pressure. An example of how to analyze this system as a control volume with no spatial gradients is available in gas dynamics textbooks.[4,5]

If a large hole is created in the conduit, such that the depressurization time approaches the acoustic time scale, then the leak is considered fast. A fast leak of high pressure gas exhibits a spatially nonuniform pressure profile called an expansion wave. With a fast leak the expansion wave creates axial gradients within the conduit (a gradient in the direction of flow) in pressure, temperature, and gas density. A complete description of the fluid dynamic processes involved during gas venting would require a numerical solution of the governing equations for a compressible fluid. The method of characteristics is ideal for this challenge. However, such a simulation would not only be complex but it would also be too specific to the particular situation analyzed. Some insight to the venting process can be obtained by considering a simpler problem that yields an analytical solution.

The simpler problem assumes that the conduit is permanently closed on one end and closed on the other end with a frangible diaphragm. The conduit is initially filled with high pressure gas (gas at a pressure greater than atmospheric pressure). At time zero the frangible diaphragm is broken and the gas is vented out of the open end into the atmosphere. This version of the expansion wave problem is equivalent to the withdrawal of a piston from a conduit.[6],[7] In the spirit of developing the simplest description of the situation, attention is focused on the propagation of a single expansion wave. In reality, one would expect to observe multiple expansion waves with wave reflection off of the closed end. Consideration of a single expansion wave will convey the essential physics. Figure 3 depicts the trajectory of this expansion wave process.

---

4 Saad, M.A. *Compressible Fluid Flow*. Englewood Cliffs, Prentice-Hall, pp. 98-101, 1985.

5 Zucrow, M.J.. and Hoffman, J.D. *Gas Dynamics, Volume 1*. New York, John Wiley, pp. 177-178, 1976.

6 Anderson, J.D. *Modern Compressible Flow with Historical Perspective*. New York: McGraw-Hill, pp. 196-202, 1982.

7 Thompson, P.A. *Compressible Fluid Dynamics*, New York: McGraw-Hill, pp. 392-398, 1972.

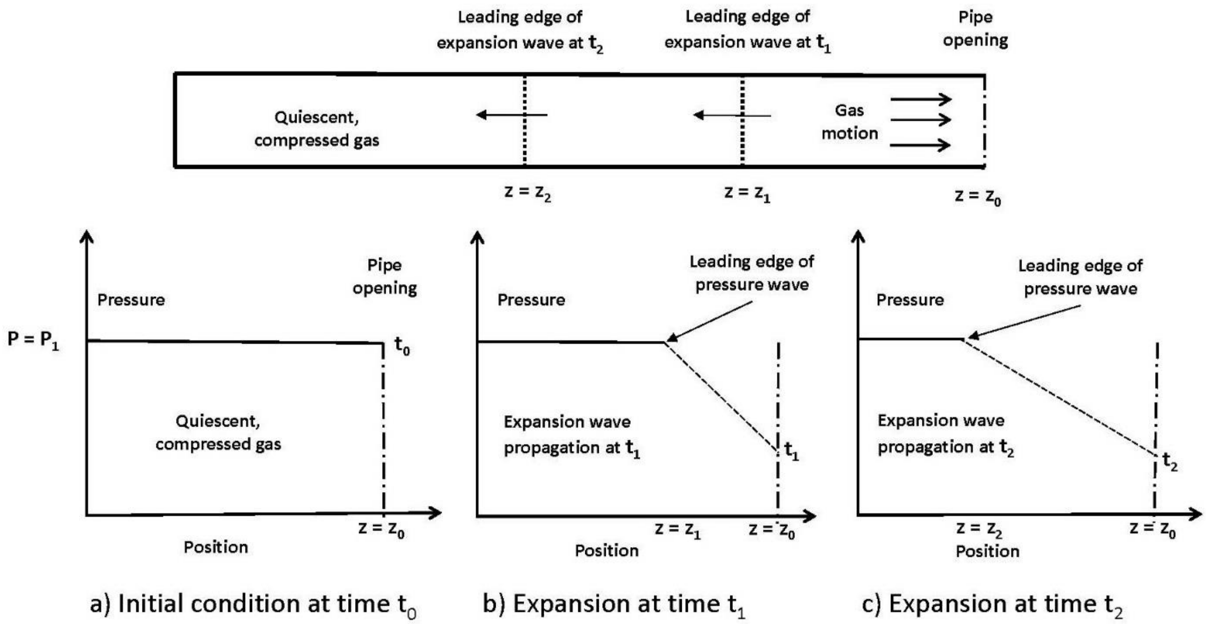


Figure 3 Progression of an expansion wave in a conduit

The expansion waves causes the pressure inside the conduit to fall below the initial pressure. The magnitude of this pressure decline depends on the speed of the piston which in this example is equal to the flame speed. The pressure behind the expansion wave can be calculated from the following equation:

$$\frac{P_2}{P_1} = \left[1 - \frac{1}{2}(\gamma - 1)\frac{\Delta v}{a_1}\right]^{\frac{2\gamma}{\gamma-1}}$$

where P_2 is the absolute pressure in the expanded region, P_1 is the absolute pressure in the undisturbed region, γ is the specific heat ratio, Δv is the flame speed, and a_1 is the speed of sound in the undisturbed region. If the piston speed is sufficiently fast, the pressure inside the conduit can drop to a level below atmospheric pressure. The influence of flame speed on the final expansion pressure is demonstrated in

Table 1 using two fluids for comparison: air and combustion products.

Table 1 Expansion pressure ratio for different flame speeds

Flame speed, m/s	Pressure ratio, air[8]	Pressure ratio, combustion products[9]
10	0.960	0.968
30	0.885	0.905
100	0.660	0.716
300	0.265	0.356

Once the expansion wave hits a solid boundary, it is reflected and travels back towards the opening. In a matter of seconds, this wave reflection process eventually brings the conduit to a quiescent condition at atmospheric pressure. However, even though it is transient, the partial vacuum condition in the conduit can cause the cylindrical geometry to become unstable leading to its collapse. The mechanics of the collapse is the subject of the next section.

3 Mechanics of Collapsed Ducts

When the pressure inside of a duct (P_i) differs from the pressure outside of the duct (P_o), stress is imposed on the duct wall (see Figure 4). If the difference in pressures becomes too large for the wall to withstand, the duct itself may fail. However, the failure mode differs if due to an internal overpressure (i.e., $P_i > P_o$) than if due to an external overpressure or an internal vacuum (i.e., $P_i < P_o$). As a result, the critical pressure difference that may result in failure can vary significantly. The difference can be explained by examining the nature of the failure mode for each limit: excess internal pressure causes the duct to rupture,[10] whereas excess external pressure causes the duct to collapse (or buckle).[11]

8 The properties of air are assumed to be T = 300 K, P_1 = 2 bar, γ = 1.4, and M = 29 kg/kmol, a_1 = 347 m/s.
9 The properties of the combustion products are assumed to be T = 400 K, P1 = 5 bar, γ = 1.2, M = 30 kg/kmol, a_1 = 364 m/s.
10 Methods for the Calculation of Physical Effects due to Releases of Hazardous Substances. TNO Yellow Book.
11 de Paor, et al. Prediction of vacuum-induced buckling pressures of thin-walled cylinders. *Thin-Walled Structures.* 55 (2012) 1-10.

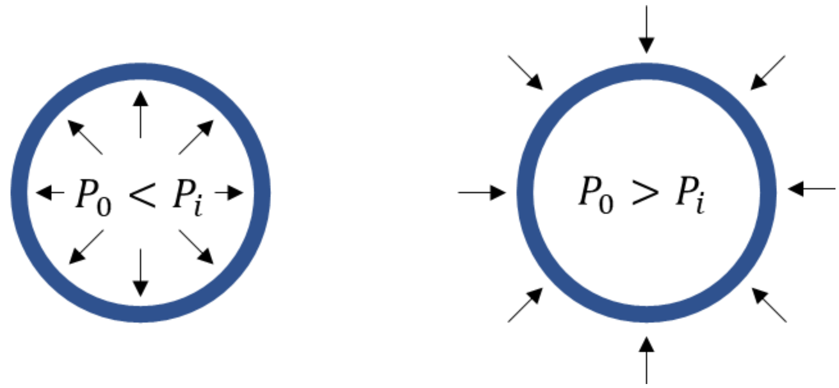


Figure 4. Conceptual diagrams for a thin walled cylinder subjected to (left) an internal overpressure and (right) and external overpressure.

Consider the following related analogy: a typical aluminum beverage can will withstand large internal pressure imposed by carbonated beverages (e.g., up to 6 bar or 90 psi).[12] The elevated internal pressure keeps most of the carbon dioxide in solution, ensuring a fizzy (not flat) beverage. However, once the can is opened, the internal pressure will relieve through the opening, and the shell is now considerably more fragile to external forces than it was to internal forces. The most basic explanation is as follows: for the container to deform any significant amount due to internal overpressure would require the metal either stretch or fracture. However, a collapse merely requires bending. The thin aluminum forming a beverage can has high tensile strength but has very little resistance to bending. Thus, it is easy to crush the can but hard to rupture it from internal overpressure. Related phenomena explain why ducts designed to convey combustible dust may not rupture during an explosion event, despite significant overpressure, but rather may collapse due to the subsequent compression waves that create a relatively mild internal vacuum. In the following sections, we discuss these phenomena in greater detail.

3.1 Theory of Shells

To understand the difference between rupture and collapse, it is worth briefly discussing the theory of shells, a key tool utilized to describe how relevant structures respond to external forces. A thorough treatment of the theory of shells is given in the book by Ventsel and Krauthammer, titled *Thin Plates and Shells*.[13] In this context, a shell is defined as a body bounded by two curved surfaces, where the distance between the surfaces is small in comparison with other body dimensions. By surfaces, this definition refers to the inner and outer surfaces of the wall, e.g., the inside and outside of a spherical or cylindrical vessel. Thus, for the theory of shells to be applicable, the vessel should have curved walls that are thin relative to the other dimensions of the vessel. A shell can be approximated by integrating the stress distribution throughout the shell

[12] Ward-Bailey, J. "The surprising science behind the aluminum soda can." The Christian Science Monitor. April 14, 2015. url:https://www.csmonitor.com/Science/Science-Notebook/2015/0414/The-surprising-science-behind-the-aluminum-soda-can

[13] Ventsel, E. and Krauthammer, T. *Thin Plates and Shells*. 2001.

into a "middle" surface that reduces the governing equations to two dimensions (axial and circumferential, in the case of a cylinder).

The primary distinction between a shell and a plate is the inherent curvature that influences the shell's behavior under loading. As a result, bending cannot be separated from stretching, and so compressive and tensile displacements are coupled. Shells are categorized by their type of curvature and their thickness. Here, we focus on circular cylinders with thin walls, where the maximum ratio of the wall thickness to the radius of curvature is much smaller than unity. Most circular ducts used to transport combustible dust meet this description.[14]

3.2 Rupture vs Collapse

A thin, elastic shell supporting an external load by means of internal forces (stress resultants) may be appropriately loaded and supported such that the bending and twisting moments are negligible.[15] This state of stress is referred to as the membrane (or momentless) state of stress, and it permits a further reduction of the governing equations into what is referred to as the membrane theory of shells. This theory is applicable when bending cannot occur inextensionally, i.e., these surfaces cannot be deformed without stretching or shrinking the middle surface. One family of such surfaces are convex, closed surfaces, such as a cylindrical duct supported by circular rings. For example, a cylinder cannot be bent while maintaining a circular cross-section without the "middle surface" stretching in some areas and shrinking in others. Consider the extremum where a cylinder is bent until its flat (circular) ends meet, forming a torus (or doughnut-shaped shell). A torus has a different outer circumference than inner circumference. Thus, to deform the straight cylinder into the round torus, portions of the cylinder must be stretched while other portions must be compressed. On the contrary, a flat sheet can be bent into a cylinder without elongating the middle surface, and thus membrane theory is not appropriate.

3.2.1 Critical Pressure for Rupture

If the internal pressure of a duct increases, the tendency of the material is to deform to increase the internal volume accordingly. However, if the duct wall is in the membrane state of stress, the resistance to this stretching is provided by the strength of the material involved. Because a cylindrical duct is a confex, closed surface, it cannot increase its volume any further without stretching; thus, additional pressure results in additional stress in the duct wall. The wall can accommodate this stress up to a point without deforming permanently. However, if the internal pressure continues to rise, the wall will ultimately yield and/or fracture, rupturing the duct.[16]

Figure 5 shows a simplified force balance around a long, thin-walled duct of radius r and thickness t, assuming the circumferential stress is uniform throughout the thin wall. This force

---

[14] Note, because square and rectangular ducts lack inherent curvature, their mechanics are not properly described by this theory.

[15] Ventsel, E. and Krauthammer, T. *Thin Plates and Shells*. 2001. Chapter 13

[16] Premature failures may also be induced by factors such as corrosion, erosion, overheating, fatigue, or material defects, or external impact. However, these are outside of the scope of the current discussion. More information can be found in sources such as Lee's Loss Prevention in the Process Industries, section 17.27, or Methods for the Calculation of Physical Effects due to Releases of Hazardous Substances. TNO Yellow Book. p. 7.16.

balance reveals two principal stresses: a hoop stress along the circumference of the duct, given by:[17]

$$\sigma_h = \frac{\Delta P * r}{t}$$

and a longitudinal stress along the axis of the duct, given by:

$$\sigma_l = \frac{\Delta P * r}{2t}$$

These stresses are explicitly dependent on the pressure difference between the inside and outside of the duct, $\Delta P = P_i - P_o$, as well as the radius of the duct, *r*, and the thickness of the duct, *t*. Note, the hoop stress is exactly twice the longitudinal stress, and thus represents the largest principal stress.

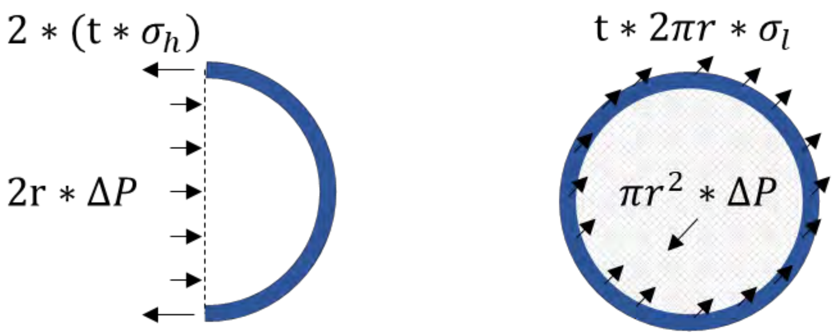


Figure 5. Simplified force balance around a cylindrical shell where a constant stress across the wall is assumed.

The simplest approximation for the critical pressure at which the cylinder will burst is given by the maximum-stress theory of failure, which assumes that failure occurs when the largest principal stress reaches the yield stress.[18] That criteria is given by:

$$\Delta P_{cr,rupture} = \sigma_{cr} \left(\frac{t}{r}\right)$$

where σ_{cr} is the critical stress at the point of rupture. More accurate estimates for the critical pressure can be calculated but are beyond the scope of this discussion. For an existing vessel with specified maximum allowable working pressure (MAWP), it is common to estimate the critical pressure for rupture to be four or five times the maximum allowable working pressure.[19]

---

[17] Avallone, E.A. and Theodore, T.B. *Marks' Standard Handbook for Mechanical Engineers*. 10th Edition. 1996. p. 5-45.

[18] Avallone, E.A. and Theodore, T.B. *Marks' Standard Handbook for Mechanical Engineers*. 10th Edition. 1996. pp. 5-48 and 5-49.

[19] Crowl, D.A. and Louvar, J. F. *Chemical Process Safety*. 2nd Ed. 2002. p. 356.

3.2.2 Critical Pressure for Collapse

A duct subjected to an external overpressure (or internal vacuum) is subject to a different scenario than the membrane stress state, and its failure is more challenging to predict.[20] In practice, many vessels and ducts are designed without any intension for use under internal vacuum or external overpressure. These shells can be economically designed with thin walls made of materials with high tensile strength, ideally suited for service in a membrane stress state. However, these shells are not as robust to the compressive stresses and may collapse (or buckle) at much lower magnitude vacuum pressure than might be anticipated based upon their design overpressure.

The first systematic experimental effort to understand the phenomenon of duct collapse was performed in 1858 by Fairbairn.[21] At that time, the nascent steam boiler industry was increasing working pressures from 10 psi to 50 psi, and in some cases approaching 150 psi, but the "principles of construction [had] not kept pace." The primary focus of the study was the growing use of internal flues and tubes subjected to external pressures within the boiler. The practical conclusion of the report was that the external shell of a boiler of "ordinary construction" was capable of supporting internal pressures three to four times greater than the internal flues could withstand without collapse. This study helped explain an increase in the number of boiler explosions that initiated due to the collapse of an internal flue.

While several modeling efforts attempted to explain the 1858 results, the next significant development in the understanding of the observed phenomena occurred in 1906, when a pair of systematic experimental studies were published by Stewart and by Carmen and Carr.[22,23] A primary learning from these studies was that, for tubes longer than a critical length, an empirical relationship could be formulated between critical pressure and the ratio of pipe thickness to pipe radius cubed.[24] A more generalized form of the empirical relationship was presented in a 1941 article by Sturm, which continues to be provided in modern references:[25,26]

$$\Delta P_{cr,collapse} = KE\left(\frac{t}{d}\right)^3$$

Where *d* is the diameter the shell, *t* is the thickness, and *K* is a numerical coefficient whose form varies depending upon the type of loading, the type of supports, the length, radius, and outer-

---

20 Ventsel, E. and Krauthammer, T. *Thin Plates and Shells*. 2001. Chapter 19.

21 Fairbairn, W. On the Resistance of Tubes to Collapse. *Philosophical Transactions of the Royal Society of London*. Vol. 148. 1858. pp. 389-413.

22 Stewart, R.T. Collapsing Pressure of Bessemer Steel Lap-Welded Tubes, Three to Ten Inches in Diameter. *Transactions of the American Society of Mechanical Engineers*. Vol. 27. 1906. pp. 730-822.

23 Carmen, A.P. and Carr, M.L. Resistance of Tubes to Collapse. *University of Illinois Engineering Experiment Station.* Bulletin No. 5. June 1906.

24 Windenburg, D.F. and Trilling, C. Collapse by Instability of Thin Cylindrical Shells Under External Pressure. *Transactions of the American Society of Mechanical Engineers*. Vol. 56, No. 11. 1934.

25 Sturm, R.G. A Study of the Collapsing Pressure of Thin-Walled Cylinders. *University of Illinois Engineering Experiment Station*. Bulletin No. 329. Vol. 29, No. 12. 1941.

26 Avallone, E.A. and Theodore, T.B. *Marks' Standard Handbook for Mechanical Engineers*. 10th Edition. 1996. pp. 5-45 and 5-46.

shell diameter of the duct. The modulus of elasticity, E, may also be substituted for modified forms to capture non-linear or plastic action. For very long cylinders, the problem can be reduced to a stability analysis of a ring of unit length with the same radius and thickness as the cylinder. In this case, minimum value of critical pressure for collapse is given by:[27,28]

$$\Delta P_{cr,collapse} = \frac{E}{4(1-\nu^2)}\left(\frac{t^3}{r^3}\right)$$

where the additional parameter υ is Poisson's ratio for the material. This would represent a lower bound for the critical pressure for collapse of cylindrical shells, since shorter cylinders should be more stable. The critical length above which a cylinder can be considered "very long" varies by source, but one such example, attributed to Southwell, is:[29]

$$L_c = \left(\frac{16\sqrt{3}\pi}{27}\sqrt[4]{1-\nu^2}\right) r\sqrt{\frac{r}{t}}$$

For typical values of ν for steel and aluminum (0.25 and 0.33 respectively),[30,31] the coefficient is between 3.13 and 3.17. Thus, for a duct about 1 ft in diameter (300 mm) with a 0.02 inch (0.5 mm) wall thickness, the critical length is about 26 feet (8 m) for both steel and aluminum. Using the same parameters, and typical values of the modulus of elasticity for steel and aluminum (200 GPa and 69 GPa respectively), the above equation predicts a critical pressure for collapse of about 0.3 psig for steel and 0.1 psig for aluminum.[32,33] Note, these value assumes geometrically perfect cylinders, and imperfections present in real cylinders reduce the buckling capacity under uniform external pressure.[34] To account for the effects of real geometry, an empirical formula was developed for steel tubes by averaging the collapse pressure of "a great many commercial steel tubes taken at random from stock."[35,36] The result was an equation that reduced the predicted critical pressure by about 25% from the analytical result above.

Although, estimates are further complicated by the fact that these results represent collapse values for long, unstiffened cylinders, and in practice, ducts often have stiffeners, joints, or other

---

27 Windenburg, D.F. and Trilling, C. Collapse by Instability of Thin Cylindrical Shells Under External Pressure. *Transactions of the American Society of Mechanical Engineers*. Vol 56, No. 11. 1934.

28 Ventsel, E. and Krauthammer, T. *Thin Plates and Shells*. 2001. Equations 19.51-52.

29 Southwell, R.V. On the Collapse of Tubes by External Pressure. *Phil. Mag.*, I, May, 1913, pp. 687-698; II, Sept., 1913, pp. 502-511; III, Jan., 1915, pp. 67-77.

30 MatWeb Material Property Data for Steels, General Properties. Accessible at matweb.com.

31 Properties of Wrought Aluminum and Aluminum Alloys. ASM Handbook, Volume 2: Properties and Selection: Nonferrous Alloys and Special-Purpose Materials. 1990.

32 MatWeb Material Property Data for Steels, General Properties. Accessible at matweb.com.

33 Properties of Wrought Aluminum and Aluminum Alloys. ASM Handbook, Volume 2: Properties and Selection: Nonferrous Alloys and Special-Purpose Materials. 1990.

34 de Paor, et al. Prediction of vacuum-induced buckling pressures of thin-walled cylinders. *Thin-Walled Structures.* 55 (2012) 1-10.

35 Windenburg, D.F. and Trilling, C. Collapse by Instability of Thin Cylindrical Shells Under External Pressure. *Transactions of the American Society of Mechanical Engineers*. Vol 56, No. 11. 1934.

36 Carmen, A.P. and Carr, M.L. Resistance of Tubes to Collapse. *University of Illinois Engineering Experiment Station*. Bulletin No. 5. June 1906.

structural components that result in collapse pressures that are often significantly higher than the long cylinder limit. Cylindrical shells of subcritical length have been studied using structural stability theory, but the predicted critical pressure for collapse is strongly dependent upon geometry and boundary conditions.[37] As a result, the onset of failure of a specific duct is difficult to accurately predict without detailed measurements of the real duct geometry and the use of numerical methods. Nonetheless, a variety of equations have been developed from classical theory for use in different circumstances which perform relatively well against experimental results.[38,39]

3.3 Comparison of Rupture and Collapse Pressures

Fairbairn's 1858 study compared the expected rupture pressure of the external walls of a boiler to the collapse pressure of the internal flues, noting the ratio was between three and four. However, Fairbairn did not experimentally determine the rupture and collapse pressures of similarly constructed cylindrical shells, and no subsequent studies appear to have explored this comparison. To that end, rupture and collapse pressures for commercially available steel spiral pipe two different manufacturers was obtained and examined.[40] Data was available across a range of diameters and gauges (a measure of wall thickness). In total, burst and collapse pressures were available for 61 different products (combinations of diameter and gauge) from Manufacturer 1, and 47 different products from Manufacturer 2.

Figure 6 shows the ratio of rupture pressure to collapse pressure plotted against the ratio of the radius of the duct to the wall thickness (r/t), as reported by their manufacturers Manufacturer 1 (top) and Manufacturer 2 (bottom), on the same scale for comparison. Note, as the gauge number increases, the thickness decreases. Also, the ratio r/t was much less than unity in this data set, so the x-axis was scaled by a factor of 10^3.

---

37 de Paor, et al. Prediction of vacuum-induced buckling pressures of thin-walled cylinders. *Thin-Walled Structures.* 55 (2012) 1-10.

38 de Paor, et al. Prediction of vacuum-induced buckling pressures of thin-walled cylinders. *Thin-Walled Structures.* 55 (2012) 1-10.

39 Windenburg, D.F. and Trilling, C. Collapse by Instability of Thin Cylindrical Shells Under External Pressure. Transactions of the American Society of Mechanical Engineers. Vol 56, No. 11. 1934.

40 Sheet Metal Connectors, Inc. and Spiral Manufacturing Co., Inc.

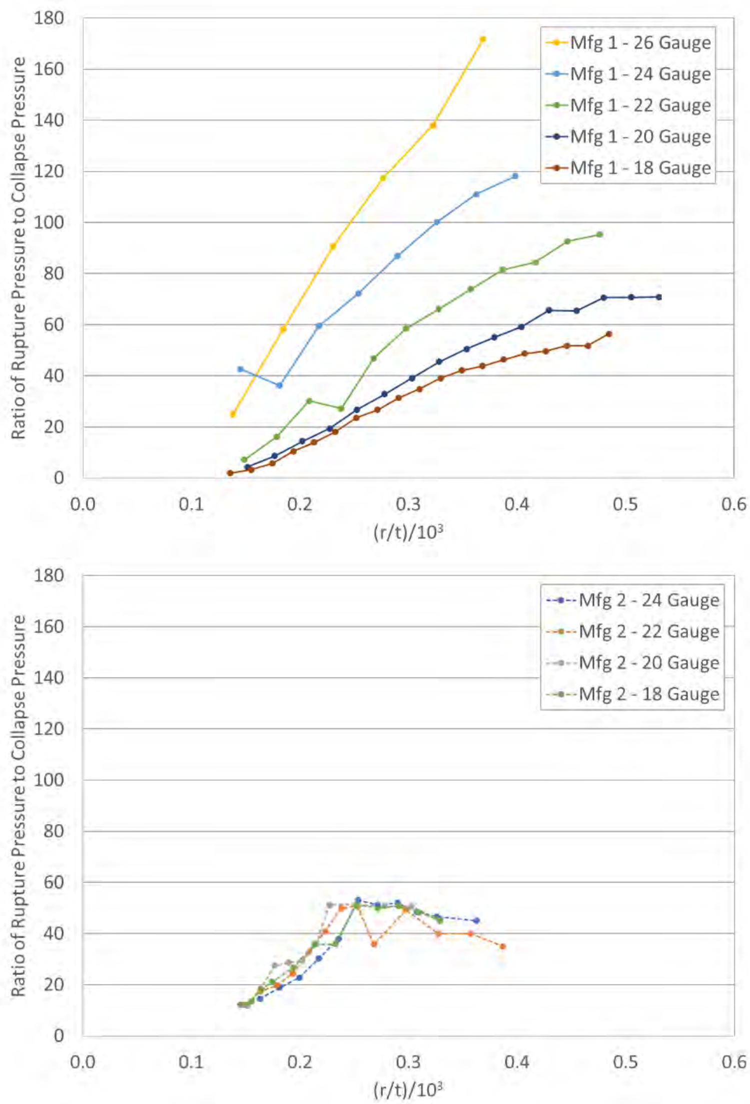


Figure 6. Plot showing the ratio of the burst and collapse pressures versus ratio of the radius and wall thickness (r/t) for spiral ducts of varying manufacturer and gauge.

In both cases, the ratio of rupture pressure to collapse pressure initially increases as the ratio of the radius to the thickness increases. For Manufacturer 1, the trend is approximately linear, but there is a different slope for each gauge (although 18 gauge and 20 gauge were similar in slope). For Manufacturer 2, the curves are much more nonlinear, but the scaled behavior is much more quantitatively similar, regardless of gauge. The ratio of pressures also initially increases, but the increase is less linear and relatively insensitive to gauge (beyond the dependence embedded in the x-axis scaling). Once r/t exceeds around 0.2, ratio becomes relatively constant at values between 35 and 55. Clearly, there is a significant potential for variability in rupture and collapse performance between manufacturers, and between different combinations of diameter and thickness. The ratio of rupture pressure to collapse pressure was close to 1 for the thickest, smallest radius duct from Manufacturer 1 (1.8 for a 14-inch diameter, 18 gauge duct), but it was two orders of magnitude greater for the thinnest, smallest radius duct from the same manufacturer (up to 172 for a 16-inch diameter, 26 gauge duct). On the contrary, it was a relatively tight range of ratios, between 12 and 53 for the entire data set of 47 products offered by Manufacturer 2.

The relationship between the rupture pressure and the collapse pressure for a duct can vary widely, and the collapse pressure is sensitive to a broad set of factors. As is evident, there can be significant variability in performance of ductwork, especially when comparing ducts manufactured by one company versus another. Thus, when critical pressure for collapse is relevant, either from a design or a forensic perspective, it may be prudent to inquire with the manufacturer.

4 Case Studies

The authors of the current study have observed the phenomenon of duct collapse most frequently after combustible dust deflagrations. These observations can result in confusion and misunderstanding, as the common expectation after an explosion is to see signs of internal overpressure. The possibility of developing an internal vacuum is less well-known. Some representative examples are discussed below.

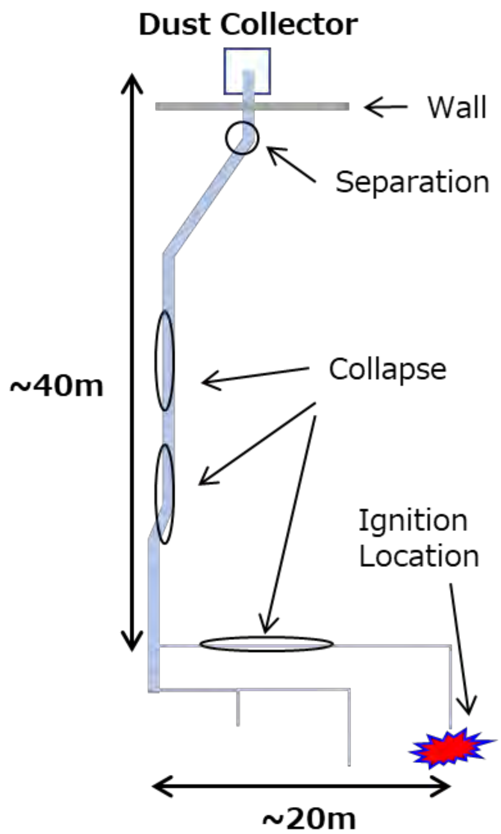


Figure 7. Approximate sketch of the dust collector system pictured in the previous figure. Ignition occurred at one of three process locations served by the dust collection system. The dust collector was protected by explosion panels, which functioned during the event.

The first case study examines an explosion that occurred at a facility that processed polymeric material. A process upset occurred that resulted in a partial shutdown of an extruder. The partial shutdown included shutting down a nitrogen purge line, but the extruder screws remained operational. As a result, material in the extruder was heated to autoignition, and a resulting deflagration spread into the dust collector system. Dust sediment present in the ducts became involved in the deflagration, which ultimately propagated to the dust collector and was vented through explosion panels. The layout of the dust collection system relative to the ignition location and the dust collector is shown in Figure 7. The damage was limited to the extruder equipment and the dust collection system. Three separate portions of duct collapsed (buckled) as a result of the incident, and duct separated at a 45-degree elbow immediately prior to exiting the building. Photos of the collapsed duct are shown in Figure 8.

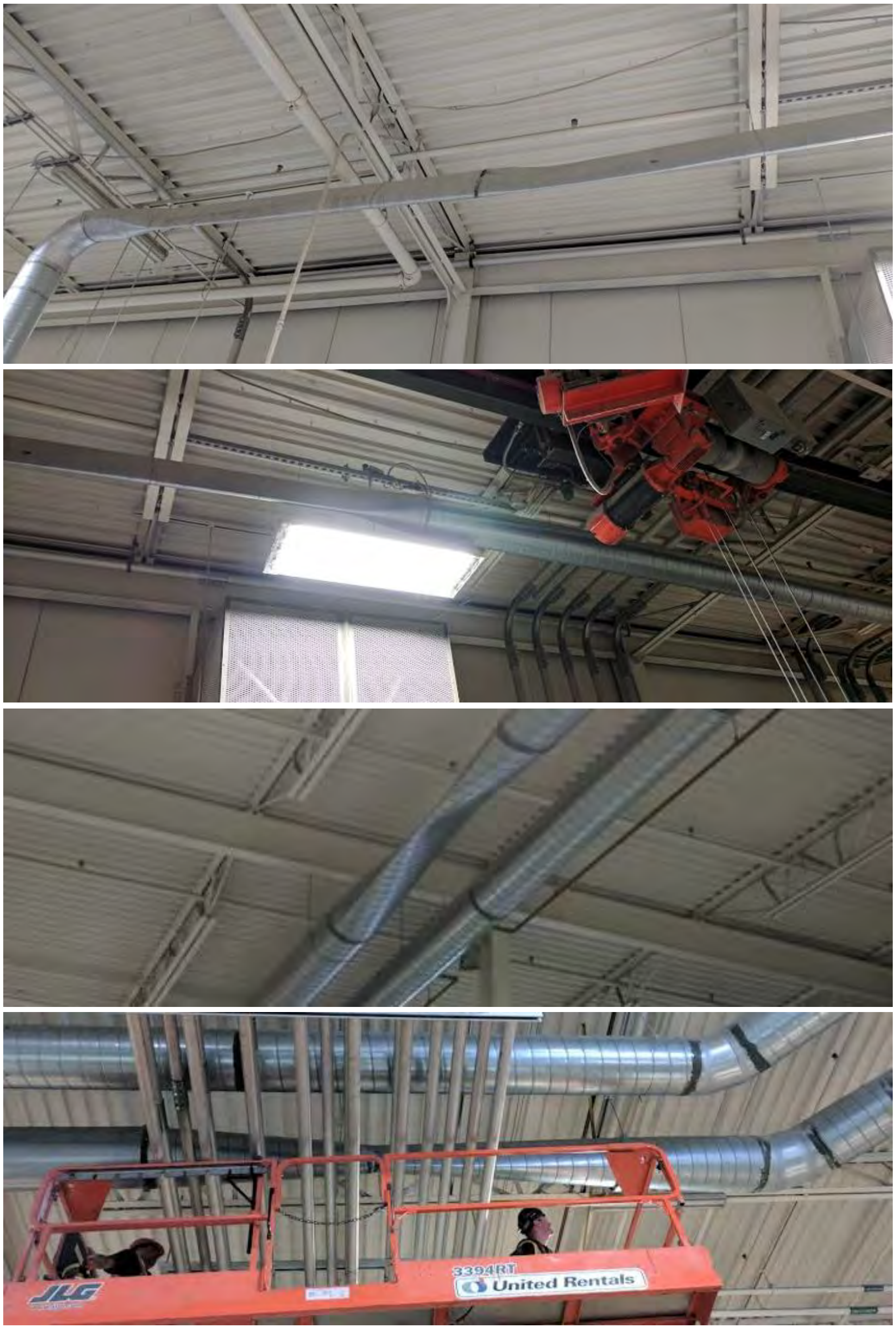


Figure 8. Three different collapse locations after a dust deflagration. The top two images capture the extents of a very long, continuous collapse of a 10-inch spiral duct. The bottom image two images are from different portions of the dust collection system, closer to the dust collector, where the diameter was 18 inches. The duct also separated at a 45-degree elbow immediately prior to exiting the building. The relative location of the collapses

Another case study prominently featuring collapsed duct involved a dust explosion at a grain elevator. Material that had self-heated to the point it began to smolder was being removed when an explosion involving carbon monoxide and smoke occurred. This explosion propagated to an elevator leg and then into the dust collection system, which included ducts that ran along the exterior of the structure to an external dust collector. Portions of this exterior duct collapsed as a result, as shown in Figure 9.

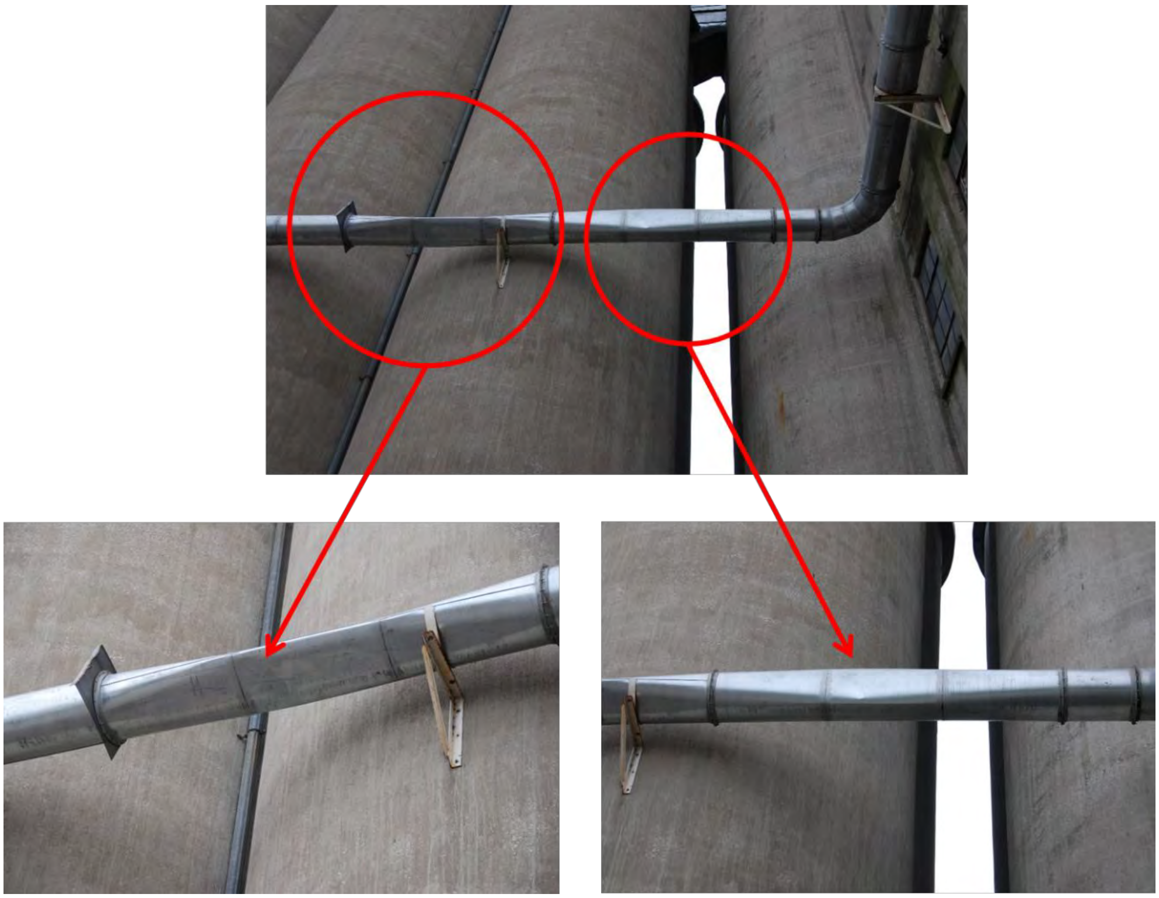


Figure 9. Duct leading to an exterior dust collector from a series of drag conveyors and bucket elevators. Two connected ducts collapsed, but the buckling was mediated by the flange connecting the two ducts.

A third case study involved a dust deflagration that initiated in a process vessel. While there was no indication that the deflagration wave propagated into the dust collection system, a pressure pulse did travel through the ductwork, which was followed by a compression wave. As a result, the large duct shown in Figure 10 collapsed. While the exact dimension is unknown, a relative scale can be deduced from the person seen in the lower left corner.

Figure 10. A duct (featured from two angles) that collapsed.

Finally, a fourth case study involved another grain elevator explosion. In this case, the origin and cause of the explosion was not identified, but the explosion propagated throughout much of the facility, including through the four elevator legs in the center of the concrete structure. As a result, several rectangular ducts associated with an elevator leg collapsed, shown in Figure 11.

A common thread amongst the four case studies was that a positive pressure wave propagated through each of the ducts prior to their collapse. This fact puzzled stakeholders in each case. If an explosion occurred, and a pressure wave propagated inside the duct, why did it collapse and not rupture? A likely explanation is the partial vacuum created when the subsequent expansion wave passed through the same conduit. Evidently, the ducts were capable of handling the overpressure without rupture, but they could not withstand the vacuum, and collapsed.

Figure 11. Collapsed rectangular duct. Note that the shorter section in the top photograph did not collapse, whereas longer sections did.

5 Conclusions

The propagation of a dust deflagration in interconnected process vessels can result in a broad diversity of damage patterns. While damage patterns consistent with positive overpressure are to be expected, the ductwork that connects these vessels will often exhibit signs of collapse. As demonstrated in this paper, the collapsed state can occur due to one of two causes: an externally applied overpressure (external pressure greater than internal pressure) or the formation of a partial vacuum due to the propagation of expansion waves inside the duct. In the authors' experience the expansion wave mechanism is the more common explanation. The utility of these observations is the contribution towards better understanding of the dynamic events associated with a dust deflagration.

6 References

Footnotes will be converted to reference citations.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

The Nature of Flammable Cloud Volumes in Semi-confined Environment under the Influence of Flow of Air

Karen Silgado Correa, Tatiele Dalfior Ferreira, Sávio Vianna*
University of Campinas
Albert Einstein 500. Campinas. SP – Brazil
*Presenter E-mail: svianna@unicamp.br

Abstract

In the Explosion Risk Analysis (ERA), ventilation and dispersion calculations using Computational Fluid Dynamics (CFD) are usually considered when the level of confinement and congestion cannot be neglected. As far as the dispersion analysis is considered, alternative approaches are sought when a large number of simulations are required. Setting many scenarios and simulate them all is not always suitable within the timeframe of real engineering design. As a result, semi-empirical dispersion models and several procedures based on statistical approaches using CFD have been proposed to improve the robustness and the accuracy of prediction of the flammable gas cloud volume. In addition, notwithstanding the use of Response Surface Method (RSM) and Frozen Cloud Approach (FCA), it is convenient to address the problem on the basis of the physics underlying the dispersion of a scalar in the chemical process area. Following this line of reasoning, we propose a new dimensionless number balancing the transport of the flammable cloud and the accidental leak rate. Numerical experiments have shown that the dimensionless number is related to the angle of the wind direction as the angles in a circle are related to the phase angle in a sine wave, $V \sim \sin\left(k\frac{\phi}{\pi} + \beta\right)$, where $\hat{V}$ is the nondimensional flammable cloud volume and ϕ the phase angle. The numerical findings suggest a periodic function comprising harmonically sinusoids in the same fashion put forward by Fourier and observed in the analytical solutions of diffusive transport equations.

Keywords: dispersion modelling, CFD, dimensionless cloud volume.

1 Introduction

The estimation of flammable cloud volumes has been widely investigated in recent years in order to minimize the risk of accidental releases into the atmosphere. When a release is given, the jet flow acquires a high momentum which afterwards is diluted and dispersed by the influence of the atmospheric turbulence. The behaviour of this cloud is a complex phenomenon to analyse due to the different parameters involved in the flow dynamics. These parameters are the leak rate, the wind speed, the leak direction, release duration and other actions of mitigation [1, 2, 3, 4]. In the evaluation of the incidence of these affecting factors in the cloud behaviour have been done by numerous methodologies. These methods may be based on experimentation or by statistical concepts [1, 5], neural networks [4], numerical modelling by using Computational Fluid Dynamics (CFD) [3, 6], dense gas modelling [7], among others. However, the estimation of the physical understanding of the phenomena is still places a large burden on the researchers. Due to the complexity of the dispersion phenomena, this work makes use of dimensional analysis to identify the relationship of the affecting parameters with the flammable gas cloud volume. This dimensional analysis will be further used to develop a mathematical model by understanding the physical behaviour of the cloud after a release in the atmosphere.

This study is the result of an extensive evaluation of numerous cases, and the aim is to analyse the accuracy of the equations proposed to estimate flammable cloud volumes, that is, the dimensional volume and the mathematical model.

2 Methodology

The dispersion analysis was carried out in a semi-confined geometry designed in CFD-FLACS to calculate the equivalent stoichiometric gas cloud (Q9) at different case scenarios. The scenarios were set within four sets considering four main affecting parameters (leak rate, leak direction, wind speed, and wind direction). Each set comprised the variation of at least one of these parameters. To initiate the dispersion evaluation, it was assumed a single case (up-leak jet direction with a leak rate of 50 kg/s and a 6 m/s of wind speed varying the wind direction), afterwards, subsequent cases were performed to determine potential case scenarios after parameters were varied. The dispersion evaluation led to obtain the Q9 values for all the simulated cases, in which were only considered the largest cloud volumes for each group of scenarios. In total, 27 groups of scenarios and 17 different grids were performed within the four sets stablished in the entire analysis.

As the objective is to obtain a novel alternative in predicting the flammable cloud volume after accidental discharges, we sought to couple the affecting parameters with the Q9 outcome through dimensional analysis. The evaluation of this relationship generated a dimensionless volume that explains physically the dispersion phenomena. This dimensionless number $\hat{V}$, obtained by employing the Buckingham Pi theorem, evaluates the gas convective flow with the release momentum over time. The development of a dimensionless $\hat{V}$ allows to evaluate the parameters of leak rate, wind speed, density and the Q9 together. After Q9 results, $\hat{V}$ was calculated to have a physical understanding of the dispersion phenomena and being able to model it. With respect to the geometry, the wind rose was established as is shown in Figure 1.

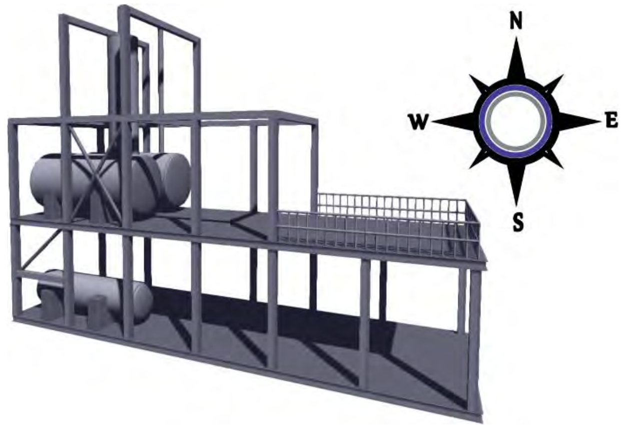


Figure 1. Geometry model and wind direction configuration

3 Results

The analysis led to observe that the flammable cloud volume (V_f) depends on different parameters. These parameters are related to the leak rate ($\dot{q}$), wind speed (u), fluid properties (ρ), leak direction (θ), geometry (L) and the wind direction (β). Considering this study, we obtain a non-dimensional number $\hat{V}$ that describe the dispersion phenomena given by:

$$\hat{V} = \frac{u^{3/2}\rho^{3/2}V_f}{\dot{q}^{3/2}} \tag{1}$$

Calculations showed that $\hat{V}$ ranged from 0.16 to 62.3 for cases simulated from 0.5 kg/s to 550 kg/s of leak rate, 1 m/s to 12 m/s of wind speed, with all wind directions (N, E, S, NE, NW, SE, SW, W), and for all leak jet directions (up, down, back, left, right, front).

In the evaluation of the cloud behaviour after accidental releases, we only considered the largest values of the flammable cloud volumes (Q9) for each group of dispersion scenarios. To develop a mathematical model, we analyse a specific group of simulated cases. This group was set with two parameters fixed (wind speed and leak rate) varying the wind direction for each leak jet direction. Based on the dimensional analysis, the proposed a model represented by the Equation 2, contains two functions, the cosine representing the sinusoidal behaviour and an exponential to the wake conditions. The model is also a function of two main angles, one referred to the wake angle (α) and the other to the wind direction (β). Both involving the influence of the wake volume (V_w), the mean (ϵ), amplitude (δ), and variables (A, B).

$$\hat{V}(\alpha, \beta) = \epsilon + \delta\cos(A\beta) + V_w \exp[-B\,(\beta - \alpha)^2] \tag{2}$$

After calculating $\hat{V}$, the sinusoidal form is seen in Figure 2 where group 8B and 8C (Table 1) are plotted. As we noticed, the curve tended to follow a periodical waveform, and then a slightly exponential behaviour is perceived as the wind direction varies.

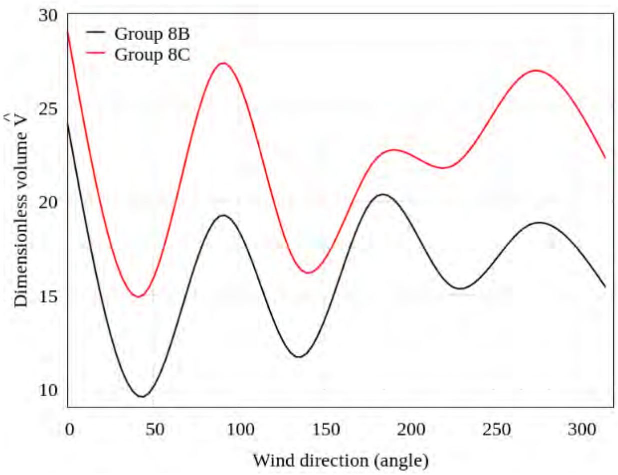


Figure 2. Representation of the waveform of the cloud volume based on the dimensional analysis for groups 8B and 8C.

In the non-dimensional flammable volume ($\hat{V}$) results, it was also identified some variations in wake angle in particular scenarios and conditions simulated. We found that in various cases, there were different values of wake angle representing the largest flammable cloud volume. Therefore, in order to see how this behaviour can affect the estimation of flammable cloud volumes, two different evaluations by using the proposed model were performed.

One first evaluation implied to plot four random cases (Table 1) at up leak direction divided into 12 groups and assuming that all the groups had the same wake angle (west wind direction or 270 degrees). The west wind direction according to the geometry (Figure 1) would be equivalent to the most likely to produce the largest cloud volume due to the re-circulation zone generated in the module when the flow encounters the objects (vessels). Based on this consideration, the CFD results are compared with the model (Figure 3) to see the agreement between the data.

Table 1. Group of scenarios used in the evaluation of the proposed model

Group	Parameters fixed*	Parameter varied
4A 4B 4C	5 kg/s leak rate	Wind direction
5A 5B 5C	25 kg/s leak rate	
7A 7B 7C	50 kg/s leak rate	
8A 8B 8C	100 kg/s leak rate	

* Each parameter fixed was measured at 2 m/s, 6 m/s, and 8 m/s of wind speed and up leak direction

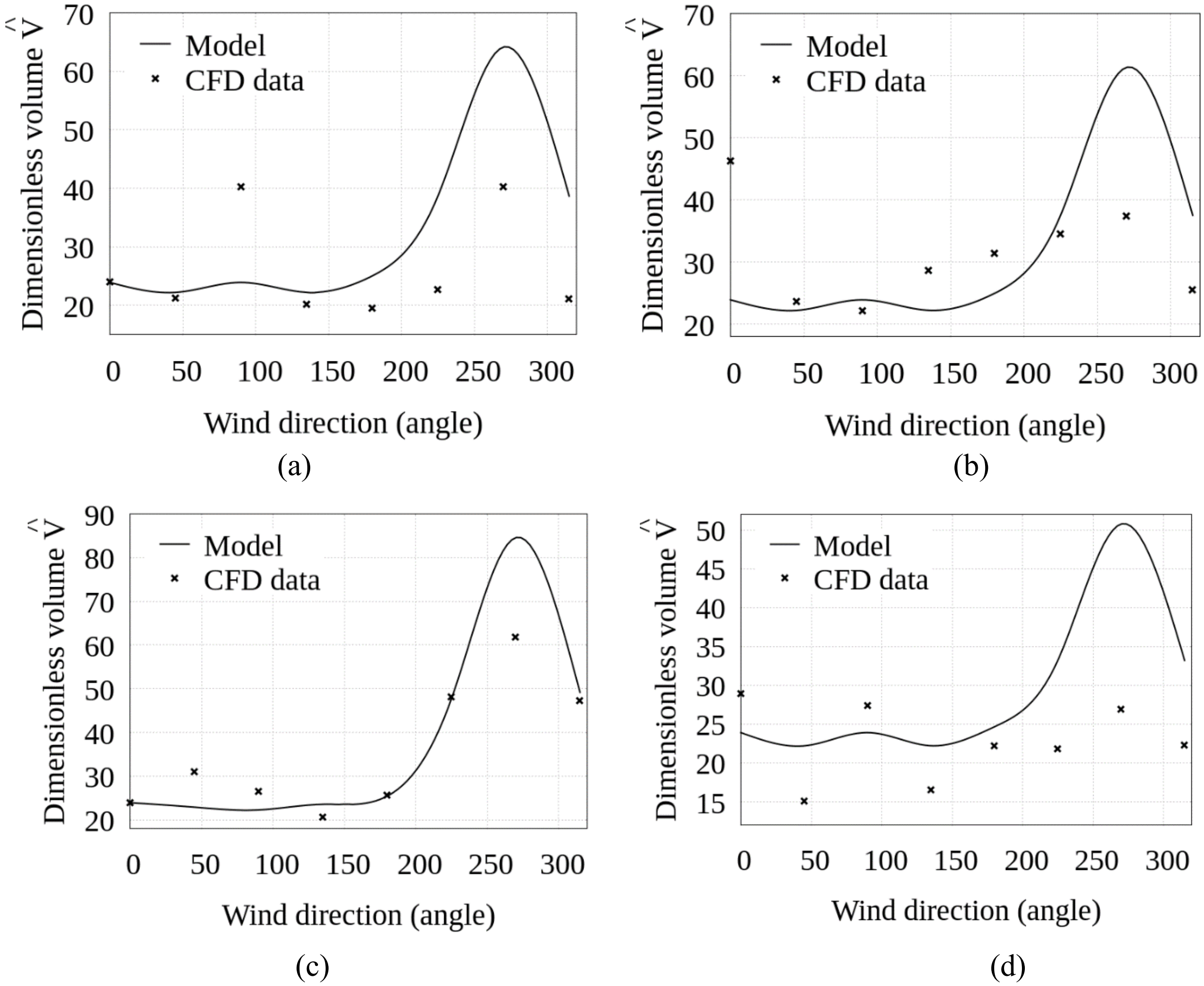


Figure 3. Comparison between the model and CFD data: (a) 5 kg/s at 8 m/s, (b) 25 kg/s at 8 m/s, (c) 50 kg/s at 6 m/s, and (d) 100 kg/s at 8 m/s.

Initially, Figure 3 shows four random groups from Table 1 considering the same wake angle (West). It is observed the model agreement after comparing it with CFD data for each wind direction. In this figure, the CFD data were the values obtained by using the Equation 1. It is also seen that the model begins estimating the sinusoidal behaviour, and then employs the exponential function to model the largest volume, which corresponds to the wake volume in the module at certain conditions.

Now, for all the cases in Table 1, Figure 4 represents the four leak rates (5 kg/s, 25 kg/s, 50 kg/s and 100 kg/s), with the same assumption of having the same wake angle. It is observed that for wind speed from 6 m/s to 8 m/s, the model presents a good agreement (Figure 4). However, even the scatter shows that the wind speed at 2 m/s is uncovered, the model can overpredict it. As in the entire dispersion analysis was identified that the highest Q9 changes were at leak rates going from 25 kg/s to 200 kg/s and wind speed from 2 m/s to 8 m/s, it is seen that the model may offer a good accuracy in the estimation of the cloud in these likely ranges.

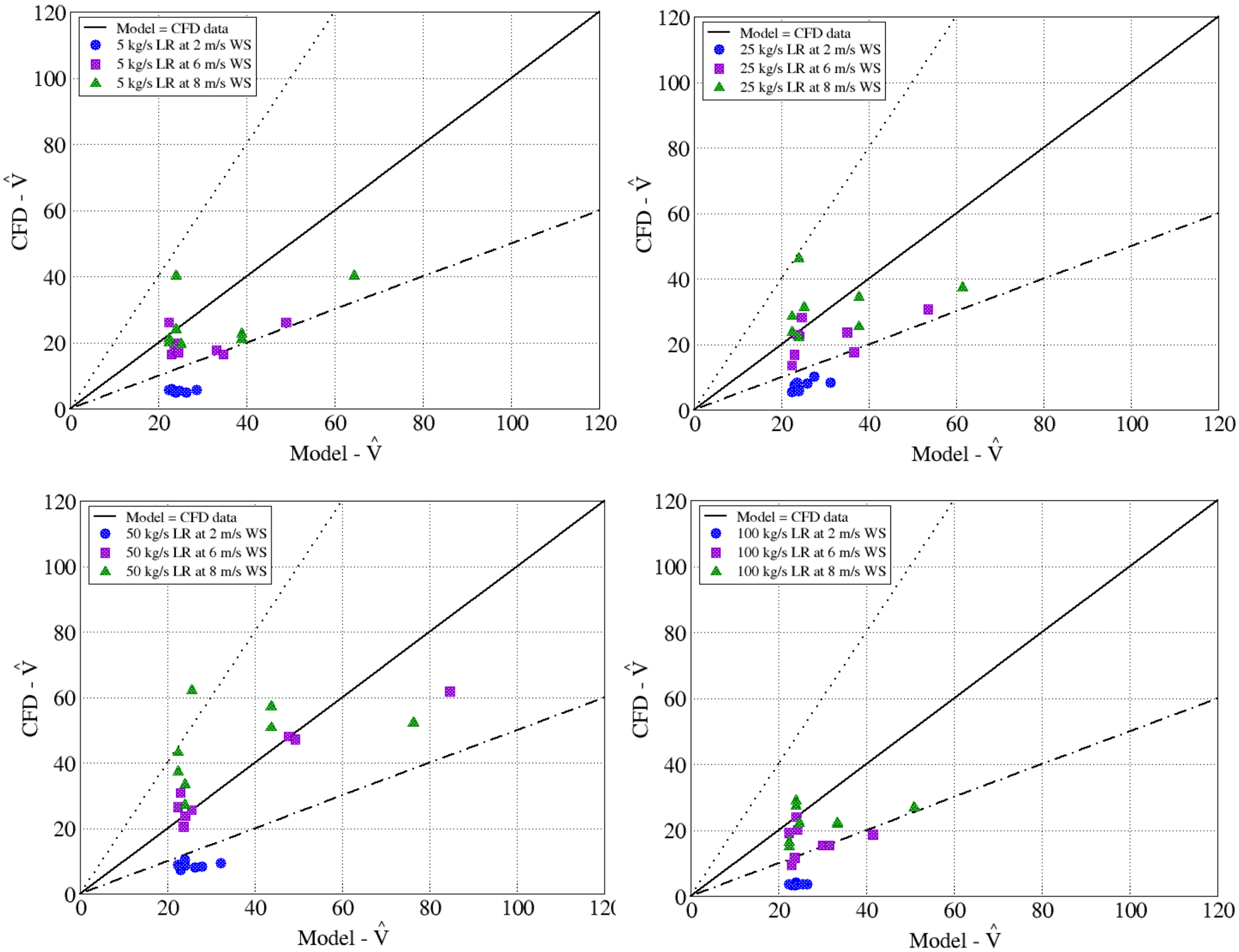


Figure 4. Comparison between CFD data, and the model at different values of leak rate (LR) and wind speed (WS).

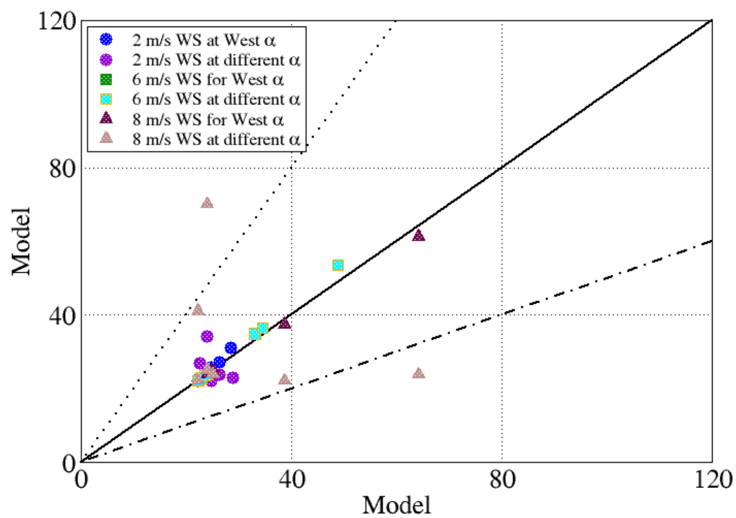


Figure 5. Comparison between data obtained by the proposed model at West wake angle with the data considering different wake angles (α).

The second evaluation comprised different values of wake angles as it was obtained during the analysis for each scenario. The variations of wake angle might be possible due to the geometry configuration and the association between variations of wind direction and leak direction. The representation of data obtained at different wake angles with the assumption of same wake angle is shown in Figure 5. From this figure, we can conclude that the discrepancies in evaluating the wake conditions aforementioned for all the cases are negligible. It suggests that the proposed model seems to be a good alternative in the estimation of flammable gas cloud volumes for both cases (different wake angles and same wake angle) without affecting the accuracy.

4 Conclusion and Future work

The current work evaluates the development of a dispersion model on the basis on the physics that may be used to estimate the flammable cloud volume after accidental releases. During the analysis, it was addressed two different evaluations to observe the reliability of the proposed model. It was determined that the proposed model seems to be accurate no matter the determination of fixed or a variable wake angle because the differences between the data calculated by the model at both conditions are minimal.

The dispersion analysis indicated that the flammable cloud volume follows a wavy pattern when it is related to the angle of the wind direction. The analysis also resulted in a dimensionless number that relates the leak rate, density and the wind speed with the flammable cloud volume leading to the development of a mathematical model that associate it with the wind direction. As future work, we will keep evaluating and improving the mathematical model to obtain better agreement for lower values of wind speeds.

5 References

1. Shi, J., Li, J., Zhu, Y., Hao, H., Chen, G., Xie, B. (2018). A simplified statistic-based procedure for gas dispersion prediction of fixed offshore platform. Process Safety and Environmental Protection. 114, 48–63.
2. Azzi, C., Rogstadkjernet, L., Wingerden, K., Choi, J., Ryu, Y. (2016). Influence of scenario choices when performing CFD simulations for explosion risk analyses: Focus on dispersion. Journal of loss prevention in the process industries. 41, 87-96.
3. Qiao, A., Zhang, S. (2010). Advanced CFD modeling on vapor dispersion and vapor cloud explosion. Journal of loss prevention in the process industries. 23, 843-848.
4. Shi, J., Li, J., Khan, F., Zhu, Y., Li, J., Chen, G. (2018). Robust data-driven model to study dispersion of vapor cloud in offshore facility. Ocean Engineering. 161, 98-110.
5. Ferreira, T.D and Vianna, S.S.V. (2014). A Novel Coupled Response Surface for Flammable Gas Cloud Volume Prediction. International Journal of Modeling and Simulation for the Petroleum Industry. 8, 8-16.
6. Dasgotra, A., Teja, G.V.V., Sharma, A., Mishra, K. (2018). CFD modeling of large-scale flammable cloud dispersion using FLACS. Journal of Loss Prevention in the Process Industries. 56, 531-536.
7. Spicer, T.O., Havens, J. (1996). Application of dispersion models to flammable cloud analyses. Journal of Hazardous Materials, 49, 115 – 124.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Image processing techniques for the characterization of explosively driven dispersions

J.M. Buchlin[a], S. Courtiaud[b], Charline Fouchier[a,*], D. Laboureur[a], E. Lapébie[b]
[a]Institut von Karman, 72 chaussée de Waterloo, 1640 Rhode Saint Génèse, Belgium
[b]CEA, DAM, GRAMAT, F-46500, Gramat, France
*Presenter E-mail: charline.fouchier@vki.ac.be

Abstract

Dispersions driven by explosions are challenging to characterize mainly due to the extreme test conditions, the different time and spatial scales of the flow, and the variation of intensity due to the combustion.

An intensity based optical method to characterize the dispersion driven by an explosion is proposed. The velocity and intensity maps of the dispersion are accessed through the post-processing of the images of the dispersion. These images can be obtained either from a global visualization (using a light source, such as in the image given in Figure 1, or the combustion light itself) or from a transversal visualization (using a laser sheet illuminating inside the cloud, such as in the image given in Figure 2).

The developed method is organized into three steps. First, the contour of the cloud is detected via a dynamic grey-scale threshold criterion. The dispersion contours allow the computation of the velocity of the expansion as long as the plume presents a regular edge. Then, Large-Scale Particle Image Velocimetry technique is applied to obtain the velocity map of the dispersion. Additionally, information about the combustion phenomenon can also be accessed via an intensity-based analysis.

The method has been initially verified using a numerical test case. It has been thereafter applied on different experimental measurements presenting challenging features such as variations of light intensity, time scales, and spatial scales.

Figure 1: Talc dispersion illuminated by a powerful light source.

Figure 2: Talc dispersion illuminated by a laser sheet coming from the left.

Keywords: Explosion, Two-phase flow, Dispersion Influential Factors

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Storage vessels in the proximity of wild fires

V. Casson Moreno[1], V. Cozzani[1] M. Papadaki[2]*, G.E. Scarponi
[1]Laboratory of Industrial Safety and Environmental Sustainability - DICAM
University of Bologna, via Terracini 28, 40131 Bologna, Italy
[2] Environmental Engineering Department, University of Patras, Seferi 2, Agrinio, GR30100,
*Presenter E-mail: marpapadaki@upatras.gr

Abstract

In the last decade, the occurrence of uncontrolled wildfires all over the planet became more frequent. Those fires have at least provoked serious human disasters. (Kumagai, *et al*., 2004). The climate change accompanied by a number of other identified or unknown factors may be the cause. As with earthquakes, storms, floods, the severity of potential wild fires reaching an industrial site have to be included in chemical plant's safety assessment and management. However challenges arise as the magnitude and frequency of them are difficult to predict but also their impact on process units is difficult to assess mostly due to lack of data and our epistemic uncertainty of process units failure modes (Reniers, et al. 2018). In this study, the predicted effects of wild-fires on storage tanks are assessed and preventive measures are proposed.

Employing a hypothetical fuel storage plant Khakzad, 2015 has presented a methodology based on dynamic Bayesian networks to model the spatial and temporal evolution of domino effects. Here, domino effects related to wildfires on large storage vessels under different conditions are considered and hazardous scenarios, their propagation and measures for their prevention or mitigation are also discussed.

Keywords: flammable inventory, toxic compounds, storage vessel heat-resistance, domino-effects

References

N. Khakzad (2015), Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures, *Reliability Engineering and System Safety* **138**, 263–272.

Y. Kumagai, M. S. Carroll, and P. Cohn, (2004) Coping with Interface Wildfire as a Human Event: Lessons from the Disaster/Hazards Literature, *Journal of Forestry*, **September,** 28-32.

G. Reniers, N. Khakzad, V. Cozzani and F. Khan (2018). The impact of nature on chemical industrial facilities: Dealing with challenges for creating resilient chemical industrial parks a Faculty, *Journal of Loss Prevention in the Process Industries*, **56**, 378–385.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

SafeOCS Industry Safety Data: The Value Proposition for the Oil & Gas Industry

Demetra V. Collia and Roland L. Moreau* (contractor)
U.S. Department of Transportation, Bureau of Transportation Statistics
Washington, D.C. 20590
*Presenter's E-mails: rlm13@comcast.net, demetra.collia@dot.gov

Abstract

This paper summarizes efforts by the U.S. Department of Transportation, Bureau of Transportation Statistics (BTS) to develop and manage an industry-wide safety data framework under an agreement with the U.S. Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE). The Industry Safety Data (ISD) program provides a trusted, proactive means for the oil and gas industry to voluntarily and securely report safety information to identify early warnings of safety problems by uncovering hidden at-risk conditions not previously exposed from analysis of reportable accidents and incidents. Besides agency-reportable incidents, this program captures near miss and other significant safety event information that is maintained by individual companies as part of their internal safety programs. Phase I of this program was completed in June 2019, and plans are progressing to expand industry participation.

Companies have long realized the benefits of collecting and analyzing data around safety and environmental incidents to identify risk, then develop systems and processes to prevent recurrence. These activities have been supported and supplemented by industry associations that collect and share event information and develop recommended practices to aid in performance improvement. In high-reliability industries, such as aviation and nuclear, it is common practice to report and share events among companies and regulators to identify hidden trends and create or update existing recommended practices or regulations.

The challenge for the oil and gas industry operating within the U.S. Gulf of Mexico Outer Continental Shelf (OCS) was that, while industry associations and the regulator were collecting data on significant incidents, lesser safety events or observed unsafe conditions/behaviors are not required to be reported and therefore may go unnoticed as a trend until a major event occurs. This represented an opportunity for industry, BSEE, and BTS to collaborate on a means of gathering incident data that would allow for analysis and identification of trends or events of significance enabling appropriate interventions to prevent major incidents. The value proposition of this effort is development of a comprehensive safety data repository that facilitates the continual

improvement in safety and environmental performance from the implementation of learnings shared from trends or lesser incidents and events occurring within industry.

Keywords: Incident Investigation; Metrics; Near Miss Reporting; Lessons Learned; Data Collection and Sorting; Incident Recording, Reporting, and Analysis; Incident Classification

1 Introduction

In the aftermath of the Deepwater Horizon oil spill, the oil and gas industry, regulators, and other stakeholders recognized the need for increased collaboration and data sharing to augment their ability to identify safety risks and address them before an accident occurs. The SafeOCS Program is one such collaboration between industry and government. It is a voluntary confidential reporting program that collects and analyzes data to advance safety in oil and gas operations on the Outer Continental Shelf (OCS). BSEE established the program with input from industry, and then entered into an agreement with BTS to develop, implement, and operate the program.

As a statistical agency, BTS has considerable data collection and analysis expertise and the statutory authority to protect the confidentiality of the reported information and the reporters. BTS has also developed and operated confidential near miss reporting systems for the railroad and metro transit industries and has a detailed working knowledge of data management systems utilized by other industry sectors. Although the SafeOCS program is supported by BSEE and maintained by BTS, input from industry has been instrumental and this safety data framework is intended to benefit *all* stakeholders.

These companies volunteered their staff time and resources over the course of almost two years to assist BTS in the ground work required to design the SafeOCS ISD database. An important outcome of these efforts was identification of the core data fields that became part of the initial SafeOCS ISD program. The latter involved a detailed discussion of each proposed data field to ensure that the information captured would enable industry to have meaningful discussions of the results and prospective mitigative measures that could be taken to enhance safety in the field.

1.1 Solving for the Gap

Across industries, companies have long realized the benefits of collecting and analyzing data around safety and environmental events to identify risks and take actions to prevent reoccurrence. These activities have been aided by industry associations that collect and share event information and develop recommended practices to improve performance. In high-reliability industries such as aviation and nuclear, it is common practice to report and share events between companies and for the regulators to identify hidden trends and create or update existing recommended practices, regulations, or other controls.

The challenge for the offshore oil and gas industry was that industry associations and the regulator were collecting data on agency-reportable incidents, but other high-learning value events or observed conditions/behaviors could go unnoticed as a trend until a major event occurred. This represented an opportunity for the industry and the offshore regulator (BSEE) to collaborate on a means of gathering safety event data that would allow for analysis and identification of trends, thereby enabling appropriate interventions to prevent major incidents and foster continuous improvement.

Supplementing existing systems and processes for reporting events would allow all stakeholders the ability to gain insight from a broader range of safety events. Key aspects of SafeOCS ISD include:

- Providing a central repository for safety-related data collection, analysis, and sharing of learnings;
- Identifying the type of data that will provide valuable information;
- Gaining alignment on event data definitions and associated metadata;
- Utilizing a secure process for collection of data where adverse legal actions cannot be taken against data submitters nor can raw data be used for regulatory development purposes;
- Implementing a robust methodology for identifying systemic issues;
- Disseminating the findings to stakeholders who can then take actions to reduce or eliminate process and personal safety risks; and
- Providing opportunities for participating companies to compare internal data with aggregated results.

> "The opportunity for the next step change in safety performance appears to be in a substantial increase in the sharing of data across industry. Leading practices in other industries (i.e. transportation) may be adopted in the oil and gas industry to similar effect…"
>
> International Regulator's Forum on Global Offshore Safety, June 2018

The concept of sharing lessons learned from safety events aligns with BSEE's Safety Culture Policy Statement[1] wherein BSEE encourages companies to seek out and implement "continuous improvement opportunities to learn about ways to ensure safety and environmental stewardship." Other elements of BSEE's safety culture policy that directly support the SafeOCS ISD Program include:

- Focusing on hazard identification and risk management to flag issues potentially impacting safety;
- Encouraging inquiring attitudes by continuously considering and reviewing existing conditions and activities to identify discrepancies that might result in inappropriate action; and
- Maintaining an open and effective safety communication environment.

1.2 The Importance of Capturing and Sharing Safety Event Data

Major incidents, although rare, serve to underscore the need for collecting information on precursor events that can anticipate the potential for a major incident. It is important to understand precursor events (including near-misses), barrier integrity as it relates to incident prevention and mitigation, and high-value learning events. Barriers are systems, processes, or engineering

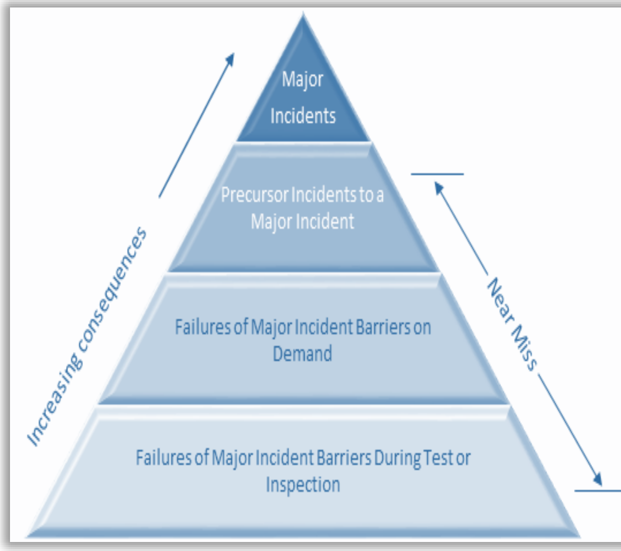
[1] BSEE Final Safety Culture Policy Statement, May 2013.

solutions that are designed to prevent incidents from occurring.

The scope of the data with potential learning opportunities ranges from major incidents that result in personnel injuries or fatalities to near-miss events and significant observations of unsafe conditions and/or actions, as depicted in the safety triangle in Figure 1. Various studies have corroborated a many to one relationship between lesser and more significant incidents.

It is critical to understand the types of events, conditions, or behaviors that are noted prior to a more significant event occurring and work to strengthen the controls that are intended to reduce or eliminate the chance of an incident.

Figure 1: Safety Triangle



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Therefore, the objective of the SafeOCS ISD Program is to capture this data so they can be analyzed for trends and learnings can be implemented with the goal of preventing more serious events. This approach allows all companies working on the OCS to prioritize resources to ensure that they have controls in place to minimize the risk of a significant event.

1.3 Data Protection and Confidentiality

SafeOCS operates under a Federal law, the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), which requires that the program protect any identifying, sensitive or proprietary information it collects and prohibits its release to unauthorized persons or organizations. Information submitted under CIPSEA can be used only for statistical purposes.

1.3.1 CIPSEA Protections

- No government agency may require, for any reason, a copy of a respondent's report
- Courts cannot require a copy of any respondent's report
- Reports are immune from the legal process and cannot be admitted as evidence
- Reports are **exempt** from Freedom of Information Act (FOIA) requests
- Information may not be disclosed in identifiable form for any non-statistical purpose without the informed consent of a respondent

CIPSEA protected data cannot be used for enforcement or regulatory purposes.

1.3.2 *Protected Information*

- Original SafeOCS reports provided directly to BTS

- Any SafeOCS working documents
- Supplemental reports resulting from incident investigations that are submitted to BTS as part of the event record
- Sections of root cause analysis reports developed by designated subject matter experts (SMEs)
- All of the above whether paper or electronic

1.3.3 Non-Disclosure Agreements (NDAs)

Anyone working on a SafeOCS data collection is subject to a non-disclosure agreement as mandated by CIPSEA. Willful disclosure of confidential information by federal employees, agents, and contractors is subject to strict criminal and civil penalties for noncompliance.

CIPSEA protections do not apply to non-confidential information, including preventative safety actions recommended for implementation by SMEs or stakeholders, and any documents developed for public dissemination using confidential data.

2 Development of ISD Phase I

2.1 Development Timeline

In 2013, BSEE approached BTS expressing interest in establishing a near miss reporting program for the offshore oil and gas industry whereby company employees could individually submit on a voluntary basis safety event data at the time of occurrence. BSEE hosted a series of public meetings in 2014 to introduce this new initiative to industry. While offshore oil and gas companies recognized the benefits to this approach, they preferred not placing this reporting burden on individual employees and suggested instead that it would be more effective for companies to provide the requested information after the event details had been verified.

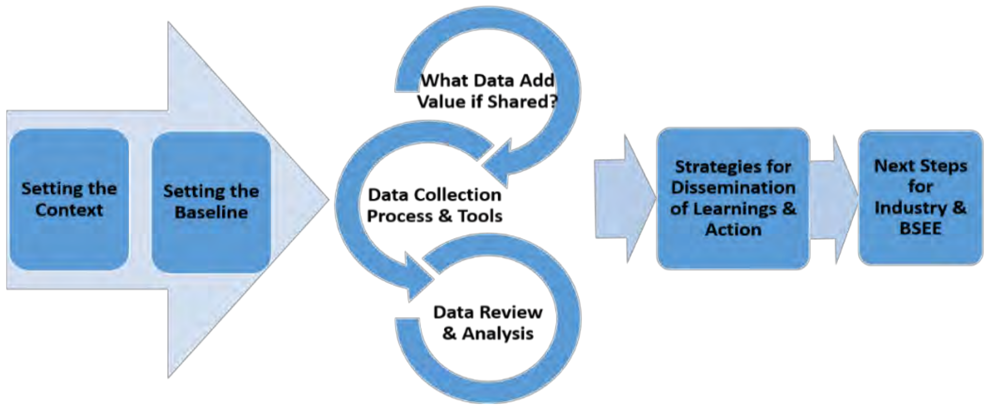
In 2014, BSEE approached the Society of Petroleum Engineers (SPE) regarding a proposed opportunity for industry and government to collaborate on development of a voluntary industry-wide near miss data collection framework and management database. The goal of this effort was intended as a resource to provide guidance to industry and enhance its ability to capture and share key learnings from safety and environmental events that were not currently being captured. In the spirit of continuous improvement, a related objective was to bring government and industry together to make a safe industry even safer through open data sharing, to enhance public confidence in the industry.

2.2 Laying the Groundwork: SPE/BSEE Summit

From 2014-2016, BSEE and SPE worked with a team of industry representatives, as well as BTS, aviation, and shipping experts to identify potential best practices for the capture and sharing of key learnings from safety and environmental events that were not currently being captured. The collaboration culminated in BSEE and SPE co-sponsoring a summit in April 2016 that included 62 representatives from 47 companies, both within and external to the oil and gas industry, to engage in a dialogue on what it would take to develop an industry-wide safety data management database. The high-level agenda for the summit is shown in Figure 2. The summit Technical

Report[2] included an action item to create and pilot a process and database for aggregating and analyzing industry safety data as part of a centralized framework.

Figure 2: 2016 SPE/BSEE Summit Agenda



SOURCE: SPE Technical Report: Assessing the Processes, Tools, and Value of Sharing and Learning from Offshore E&P Safety Related Data," September 2016

Although the scope of the summit initially focused on near-misses, the summit participants expanded the scope to include a broader range of safety data with learning value. The change in scope was intended to better position the effort to aid industry in achieving improved safety performance. The summit also clearly framed an additional goal of the effort: to avoid creating an additional layer of reporting expectations over and above the current requirements by regulators and industry associations.

2.3 Initiating ISD Phase I

Following issuance of the SPE Technical Report, BTS initiated efforts to form a team of companies interested in participating in ISD Phase I. Invitations were sent to individual companies asking them to participate in the Phase I effort as early implementers and to assist BTS in designing the safety data management framework. Once nine (9) companies expressed interest, the Phase I effort commenced. The nine companies represented a cross-section of companies operating in the Gulf of Mexico (GOM) as it included a mix of operators, service and drilling contractors.

As noted in the Introduction, BTS had already been designated as the repository to collect and analyze mandatory Well Control Rule (WCR) and Safety and Pollution Prevention Equipment (SPPE) data reports submitted by companies working in the OCS as required by regulation. BTS was therefore the logical choice to collect and analyze safety data reports submitted voluntarily by companies participating in the program.

In January 2018, BTS formed the Phase I Planning Team consisting of SMEs from each of the nine companies. The team agreed that the primary objective of Phase I was to develop a *proof of*

[2] "SPE Technical Report: Assessing the Processes, Tools, and Value of Sharing and Learning from Offshore E&P Safety Related Data," September 2016

concept for a proposed industry-wide safety event database, and the team also recognized the importance of industry input to maximize benefits of the end products. The Planning Team members further agreed on the following scope of their responsibilities:

- Discuss the type of data that should be submitted to ensure that the data captured has appropriate learning value, which may include, but is not limited to reportable and non-reportable events, near-misses, observations, unsafe conditions, stop work events, and associated metadata.
- Coordinate with BTS on the effectiveness of the SafeOCS ISD Program design and process, including potential enhancements to consider for the data aggregation and review processes.
- Review the SafeOCS ISD draft report and provide feedback prior to BTS approval and release.
- Participate (if desired) in one or more Data Review Teams, as appropriate, or suggest alternative representatives from their respective companies to be Data Review Team members.

It was important to set realistic and achievable goals for the desired outcomes of Phase I recognizing that such an effort to collect and analyze data across the industry had not been undertaken before. As such, the key objectives for Phase I were as follows:

1. Develop a process that overcomes the challenges of collecting and aggregating safety data from disparate company-specific databases, without requiring those companies to reformat their data;
2. Test the data aggregation process to identify and merge (as appropriate) potential duplicate records for the same event;
3. Analyze the aggregated data set and present findings on trends or events of significance; and
4. Provide recommendations on how the industry might utilize and benefit from SafeOCS ISD reports.

Meetings between BTS and the Planning Team members were held from July 2018 through April 2019 to review and discuss the aggregated data, as well as to brainstorm program enhancements that should be considered. These meetings also addressed how best to characterize the aggregated data to provide optimum sharing and learning opportunities for industry.

3 SafeOCS ISD Process Overview

The ISD Phase I effort resulted in the development of a process for data collection, analysis, and dissemination. Since Phase I was a pilot, its governance process was fully developed over the course of the effort. Moving forward, the ISD Program will follow a substantially similar governance process; where differences exist, they are noted below. The overall process that governed ISD Phase I is described in the subsections below.

3.1 Agreement with BTS

Each of the nine companies executed an agreement with BTS that detailed the scope of engagement between the company and BTS:

- Type of data to be submitted (i.e., safety and environmental events, near-misses, etc.);
- Event date ranges (i.e., number of years) of submitted data;
- Format of the data set to be provided to BTS;

- Company’s expectations regarding data review and analysis of its own data; and
- Company’s rights to its own data.

Moving forward after Phase I, new ISD participants will execute a Memorandum of Understanding (MOA) with BTS when they decide to participate. The MOA addresses the same information as the agreements used for ISD Phase I participants.

3.2 Data Collection

Upon signing the agreement, each company provided data to BTS for inclusion in the ISD Phase I database via an online portal. Online portal users created a profile through the SafeOCS website which employs a two-factor authentication method for logging in. This process ensures that data files are subject to the confidentiality protections of CIPSEA.

3.3 Data Review and Processing

BTS staff, with assistance from independent industry SMEs, processed and prepared the data for further review and analysis. BTS mapped all submitted data to the core data fields in SafeOCS ISD to allow for effective and meaningful aggregation and analysis. Part of the review was to identify reports that may be redundant due to submittal from more than one source (e.g., operator, service provider, drilling contractor, construction contractor). To avoid duplication, BTS used data matching and data mining techniques to consolidate information from multiple reports on the same event.

3.4 Statistical Analysis

After the initial data preparation, BTS analysts conducted exploratory data analysis to ensure data quality. Assisted by independent industry SMEs, BTS conducted analyses of the aggregated core data to identify trends and specific high-value learnings.

3.5 Data Review Team

BTS established a Data Review Team to assess, review, and analyze data to identify trends and specific high-level learnings. The Data Review Team comprised representatives from the nine participating companies, as well as BTS staff and the independent industry SMEs. Each team member received confidentiality training, signed a Non-Disclosure Agreement (NDA), and were designated as agents under CIPSEA. Unlike the independent industry SMEs who assisted BTS staff, industry SMEs assessed and analyzed only aggregated data, but they could also access and analyze their own company data.

The Data Review Team also assisted BTS with preparation of the draft report capturing the results of the aggregated data analyses and observations. All work performed by Data Review Team members took place in designated secure work spaces.

3.6 Disclosure Review Board

BTS also established a Disclosure Review Board to review the draft report in accordance with CIPSEA disclosure requirements and expected compliance with principles and practices of a statistical agency. For Phase I, the Data Review Team served as the Disclosure Review Board. The Disclosure Review Team responsibilities included ensuring that the identity of individuals and data contributors are protected from direct and indirect disclosure. Moving forward, the Data Review Team(s) and the Disclosure Review Board will differ in membership.

3.7 BTS Internal Review Process

Based on recommendations from the Disclosure Review Team, all final determinations of whether to disclose a final document rest solely with the BTS Confidentiality Officer. Within BTS, the report was reviewed by the ISD Program Director prior to review and approval by the BTS Director.

3.8 Report Publication

Upon publication of this report, industry may engage with other stakeholders and industry organizations to address the report findings. BTS may also act as the technical representative on statistical issues and data quality issues.

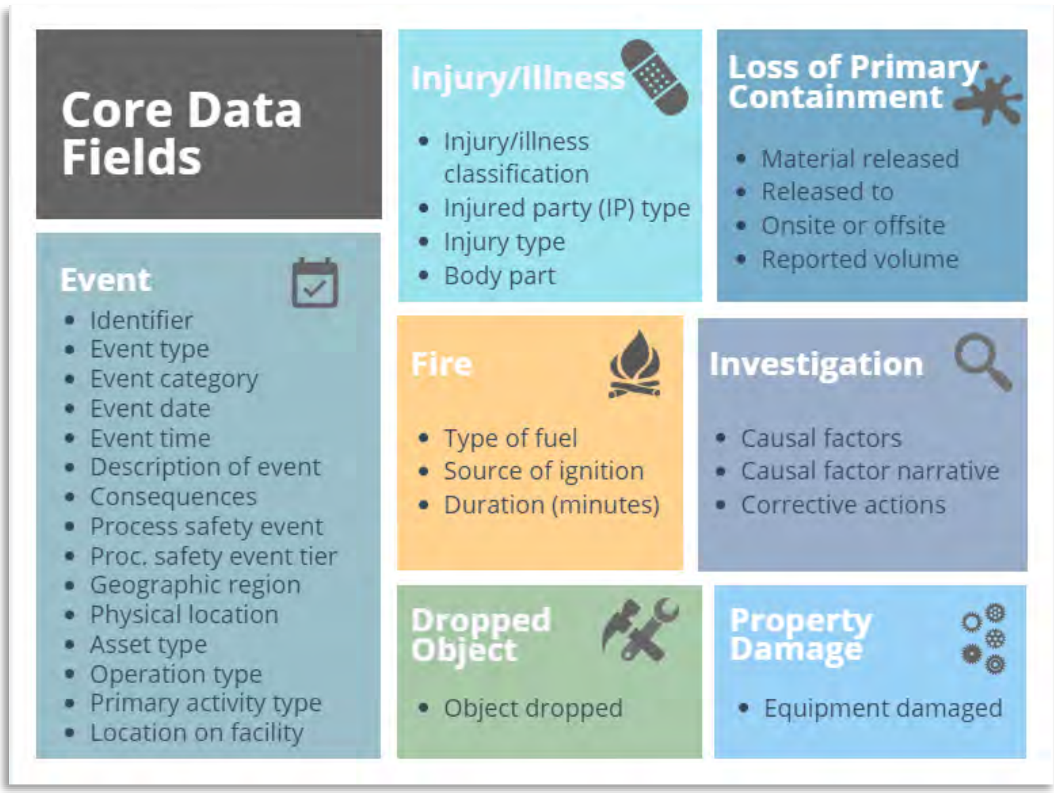
4 Phase I Study Protocol

With input from the ISD Phase I Planning team, BTS developed a study protocol, including the *scope of core data* fields to be included and the *data mapping* - the process for conforming data to the standardized template.

4.1 Scope of Core Data

A key focus area for the Phase I Planning Team was to identify the core data fields that should be considered for SafeOCS ISD. After comparing what each company was capturing, the group agreed that collecting the core data fields listed in Figure 3 would deliver the most value to industry and enhance industry's ability to learn from safety-events and mitigate future occurrences.

Figure 3: ISD Database Core Data Fields



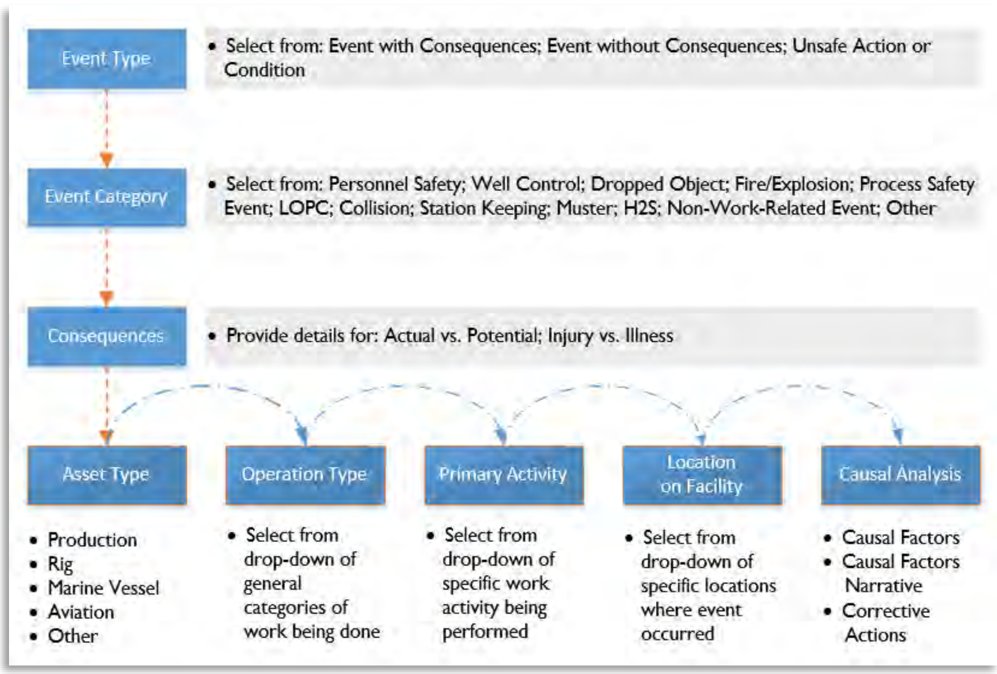
SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

4.2 Data Mapping Process

Working with SMEs, BTS then mapped all data submissions to a standardized format to allow the data to be aggregated and completed a detailed analysis of the aggregated data to demonstrate what can be accomplished on an industry-wide basis to analyze the causal factors and identify trends. All data reviewers were subject to non-disclosure requirements mandated by CIPSEA.

The data mapping process entailed matching the company's data to the SafeOCS ISD core data fields to provide consistency in how data are captured and allow for a more meaningful analysis. Each company's datasets were first limited to events that occurred in the Gulf of Mexico OCS. A SafeOCS ISD *codebook* was then developed to aid BTS staff (assisted by internal SMEs) with consistently mapping company-specific data submissions to the SafeOCS ISD database.

Figure 4: Data Mapping Process for ISD Events



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019

Each event was reviewed in the following manner (Figure 4):

1. the event type was categorized as either an event with or without consequence or an unsafe condition or act (e.g., safety observation)
2. each event was then flagged to the overarching characteristics involved. Note that any single event could trigger multiple characteristics, so more than one characteristic may apply (e.g., a Loss of Primary Containment Event (LOPC) event might also be classified as a process safety event depending on event circumstances)
3. consequences of the event, if any, were identified, such as whether the event resulted in an actual injury or illness
4. once the event characteristics were mapped, the focus then shifted to where the event occurred and what specific activity was happening at the time

5. the last step in the data mapping process focused on investigation of the incident and any identified causal factors, as this is likely where most of the key learnings will be identified; if a company submitted more than one causal factor, all of the those provided were entered into the database

For the causal analysis (step 5 above), Phase I members agreed to use a list of fifteen (15) Areas for Improvement (AFI) developed by the Center for Offshore Safety as a starting point, with the addition of three supplementary causal factors (leadership, human factors, and human performance) based on the data submitted, as well as BTS' experience in analyzing data from other industries. The eighteen (18) causal factors are listed in Figure 5 below.

Figure 5: ISD Event Causal Factors

GENERAL CATEGORY	CAUSAL FACTOR
PHYSICAL FACILITY, EQUIPMENT, AND PROCESS	• Process equipment and design • Process or equipment material selection, fabrication, and construction • Process or equipment reliability • Instrument, analyzer, and controls reliability
ADMINISTRATIVE PROCESSES	• Risk assessment and management • Operating procedures or safe work practices • Management of change • Work direction of management • Emergency response
PEOPLE	• Personnel skills or knowledge • Quality of task planning and preparation • Individual or group decision-making • Quality of task execution • Quality of hazard mitigation • Communication • Human factors • Human performance • Leadership

SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

5 Phase I Data Review and Analysis

The results of the data review and analysis process described here are illustrative of what could be implemented for the SafeOCS ISD Program as the database grows. It is important to note that the results, trends, and observations presented in this section are representative of only the nine (9) companies participating as early implementers and should not be interpreted as being representative of the entire offshore industry sector.

5.1 Data Description

For Phase I, nine companies submitted industry safety data for 2014-2017. The submitted data was in different formats, spanned across different years, and included different geographic regions. Though all nine companies submitted data, not all submitted data for each reporting year and some companies included events that were outside of OCS Gulf of Mexico (GOM).

To allow focus on offshore activities, the data analyzed excludes events occurring on land-based support facilities, such as shore bases, fabrication yards, and shipping terminals. Also excluded were events that occurred at the terminal or heliport unless the marine vessel or helicopter was *en route* to or from an offshore location.

Of the offshore events, 4.2 percent were considered *non-work-related* as defined by OSHA 1904.5(b)(2). For example, a non-work-related event could be an illness or injury that occurred off property but continued or worsened while offshore. Other examples of non-work-related events excluded were security violations; drug and alcohol violations; personal illnesses or health conditions; and injuries identified by the submitting company as non-work-related because they occurred while the employee was off duty. Of the non-work related events, nearly three-quarters involved an injury or illness that happened *off property* (e.g., cold/flu related symptoms or a back injury doing home yard work that caused pain while the employee was offshore); approximately one-fifth involved *off duty* injuries occurring in or near the crew accommodations (e.g., getting in/out of bunk beds, slipping in the shower, tripping on stairs, etc.); and a few events involved *possession of banned items* (alcohol, drugs, etc.).

5.2 Analysis Structure

The data analysis section starts by examining overall information about the 8631 events. Results are then grouped into three focus areas: *process safety*, *personal safety*, and *environmental stewardship.*

Process safety hazards in the oil and gas industry generally involve the potential release of harmful substances arising from operations of a drilling rig or production platform (e.g., well or production operations). Process safety hazards have the potential for serious consequences, such as loss of the facility, fatalities, damage to the environment, or harm to the company's reputation and financial health. Significant process safety incidents are typically low-frequency high-consequence events. Because these types of incidents are relatively infrequent, an important source of data is potential leading indicators found among incidents in the bottom portion of the safety triangle.[3]

Personal safety hazards involve the potential for harm to personnel due to injury or illness. Most injuries and fatalities arise from personal safety hazards rather than process safety hazards, and many companies employ mature data collection processes for personal safety incidents at all levels of the safety triangle. As with process safety, an opportunity exists to seek additional learnings from personal safety events that are often viewed as less significant but given different circumstances could result in injury. The SafeOCS ISD Program is seeking to capture personal safety data to support the identification and development of appropriate controls such as training, operating procedures and practices, or competency assessments.

Environmental stewardship hazards have the potential to harm ecosystems by polluting waters, killing wildlife, and/or contaminating habitats. Given the sensitivity of the environment where offshore activities occur, companies working in the GOM must exercise appropriate practices to protect the environment. The SafeOCS ISD Program seeks to capture events involving environmental hazards to support the development and/or improvement of appropriate controls.

This analytical structure is intended to present results in a way that facilitates use by industry and other stakeholders to advance safety and environmental protection. With increased industry participation in SafeOCS ISD, a similar analysis of a larger and more representative dataset could highlight potential problem areas and best practices that could apply more broadly.

6 Data Analysis

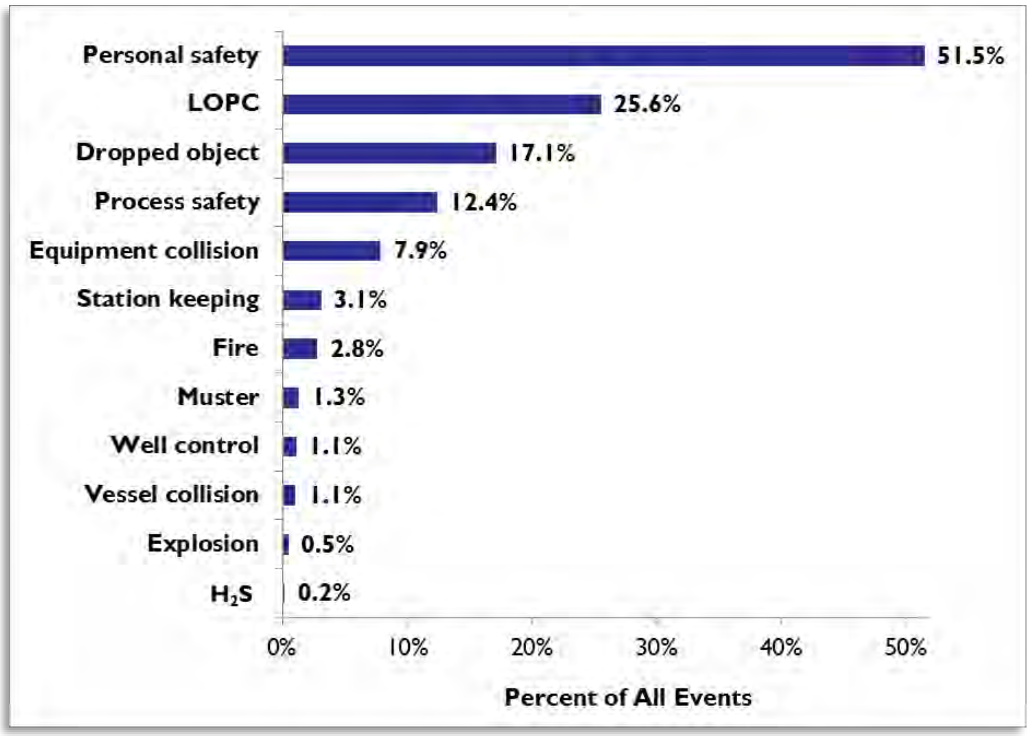
6.1 All Event Summaries

The Data Analysis section begins with a summary description of all safety events using core data fields, categories and characteristics. Of the total events, about 80 percent were e*vents with consequences* and the remainder were *events without consequences*. For "*events without consequences*," behavior-based events and safety observations were excluded from the scope of the pilot.

[3] See also, Int'l Assoc. of Oil & Gas Producers, Process safety – Recommended practice on Key Performance Indicators, Report No. 456, Nov. 2018 ("[Because process safety failures are relatively infrequent, it is] necessary to broaden these analyses to learn from events with less serious outcomes.")

Figure 6 illustrates the types of events reported using the *event category* field. SafeOCS allowed companies to make multiple selections to describe events as appropriate since multiple safety categories can be involved in a single event. The *personal safety* category was selected over 50 percent of the time to describe safety events. As a result, the total of the individual categories exceeds the total number of events.

Figure 6: Submitted Events by Category

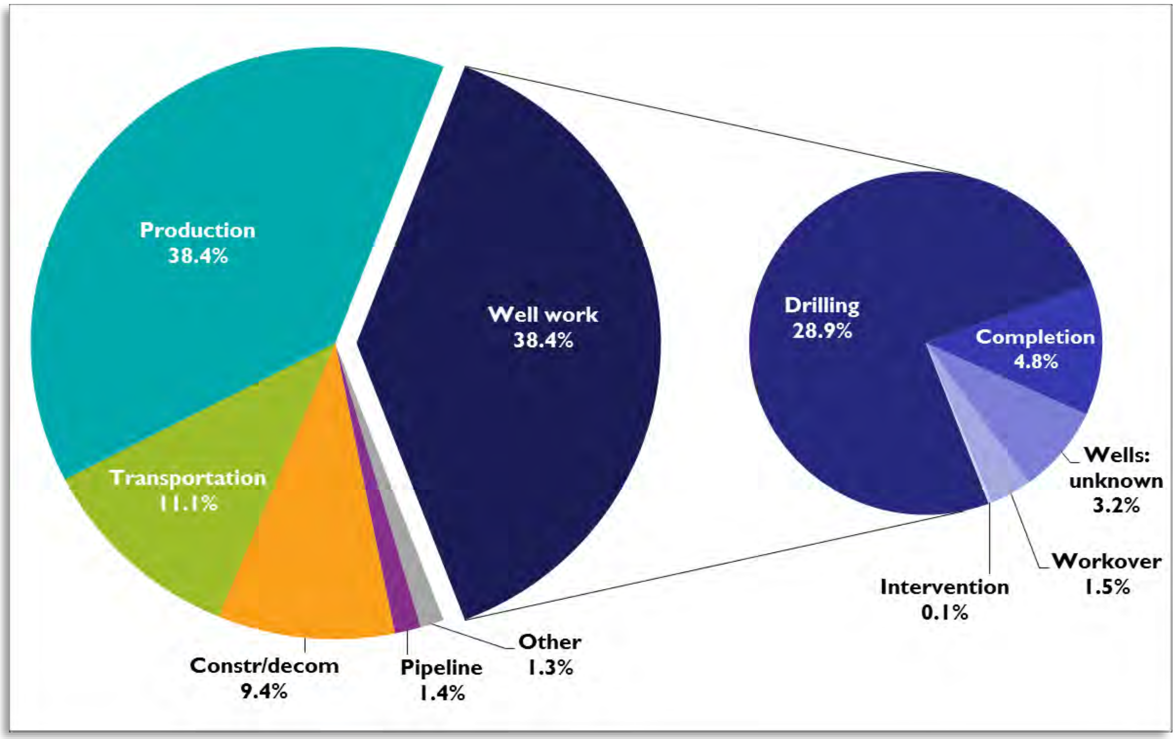


SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Events involving *collisions* were separated into two categories: 1) *vessel collision* for those involving marine or aviation vessels and 2) *equipment collision* for events involving objects striking equipment (e.g., a suspended load striking a handrail). It is important to note that dropped objects that land on the deck or strike equipment are not considered equipment collisions.

Figure 7 shows the reported events by groups of related *operations* that were ongoing when events occurred. Some operations were combined for ease of display. For example, *drilling*, *completion*, *workover*, *intervention*, and *plugging and abandonment* were combined into *well work*. Most of the reported events happened during *well work* and *production* operations.

Figure 7: Ongoing Operation When Event Occurred

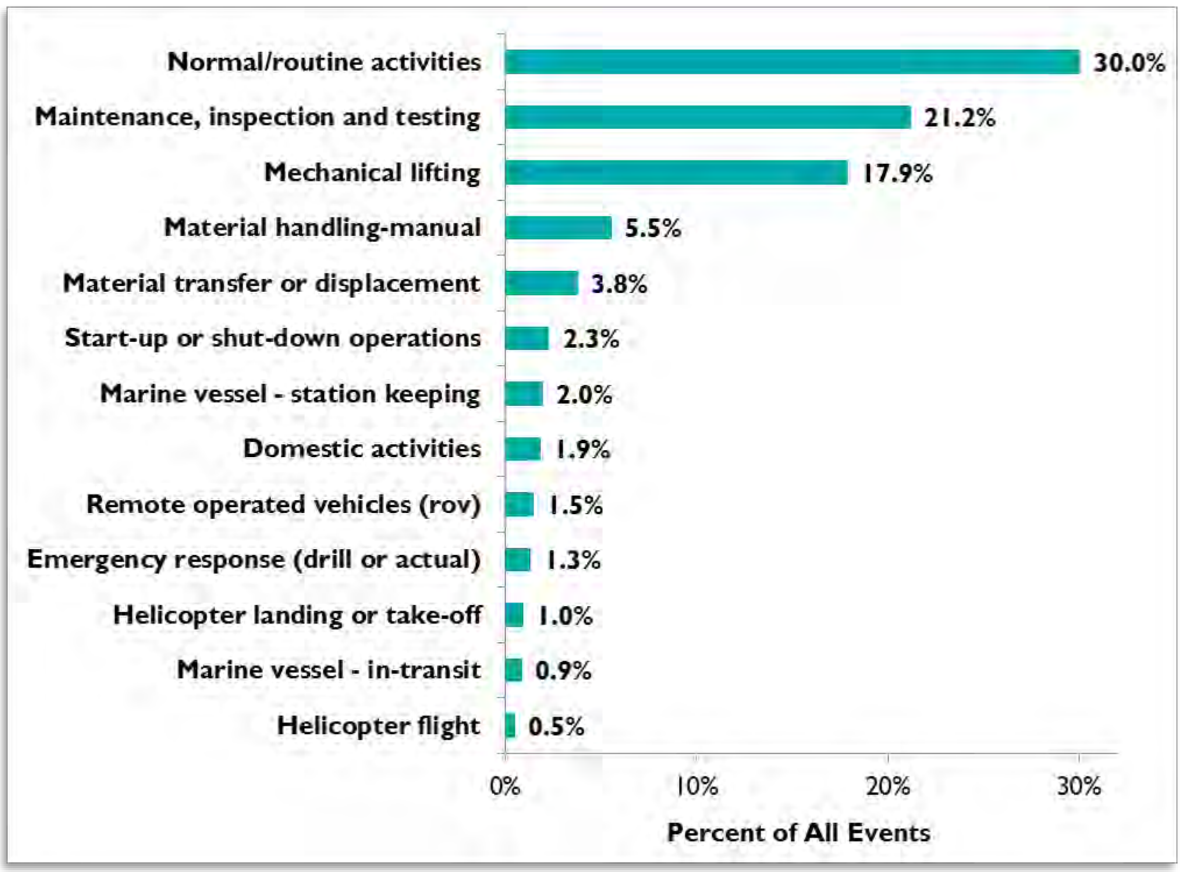


SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Figure 8 shows the breakdown of events by the *primary activity* being performed at the time of the event. Events occurred, most frequently, during these activities: *normal/routine activities*; *maintenance, inspection, testing*; and *mechanical lifting*. Most events occurred during *normal/routine activities*; however, there isn't a standard definition of this activity, which makes it difficult to classify events accurately.

For example, some companies may designate *mechanical lifting* as a *normal/routine activity*, rather than mechanical lifting. *Maintenance, inspection and testing, as well as mechanical lifting* activities are common across both *well* and *production* operations, which explains the high percentage of events in those primary activities.

Figure 8: Primary Activity Underway When Event Occurred

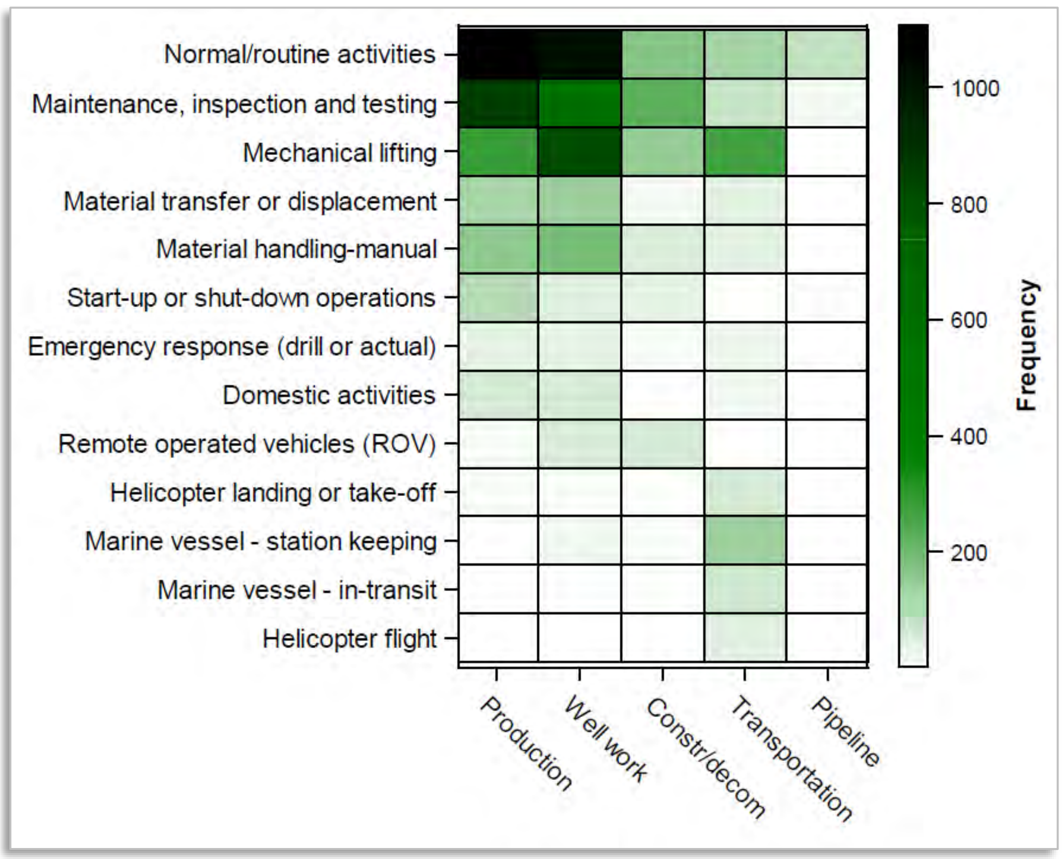


SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Figure 9 is a heat map diagram that shows the relative frequency of events given the combination of two parameters: *primary activity type* and *operation group*. Heat maps can be useful in making observations about unexpected combinations of parameters. The higher the frequency, the more intense the color in the box that represents that combination.

For example, events happening during *normal/routine activities* occurred most often during either *production* or *well work.*

Figure 9: Primary Activity Type by Operation Type

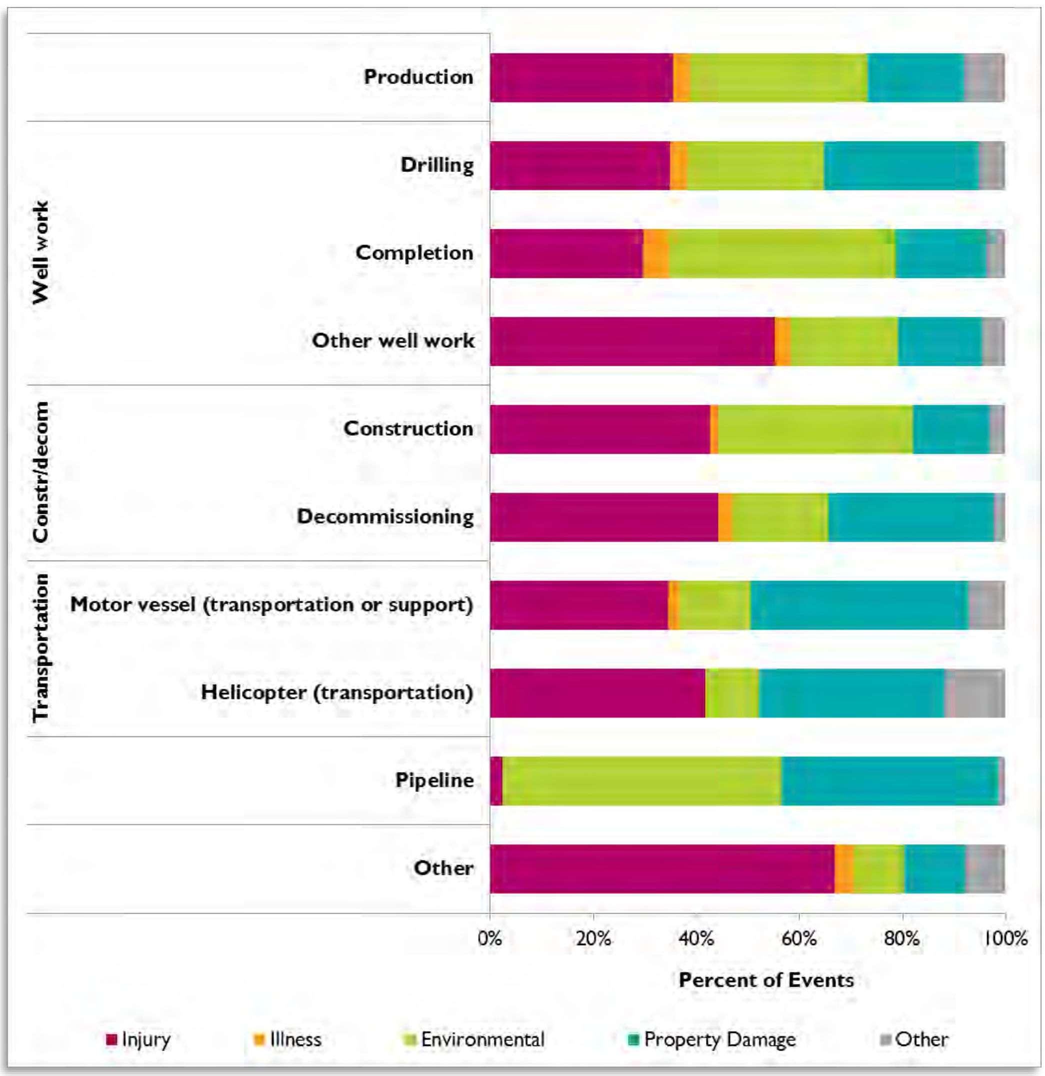


SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Figure 10 illustrates the *consequences* of events by *operation group*. Each row shows the percent of events for the listed *operation* whose consequences were *injury*, *illness, environmental*, *property damage* or *other*. For this data field, submitters could assign multiple *consequences* to one event. Almost all operation types had a similar breakdown of the consequences. *Pipeline* operations had very few injuries in this data set, as pipeline operations may involve less human interaction, compared to other operation types.

The *other well work* subcategory includes *workovers*, *interventions*, *abandonments*, *wireline work*, and *coil tubing work*. The *other* category primarily represents events for which the asset type and operation type were both unknown. It also includes a few cases from seismic and commissioning operations.

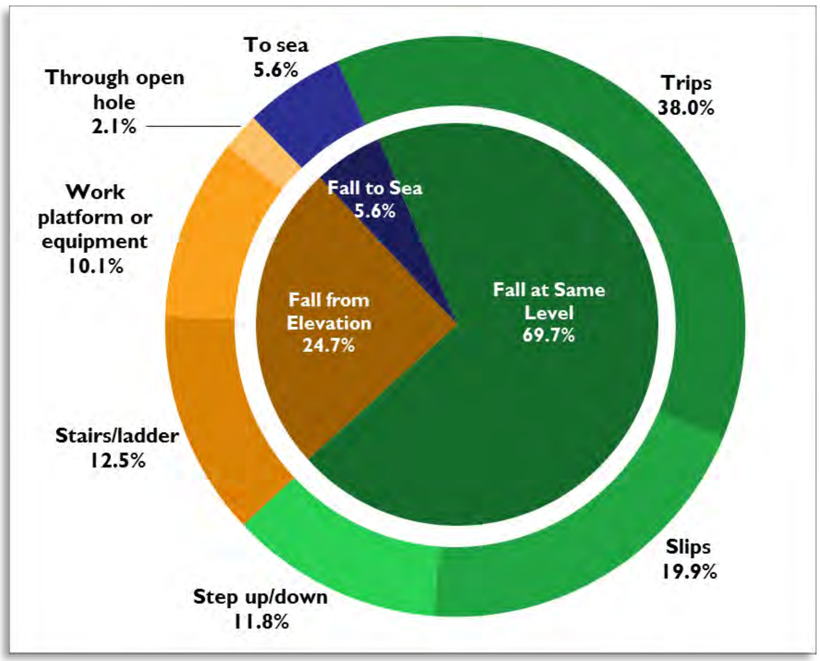
Figure 10: Consequences by Operation



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

Finally, Figure 11 shows the frequency of the types of falling events reported. *Slips* and *trips* were the main cause, accounting for 57.9 percent of falls. *Falls from elevation* accounted for 24.7 percent of the total falls; however, falls from elevation resulted in more serious injuries. A closer review of the 2014 – 2017 data revealed many falls resulting from deficiencies in platform grating, and this may be an area for improvement in future data collection and analysis.

Figure 11: Types of Falling Events



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics, ISD Program, August 2019.

As noted earlier, similar analyses were completed for more specific areas such as process safety, personal safety, and environmental impacts. A more detailed discussion of these additional analyses can be found in the BTS report "Industry Safety Data Program for the Oil and Gas Industry – Phase I Report" which can be found at www.safeocs.gov .

7 Learnings from Phase I

7.1 Key Learnings

BTS and representatives from the nine participating companies believe that ISD Phase I was successful in demonstrating the feasibility of the ISD Program. They were able to prove that it was possible for companies to submit data to BTS in different formats and for BTS to then map the data to a common SafeOCS structure to allow for effective and meaningful data aggregation, review, and analysis. The key learnings from Phase I are summarized as follows:

- ISD Phase I participating companies agreed on the value of sharing data for both consequential and lesser events with the potential to lead to a major event.
- Legal and confidentiality concerns expressed by participating companies were satisfied with the protections afforded under CIPSEA and with the signing of an agreement between BTS and each company.
- BTS developed a process to successfully map data from separate companies to a single database thereby addressing the technical challenge associated with collecting, mapping, and aggregating data from different company-specific databases.
- The Phase I Planning Team identified core data fields that all participating companies should be expected to share to generate meaningful data analyses that provides learning opportunities for industry to further improve safety.
- Despite the limited data sample (nine companies), which was not representative of the entire industry, it was possible to complete meaningful analyses of the aggregated data.

7.2 Recommendation for Facilitation and Enhancement of Data Analysis

A key aspect of the SafeOCS ISD Phase 1 Program is that BTS was willing to accept data in whatever format would make it easiest for companies to submit. BTS data analysts and independent industry SMEs were then responsible for *mapping* the company-specific data to the SafeOCS database. As the SafeOCS ISD Program progresses, it will be important to consider the following enhancements to both the program itself and the company-specific data submissions, to facilitate data mapping and enhance data analysis:

- To enhance the depth of analysis, companies should consider submitting additional information about unsafe actions or conditions (e.g., safety observations) that may be precursors to events if circumstances at the time of the event would have been different.
- Participants are encouraged to consider how they may improve integration of their company's data management systems. A challenge faced by some companies when submitting data was the lack of integration across separate data management systems that may exist within a company, which can make data submission of the requested core data fields more cumbersome.
- BTS may consider expanding the use of drop-down menus to harmonize entries and address the challenges encountered around data field inconsistencies and misspellings.

- Given that a key premise of the SafeOCS ISD program is to capture more than what is currently required by regulation, all participants are encouraged to provided data related to safety events that may occur while off-shift.

- Some of the property damage information provided was aligned with the regulatory dollar threshold for those events, and information about lesser property damage events may not be consistent across companies. Therefore, all companies are encouraged to provide property damage information regardless of dollar impact.
- All companies are encouraged to consider quantifying the seriousness (potential injury consequences) of dropped objects using an industry recognized dropped objects calculator based on the mass of the dropped object and the distance it fell.
- To further assist with identifying and merging multiple records submitted for the same event either by the same company or their contractors, it would be helpful if company-specific data files highlighted which operator the work was being performed for, or which contractor was conducting the work.
- Participants should consider the following recommendations regarding causal factors, which are important in identifying potential patterns and trends in the types of events that may be of concern on an industry-wide basis and warrant further analysis.
    - Participants should either provide more information about causal factors and/or more detailed text descriptions of the event.
    - To the extent practicable, companies submitting data should strive to provide additional event details (such as incident investigation reports, photos, etc.) as this will allow for more meaningful analyses. Examples include:
        - Avoiding redacting information that could otherwise prove beneficial during the data mapping and aggregation processes.
        - Avoiding merged or hidden cells.
        - Clarifying expectations on how to manage events attributed to *third parties*.

8 Next Steps

8.1 Outreach to Grow Participation

- As the number of SafeOCS participating companies grows, more data can be captured, analyzed for trends, and actioned with the goal of preventing more serious events. BSEE and BTS will continue outreach efforts to inform additional companies about the SafeOCS ISD Program and encourage participation.
- As SafeOCS ISD progresses beyond Phase I with an increased number of participants, BTS will consider hosting a detailed orientation that discusses the following:
    - Minimum data submission expectations, including supporting event narratives
    - Specific BTS activities involved with data processing
    - BTS secure data room setups
    - Timing for submissions

8.2 Use of Learnings from SafeOCS ISD Reports

- Industry may consider using the knowledge gained through this program to:
    - Develop new or modified risk controls and support systems, such as training or awareness programs
    - Host workshops and other similar events to discuss causal factors and develop actions to prevent reoccurrence

- BSEE and BTS will work with industry to plan workshops or other sharing/lessons learned sessions to review aggregated results, network, and discuss potential actions to prevent recurrence and thereby improve safety.

8.3 Enhancements to SafeOCS ISD Program

BTS will:

- Continue to engage in informed discussions with industry stakeholders, including oil and gas operators, drilling contractors, service companies, original equipment manufacturers (OEMs), and BSEE, to ensure the SafeOCS ISD Program provides value to stakeholders.
- Focus on system upgrades and capabilities, including a possible dashboard, to allow companies to view their own data online for purposes of comparing their performance against the aggregated results.
- Consider, as appropriate, developing white papers on specific safety issues, such as transportation-related or other safety events.
- Continue to plan for cross-linking the SafeOCS ISD database with the databases of the other SafeOCS programs (i.e., SafeOCS Well Control Equipment (WCR) Failure Reporting Program, and the SafeOCS Safety and Pollution Prevention Equipment (SPPE) Failure Reporting Program), as well as other data sources to provide more complete event details and evaluate potential correlations.
- Work toward developing analytical tools to identify low frequency events that could indicate the potential for a significant event (e.g., predictive modeling).
- Continue engaging with BSEE to discuss trends seen in both SafeOCS ISD data as well as BSEE data

8.4 Program Governance

With completion of the pilot effort and looking forward to broadening the SafeOCS ISD program to include more participants, BTS established a Steering Committee. It is composed of company representatives, each of whom must be designated as *agents* under CIPSEA, and the team is led by BTS. The team consists of 9-12 participants - BTS staff members, BTS independent industry SMEs, company SMEs, and others as deemed appropriate by BTS. It is charged with providing input to BTS on the SafeOCS ISD program effectiveness and enhancement opportunities. Company SMEs are selected from companies that are actively submitting data to the SafeOCS ISD program. BTS will ensure that the Steering Committee represents a cross-section of industry companies. Members will serve a three-year renewable term, with one-third of the members turning over each year.

Roles and responsibilities of the Steering Committee include:

- providing feedback and suggestions on ways to increase awareness of the SafeOCS ISD program among industry organizations,
- discussing plans for workshops or other sharing/lessons learned sessions to review aggregated results,
- promoting industry networking to address potential actions to prevent recurrence and thereby improve safety, and

- focus on development of a dashboard to allow companies to view their own data online for purposes of comparing their own performance against the aggregated results.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Modelling Ice and Wax Formation in a Pipeline in the Arctic Environment

Ben Bbosa[b.], Zhengdong Cheng[a.], Dali Huang[c.], M. Sam Mannan[a.], Michael Volk[b.], Hongfei Xu* [a]

[a.] Mary Kay O'Connor Process Safety Center,Artie McFerrin Department of Chemical Engineering, Texas A&M University System, College Station, Texas 77843-3122, USA

[b.] McDougall School of Petroleum Engineering, The University of Tulsa, Tulsa, Oklahoma 74104, USA

[c.] Department of Materials Science and Engineering, Texas A&M University, College Station, TX, USA.

*Presenter E-mail: hongfeixu@tamu.edu

Abstract

In the Arctic environment, fluid temperature in pipeline can drop below the freezing point of water, which causes wax and ice to form on pipeline surface. Solid formation on pipeline surface can lead to flow assurance and process safety issues, such as blockage of pipeline, pipeline component failure, and the release of hazardous liquid. The blockage of pipeline can cause additional burden or failure to pumping system. Remediating the plugging requires shutdown of pipeline operation, which cause tremendous cost and delay to the entire production system. Ice and wax deposition in pipeline is a slow process. Pigging operation can be used to remove the deposits on pipeline surface. However, if deposition is too thick, pipeline blockage can still occur. In order to prevent pipeline blockage, ice and wax deposition rates are required to be estimated. This paper investigates ice and wax deposition rates in a 90 km pipeline. A fundamental model for both ice and wax deposition is proposed using first principles of heat and mass transfer. The interaction between water and wax is analysed.

Keywords: Modeling, Two-Phase Flow, Ice and wax deposition, Pipeline plugging, Operations

1. Introduction

The Arctic is the region within approximately 66 degrees North parallel, including parts of Alaska (USA), Canada, Greenland (Denmark), Iceland, Sweden, Norway, Finland, and Russia (Johnstone, 2014). The existing fields beyond the rctic Circle account for 10% of the world's existing conventional resources (Gautier *et al.*, 2009). The hydrocarbon potential of the Arctic region is considered as the final frontier for conventional hydrocarbon development. In oder to ensure contninuity in oil supply to global energy needs, oil companiesled to the oil and gas exploration and production activities in harsh environment including extremely low tempearutres (Kaiser *et al.*, 2016).

Process safety and flow assurance challenges exsit due the harsh operating conditions in the Arctic (Khan *et al.*, 2015). In addition to common flow assurance challenges, such as wax, hydrates, and corrosion issues, water or ice can also be a problem (Xu *et al.*, 2018). In the low temperature conditions, even traceable amount of water in pipeline can cause ice formation, leading to pipeline blockages and associated risks. For example, It was reported that ice plugging deplayed the restart of the Poplar pipeline system gathering crude oil from Montana and North Dakota (Sunne, 2015). The potential risk of ice formation also draw the attention of Trans-Alyeska Pipeline Systems (TAPS) (Alyeska Low Flow Impact Study Team, 2011). The possible delining throughts in the pipeline can decrease its oil temperature below water freezing point. Ice formation can can lead to restruicting flow and plugging of pipeline, which can causes pump overburden or even failure. In addition, ice can also lead to temperature and pressure transducer failure. The remediation of a plug may be costly and can lead to environmental issues (Comfort *et al.*, 2008; Huang *et al.*, 2011).

We focuses on two flow assurance solids in this study, wax and ice. Wax deposition is an existing flow assurance issue for pipelines in a cold environment, such as the Arctic or subsea. Ice deposition is an potential issue for pipeline in the regions where environmental temperature can drop below water freezing point. When hot oil flows along the pipeline in cold regions, such as subsea and Arctic regions, heat is lost through the pipe wall to the cold environment. The decreasing oil temperature leads to the decreasing solbility of the heavier components in the bulk oil (Han *et al.*, 2010). As a result, wax deposition may occur. A wax deposition model is to calculate the location and the growth rate of the wax layer . A variety of thoeries were proposed to describe the wax deposition process, including molecular diffusion, shear dispersion, Brownian diffusion and gravity settling (Burger *et al.*, 1981). Experiments have shown that molecular diffusion is the main mechanism for wax deposition (Singh *et al.*, 1999). In addition to the growth of wax deposition layer, wax molecule can diffuse within the deposition layer, increasing wax fraction in the deposition layer, which is so called “wax aging” (Aiyejina *et al.*, 2011).

Modelling of ice formation and its deposition on a surface has been widely studied in meteorology, aviation, and the refrigeration industries (DeMott *et al.*, 1983; Kim *et al.*, 2014; Messinger, 1953; Myers & Charpin, 2004; Niezgoda-Żelasko & Zalewski, 2006a; Walker, 2002). In meteorology, depends on the environmental temperature and the state of water, hoar frost, rime, or glaze ice can form on a surface (Walker, 2002). Modeling the growth rate of one ice morphology needs to consider its forming conditions. For example, Hoar frost is due to the sublimation of water vapor on a surface, and thus molecular diffusion is the main forming mechanism. Other morphologies needs to take consider of water films on surface or droplets in the ice formation process. In aviation industry, aircraft icing can pose a serious threat to flight safety (Cooper *et al.*, 1984). The modelling of aircraft icing considers air flow, water droplets trajecties, as well as surface growth mode (Myers & Charpin, 2004). Although few published work studied ice formation in hydrocarbon flow lines, experimental and numberical simulation of ice slurry flow in pipe are widely reported in refrigeration industries (Grozdek *et al.*, 2009). Models for ice slurry flow considers the factors such as composition of ice slurry, pipe shape, and concentraction (Chhabra & Richardson, 2011; Niezgoda-Żelasko & Zalewski, 2006b).

The objective of this study to model ice and wax deposition in a liquid hydrocarbon and low water cut system. Molecular diffusion is assumed for the formation mechanism for wax deposition, ice deposition, and the deposition with wax and ice mixture. The interaction between ice and wax in the deposition are studied.

2. Model Development

2.1 List of assumptions

We adopt several common assumptions when modelling the velocity, heat exchanges, and wax and ice deposition. These include the following.

1) The oil behaves as a Newtonian fluid.
2) Molecule diffusion dominates the mass transfer of wax and water (ice) in both the bulk fluid and the deposits.
3) The formed deposition layer cannot be sloughed off by fluid shear.
4) Thermal conductivities of ice and wax are assumed to be constant, which are not function of temperature.
5) The environmental temperature is constant along the pipeline, not changing with geography.
6) The inlet fluid properties and flow rate remain unchanged.

The 2) assumption indicates in this study the growth of deposition is due to molecular diffusion, not by solid particle settlement. The precipitated wax particles stay in the bulk fluid. In addition, the water content in this study is extremely low. Only dissolved water in oil is considered. Deposition growth due to settlement of free water droplets and ice particles is ignored in this study.

2.2 Governing equations

In order to quantify the deposition rate, the transport euqaitons are solved first to obtain the velocity, temperature, and concentraciton profiles in the bulk fluid. Firstly, the velocity profile is obtained using the following analytical solutions for laminar flow and turbulent flow.

For laminar flow (i.e. Reynolds number (Re) smaller than 2000),

$$v_z(r) = 2 * v_{z,ave} * (1 - \left(\frac{r}{R}\right)^2) \tag{1}$$

For turbulent flow, Re>2000 (Deen, 1998),

$$v_z = v_z^+ * \sqrt{\frac{\tau_w}{\rho}} = v_z^+ * (y^+ * \frac{v}{y}) \tag{2}$$

where v_z^+, y^+, f and v are defined as follows.

$$v_z^+ = \begin{cases} y^+ & y^+ \leq 5 \\ 5lny^+ - 3.05 & 5 \leq y^+ \leq 30 \\ 2.5lny^+ + 5.5 & 30 \leq y^+ \end{cases} \tag{3}$$

$$y^+ = \frac{y}{v}\sqrt{\frac{\tau_w}{\rho}} = \left(1-\frac{r}{R}\right)\frac{Re}{2}\sqrt{\frac{f}{8}} \tag{4}$$

$$f = \frac{0.305}{Re^{0.25}} \tag{5}$$

$$v = \frac{\mu}{\rho} \tag{6}$$

A backward implicit numerical scheme is used to solve the heat and mass transfer equations, which can give a stable solution (Pletcher *et al.*, 2012). The heat and mass transfer equations are expresses as follows

(Heat transfer) (7)

$$v_z\frac{\partial T}{\partial z} = \frac{1}{r}\frac{\partial}{\partial r}\left[r(\varepsilon_H+\alpha_T)\frac{\partial C}{\partial r}\right]$$

(Mass transfer) (8)

$$v_z\frac{\partial C}{\partial z} = \frac{1}{r}\frac{\partial}{\partial r}\left[r(\varepsilon_M+D_{wo})\frac{\partial C}{\partial r}\right] - k_r(C-C_{ws})$$

where for laminar flow, $\varepsilon_{\mathrm{H}} = \varepsilon_M = 0$. For turbulent flow the momentum thermal and mass diffusivities can be obtained using the following correlations.

$$\varepsilon_{\mathrm{H}} = \alpha_T * \frac{Pr}{Pr_T} * \frac{\varepsilon}{v} \tag{9}$$

$$\varepsilon_{\mathrm{M}} = D_{wo} * \frac{Sc}{Sc_T} * \frac{\varepsilon}{v} \tag{10}$$

$$Pr_T = 0.85 + \frac{0.015}{Pr} \tag{11}$$

The relationship between eddy momentum diffisvity, ε, and dynamic viscosity, v is obtained using the correlations of Van Driest (1956):

$$\frac{\varepsilon}{v} = (ky^+)\left[1-\exp\left(-\frac{y^+}{A}\right)\right]^2\left|\frac{dv_z^+}{dy^+}\right| \tag{10}$$

Rate of wax precipitation is expressed using first order reaction, $k_r(C-C_{ws})$ (Huang *et al.*, 2011). The reaction constant k_r is an empirical term, which can be obtained using:

$$k_r(T) = k_r(WAT\ or\ freezing\ T) * \left(\frac{T}{WAT\ or\ freezing\ T}\right)^{1.47} * \exp\left(\frac{\gamma E}{R}\left(\frac{1}{T} - \frac{1}{WAT\ or\ freezing\ T}\right)\right) \tag{11}$$

where k_r is precipitation rate constant of wax or ice in oil and E is activation energy. Both k_r and E can be obtained through experiments. In this study, k_r uses value of 1.4 and $E = 37700$. γ is obtained using the following correlation.

$$\gamma = \frac{10.2}{V_M} - 0.791 \tag{12}$$

The boundary conditions for eqn.7 and eqn.8 are given as follows.

$$\begin{cases} T = T_{inlet,oil} & at\ z = 0 \\ \dfrac{\partial T}{\partial r} = 0 & at\ r = 0 \\ h_o(T_{out} - T_{wall}) = k_{dep}\dfrac{\partial T}{\partial r} & at\ r = r_{eff} \end{cases} \tag{13}$$

$$\begin{cases} C = C_{inlet,oil} & at\ z = 0 \\ \dfrac{\partial C}{\partial r} = 0 & at\ r = 0 \\ C = C_{ws}(T) & at\ r_{eff} \le r \le r_{inner\ radius} \end{cases} \tag{14}$$

where r_{eff} is effective flowing diameter, which is the radius from the pipe centreline to the deposition surface. $C_{ws}(T)$ is concentration obtained from solubity curve, which means in the deposit, wax or ice concentraction follows liquid/solid ebuiliburm.

2.3 Deposition model

Molecular diffusion is assumed to be the deposition mechanism. Molecular diffusion occurs not only in the bulk but also in the depsotion layer. Wax or ice deposits have a porous structure with entroppaed liquid providing a pathway fo the diffusion of wax molecule within the deposit. Along the radial direction, the mass flux of wax molecules or water molecules first diffuse from the bulk to the deposition interface. Then, a second diffusion exists in the porous deposition, increasing the solid concentraction in the deposit, which is called aging phenomena. The deposition growth takes account of the flux in the bulk and the flux within the deposit, which is expressed as:

$$\rho_{gel} F_{wax} \frac{d(\delta_{deposit})}{\partial t} = J_{bulk\ to\ interface} - J_{within\ the\ deposit} \tag{15}$$

$$J_{bulk\ to\ interface} = -D_{wo_{wax}} \frac{dC_{ws}}{\partial r}\bigg|_{\substack{from\ oil \\ to\ interface}} \tag{16}$$

$$J_{within\ the\ deposit} = -D_{eff\_wax} \frac{dC_{ws}}{\partial r}\bigg|_{\substack{from\ interface \\ to\ deposit}} \tag{17}$$

Mass balance over the deposit can be expressed as:

$$\pi\rho_{gel}\left(R^2 - r_{eff}^2\right)\frac{d(F_{wax})}{\partial t} = -2\pi r_{eff} * J_{within\ the\ deposit} \tag{19}$$

$$r_{eff} = r_i - \delta_{deposit} \tag{20}$$

Within the porouse deposit, the existence of solid phase provides mass transfer resistance. To take account of the effect of solid phase on mass transfer, an effective diffusion coefficient is used in eqn 17, (Aris, 1985) which is defined as:

$$D_{eff\_wax} = \frac{D_{wo\_wax}}{1 + \frac{\alpha^2 F_{wax}^2}{1 - F_{wax}}} \tag{21}$$

where α is aspec ratio, which is related to wax concentraction, F_{wax}.

2.4 Meshing

We discretise the 2-D cylindrical pipeline (eqn 7 and 8) with finite difference method. In vertical direction, a constant grid block size is used because uniform environmental properties are assumed. The grid blocks in radial direction are logarithmically distributed, with finer meshes near the pipe wall region:

$$r_i = \left(r_{eff} * \frac{\log(i)}{\log(num_R)}\right)^{0.4} \tag{22}$$

Since the effective flowing diameter decreases when deposition occurs. The mesh in radial direction is updated for each time step.

3. Materials

If temperature in a pipline varies significantly, fluid viscosity and density can no longer be assumed as constant along the pipeline. Instead, we use viscosity function and density function to describe their relationships with temperature. In this study, we use the properties of TAPS crude oil. The density and viscosity are measured using using a Stabinger Viscometer (Anton Paar, SVMTM 3000). The obtained density and viscosity relationships with tempearutre are expressed as:

$$\rho\left(\frac{g}{cm^3}\right) = 0.877 - 0.00428 * \left[T(°C) * \frac{5}{9} + 32\right] \tag{22}$$

$$\mu(cp) = \exp(\exp\left[36.409 - 5.6959 * \log\left(T * \frac{5}{9} + 32 + 460\right)\right]) \tag{23}$$

Commercial software PVTSim is used to obtain the wax solubility and water solubitliy. Figure 1 shows the the wax solubility curve. Figure 2 the water solubility curve.

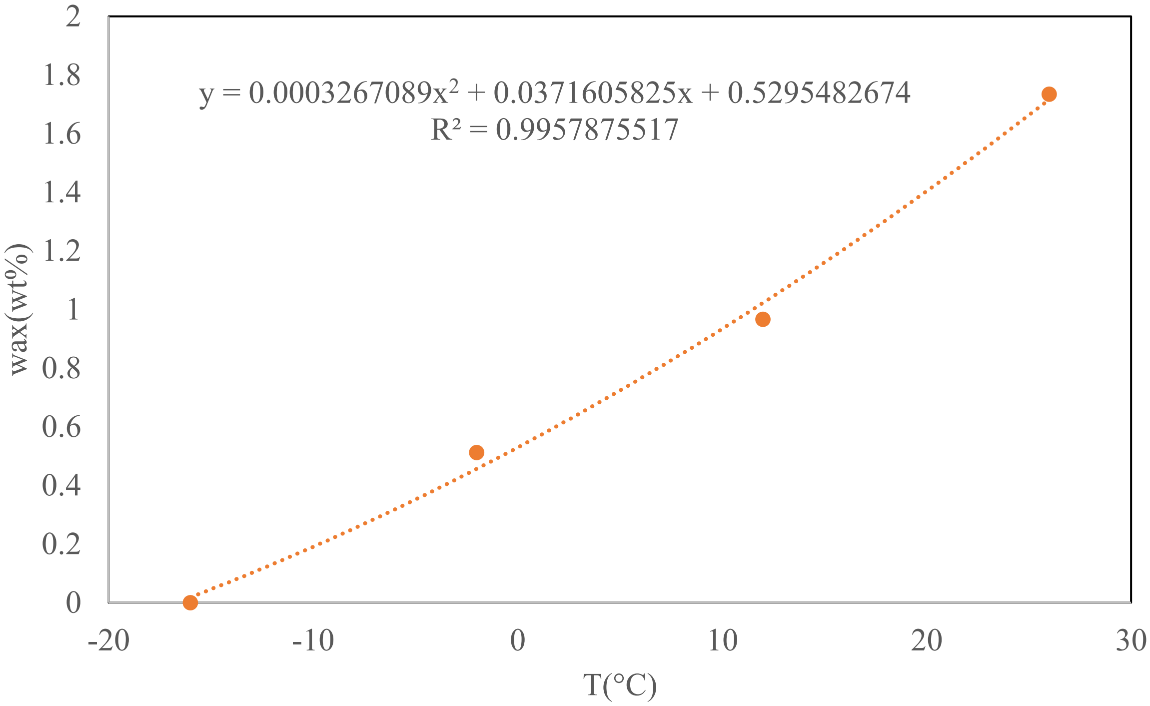


Figure 1: Wax solubility in TAPS oil

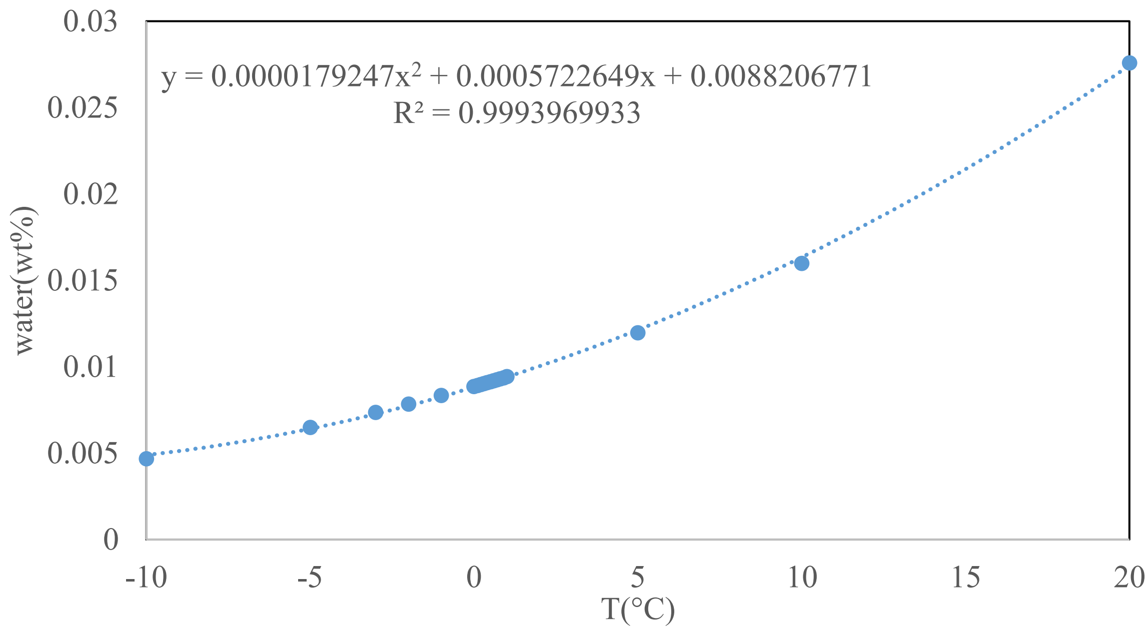


Figure 2: Water solubility in TAPS

4. Results and discussion

As oil enters the pipeline, its temperature decreases due to heat loss to the environment. When fluid temperature drops below WAT, wax precipitation occurs. Near the pipe wall region, if the pipe wall temperature is below WAT, wax deposition may occur. If the oil travelles further along the pipeline with more heat losses, its temperature can drop below freeing point of water. At these locations, the deposition is a mixture of wax and ice.

In this section, we first conduct a numerical convergence study to determine the optimal discretization of numerical models. Then, we show deposition growth and aging in the case of wax deposition without ice deposition, followed by the case of ice deposition without wax deposition. Finally, a cominbed deposition case is studied to show the interaction of ice and wax in the deposition process. Table 1 shows the pipeline geometry and thermal properties of pipeline and deposits in this study.

Table 1: Pipeline geometry and thermal properties of pipeline and deposits in this study

Parameter	Value	Units
Pipeline length	90000	m
Inner diameter	0.5	m
Pipe thickness	0.012	m
Insulation thickness	0.1	m
Thermal conductivity of ice	2.22	W/(m•K)
Thermal conductivity of wax	0.25	W/(m•K)
Water freezing point	0	°C
Wax apperance temperature	24	°C
Intial solid fraction for wax or ice	0.05	
Environmental temperature, $T_{environment}$	-7	°C
Inlet temperature of fluid,T_{in}	25.5	°C
Outside conductive heat transfer coefficient, h_o	5	W/(m^2•K)
Oil inlet flow rate	76.72	Mbbl/D
Simulation time	336	hours

4.1 Nuemerical convergence study

In this section, a numerical convergence study is conducted to determine the optimal discretization of numerical models. Deposition is not considered in this part of study. Firstly, we campare the bulk temperature, interface temperature, interface concentraction using different block number, *num-Li*, in the axial direction, as shown in Figure 3. As number of blocks increased in the axial direction, the numerical solutions tends to converge. At the pipeline outlet, bulk temperatures are -3.04, -3.34, -3.44 °C for *num-Li* equals to 1000, 3000, and 9000 respectively. We apply *num-Li=9000* for the discretization in the axial direaction.

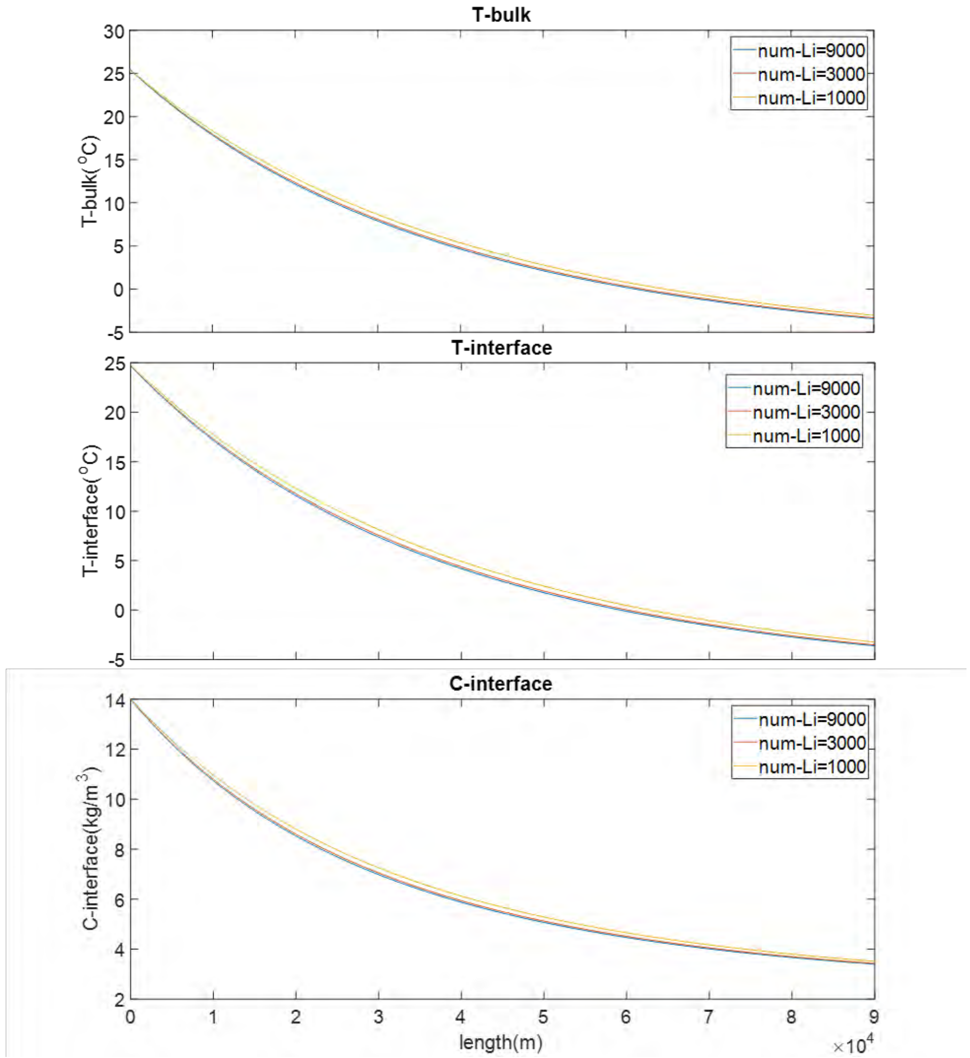


Figure 3: Comparison of bulk temperature, interface temperature, and interface wax concentraction with axial block number equals to 1000, 3000, and 9000

We campare the temperature profiles and concentraction profiles for num_R equals to 50, 100, 200, and 400 at 15000, 30000, 60000, and 90000 m, which are shown in Figure 4 and Figure 5. With increasing block number, the temperature and concnetraction tends to converge. This is consistent with the observations of Li *et al.* (2012), which stated that the cylindrical coordinate requires a large number of grid blocks to obtain a grid-independent solution in heat conduction problem. To achieve a relative accurate solution, nr=200 is used for the discretization in radial direction.

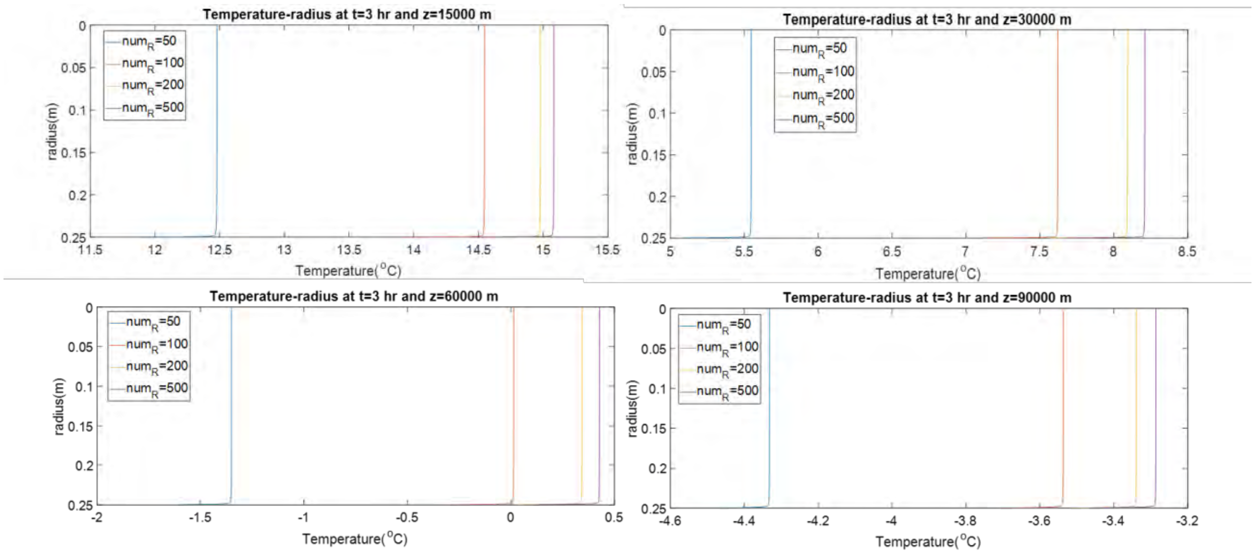


Figure 4: Comparison of temperature profile at 15000, 30000, 60000, and 90000 m with radial block number equals to 50, 100, 200, and 500

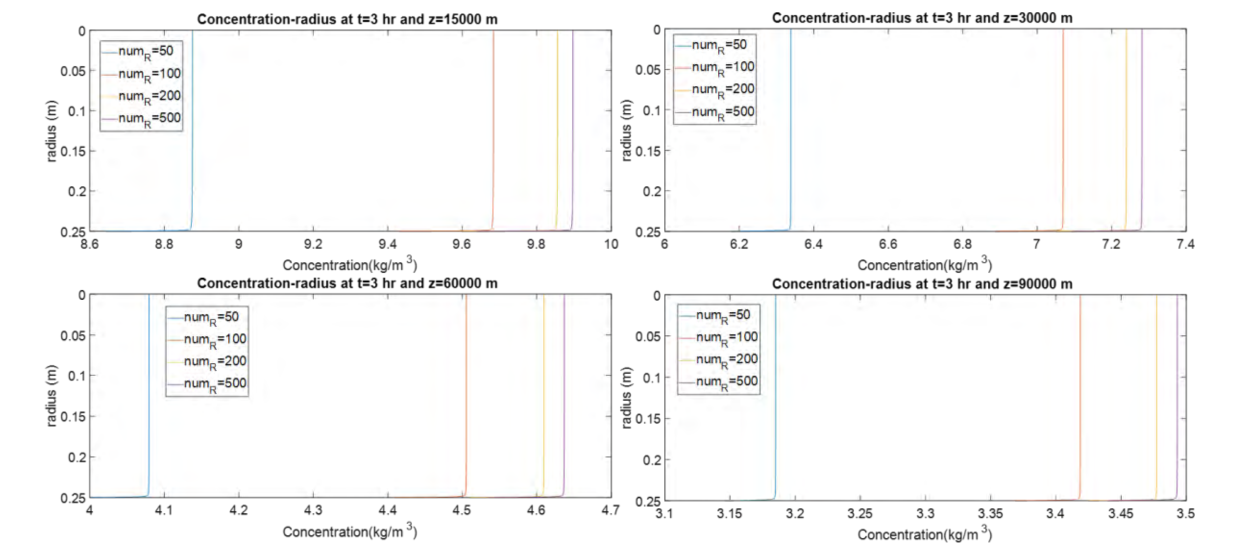


Figure 5: Comparison of concentration profile at 15000, 30000, 60000, and 90000 m with radial block number equals to 50, 100, 200, and 500

4.2 Case I:wax deposition

Figure 6 shows the axial profile of the predicted deposit thickness in the deposit. Three sections exist in the deposit profile, including no deposition, significant deposition, and insignificant deposition. In the no deposition zone (0 -1.3 km), the inner wall temperature is higher than wax appearance temperature. In the second section, the significant deposition zone, inner wall temperature drops below the WAT, which means wax molecules start to deposit in this section. A significant wax build up is observed in this section. In addition, wax deposition works as an insulation layer, reducing heat loss to the environment. Thus, the interface temperature increases as time passes by. For the loations where the interface temperature that is below WAT increase above WAT, wax deposition stops. In other words, as time passes by, the location where wax start to deposit moves to a downstream location. In the third section, due to the decrease of bulk temperature, riadial thermal gradient in the oil decreases. The driving force for wax deposition, which is the difference between bulk concentraction and interface concentration, decreases. Thus, deposition in this section is insignificant.

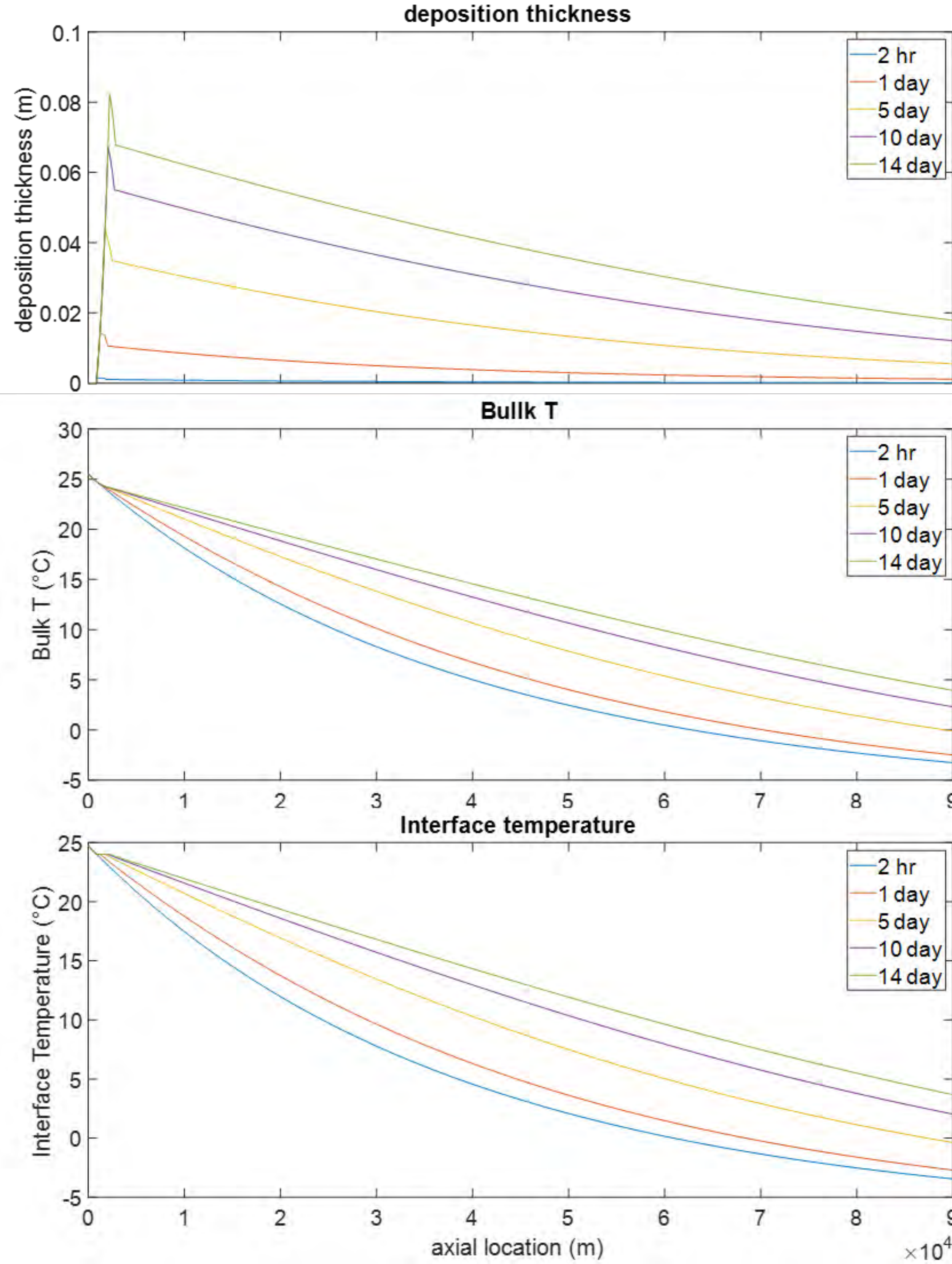


Figure 6: Prediction of the wax deposition thickness, bulk temperature, and interface temperature along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

Figure 7 shows the axial profile of the predicted wax fraction in the deposit. Similar to the thickness profile, the wax fraction has a maximum at the location where the driving force for aging reaches its maximum.

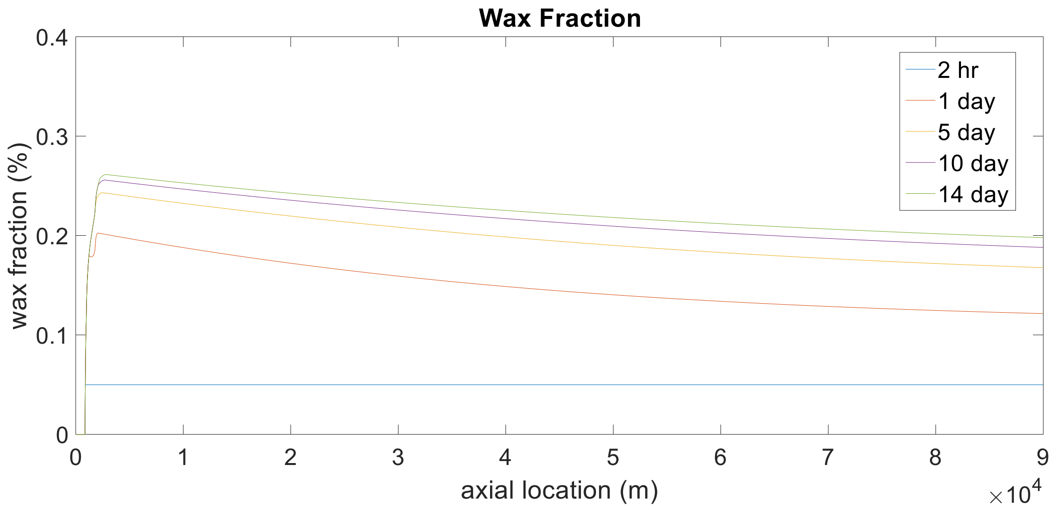


Figure 7: Prediction of the wax fraction along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

4.3 Case II: Ice deposition

If the interface temperature drops below water freezing point, ice may form. In the second case of this study, we assume wax deposition does not occure and only ice deposition occurs in the pipeline. Figure 8 shows the ice depsoiton thickness, along with the interface temperature and bulk temperature. Similar to the case of wax deposition, three sections exist in the deposition profile. In the no deposition zone, the inner wall termpature is higher than the water freezing point and thus no ice deposition is observed in this section. In the significant depsotion zone, where the driving force for ice deposition is high, the ice buildup has a mixumum in this section. In the insignificant deposition zone, ice deposition is insignificant.

By comparing with Case 1, it is found that the ice deposition rate is smaller than wax deposition rate. This is due to the smaller driving force for ice depsotion. The water concentraction and concentraction gradient are smaller than wax concentraiton and concnetration gradient. The bulk fluid temperature and interface temperature do not have a significant change compared with the wax deposition case. In the ice depsotion case, the deposition thickness is smaller than that of wax. In addition, thermal conductivity of ice is larger than that of wax (2.22 W/(m•K) for ice and 0.25 W/(m•K) for wax). Thus, the heat loss in the ice deposition case is faster than the one in the wax deposition case.

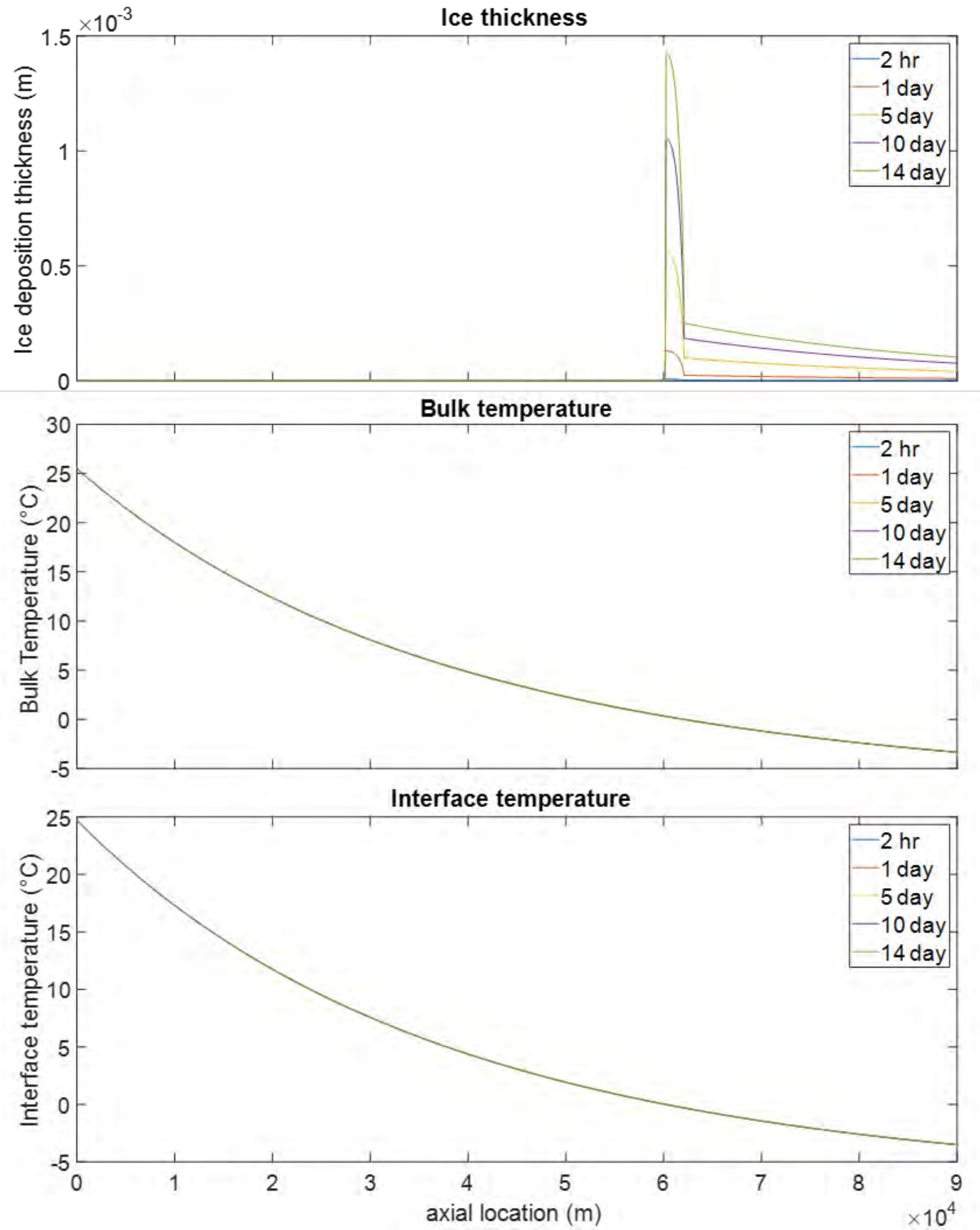


Figure 8: Prediction of the ice deposition thickness, bulk temperature, and interface temperature along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

Figure 9 shows the axial profile of the predicted ice fraction in the deposit. Similar to the thickness profile, the ice fraction has a maximum at the location where the driving force for aging reaches its maximum.

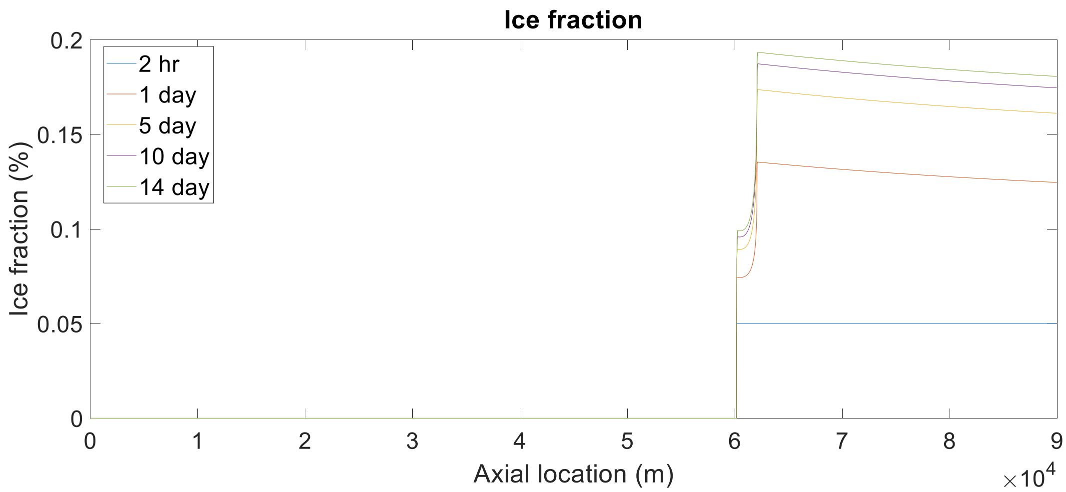


Figure 9: Prediction of the ice fraction in the ice depsotion along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

4.4 Case III: Wax-ice deposition

As oil travelled along pipeline, its temperature drops due to the heat exchange to the environment. If the fluid temperauter is below WAT but above the water freezing point, only wax depoiston occurs. If the oil travelled further and its temperature dropped below the water freezing point, both wax deposition and ice deposition occur. The interaction between these two solids exists in both the bulk fluid and deposition. To similfy the study, we assumed no ice particles in the bulk fluid due to the low concentration of water in this study. Similarly, it is assumed that wax particles do not have effects on water diffusions in the bulk. In the deposition, wax diffusion competes with water diffusion. The existence of either solid works as barriers for both wax and water diffusion in the deposition. In addition, the thermal conductivity of the deposit needs to consider the coexistence of wax and ice in the deposition.

Figure 10 shows the the axial profile of the predicted deposit thicknes, as well as the interface temperature and bulk temperature. Figure 11 shows the axial profile of the predicted wax deposition thickness, ice deposition thickness and total deposition thickness in the deposit. The total deposit thickness is the summation of wax deposition thickness and ice deposition thickness.

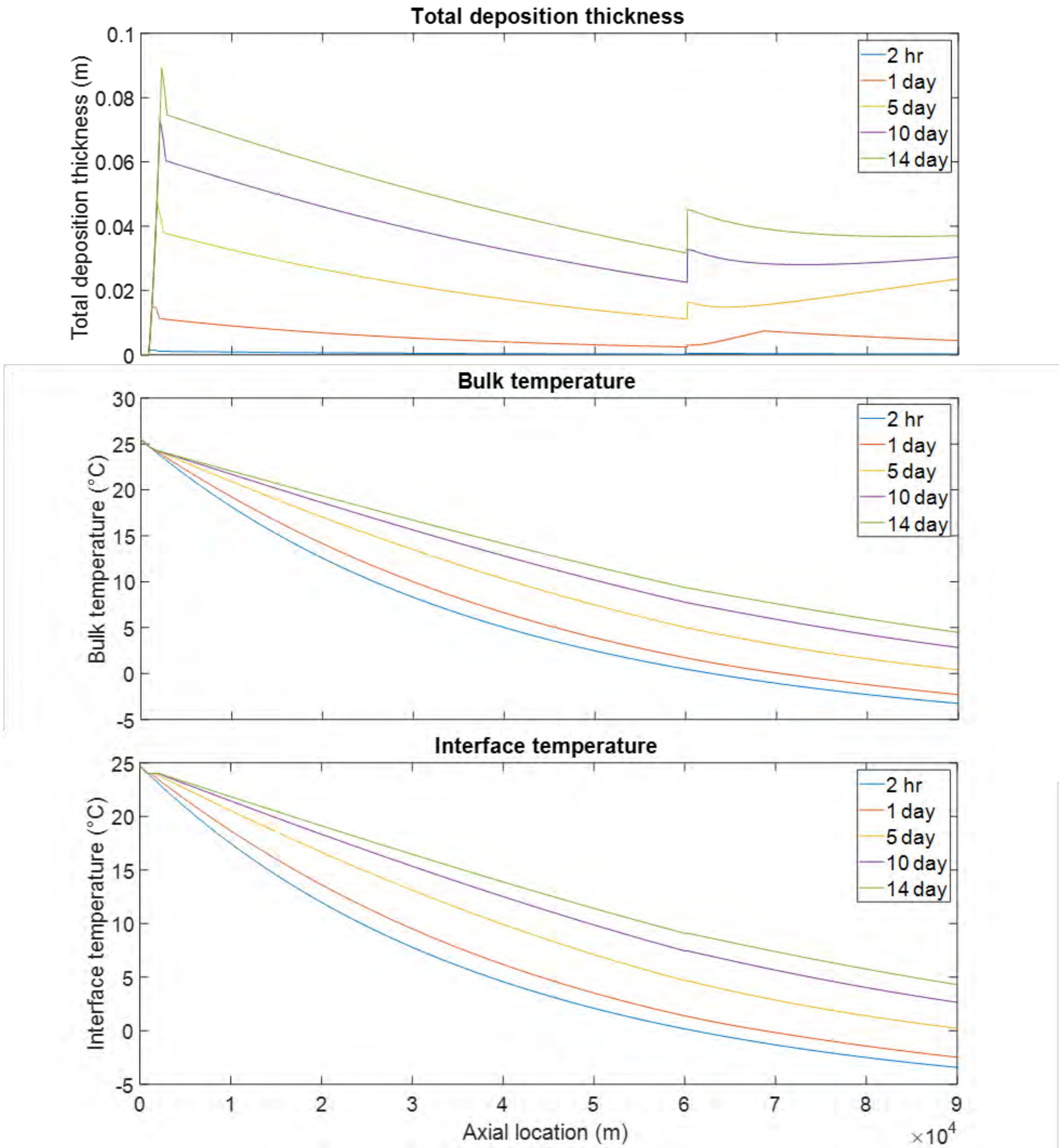


Figure 10: Prediction of the total deposition thickness, bulk temperature, and interface temperature along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

Five sections exist in the deposition profile, including 1) no deposition, 2) significant wax deposition without ice depsotion, 3) insignificant wax deposition without ice depsotion, 4) significant ice depsotion in addition to wax deposition, and 5) insignificant ice deposition in addition to wax deposition. In the no deposition zone, the inner wall temperature is higher than wax appearance temperature. As fluid travels along the pipline with more heat loss to the environment, inner wall temperature dropes below wax appearance temperature but higher than water freezing point, which indicates only wax deposition occurs. Section with sifnificatn wax deposition is first observed, followed by section with insignificant wax deposition. The deposition thickness and aging in the deposit are similar to those studied in Case I.

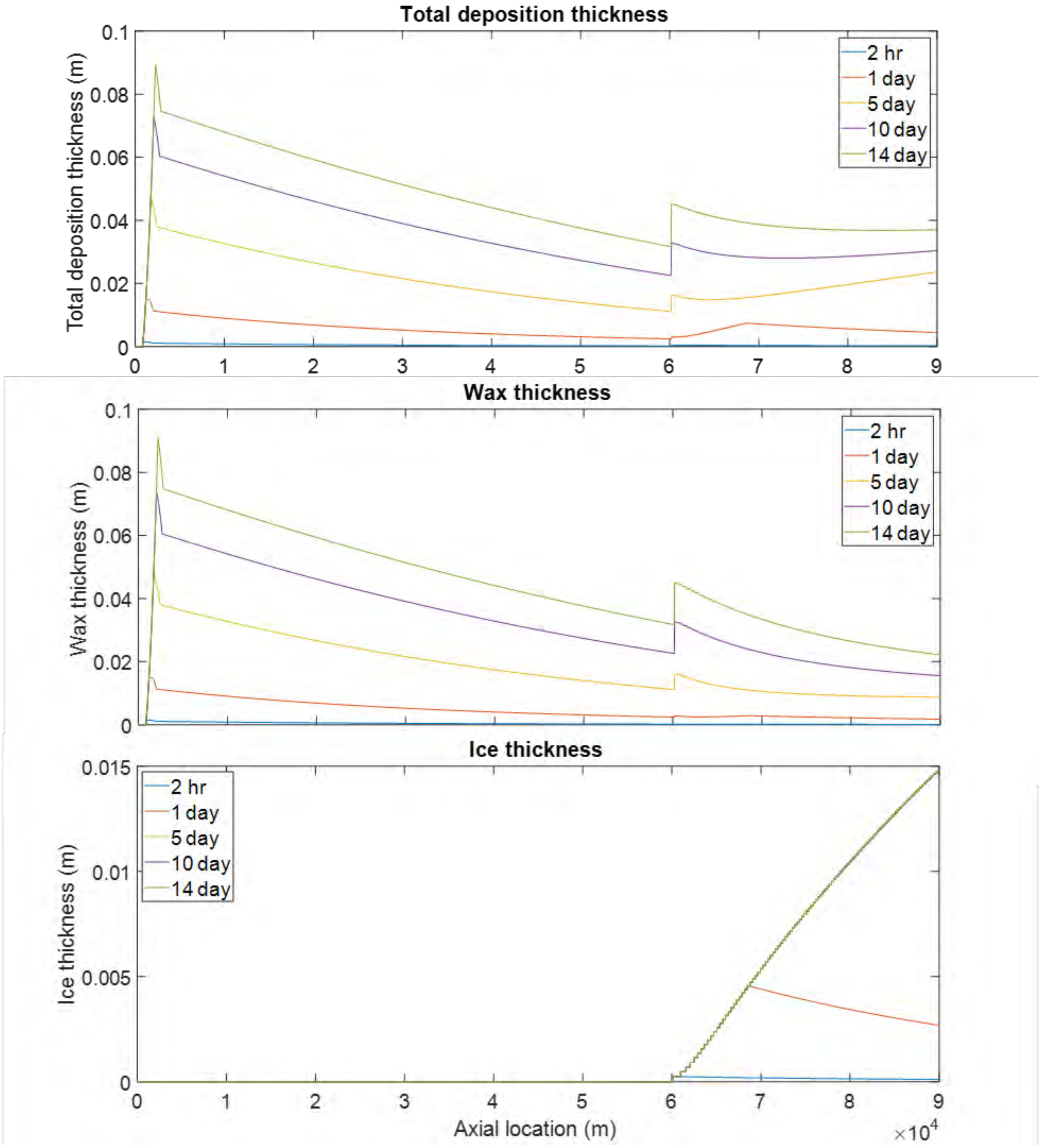


Figure 11: Prediction of the total deposition thickness, wax deposition thickness and ice deposition thickness along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

As the fluid travels further entering the fourth zone, its temperature can drops below ice freezing point, which can cause ice depsotion in addition to wax deposition. In the fourth section, significant ice deposition is observed. Unlike the ice depsotion in Case II, the competion between wax diffusion and water diffusion in the deposit, causes the ice fraction to be smaller, indicating the amount of water molecule diffused into the deposit is smaller. The decreased inner diffusion rate causes more water molucles to stay at the deposition interface, contributing to a larger ice depsotion thickness. Similarly, the decreasing inner wax diffusion rate causes a smaller wax fraction in the deposition and larger wax depsotion thickness than the ones in Case I.

Similar to Case I, the formed wax deposition along the pipeline decreased the heat loss to the environment, resulting in the increase of interface temperature and bulk tempture with time. Thus, at different times, the starting points for either wax deposition or the ice depsotion change to a further locations downstream. Especially for ice deposition, after day 5, the interface temperature along the pipeline is above water freezing point, resulting in no further ice formation. Thus, the ice thickness remained unchanged after day 5.

Figure 12 shows prediction of the total solid fraction, wax fraction and ice fraction along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days. In the zone that only have wax deposition, the total solid fraction is equal to wax fraction. In this case, it is similar to Case I. When ice start to deposit, the solid fraction is the summation of wax fraction and ice fraction in the deposit. The existence of the two solids in the deposit poses barriers for internal diffusion in the deposite. The aspect ratio in the section with both ice and wax formation is larger than the cases with only wax deposition or ice deposition. Thus, both wax and ice fractions in the deposit do not increase as fast as the one in Case I or II. Due to the decreasing internal diffusion in the deposit, the growth rate, which is the difference of bulk diffusion rate and internal diffusion rate increased in the section that has both wax and ice deposition.

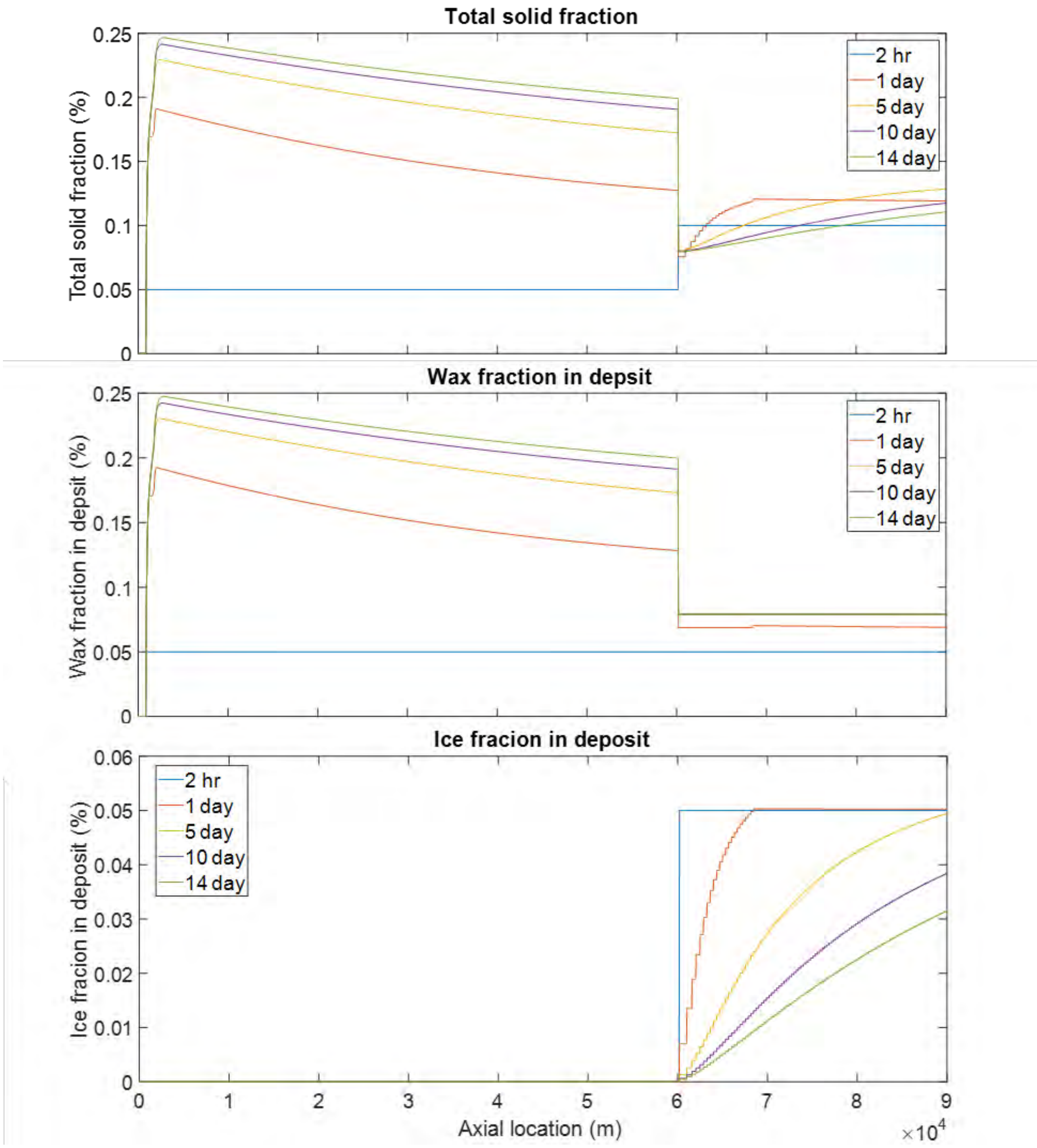


Figure 12: Prediction of the total solid fraction, wax fraction and ice fraction along the pipe at 2 hours, 1 day, 5 days, 10 days and 14 days

5. Conclusions

In this study, we developed a model base on molecular diffusion to predict wax, ice and wax-ice deposition in a pipeline with ambient temperature below water freezing point. Use three case studies, it was found that wax deposition rate is faster than ice depsoiton rate, due to the larger wax concentractio and concentraction gradient in wax deposition case. In addition, the coexistence of wax and ice deposition can lead to a more complicated deposition profile. In addition to section with only wax deposition zone, the depsotion zone mixed with wax and ice shows a competition between wax and water diffuiosn in the deposit, which slows down the solid fraction increase in the deposit. In the meanwhile, due to the decreasing internal diffusion rate, the total growth rate increases, which lead to a higher depsotion thickness than the cases with only wax or ice deposition.

References

Aiyejina, A., Chakrabarti, D. P., Pilgrim, A., & Sastry, M. (2011). Wax formation in oil pipelines: A critical review. *International journal of multiphase flow, 37*(7), 671-694.

Alyeska Low Flow Impact Study Team. (2011, 15 June 2011). Low Flow Impact Study FINAL REPORT. Retrieved from http://www.alyeska-pipe.com/assets/uploads/pagestructure/TAPS_Operations_LowFlow/editor_uploads/LoFIS_Summary_Report_P6%2027_FullReport.pdf

Aris, R. (1985). On the permeability of membranes with parallel, but interconnected, pathways. *Mathematical biosciences, 77*(1-2), 5-16.

Burger, E., Perkins, T., & Striegler, J. (1981). Studies of wax deposition in the trans Alaska pipeline. *Journal of Petroleum Technology, 33*(06), 1,075-071,086.

Chhabra, R. P., & Richardson, J. F. (2011). *Non-Newtonian flow and applied rheology: engineering applications*: Butterworth-Heinemann.

Comfort, G., Dinovitzer, A., Lazor, R., & Hinnah, D. (2008). *Offshore arctic pipeline oil spill risk assessment.* Paper presented at the 2004 international pipeline conference.

Cooper, W. A., Sand, W. R., Veal, D., & Politovich, M. (1984). Effects of icing on performance of a research airplane. *Journal of Aircraft, 21*(9), 708-715.

Deen, W. M. (1998). *Analysis of transport phenomena* (Vol. 2): Oxford University Press New York.

DeMott, P. J., Finnegan, W. G., & Grant, L. O. (1983). An application of chemical kinetic theory and methodology to characterize the ice nucleating properties of aerosols used for weather modification. *Journal of Climate and Applied Meteorology, 22*(7), 1190-1203.

Driest, E. V. (1956). On turbulent flow near a wall. *Journal of the aeronautical sciences, 23*(11), 1007-1011.

Gautier, D. L., Bird, K. J., Charpentier, R. R., Grantz, A., Houseknecht, D. W., Klett, T. R., . . . Schuenemeyer, J. H. (2009). Assessment of undiscovered oil and gas in the Arctic. *Science, 324*(5931), 1175-1179.

Grozdek, M., Khodabandeh, R., & Lundqvist, P. (2009). Experimental investigation of ice slurry flow pressure drop in horizontal tubes. *Experimental Thermal and Fluid Science, 33*(2), 357-370.

Han, S., Huang, Z., Senra, M., Hoffmann, R., & Fogler, H. S. (2010). Method to determine the wax solubility curve in crude oil from centrifugation and high temperature gas chromatography measurements. *Energy & Fuels, 24*(3), 1753-1761.

Huang, Z., Lee, H. S., Senra, M., & Scott Fogler, H. (2011). A fundamental model of wax deposition in subsea oil pipelines. *AIChE Journal, 57*(11), 2955-2964.

Johnstone, R. L. (2014). *Offshore oil and gas development in the Arctic under international law: risk and responsibility*: Martinus Nijhoff Publishers.

Kaiser, B. A., Fernandez, L. M., & Vestergaard, N. (2016). The future of the marine Arctic: Environmental and resource economic development issues. *The Polar Journal, 6*(1), 152-168.

Khan, F., Ahmed, S., Yang, M., Hashemi, S. J., Caines, S., Rathnayaka, S., & Oldford, D. (2015). Safety challenges in harsh environments: Lessons learned. *Process Safety Progress, 34*(2), 191-195.

Kim, C. K., Stuefer, M., Schmitt, C. G., Heymsfield, A., & Thompson, G. (2014). Numerical modeling of ice fog in interior Alaska using the weather research and forecasting model. *Pure and Applied Geophysics, 171*(8), 1963-1982.

Li, W., Yu, B., Wang, X., Wang, P., & Sun, S. (2012). A finite volume method for cylindrical heat conduction problems based on local analytical solution. *International Journal of Heat and Mass Transfer, 55*(21-22), 5570-5582.

Messinger, B. L. (1953). Equilibrium temperature of an unheated icing surface as a function of air speed. *Journal of the aeronautical sciences, 20*(1), 29-42.

Myers, T. G., & Charpin, J. P. (2004). A mathematical model for atmospheric ice accretion and water flow on a cold surface. *International Journal of Heat and Mass Transfer, 47*(25), 5483-5500.

Niezgoda-Żelasko, B., & Zalewski, W. (2006a). Momentum transfer of ice slurry flows in tubes, experimental investigations. *International journal of refrigeration, 29*(3), 418-428.

Niezgoda-Żelasko, B., & Zalewski, W. (2006b). Momentum transfer of ice slurry flows in tubes, modeling. *International journal of refrigeration, 29*(3), 429-436.

Pletcher, R. H., Tannehill, J. C., & Anderson, D. (2012). *Computational fluid mechanics and heat transfer*: CRC press.

Singh, P., Fogler, H. S., & Nagarajan, N. (1999). Prediction of the wax content of the incipient wax-oil gel in a pipeline: an application of the controlled-stress rheometer. *Journal of Rheology, 43*(6), 1437-1459.

Sunne, S. (2015). Ice may delay restart of pipeline's breached Montana section. Retrieved from http://www.reuters.com/article/us-bridgerpipeline-oilspill-idUSKBN0KS1VE20150120

Walker, M. (2002). The science of weather: What's the difference between 'rime','glaze'and 'hoar frost'? *Weather, 57*(4), 143-143.

Xu, H., Bbosa, B., Pereyra, E., Volk, M., & Mannan, M. S. (2018). Oil transportation in pipelines with the existence of ice. *Journal of Loss Prevention in the Process Industries, 56*, 137-146.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

External Fire Impacts on the Interior Temperature of a Building

Benjamin R. Ishii* and Cristian Jimenez
Quest Consultants Inc. ®
Norman, Oklahoma
*Presenter E-mail: bri@questconsult.com

Abstract

Facility siting studies are an important part of process safety, and are required for facilities that fall under OSHA's PSM program. Facility siting is frequently interpreted as performing a building siting study which adheres to the guidance given in API RP 752. The guidance recommends that all occupied buildings be evaluated for fire impacts. Both jet fires and pool fires can create a significant thermal radiative flux on buildings and are routinely evaluated in siting studies. Buildings that may be impacted by thermal fluxes exceeding threshold values often require an advanced analysis, especially when a non-flammable building may experience a high flux for a short duration. For these scenarios, the interior temperature rise, rather than structural impacts, may be the dominant occupant threat. This paper explores the impacts of an external fire on the interior temperature of a building. The Fire Dynamics Simulator (FDS), a computational fluid dynamics (CFD) code, is applied to this scenario.

Keywords: CFD, jet fire, pool fire, thermal hazard, building siting

1 INTRODUCTION

Protection of plant personnel for facility siting purposes is typically addressed through the application of the American Petroleum Institute (API) recommended practice (RP) 752[1], which is primarily focused on the location and vulnerability of occupied buildings. These buildings, where personnel carry out their duties, are assumed (within the context of API RP 752) to provide some protection from accidents that may occur at the facility. However, the potential effects on personnel in buildings are highly dependent on the way the equipment and processes are laid out within the facility, the type of building construction, and the distribution of buildings within the plant boundaries, specifically their proximity to hazardous chemicals at the plant.

An analysis conducted to satisfy API RP 752 generally should include three classes of hazards:

- Explosion overpressure or blast wave exposure
- Fire radiation exposure, including pool fires, jet fires, and exposure to an ignited flammable vapor cloud (flash fire)
- Toxic gas exposure

The focus of this work addresses internal temperature rise in buildings due to exposure from fire radiation.

2 FIRE RADIATION IMPACTS

Occupied buildings can be impacted by many forms of fire radiation including:

- Fireballs due to instantaneous releases of flammable fluids, including boiling liquid expanding vapor explosions (BLEVEs)
- Vapor cloud fires (flash fires) due to a release that forms a flammable vapor cloud
- Jet (torch) fires due to continuous, pressurized releases of flammable fluids
- Pool fires due to pooled releases of flammable liquids

The vulnerability of building occupants to fire radiation is certainly mitigated by the building being a physical barrier to the direct effects of fire radiation. However, there are several concerns for the building itself that affect occupant vulnerability:

- Building materials that are combustible could be ignited if the radiative flux and exposure duration are sufficient;
- The integrity of non-combustible materials can be compromised due to degradation or deformation following exposure to radiative heat flux for a sufficient exposure time, resulting in building collapse; or,
- The increased temperature of the building shell exposed to thermal radiation results in a significantly increased interior temperature.

In cases where the building is exposed to thermal radiation and the building does not ignite, there is a possibility for the interior air temperature to increase such that the environment is inhospitable to building occupants. The internal air temperature is a function of the building properties, exposure time, and the intensity of the incident thermal radiation. The vulnerability of building occupants depends on the elevated temperature, the exposure duration, and humidity.

In all cases of exposure to thermal radiation, the magnitude of the radiative flux and the duration of exposure are equally important variables. The principle behind this, whether the exposure is burns to a person's skin, ignition of wood, or weakening of structural steel, is the temperature rise that occurs. For building interior temperatures, the principles are the same; the flux, magnitude, and exposure duration affect the building shell such that the interior temperature rises.

3 BUILDING SITING

The methodology and tools available for safety siting studies are generally well known within the process safety community. The methodology can be structured as a staged process that allows the study to stop at multiple points when the analysis shows that the impacts, or risk, to the subject population (building occupants) is found to be tolerable. These methodologies have been summarized in several published papers[2] [3].

The specifics of radiative loading on buildings has been addressed by various international agencies[4] [5] [6]. In these publications, the vulnerability of building occupants was estimated using a fixed value of thermal radiation (e.g., 35 kW/m^2) without any mention of the duration of exposure.

Recent studies have shown that building structures may be able to withstand higher levels of thermal radiation (above 35 kW/m^2) without losing structural integrity[7][8]. However, higher radiation values and/or longer durations may impact the temperature in buildings such that occupants are put in danger from hyperthermia or hyperpyrexia. The cutoff between the hyperthermia and hyperpyrexia is distinguished by a core temperature of 41 ºC[9]. Humans can withstand higher temperatures for short durations. For example, many people enjoy 5 minute stays in saunas, which are kept at approximately 80 ºC. The physiological impact is better described as a function of air temperature, humidity, and duration. But for the purposes of this paper, the simple threshold of 41 ºC is sufficient.

In addition previous work has been performed to show that CFD models can predict temperature rise in buildings due to external heat loads. Chakrabarty et al. utilized CFD models to compare temperature rise in a blast resistant module to a concrete masonry building, where both buildings were exposed to external thermal radiation[10]. Raibagkar and Edel modeled internal building temperatures due to thermal radiation exposure to the sides and top of a building[11].

4 CFD Software

The fire dynamics simulator (FDS) is a computational fluid dynamic CFD software developed by the National Institute of Standards and Technology (NIST). FDS began as a finite difference model of fire driven fluid flows. The software also computes thermal radiation transport equations using a finite volume technique. A full description of the model is given in the FDS Technical Reference Guide[12].

In FDS heat is transferred through convection, conduction, and radiation. FDS employs a 3-dimensional mesh to simulate convection, fluid flow, etc., but in some cases a one dimensional simulation can increase the speed of the calculation, as is the case for conduction through solids. By default FDS simplifies heat conduction through solids by simulating one dimensional heat conduction. FDS solves the following equation:

$$\rho c_p \frac{\partial T}{\partial t} = \frac{\partial}{\partial x}\left(k \frac{\partial T}{\partial x}\right) + q$$

Where

ρ = Density

c_p = Heat capacity

k = Conductivity

q = Rate of energy from chemical reactions and radiative absorption

5 Numerical Modeling

Two buildings were modelled with FDS. The first building was modelled as a concrete building with metal doors, similar to the building modelled by Raibagkar. The second building was modelled with the same metal doors, but the walls and ceiling are constructed with a skin of metal, insulation, and gypsum board. The physical properties of the materials used in the modeling are presented in Table 1. For the concrete building, the ceiling consisted of 50.8 mm (2 in) concrete and the concrete walls consisted of 152 mm (6 in) of concrete. All doors in this study were modelled as one inch of insulation sandwiched between two layers of 18 gauge steel. For the insulated metal building, the walls and ceilings of the metal building consisted of 24 gauge steel, 88.9 mm (3.5 in) of insulation, and 12.7 mm (0.5 in) of drywall or gypsum board.

Both buildings are 13 m by 7 m and 4.5 m tall. Each building has two doors located on the opposite long sides of the building. The building is illustrated in Figure 1.

Table 1. Properties of Building Materials

Material	Specific Heat [kJ/kg K]	Conductivity [W/m K]	Density [kg/m3]
Concrete	1.04	1.8	2280
Steel	0.46	45.8	7850
Insulation	1.7	0.05	28
Gypsum Board	0.95	0.19	700

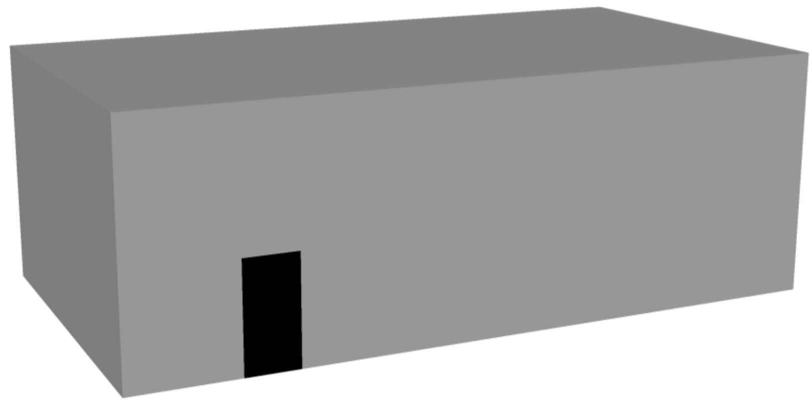


Figure 1. 3-Dimensional View of Building

In the study performed by Raibagkar all sides and the top of the building were exposed to thermal loads. In most fire scenarios, only one to three faces of a building are exposed to thermal radiation at one time. One face of the building exposed to a constant and even level of thermal radiation was applied to this study to simulate a more realistic single fire scenario. Both buildings were exposed to thermal radiation on one 13m by 4.5 m wall. The metal building was exposed to 35 kW/m^2 for one hour. The concrete building was modelled with the following thermal radiant levels for one hour.

- 35 kW/m^2
- 50 kW/m^2
- 75 kW/m^2
- 100 kW/m^2

The model did not account for smoke generation, smoke infiltration, or fire impingement. The scope of this paper is focused solely on occupant vulnerability due to the interior temperature of the modeled buildings.

6 RESULTS

Figure 2 shows the rise of the internal air temperature due to thermal flux on a single face of a concrete building. The temperature is measured in the center of the building at a height of 1.8 meters. All four curves show that there is about a 350 second delay in the temperature rise. The results show that the internal temperature exceeds 41 ºC for exposure to 50 to 100 kW/m^2 at the end of one hour.

Figure 3 presents the temperature history at the center of the building at 1.8 m height, the interior face of the wall, and the interior face of the door for a concrete building exposed to 35 kW/m^2. The data shows that the heat transfer is dominated by the metal door in the first 20 minutes and then the wall drives the rise in temperature.

The results of an insulated building with metal siding with one face exposed to 35 kW/m^2 is presented in Figure 4. Again the results show a similar 350 second delay in temperature rise in air temperature as also shown in Figure 2. The results show that the temperature rises to 45 ºC after one hour. The heat transfer is dominated by the door for the first 10 minutes and the interior wall temperature exceeds the interior door temperature between 15 and 20 minutes after the scenario begins.

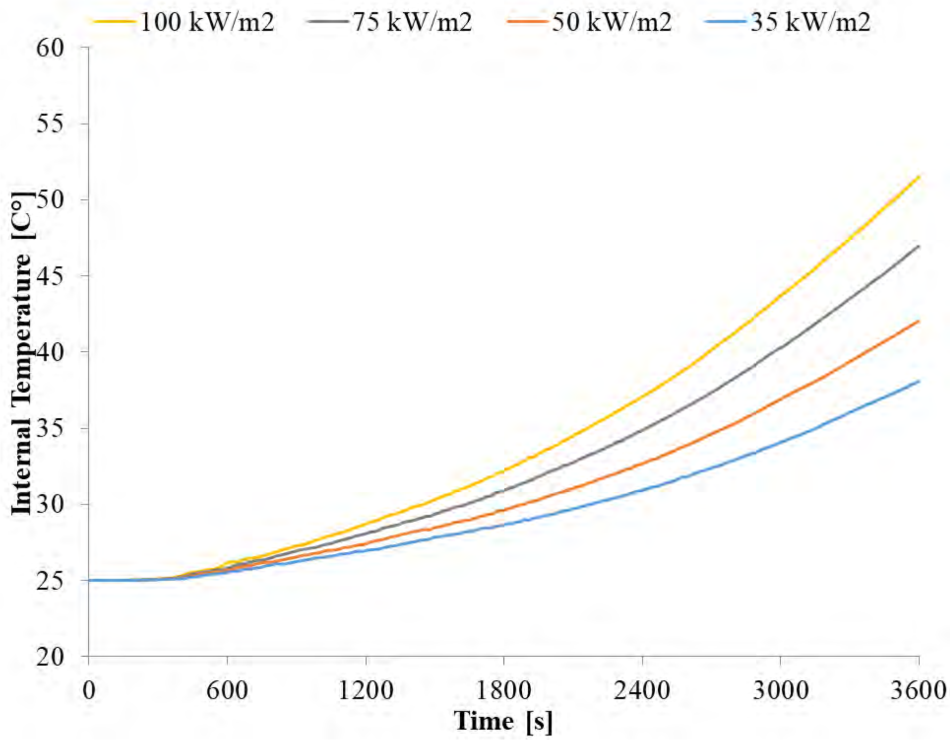


Figure 2
Internal Temperature of a Concrete Building with One Side Exposed to Thermal Radiation

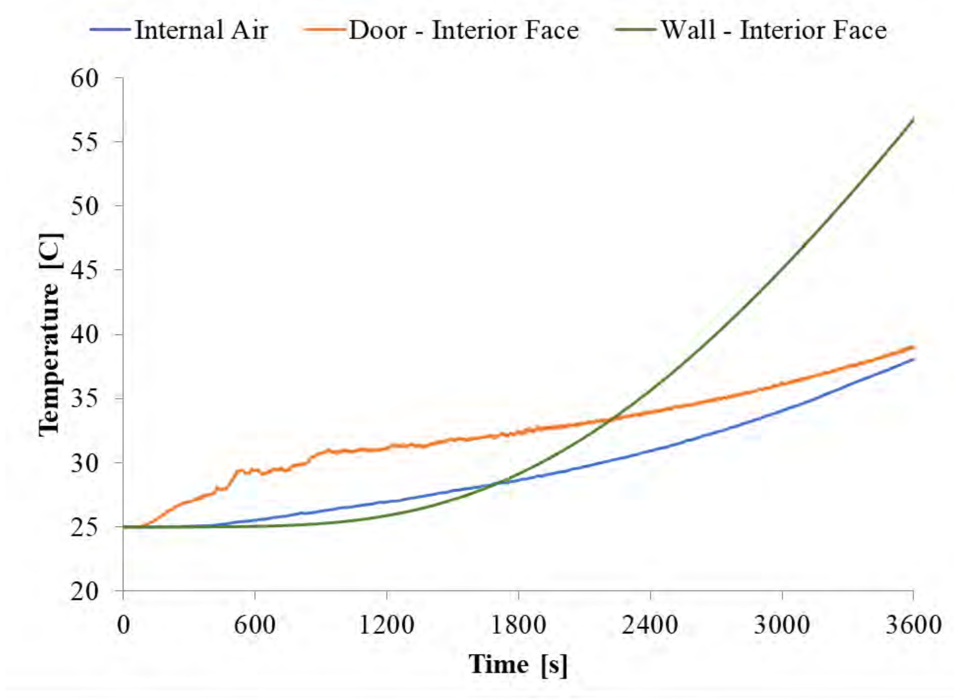


Figure 3
Temperatures in a Concrete Building with One Side Exposed to 35 kW/m^2

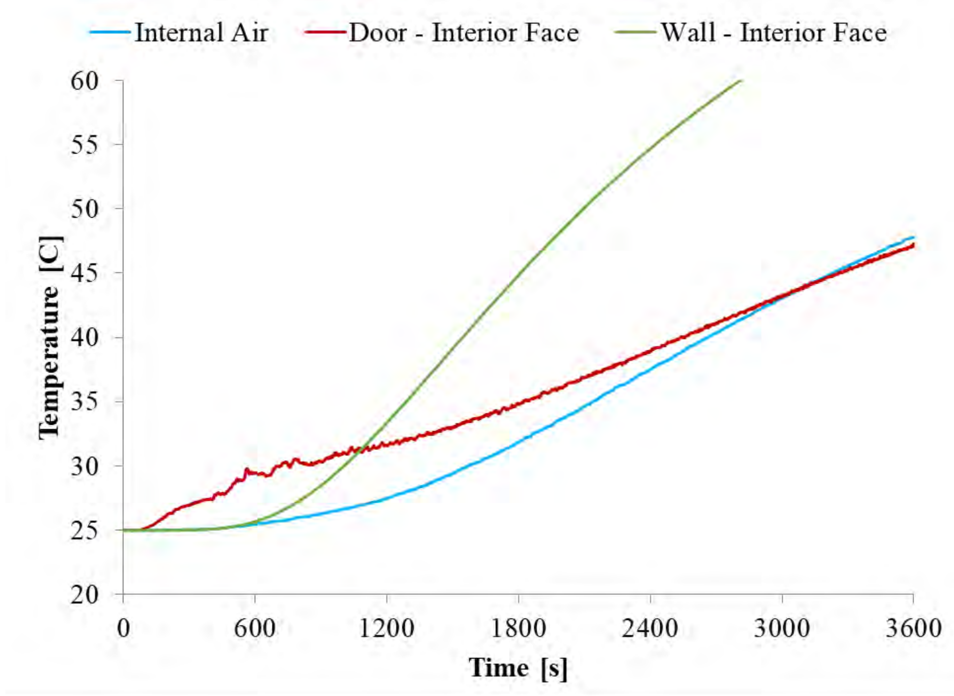


Figure 4
Temperatures in a Metal Building with One Side Exposed to 35 kW/m^2

7 Conclusion

Based on the analysis results provided above, the following conclusions and observations are drawn:

- CFD tools, such as FDS, can successfully model the temperature rise in a building due to exposure to thermal radiation from a fire.
- Buildings with non-flammable exteriors may offer occupants shielding from high levels of fire radiation (greater than 35 kW/m^2) especially for short durations.
- The protection that building may provide occupants depends on the building materials.
- Building siting and shelter in place designation should consider the duration and intensity of potential fires.

8 REFERENCES

[1] API (2009). *Management of Hazards Associated with Location of Process Plant Permanent Buildings*. API Recommended Practice 752, American Petroleum Institute, 1220 L Street, Northwest, Washington, D.C. 20005, Third Edition, December 2009.

[2] Marx, J. D., and Ishii, B. R. (2016), *A Comprehensive Approach to API RP 752 and 753 Building Siting Studies,* Journal of Loss Prevention in Process Industries, Volume 44, November 2016, pages 748-754.

[3] Cornwell, J. B., and Ishii, B. R. (2018), *What API RP 752 Does Not Tell You – But People Will Ask*, Presented at the 14th Annual Global Congress on Process Safety, Orlando, FL, April 2018.

[4] Technica, Ltd. (1988). *Techniques for Assessing Industrial Hazards*. World Bank technical paper number 55, prepared by Technica, Ltd., London, England, 1988.

[5] TNO (1989), *Methods for the Determination of Possible Damage to People and Objects Resulting from Releases of Hazardous Materials* (the Green Book). The Netherlands Organization of Applied Scientific Research, Voorburg, The Netherlands, December, 1989.

[6] TNO (2005), *Guidelines for Quantitative Risk Assessment* (the Purple Book). CPR 18E, the Netherlands Organization for Applied Scientific Research, Committee for the Prevention of Disasters, The Hague, Netherlands, 2005.

[7] Marx, et. al. (2018), *Radiant Heat Flux Impact Criteria for API RP 752 Building Siting Studies*, Presented at the 14th Annual Global Congress on Process Safety, Orlando, FL, April 2018.

[8] Marx, et. al. (2018), *Evaluating the Transient Radiant Heat Flux Impacts to Occupied Buildings*, Presented at the Mary Kay O'Connor Process Safety Center International Symposium, College Station, TX, October, 2018

[9] Sharma, H.S. (2011), Neurobiology of Hyperthermia. Volume 162 of Progress in Brain Research, Elsevier.

[10] Chakrabarty, A., Edel, M., Raibagkar, A., Aloqaily, A. (2011), *Thermal Hazard Evaluation for Process Buildings Using CFD Analysis Techniques,* Presented at the 7th Annual global Congress on Process Safety, Chicago, IL.

[11] Raibagkar, A., Edel, M. (2013), *Impact of Thermal Hazards on Process Buildings Using CFD Techniques,* Presented at the ASME 2013 Pressure Vessels and Piping Conference, Paris, France, July 2013.

[12] FDS - McGrattan, K.B., et al. "Fire Dynamics Simulator: Technical Reference Guide." NISTIR.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Experimental Study of an Iron-Based Metal-Organic Framework as Flame Retardant for Poly (methyl methacrylate) (PMMA)

Elizabeth Joseph, Ruiqing Shen*, Qingsheng Wang, and Hongcai Zhou
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University System
College Station, Texas 77843-3122, USA
Department of Chemistry
Texas A&M University
College Station, Texas 77843-3255, USA
*Presenters' E-mail: ruiqing@tamu.edu, qwang@tamu.edu

Abstract

Poly (methyl methacrylate) (PMMA) is a kind of widely used thermoplastic in the family of poly (acrylic ester)s due to its good mechanical properties, like good moldability, high resistance to UV light and weathering, high strength, and excellent dimensional stability. However, PMMA is also characterized by limited heat resistance, poor thermal stability, and high flammability. Metal-organic frameworks (MOFs) are a new class of porous materials, which possess unique physicochemical properties and have attracted considerable interests from different fields, such as energy, gas storage and separation, and catalysis. Additionally, because of their inorganic−organic hybrid nature, MOFs are usually compatible with polymers to form composites. PCN-250 is an iron-based MOF with nitrogen-containing structure and it is chemically stable and physically robust. So far, it can be economically synthesized in large scale. In this study, PCN-250 is used as a potential flame retardant for PMMA. To evaluate the performance of PCN-250 with different concentrations, the thermostability and flame retardancy of the PMMA composites are systematically investigated using thermal gravimetric analysis (TGA) and cone calorimetry. This study will give us some insight about the application of MOFs as a new kind of flame retardant to enhance and improve the fire safety of polymer materials.

Keywords: Polymerization, Flammability

Introduction

The polymeric materials provide numerous advantages to society in everyday life, like being versatile, light weight, corrosion-resistant, electrically insulating, and easily processable. They are widely used almost everywhere in buildings, housing, vehicles, aircraft, commercial products etc. However, the high flammability is an obvious disadvantage related to many synthetic polymers, due to their energy-dense hydrocarbon-based nature, which is exposing life safety to more fire hazards [1]. Improving the fire retardancy of polymeric materials is an increasingly important strategy to limit their flammability by adding some flame retardant fillers to the polymers. With a relatively low loading of well dispersed nanoscale flame retardant fillers, the nanocomposites have been found to be able to achieve better thermal stability and performance in a fire, while still maintaining or even improving their mechanical properties [2]. So far, various inorganic nanoscale fillers have been investigated to enhance the flame retardancy of different polymers, like clay [3], graphite [4], metal oxide nanoparticles [5], carbon nanotube [6, 7], and spherical silica [8, 9]. However, for these inorganic nanoscale fillers, they act mostly in the condensed phase by transporting to the surface to forma thermally stable ceramic surface layer and/or promoting the formation of char layer during the flaming combustion of polymers. These protective layers act as a thermal shield to block heat transfer to the polymer and as a barrier to oxygen transfer from flame to the polymer underneath and of degradation products from the polymer to the flame. Through this behavior, the intensity of fire can be reduced noticeably by prolonging the burning process, but for most flame retardant polymer nanocomposites, their total heat release does not change much.

Metal-organic frameworks (MOFs) have received much attention in recent years especially as newly developed porous materials. MOFs are essentially formed by connecting together metal ions with polytopic organic linkers together through coordination bonds and other weak interactions or noncovalent bonds (H-bonds, p-electron stacking, or van der Waals interactions) [10]. Due to the inorganic-organic hybrid nature, MOFs usually have better compatibility with polymers to form polymer composites. Thermal degradation of MOFs is an endothermic process associated with node–linker bond breakage. When being exposed to heat, MOFs not only absorb more heat by their endothermic degradation process, but also decompose the metal-containing units and the organic ligands in this process to release metallic oxides in the condensed phase and gaseous products in the vapor phase. In this condensed phase, these metallic oxides left, especially transitional metals, may be able to quickly from C-C bonds during burning, thus helping convert flammable polymers into thermally stable carbon char [11]. Additionally, if properly designed to contain the elements of oxygen, nitrogen, or phosphorous, the gaseous products can work as smoke suppressants and contribute to reduce the concentration of combustion supporters in the gaseous phase. Through these strong synergistic effect among different flame retardant mechanisms discussed above, NOFs-based polymer composites have the potential to achieve better flame retardancy and thermal stability. However, few research has been conducted in this area.

Poly (methyl methacrylate) (PMMA) is a kind of widely used thermoplastic in the family of poly (acrylic ester)s due to its good mechanical properties, like good moldability, high resistance to UV light and weathering, high strength, and excellent dimensional stability. However, PMMA is also characterized by limited heat resistance, poor thermal stability, and high flammability. PCN-250 is an iron-based MOF with nitrogen-containing structure and it is chemically stable and physically robust. So far, it can be economically synthesized in large scale. In this study, PCN-250 is used as a potential flame retardant for PMMA. To evaluate the performance of PCN-250 with different concentrations, the thermostability and flame retardancy of the PMMA composites are systematically investigated using thermal gravimetric analysis (TGA)/differential scanning calorimeter (DSC) and cone calorimetry.

Experimental

References

1. Bellucci, F.; Camino, G.; Nicolais, L., Flammability of Polymer Composites. In Wiley Encyclopedia of Composites, John Wiley & Sons, Inc.

2. Morgan, A. B., & Wilkie, C. A. (Eds.). (2007). Flame retardant polymer nanocomposites. John Wiley & Sons.

3. Pavlidou, S.; Papaspyrides, C. D., A review on polymer-layered silicate nanocomposites. Progress in Polymer Science 2008, 33, (12), 1119-1198

4. Uhl, F. M., Yao, Q., Nakajima, H., Manias, E., & Wilkie, C. A. (2005). Expandable graphite/polyamide-6 nanocomposites. Polymer Degradation and Stability, 89(1), 70-84.

5. Friederich, B.; Laachachi, A.; Ferriol, M.; Ruch, D.; Cochez, M.; Toniazzo, V., Tentative links between thermal diffusivity and fire-retardant properties in poly(methyl methacrylate)-metal oxide nanocomposites. Polymer Degradation and Stability 95, (7), 1183-1193.

6. Patel, P.; Stec, A. A.; Hull, T. R.; Naffakh, M.; Diez-Pascual, A. M.; Ellis, G.; Safronava, N.; Lyon, R. E., Flammability properties of PEEK and carbon nanotube composites. Polymer Degradation and Stability 97, (12), 2492-2502.

7. Kashiwagi, T.; Du, F.; Winey, K. I.; Groth, K. M.; Shields, J. R.; Bellayer, S. P.; Kim, H.; Douglas, J. F., Flammability properties of polymer nanocomposites with single-walled carbon nanotubes: effects of nanotube dispersion and concentration. Polymer 2005, 46, (2), 471-481.

8. Shen, R., Hatanaka, L. C., Ahmed, L., Agnew, R. J., Mannan, M. S., & Wang, Q. (2017). Cone calorimeter analysis of flame retardant poly (methyl methacrylate)-silica nanocomposites. Journal of Thermal Analysis and Calorimetry, 128(3), 1443-1451.

9. Ahmed, L., Zhang, B., Shen, R., Agnew, R. J., Park, H., Cheng, Z., ... & Wang, Q. (2018). Fire reaction properties of polystyrene-based nanocomposites using nanosilica and nanoclay as additives in cone calorimeter test. Journal of Thermal Analysis and Calorimetry, 132(3), 1853-1865.

10. Furukawa, H., Cordova, K. E., O'Keeffe, M., & Yaghi, O. M. (2013). The chemistry and applications of metal-organic frameworks. Science, 341(6149), 1230444.

11. Morgan, A. B. (2019). The future of flame retardant polymers–Unmet needs and likely new approaches. Polymer Reviews, 59(1), 25-54.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Development of a Blast-Resistant Roller Shutter Door

Darrell Barker*, Jerry Collinsworth, and John Puryear
ABS Group
140 Heimer Rd. Suite 300, San Antonio, TX
Michael Wong, Leow Chyan
Gliderol Doors (S) Pte Ltd
86 International Rd. Singapore
*Presenter E-mail: dbarker@absconsulting.com

Abstract

Conventional roller shutter doors can become hazardous debris when subjected to blast loading. To mitigate this hazard, Gliderol and ABS Consulting are developing a blast-resistant roller shutter doors. The two-phase development includes finite element analysis (FEA) to design the door system and shock tube testing to validate the design. The first phase includes analysis of concept and performance testing of door components to gather data necessary to develop an FEA model of the entire door. The second phase entails detailed design development, analysis and validation of the full-scale door system.

In this paper, details of the first phase FEA modelling and blast testing are discussed. Design blast loads and structural performance requirements are presented. Candidate geometries considered for the curtain panels are described along connections and anchorage configurations. FEA modelling techniques for accurately capturing large deflections and dynamic response are discussed along with a comparison of component blast testing with FEA model results is presented. Modelling and blast testing planned for phase 2 are also described.

Keywords: roller shutter door, blast loading, finite element analysis, shock tube testing

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Lessons from Risk Assessment of 6th Generation Drill-ships and Sem-Submersibles

Wael Abouamin* PE
Energy Risk Consulting
23501 Cinco Ranch Blvd H-120-303
Katy, TX 77494
*Presenter E-mail: Wael.abouamin@energyriskconsulting.net

Abstract

Building a deep-water drilling rig that incorporates the latest technology while meeting internal requirements, client specifications, and budget constraints, can be a daunting challenge. Doing so in a post-Macondo environment with a shortage of qualified personnel to man the rig adds even more obstacles to overcome. Ensuring that a variety of rig systems supplied by different vendors will be integrated into a workable rig that is properly maintained is another task for the drilling contractor.

The risk management plan was implemented in the form of individual risk assessments focused on each of various systems utilizing primarily the failure modes effects and criticality (FMECA) methodology. It can be quite surprising to evaluate the results of these sessions and realize how powerful these tools can be and how effective they can be in identifying potential faults and weaknesses in the systems. Maintaining a global view of the rig while carrying out the individual risk assessments was critical to ensure overall integration of the systems.

The paper results will highlight examples of findings across a wide spectrum of rig systems, from the cooling water system of active heave drawworks braking resistors to NOVEC release on an F&G detection system to challenges on a pipe handling system. Each example will have its own unique circumstances, but they all highlight the importance and value of implementing an effective risk management strategy.

This paper also demonstrates that implementing a risk management plan during the design and construction of the rigs can help reduce risks associated with major accidents and downtime. This can be accomplished by applying the results of the risk assessments into training of personnel, updating of operational procedures, updating of maintenance procedures, modifying designs, changing control systems and re-programming software. This paper presents the results of risk

assessments applied to semi-submersibles and drill-ships, all 6th generation deep-water drilling rigs.

Keywords: Risk Assessment, Risk Management, Mechanical Integrity, Human Factors, Interfaces, Training and Performance, FMEA

1 Introduction

Building a deep-water rig that incorporates the latest innovations of technology and automation is a challenge that requires planning, coordination, and a thorough understanding of the limitations of people and machines. Implementing a risk assessment and management program is an essential part of the rig building process.

Figure 1 - 6th Generation Drill ships

Consider some of the challenges facing a drilling contractor in building a modern 6th generation ultra-deep-water rig:

- Highly complex systems designed and manufactured by multiple vendors
- Integrating complex systems with the shipyard-built systems
- Highly automated systems that require coordination and integration
- Highly automated systems that need to be operated by rig personnel

- Highly automated systems that need to be maintained (and, if required, repaired) by rig personnel
- Maximize up-time and minimize downtime while maintaining safety and equipment integrity

2 Methodology

2.1 Risk Assessment Objective

The primary objective of a risk assessment is to identify, understand, and implement measures to mitigate the risks associated with the design and operation of the rig, systems, and equipment.

Risk assessment is a very broad term that is used in many different contexts: financial, technical, project management, design, manufacturing, etc. It is important to define what we mean when use the term *risk assessment*. In our context, the following broad steps comprise the risk assessment process:

1. Hazard Assessment
2. Risk Evaluation
3. Risk Mitigation

It is not our objective to explain in detail the risk management strategy that can be implemented; a risk assessment is one of the steps in the process. In general, this paper presents the risk assessment process based on numerous past projects and experiences. The primary tool utilized was the failure modes, effects and criticality assessment (FMECA). This is a well-established methodology in the oil and gas industry that was originally developed for use in the aerospace (and military) industry to analyse complex systems. The methodology was modified to suit the particular needs of the systems and situations to be reviewed for the project. This modification to the methodology included heavy emphasis on preparation, participation, and technical content, particularly in the function description of components. The following figure portrays the FMECA process:

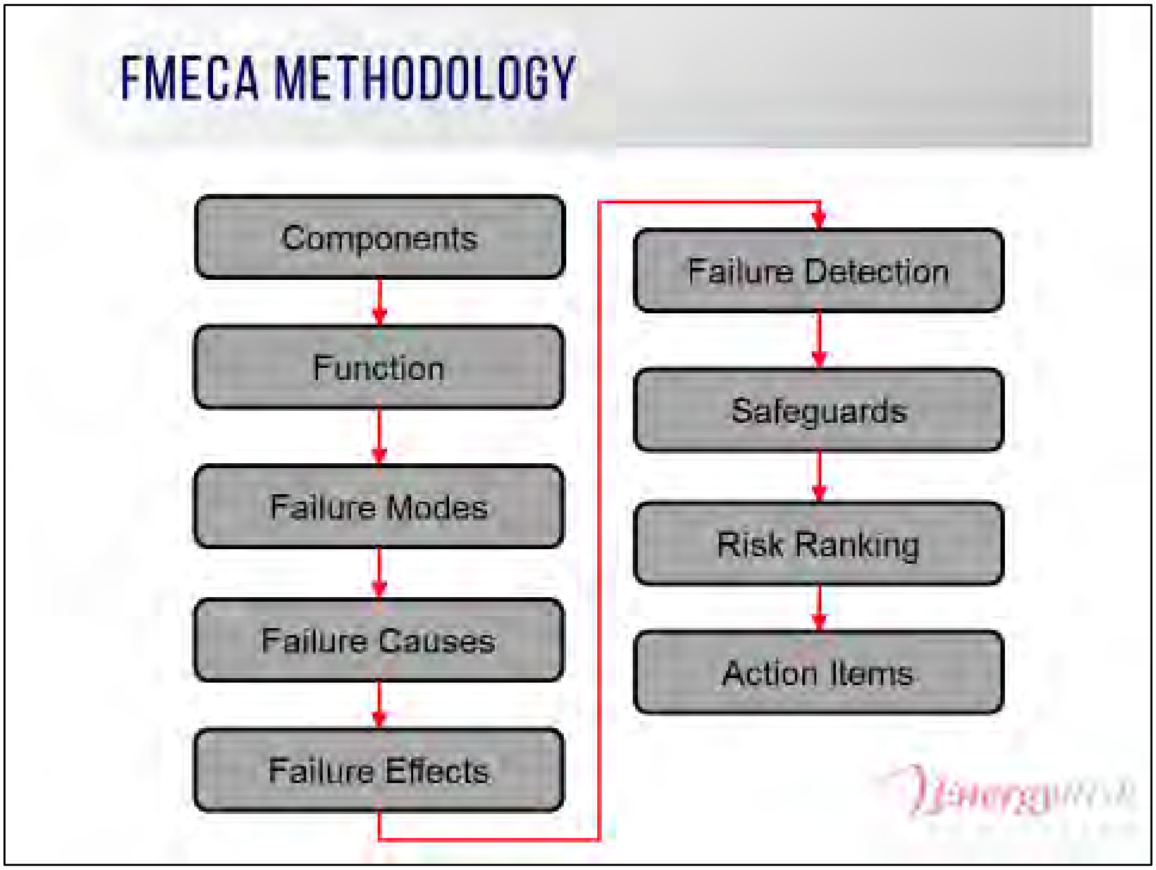


Figure 2 Typical FMECA Methodology

The following typical questions were asked during the risk assessment:

- What are the major components in the system?
- How can those components fail?
- What root causes create those failures?
- How can those failures affect the performance of the component?
- How can those failures affect the performance of the system?
- How can those failures affect the performance of the rig?
- What can be done to eliminate the failure?
- What can be done to minimize the likelihood of the failure occurring?
- What can be done to reduce the consequences if the failure occurs?
- Can you detect the failure? (Is it a hidden failure?)
- What is the required maintenance and inspection on the system components?
- How can you improve the system performance?

2.2 Level of Detail

The process emphasizes preparation, participation, and technical content. This approach maximizes the value of the participants' time in the session and extracted the most relevant information via productive discussions throughout the assessment. In an attempt to demonstrate the level of detail that is involved, the following figure shows a sample truncated line item in the FMECA spreadsheet describing a temperature transmitter on an electric motor. This is presented to indicate the detailed description and emphasis on technical content in the sessions. It also shows the level of preparation that is required to maximize effectiveness:

<table>
<tr><th>COMPONENT</th><th>FUNCTION</th><th>FAILURE MODE</th><th>FAILURE CAUSE</th></tr>
<tr><td rowspan="2">TRANSMITTER TEMPERATURE - MOTOR #1</td><td rowspan="2">There are two RTD's (Resistance Temperature Detector), one of which is a spare, for each motor winding. There are 3 temperature sensors used per motor. Any one sensor with a temperature above 160C generates an alarm. Two sensors above 180C generates a trip of the affected motor.

With hi-hi of two sensors:

1. AHC: heave compensation continues, affected motor will trip
2. non AHC: ALL motors (including affected motor) are used to slow down the drawworks, and zero speed is set. Mechanical brakes are set.

The range of the temperature sensor is 0C to 200C. It generates a 4-20mA signal. This signal is sent to DW Control System PLC. The PLC performs all processing on the signals other than validation of signal integrity. The temperature transmitter has a loop monitoring function that monitors the element (RTD) status. If the transmitter detects a failure of the RTD then a high amp signal (greater than 20mA) is sent to the DW Control System PLC.</td><td>Loss of signal</td><td>Wire break, termination failure, transmitter failure</td></tr>
<tr><td>Erroneous signal</td><td>Transmitter failure, EMI</td></tr>
</table>

Figure 3 FMECA Spreadsheet Sample

2.3 Bottom Up Approach

It is worth noting that the FMECA approach used is a bottom up approach. To ensure that systems are integrated correctly, we emphasized that failure escalation from component to sub-system to system to the entire rig.

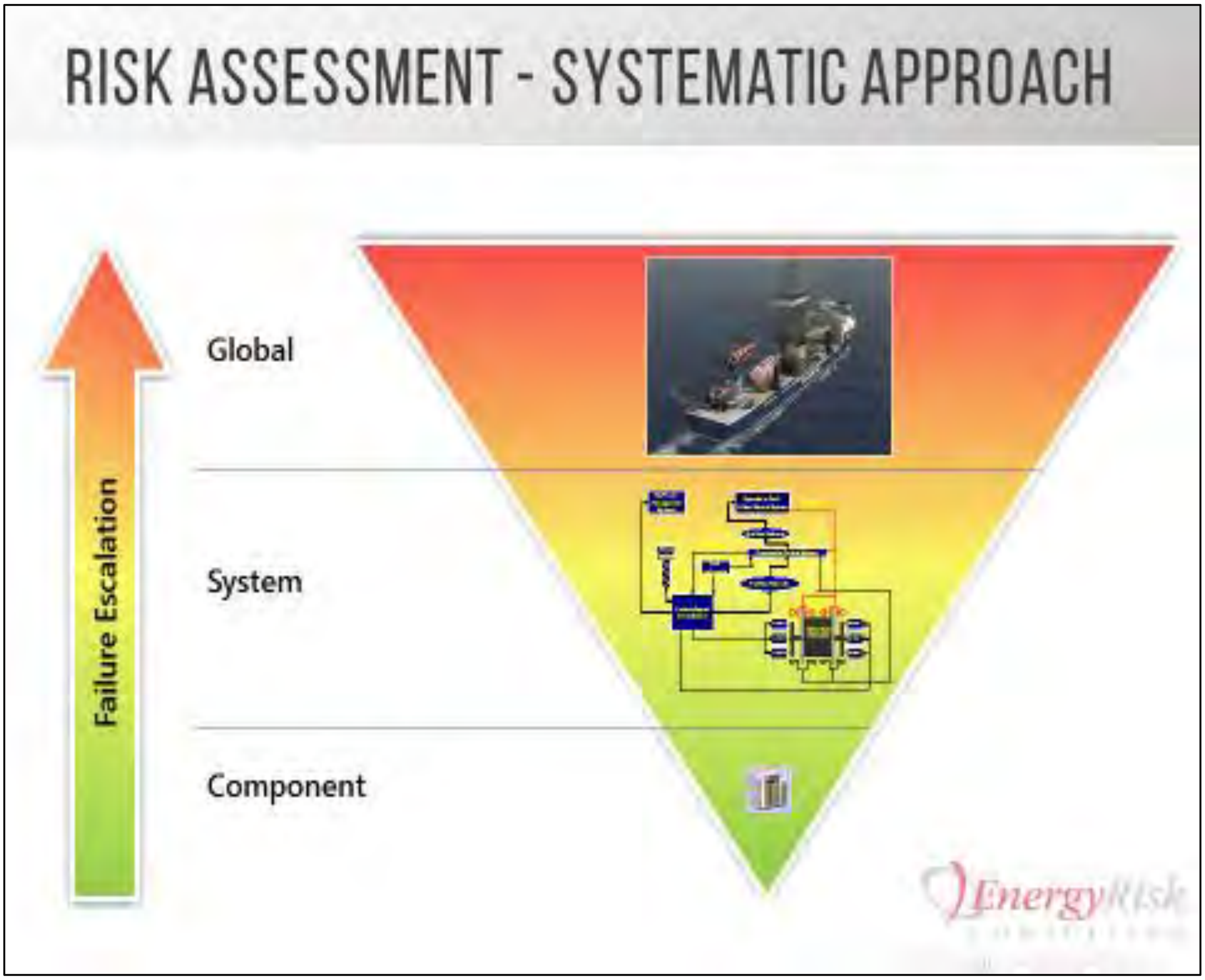


Figure 4 Bottom Up Approach

Participation was also a very important factor in ensuring the success of the risk assessment. We are referring to participation from the equipment manufacturer and the rig crews (driller, assistant driller, mechanic, electrician, chief engineer, tool pusher, etc.). Determining the level of participation and the personnel to participate is based on the system or systems being analysed. Obviously, systems that are heavy on electrical and electronic components, such as the drilling control network or anti-collision system, will involve the electrical disciplines on the rig. Participation of the rig crew also serves as an excellent training and educational opportunity. As the components, systems, and the rig is being analysed, detailed discussions inevitably arise leading to improved understanding of the design, operation, and maintenance of the systems. It also potentially leads to improvements in the design based on the feedback from the equipment users to the manufacturer.

Timing of the risk assessment is a critical factor in ensuring success and maximum benefit. We are referring to the timeframe between detailed design and manufacturing. During this time, there is enough detail in the design to have a thorough and proper analysis, yet it is not too late (or too expensive) to modify the design should any flaws be discovered, improvements suggested, or recommendations proposed.

2.4 Hierarchy of Approach

Once the hazard identification and risk evaluation have been carried out, the final step in the process is to implement mitigations to address the identified risks. Generally, the hierarchy of approach is:

A. Implement measures to *eliminate the risks*
B. Implement measures to *reduce the likelihood* of the risks
C. Implement measures to *reduce the consequence*

Risk Elimination - eliminating the identified risk can occur in many forms, and via many techniques and processes. This can be accomplished through physical changes such as structural design modifications or adding or removing components (such as valves, sensors, pumps, etc.). There are numerous possibilities and options. It is important to note here, however, that implemented changes need to be incorporated in the risk assessment, otherwise there is a danger in introducing new hazards that have not been evaluated.

Risk Likelihood Reduction - implementing measures to reduce the likelihood of events occurring can also be carried out in different ways. Examples include increased maintenance and inspection frequency. Another technique could be to increase capacity to a particular system (such as additional pump to a hydraulic system). Operational procedures can be updated or modified to reduce the load on a system, such the electrical generation on the rig.

Risk Consequence Reduction - reducing the consequence can be accomplished by providing additional components (reduction in downtime due to inadequate spares), increased training (leading to faster troubleshooting and fixing of failures), increased in maintenance and inspection, testing frequency, etc.

The implementation of recommendations can take the form of:

- System design changes
- Software changes
- Changes to FAT (factory acceptance testing)
- Changes to commissioning testing
- Changes to SIT (system integration testing)
- Updates of the critical spare parts list
- Update of maintenance procedures
- Update of operational procedures

3 RISK ASSESSMENT EXAMPLES:

The following three (3) example findings were chosen in an attempt to demonstrate the benefit of carrying out an FMECA-based risk assessment:

A. Water Mist System Redundancy
B. Pipe Handling System Failure Escalation
C. Anti-Collision System Fault Leading to Drawworks Stoppage

3.1 Water Mist System Redundancy

In this example based on a new-build rig, a risk assessment was carried out on the fire-fighting system. Included in the assessment was the water mist system covering several critical spaces (in this case the engine room). During the FMECA, it was identified that two pumps were installed in the system, one as primary and one as a backup. After further scrutiny, however, the FMECA team discovered that there was no automatic switch-over to the backup pump. So, in a fire scenario, a failure of the primary pump would have required that rig personnel *manually* switch over to the backup pump. This design was, of course, found to be less than ideal considering the potential for fire and the criticality of the system. The result was a relatively minor modification to have an automatic switch-over system installed. This minor modification, however, resulted in a significant reduction in risk by substantially increasing the expected availability of a critical fire-fighting system.

3.2 Pipe Handling System Failure Escalation

This example highlights the importance of rig personnel understanding the systems that they are using. This was based on a real situation where a hydraulically operated pipe handling system had some contamination in the hydraulic oil. This led to frequent stoppages (due to inconsistent movement). The rig crew did not understand the problem and their attempt to troubleshoot the root cause of the failure was incorrect. They opened the machine's electrical panel and pushed the "reset" button in the hopes that would restart the system and potential solve the issue. The "reset" button, however, also served as the calibration reset. Repeat, incorrect use of the "reset" button resulted in a total failure of the pipe handling system. The end result was a need for support from an OEM technician to resolve the issue. Due to the time involved with securing the OEM technician, the consequence of the failure was escalated from a few hours of downtime (to flush out the hydraulic system and clean it) to four or five days of downtime (to send the appropriate OEM technician and troubleshoot the system). The serves as an example of reducing the consequence of failure with the correct training and system knowledge.

3.3 Anti-Collision System Fault Leading to Drawworks Stoppage

This final example demonstrates the importance of thorough system integration assessments and the complexity of inter-relationships between systems on automated rigs. In this example, while a rig was tripping out of the hole (the drawworks hoisting drill-pipe at high speed and low load), a faulty sensor in a different system (in-line compensator, which was not being used) triggered an anti-collision system shutdown. The led to the emergency brakes on the drawworks engaging very quickly, which led to a very fast stoppage of the drawworks drum at high speed, leading to the continued upward movement of the travelling block. The led the wire rope (fast-line) to move from its grooves on the crown-block (also referred to as "bird's nest"). This was a very critical failure because it had the potential to part the wire rope which could have resulted in injuries or fatalities, and/or significant equipment damage. A detailed risk assessment would have identified the critical shutdown signals from other systems and would have identified that the commands from these signals should be ignored while these systems are not in use.

4 Conclusion

We have attempted to demonstrate the importance and need for a well-planned risk assessment process during the design and construction of deep-water rigs. This is especially true for rigs that are highly automated with complex systems. The benefits include significant risk reduction, better system integration, and detailed training and understanding of these systems by the rig crews.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Study of FSRU-LNGC System Based on a Quantitative Multi-cluster Risk Informed Model

Mahmoud M. El-Halwagi [1,2], Chenxi Ji*[1,2,3,4], Zeren Jiao[1,2], M. Sam Mannan[1,2,4], Hans J. Pasman[1], James Pettigrew[1,4], and Shuai Yuan[1,2,4]
[1]The Mary Kay O'Connor Process Safety Center
[2]Artie McFerrin Department of Chemical Engineering, Texas A&M University
[3]College of Marine Navigation, Dalian Maritime University
[4] The Ocean Energy Safety Institute, Texas A&M University
*Presenter E-mail: chenxiji@tamu.edu

Abstract

The offshore LNG terminal, referred to as LNG floating storage unit or floating storage and re-gasification unit (FSRU), performs well on both building process and operation process. The LNG FSRU is a cost-effective and time efficient solution for LNG transferring in the offshore area, and it brings minimal impacts to the surrounding environment as well. This paper proposed a systematic method to integrate chemical process safety with maritime safety analysis. The evaluation network was adopted to process a comparison study between two possible locations for LNG offshore FSRU. This research divided the whole process into three parts, beginning with the LNG Carrier navigating in the inbound channel, the berthing operation and ending with the completion of LNG transferring operation. The preferred location is determined by simultaneously evaluating navigation safety, berthing safety and LNG transferring safety objectives based on the quantitative multi-cluster network multi-attribute decision analysis (QMNMDA) method. The maritime safety analysis, including navigational process and berthing process, was simulated by LNG ship simulator and analyzed by statistical tools; evaluation scale for maritime safety analysis were determined by analyzing data from ninety experts. The chemical process safety simulation was employed to LNG transferring events such as connection hose rupture, flange failure by the consequence simulation tool. Two scenarios, *i.e.*, worst case scenario and maximum credible scenario, were taken into consideration by inputting different data of evaluating parameters. The QMNMDA method transformed the evaluation criteria to one comparable unit, safety utility value, to evaluate the different alternatives. Based on the final value of the simulation, the preferred location can be determined, and the mitigation measures were presented accordingly.

Keywords: LNG floating storage and regasification unit; Quantitative multi-cluster network multi-attribute decision analysis; Maritime safety; Chemical process safety

Nomenclature

AHP	Analytic Hierarchy Process
APF	Average Possibility of Fatality
BLEVE	Boiling Liquid Expanding Vapor Explosion
FSRU	Floating Storage and Re-gasification Unit
LNGC	Liquefied Natural Gas Carrier
MADA	Multi-Attribute Decision Analysis
MCS	Maximum Credible Scenario
PLL	Potential Loss of Life
QMFMDA	Quantitative Multi-hierarchy Framework Multi-attribute Decision Analysis
RPT	Rapid Phase Transition
SUV	Safety Utility Value
UKC	Under Keel Clearance
VCE	Vapor Cloud Explosion
WCS	Worst Case Scenario

Symbol

a: The average time interval of position checks by deck officers
b: A coefficient that represents the extent of damage to a ship's hull
B_1, B_2: Breadth of Ship 1 and Ship 2
C: The width of the channel
D: Average distance between ships
D_e: Diameter of collision avoidance
D_i: Collision diameter
d: The width of channel
F: Threatened Level
f: Lateral distribution of the ship routes, often normal distribution
$f()$: The actual traffic distribution of ships
H: Depth of the channel
k_{RR}: Risk reduction factor, usually taken 0.5
L: Average vessel length
N_1, N_2: Number of ship 1, 2 passing per year
P: The probability that a vessel is involved in a collision accident during its voyage passing one assigned water area
P_c: Causation probability
P_g: Geometrical probability, collision probability without aversive measures are made.
P_x: Ship collision probability
Q_j: Number of movements of ship class j per unit time, named as traffic volume
R: Radius of Turning Circle
T: Ship's stopping distance
V: Speed of passing vessel
V_{ij}: Relative velocity
V_{rel}: Relative speed
V_1, V_2: Speed of Ship 1 and Ship 2
X, Actual length of path for one ship
Z: Distance from the centerline of the fairway
$1/r$: Distance decay curve
ρ: Traffic density, number of ships per unit area
θ: The angle that one single ship approaching the channel with

1. Introduction

Natural gas, a green fossil fuel, is liquefied via dehydration, de-heavy hydrocarbons, and deacidified. Meanwhile, the volume of liquefied Natural Gas (LNG) is approximately equal to 1/600 of that of natural gas (GIIGNL Annual Report, 2019). The high storage efficiency, low cost, and economical long-distance transportation are the main advantages of LNG. In addition, LNG serves as a civil fuel because of its eco-friendliness (high hydrogen-carbon ratio) and high calorific value.

Currently, LNG Carrier (LNGC) is the most common tool for long-distance transportation between natural gas plants and traditional LNG terminals. Since the technique of floating production, storage, and offloading keeps developing these years, many loading and discharging modes are put into use in the offshore area. The typical LNG supply chain starts at the gas exploration plants. LNG is liquefied and stored in the export terminal; through the LNGC, LNG can be transferred to import terminal to store and to carry out re-gasification process before it is sent to downstream customers for civil or industrial utilizations (Andersson et al., 2010). A floating LNG unit can substitute the traditional export terminal, acting as a liquefaction plant and LNG storage offshore, this is called floating liquefied natural gas (FLNG). On the other side, to take the place of a traditional import LNG terminal, a technology called LNG floating storage and re-gasification unit (FSRU) was adopted to store the transferred LNG and to convert the LNG to gaseous state to meet the requirements of civil and industry utilization (Aronsson, 2012).

As shown in Figure 1, the typical LNG supply chain includes gas exploration, export terminal, LNG carrier, import terminal and pipelines. LNG FSRU, which is employed to improve working efficiency of LNG import terminal, integrates the storage function with re-gasification plant, locating in the offshore or near shore areas.

Figure 1. LNG Supply Chain

Compared with traditional LNG receiving terminals, LNG-FSRU performs better on many aspects. Building time saving: an LNG-FSRU is typically commissioned in 2 years, while an onshore LNG terminal usually takes 4-5 years; Flexible to re-location: typical LNG-FSRU systems are reconfigured by LNGCs after permission procedures, and since they still can serve as transportation tools, when the natural gas market grows, they can be relocated in another area to solve emergent supply and demand problems; Cost-effective, the investment of LNG-FSRU is usually 4 to 5 times less than that of land LNG receiving terminal (Finn, 2002).

As a new concept of LNG value chain, the research of LNG FSRU has been active in the process safety community only for several years. Schleder et al. (2011) employed fault tree analysis to carry out risk analysis of FSRU. (Martins et al., 2016) completed a detailed quantitative risk analysis study of undesired events of LNG FSRU by the consequence tool and presented the safeguard actions accordingly. Most literatures of LNG FSRU risk analysis focused on the fuzzy evaluation of the sole regasification unit from the perspective of chemical safety. However, few works have been done to consider a dynamic system for both FSRU and LNGC from a systematic point of view. Therefore, the objective of this research is to propose a safety-based model for a system of FSRU and LNGC by integrating both maritime safety and chemical process safety knowledge, and we call the defined system as FSRU-LNGC integrated system. The FSRU-LNGC system includes LNGC which is to be berthed alongside the FSRU, the FSRU itself, and the operation interaction of LNGC and FSRU. Its evaluation process starts from the LNGC entering into the inner harbor area via inbound channel and ends with the completion of LNG transferring. Three consecutive processes are involved in the research, LNGC navigation, LNGC berthing alongside the LNG FSRU and cargo transferring operation between LNGC and LNG FSRU, see Figure 2.

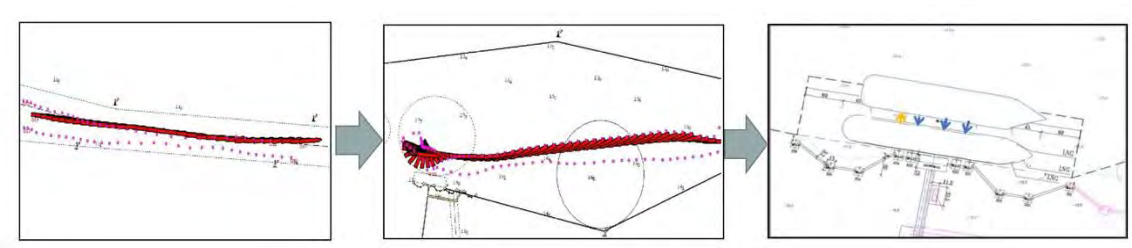


Figure 2. Defined Evaluation Processes

As shown above, the evaluation process starts with the LNGC entering the FSRU channel (navigational process), then the LNGC berthing alongside FSRU (berthing Process) and ends with the completion of LNG cargo transferring (transferring process).
A preliminary safety performance evaluation framework of the FSRU-LNGC system should be established by risk evaluation methods to build the risk model. Inspired by (Shapira and Goldenberg, 2005) and (Saaty, 1990), this study presented a quantitative multi-cluster network multi-attribute decision analysis (QMNMDA) to build a risk informed model for the defined processes of the FSRU-LNGC system. Figure 3 shows the preliminary evaluation process of the QMNMDA by incorporating the process analysis, risk assessment and attribute determination.

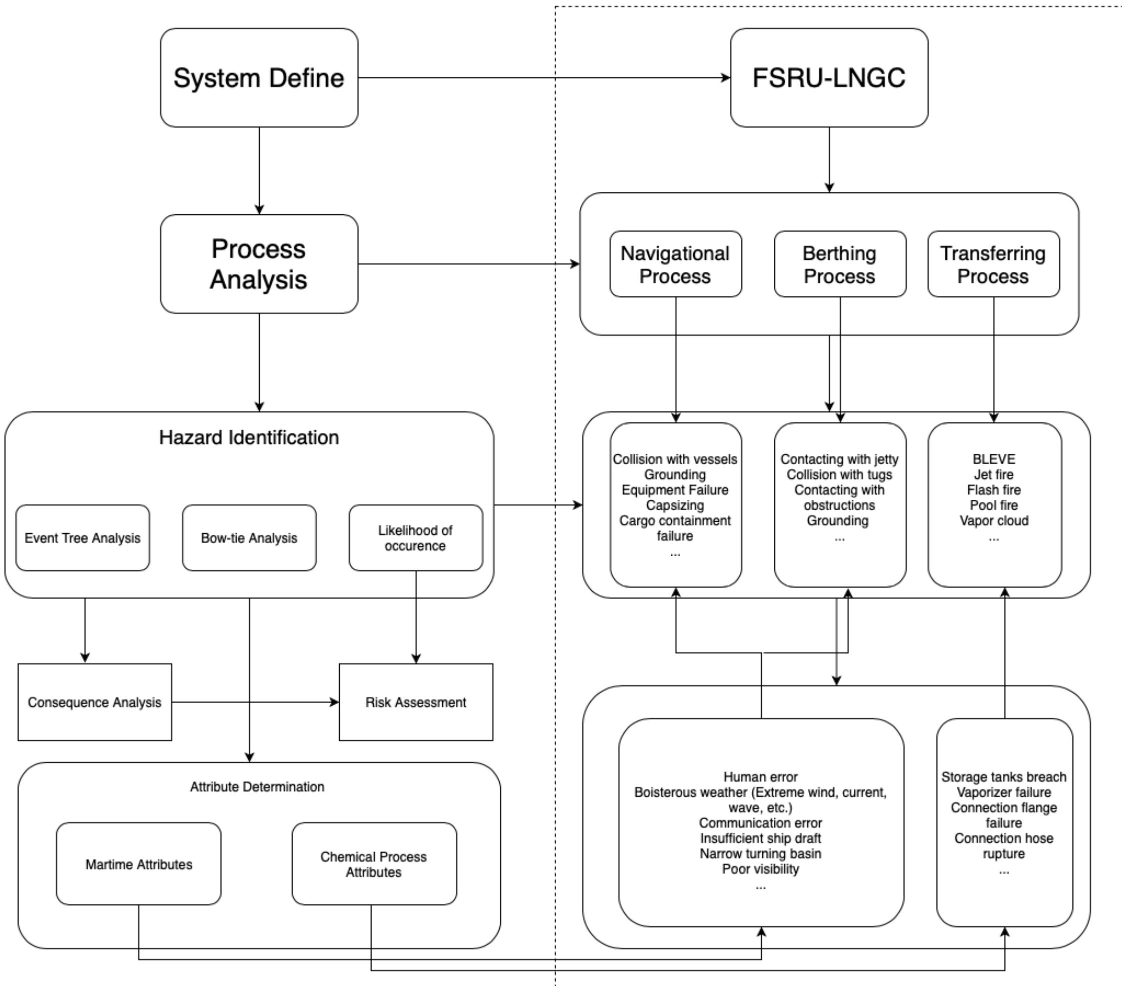


Figure 3. Proposed Evaluation Framework of QMNMDA

From the above figure, the FSRU-LNGC system will be analyzed by three processes: navigational process, berthing process and LNG cargo transferring process. Moreover, many techniques such as event tree analysis and bow-tie analysis, were adopted to identify hazards in these three processes. And the leading factors, we call attributes in the paper, of the identified hazards were categorized as maritime safety and chemical safety respectively and the corresponding attribute pools were established by detailed ship simulator study and chemical consequence analysis. The scope of this paper is restricted to operation safety of between FSRU and LNGC from a systematic safety view. Following the preliminary evaluation framework, this FSRU-LNGC study firstly analyzes the merits and demerits of relevant hazardous models for maritime safety and employs bow-tie and event-tree analysis for defined scenarios of FSRU LNGC interface. Then the ship simulator study, statistical analysis and chemical consequence analysis are carried out to build the quantitative multi-cluster model. At last, a case study of two proposed locations was adopted to investigate the safety level of FSRU LNGC systems using the model.

2. Relevant works

To establish the LNG-FSRU evaluation criteria, several factors, such as hydrographic information, navigation safety, fire and explosive risks, exclusion areas, and environment sensitivity, should be taken into consideration individually. Combined with previously recorded incidents, the most threatening hazards, collision, grounding, fire/explosion, and spillage during cargo handling, were identified by (Woodward and Pitblado, 2010)(Ji et al., 2017).

As for collision model, specifically, Fujii et al. (1974) and his group firstly proposed a model to calculate the average number of evasive actions by one ship navigating in one area. The prediction variables of his model were traffic density, diameter of collision avoidance, speed of passing vessel and relative speed. Moreover, the range of diameter of collision avoidance made the prediction values quite conservative. Macduff's model (Macduff, 1974) focused on the probable collision model, which was predicted by the geometrical probability and the causation probability. But the value of the geometrical probability will be overestimated when the angle between ship and channel is small. To determine the geometrical probability P_g, Pedersen (1995) presented a model under a two-channel situation. Channel 1 and channel 2 are assumed as two crossing channels. This model is reasonable for crossing scenario to estimate the geometrical probability due to a more practical assumption. However, the lack of ship movement data made it difficult to determine the probability distribution of ship motion. The summary of above mentioned three collision models was listed in the Table 1.

.

Table 1. Summary of Ship Collision Model

Model	Expression	Drawbacks
Fujii's Model	$N = \int_{entrance}^{exit} (\rho D_e V_{rel}/V)\, dx$	De is conservative (9.5 to 16.3 times ship length), so Pg is overestimated.
Macduff's Model	$Pg = \frac{X \cdot \bar{L}}{D^2} \cdot \frac{\mathrm{Sin}(\theta/2)}{925}$	Pg is overestimated when ɵ is small and underestimated because of the assumption of two ships are equal speed.
Pedersen's Model	$P_{\Delta t} = \frac{Q_j^{(2)}}{V_j^{(2)}} f_j^2(z_j) D_{ij} V_{ij} dz_j \Delta t$	Applicable for crossing channel situation, assume ship lateral motion as normal distribution, not very accurate for head on situation

In order to precisely simulate the head on situation in the real world, the COWI model (COWI, 2008) is applied to calculate ship collision probability.

$$Px = Pt \times Pg \times Pc \times k_{RR} = LN_1N_2 \left|\frac{V_1 - V_2}{V_1V_2}\right| \times \left(\frac{B_1 + B_2}{c}\right) \times (3 \times 10^{-4}) \times k_{RR} \qquad (1)$$

Compared to other models, the COWI model considered the risk mitigation measure and reduced the uncertainty in some extent by assuming ship motion as normal distribution. Moreover, the most likelihood situation for LNGC navigation in inbound channel is head-on situation, so the COWI model was adopted to carry out simulation for LNGC navigation safety phase. It is widely accepted that visibility is a key factor to influence coastal navigation and the leeway and drift angle, which was deemed as a significant parameter to show the vessel's maneuverability, was largely dependent on the magnitude of wind and current. Therefore, the main parameters to evaluate the collision hazard are determined as wind, visibility and the probability of following current.

On the other hand, Fujii et al. (1998) proposed his grounding model by establishing the relationship between the expected number of groundings and the predictors (causation probability, ship's speed, traffic density and shoal width). Meanwhile, Macduff (1974) adopted Buffon's needle problem to estimate Pg, the geometrical probability, and the major predictors are channel width and stopping distance of ships. These two above-mentioned models are only affected by the ship particulars while other elements related to location are set to be constant. The uncertainties of the real navigation situation are ignored in most cases, and this model merely considered historical accident data. Simonsen (1997) developed their model to estimate the expected annual number of groundings with the number of transshipments per year, the average time interval of position checks by deck officers and the transverse coordinates of shoals.

Table 2 serves as a review of above-mentioned grounding models, illustrating their expressions and drawbacks.

Table 2. Summary of Ship Grounding Model

Model	Expression	Drawbacks
Fujii's Model	$N_G = P_C D_\rho V$	Human factors, ship's maneuverability and environmental aspects were all neglected.
Macduff's Model	$P_g = \frac{4T}{\pi C}$	Causation probabilities are unknown; this model cannot recommend any risk control option. Traffic density is assumed uniformly.
Simonsen's model	$\sum_{\text{Ship class i}}^{\text{n class}} P_{C,i} Q_i e^{-C/a_i} \int_{z_{min}}^{z_{max}} f_i(z)dz$	Human factors and ship maneuverability are still neglected and effect of traffic (Q) and ship class (i) are not evidence based.

To overcome those above-mentioned drawbacks, Montewka et al. (2011) have proposed a more accurate grounding model with the consideration of the maneuverability of an individual ship and the properties of the traffic. In addition, Automatic Information System was employed to determine the distribution of the ship's motion.

$$F = M \times \frac{UKC}{H \times r} = \frac{R \times b}{d \times s \times c} \times \frac{UKC}{H \times r} \quad (2)$$

For the LNGC navigation process, the Montewka's Model was selected as the one to simulate stranding situations since it has a better interpretation and has considered ship maneuverability. Based on the above equation, the main parameters selected for grounding hazard of navigational process are channel width, channel curvature and under keel clearance.

When berthing or unberthing operation is taking place, the LNGC shows a characteristic of low speed and large drift angle (Yang, 1996). Typically, berthing operation for large ships should consider factors such as temperature, berthing ability, wind force, visibility and thunderstorm, and Bai (2010) presented the berthing influence factors as tug assistance, wind, current, longitudinal speed control, transverse speed control and angular velocity control . What is more, poor communication between crew and marine pilots during berthing operation will probably lead to marine disasters near ports, and the language and cultural diversity of seafarers needs to be considered as well (Winbow, 2002). To evaluate this complicated operation process in a quantitative way, Yang (Yang, 1996) proposed a berthing model by presenting models of ship, propeller and rudder individually and he took full considerations of interactions between each part. Yang set up a two-coordinate system, one is fixed coordinate, and the other is ship moving coordinate system. Based on Yang's theory, the LNG ship simulator was employed to perform a high-precision simulation for LNGC berthing. This simulator adopted a six-freedom motion mathematical model proposed by Zhang's research group (Zhang et al., 2007) and integrated wind disturbing force models and wave force models as the keys for external force. To evaluate the LNGC berthing operation, six main parameters were determined as, water depth of turning basin, following current speed, berth length, radius of turning area, transverse wave height and the probability of crossing wind (beam wind).

After the berthing process is completed, the LNG should be transferred from LNGC to LNG FSRU, which is a typical Ship-to-Ship LNG transferring process. Two common solutions for Ship to Ship transferring process exist, one is called side-by-side transferring pattern, and the other is called tandem transferring pattern (Liu et al., 2001). There are three liquid transferring connection hoses and one vapor counter flow connection hose. For the LNG FSRU system, many causes would result in LNG accidental release such as FSRU or LNGC tank breach, connection pipe rupture and LNG vaporizer failure. These may be the result of collision, faulty operation, bad maintenance, or be caused by a whole variety of primary low severity events, such as small igniting leaks, due to maintenance or other operations, *e.g*., at the regasification unit in which LNG is heated. Hence, in such cases secondary devastating major events are domino effects of the much less severe primary ones. Furthermore, possible associated consequence phenomena of LNGC release on water have been identified (Abbasi et al., 2010; Li et al., 2012) as Boiling Liquid Expanding Vapor Explosion (BLEVE), vapor cloud explosion (VCE), jet fire, cloud flash fire, pool fire, rapid phase transformation, cryogenic burns, *etc.* Figure 4 shows a simplified bow-tie diagram for LNG accidental release to consider both the causes and the outputs of the top event. The sequence in which these phenomena are mentioned is quite opposite to the likelihood in which they can occur. For example, in principle a BLEVE or a VCE cannot be excluded although these phenomena never have been directly observed. However, the nature of the hydrocarbon makes it possible just as if it is LPG, although less likely than LPG. BLEVE could occur if a sustained fire heats one of the tanks and the pressure relief valve would not be able to cope with the evaporation rate as happened once with an LNG loaded tank truck in Spain (Planas et al., 2015). VCE of a natural gas cloud cannot be excluded as well; in a massive cloud once ignited and meeting obstacles fast flame generated blast is possible, while even transition of the deflagration into detonation (DDT) with much stronger blast cannot be excluded. For ethane and other fuels these phenomena of DDT are observed on so-called large-scale in experiments (*e.g.,* Pekalski et al., 2014), which compared to most accidental releases in size should be considered small-scale, while the propensity to DDT of various hydrocarbons, including methane, the main component of natural gas, can be predicted

(Saif et al., 2017). However, the likelihood of the other above mentioned phenomena given a release is much higher. Rapid phase transition explosions occur when methane under certain conditions is spilled on water; but their blast is weak.

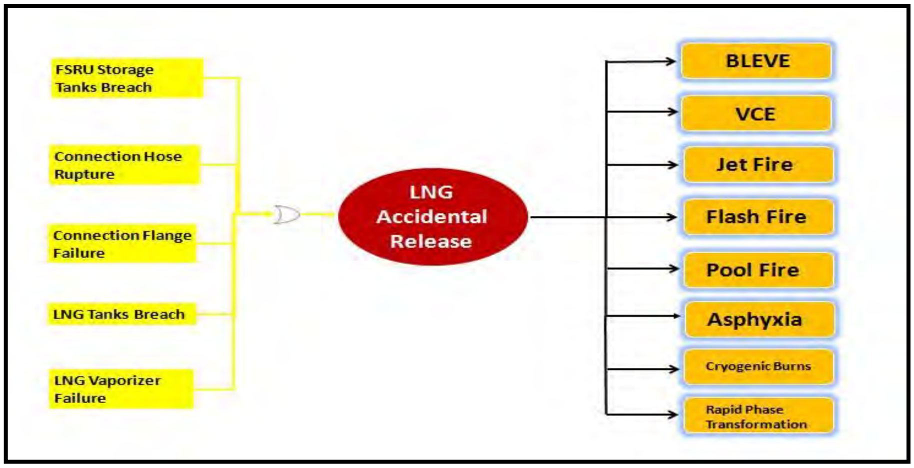


Figure 4. Simplified Bow-tie Diagram for LNG Accidental Release

As shown in above simplified bow-tie diagram, five primary causes may result in LNG accidental release for the FSRU-LNGC system: FSRU storage tank breach, connection hose rupture, connection flange failure, LNGC Tank breach and LNG vaporizer failure. Frequency of domino effects may be much greater. When LNG is released under the waterline, it will boil vehemently and convert to vapor bubble, then the LNG bubble may escape above the waterline to produce LNG vapor. For above-waterline release, jet fire, cloud flash fire and pool fire may form under different scenarios. Since a vapor cloud explosion is not likely to occur over the open water area (Hightower et al., 2004), the possible fatality related consequences taken into account here are flash fire, pool fire and jet fire, while the BLEVE, and vapor cloud are deemed as less likely consequences. Then, the flammable calculations including fireballs (instantaneous releases), jet fires (pressurized releases), pool fires (after liquid spills evaporation), and vapor cloud fires or explosion are processed based on the unified dispersion model (UDM), which is part of the DNV-GL PHAST software package.

3. Model development

Based on values and criteria there are quite a few techniques to assist a decision maker. Utility theory is a quantitative approach for decision makers to value a wide range of feasible alternatives, and it is good at finding a better solution by calculating the final utility value. Multi-attribute decision analysis (MADA) is an optimizing decision-making method to get the output of overall utility function, which is constituted by weight vectors multiplied by utility values. Based on the calculated overall utility value of each alternative, the preferred decision can be made with the maximum expected utility value (Keeney and Raiffa, 1993). In addition, opposite to AHP (Analytic Hierarchy Process), the Analytic Network Process (ANP) has a nonlinear structure and does not require independence among elements in different hierarchies. Saaty (1990) pointed out that the network of ANP is built by clusters which incorporate decision parameters. The network structure in ANP is represented in two forms, one is a graphical form and the other is a matrix form. The graphical form qualitatively represents the interaction relationship and feedback relationship between the various components that make up the network, while the matrix form quantitatively represents the degree or magnitude of interaction or feedback.

Since MADA is good at dealing with the decision-making problems among several attributes in one layer, and ANP outperforms for a case with the overall determination of different layers as here is required for the maritime and the spill risk determination. By combining these two approaches, this research developed MADA and ANP into a quantitative multi-cluster network multi-attribute decision analysis (QMNMDA). The core idea of this method is to divide the top problem into several processes first, then different processes are evaluated individually by various quantitative tools, such as risk simulation software, ship simulator and data analysis software. Next, the major hazards are identified under corresponding processes. To quantitatively evaluate different hazards, previous theories and equations may be referred to determine the major attributes which are under the hazard cluster. By considering the data availability, the risk attribute clusters can still go down to sub factor clusters to quantitatively evaluate the top object directly. Generally, QMNMDA has two aspects, one is the construction of the network, and the other is the calculation of the weight values of the ANP elements. In order to construct the structure of the problem, all the interrelationships between the elements should be well considered. When an element in one cluster depends on another, the relationship is represented by an arrow within a cluster. All of these relationships are calculated using pairwise comparisons and a supermatrix, containing the influences between elements. The ultimate power of the supermatrix is to calculate the overall weight, which is determined by a fuzzy analytic network process (F-ANP) approach. Then the risk evaluation utility value is to be determined by the Delphi method and statistical analysis. At last, the risk category is obtained based on the principle of maximum membership. Put simply, the framework determination of QMNMDA is a top-to-bottom work, and then the final evaluation is progressing bottom-to-top.

(1) Preliminary network of QMNMDA

Following the working flow as shown in Figure 3, the graphical form ANP based cluster model was established to determine the safety level for LNG FSRU locations. By evaluating operation process, hazard identification and characteristics of locations, the preferred location can be determined through the outputs of the clusters and elements, see Figure 5.

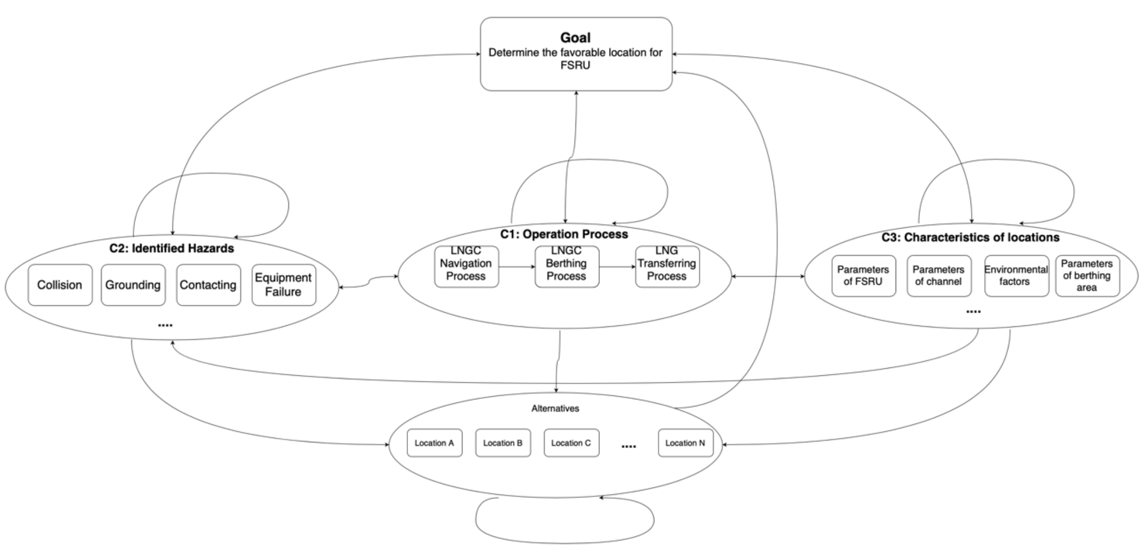


Figure 5. Preliminary network for QMNMDA model

As Figure 5 shows, the set of alternatives and evaluation factors for the evaluation objective are determined and the relationships of different elements have been established. Three operation processes have dependent relations while the relationships between any two elements in C2 and C3 are deemed as independent.

As shown in Figure 5 in the operational process there are three sub-processes. For the navigation process, the hazards are identified as collision, grounding, equipment failure, capsizing and cargo containment failure. For the berthing process, the hazards are identified as the LNGC contacting with jetty and obstructions, collision with tugs and LNG grounding due to insufficient UKC. In addition, the bow-tie diagram Figure 4 tells the possible hazards for the transferring process and that of the LNG vaporizer failure (re-gasification), being FSRU storage tanks breach, connection hose rupture, LNG tanks breach and connection flange failure.

(2) Weight calculation

Next, the F-ANP approach is employed to calculate the weight values of the three processes. This is because no historical data exist and no overall simulation is possible, hence experts have to be interviewed about the weight of the various contributing hazards. Replies of different experts will vary and will be merged into fuzzy triangle numbers. The definition of fuzzy triangle number proposed by (Chang, 1996) was presented to deal with the calculation process of overall weight values [0, 1]. The fuzzy triangle number p of evaluation set *U*, $U = (u_1, u_2, u_3, \ldots, u_n)$, is defined as $\mathrm{p} = (\mathrm{l}, \mathrm{m}, \mathrm{s})$, and $0 \leq \mathrm{l} \leq \mathrm{m} \leq \mathrm{s} \leq 1$, its membership function is $\mu(\mathrm{x})$.

$$\mu(\mathrm{x}) = \begin{cases} \frac{x-l}{m-l}, & x \epsilon (l, m] \\ \frac{s-x}{s-m}, & x \epsilon (m, s] \\ 0, & otherwise \end{cases} \tag{3}$$

where *l* and *s* stand for the lower and upper value, respectively, and *m* stands for the most probable value of $p \, \epsilon \, [0,1]$. While $\mathrm{l} = \mathrm{m} = \mathrm{s}$, p is deemed as a nonfuzzy number. Then the fuzzy triangle number based fuzzy judgement matrix can be constructed by pairwise comparisons, shown in Equation 4.

$$\mathrm{p} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n_1} \\ p_{21} & p_{22} & \cdots & p_{2n_1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n_1 1} & p_{n_1 2} & \cdots & p_{n_1 n_1} \end{pmatrix} \tag{4}$$

Where $p_{11} = p_{22} = \cdots = p_{n_1 n_1} = (0.5, 0.5, 0.5)$. p_{ij} is defined as the complementary judgment matrix for the fuzzy triangle number p, and p_{ij} is effective only when it satisfies the consistency test. In the work presented by Saaty (1990), the eigenvalue approach was proposed.

Next, the partial weight value matrix of the general supermatrix can be determined by the equation.

$$W_{11}^{(1i)'} = (d'(u_{11}), d'(u_{12}), \ldots, d'(u_{1i}), \ldots, d'(u_{n_i}))^T \tag{5}$$

$$d'(u_{1i}) = \min \mathrm{V}(C_{1i} \geq C_{1k}, C_{1h}) \tag{6}$$

After normalization, equation 5 is converted to

$$W_{11}^{(1i)} = (d \quad (u_{11}), d \quad (u_{12}), \dots, d \quad (u_{1i}), \dots, d \quad (u_{n_i}))^T \tag{7}$$

The comprehensive importance of component $u_{1i}(i = 1,2, \dots, n_1)$ is defined as C_{1i}.

$$C_{1i} = \sum_{j=1}^{n_1} p_{ij} \otimes \left(\sum_{i=1}^{n_1} \sum_{j=1}^{n_1} p_{ij}\right)^{-1} \tag{8}$$

$\mathrm{V}(C_{1i} \geq C_{1k})$ is applied to calculate the probable weight when $C_{1i} \geq C_{1k}$ is true.

$$\mathrm{V}(C_{1i} \geq C_{1k}) = \begin{Bmatrix} 1, & m_{ij}^{1i} \geq m_{ij}^{1k} \\ \frac{s_{ij}^{1i} - l_{ij}^{1k}}{s_{ij}^{1i} - l_{ij}^{1k} + m_{ij}^{1k} - m_{ij}^{1i}}, & m_{ij}^{1i} < m_{ij}^{1k} \ and \ l_{ij}^{1k} \leq s_{ij}^{1i} \\ 0, & otherwise \end{Bmatrix} \tag{9}$$

where $\mathrm{i} = 1,2, \dots, n_i;\ k = 1,2, \dots, n_1$ & $k \neq i; j = 1,2, \dots, n_1$

Then W_{11} can be obtained by repeating these procedures n_1 times.

$$W_{11} \quad = (W_{11}^{(11)}, W_{11}^{(12)}, \dots, W_{11}^{(1i)}, \dots, W_{11}^{(1n_i)})^T \tag{10}$$

At last, the matrix form of ANP, supermatrix $W_{ij}(i, j = 1,2, \dots, N)$ is determined after similar processes to get $W_{22}, W_{33}, \dots, W_{n_1 n_1}$.

$$\mathrm{W} = \begin{array}{cc} & \begin{array}{ccccccccccccc} & C_1 & & & & C_2 & & & \cdots & & C_N & \\ d(u_{11}) & d(u_{12}) & \cdots & d(u_{1n_1}) & d(u_{21}) & d(u_{22}) & \cdots & d(u_{2n_2}) & & d(u_{N1}) & d(u_{N2}) & \cdots & d(u_{Nn_N}) \end{array} \\ \begin{array}{cc} C_1 & \begin{array}{c} d(u_{11}) \\ d(u_{12}) \\ \vdots \\ d(u_{1n_1}) \end{array} \\ C_2 & \begin{array}{c} d(u_{21}) \\ d(u_{22}) \\ \vdots \\ d(u_{2n_2}) \end{array} \\ & \vdots \\ \vdots & \\ C_N & \begin{array}{c} d(u_{N1}) \\ d(u_{N2}) \\ \vdots \\ d(u_{Nn_N}) \end{array} \end{array} & \begin{bmatrix} W_{11} & W_{12} & \cdots & W_{1n_1} \\ W_{21} & W_{22} & \cdots & W_{1n_2} \\ \vdots & \vdots & \cdots & \vdots \\ W_{N1} & W_{N2} & \cdots & W_{Nn_N} \end{bmatrix} \end{array} \tag{11}$$

Following the weight value determination procedures, the weight values of process layer are calculated as below.

$$\mathrm{p} = \begin{array}{cc} & \begin{array}{ccc} k_{NP} & k_{BP} & k_{TP} \end{array} \\ \begin{array}{c} k_{NP} \\ k_{BP} \\ k_{TP} \end{array} & \begin{pmatrix} (0.5, 0.5, 0.5) & (0.4, 0.4, 0.5) & (0.2, 0.3, 0.4) \\ (0.5, 0.6, 0.6) & (0.5, 0.5, 0.5) & (0.2, 0.4, 0.5) \\ (0.6, 0.7, 0.8) & (0.5, 0.6, 0.8) & (0.5, 0.5, 0.5) \end{pmatrix} \end{array} \tag{12}$$

By calculating the comprehensive importance of component and probability when $C_{1i} \geq C_{1k}$ is true, the normalized weight value matrix of the process layer is:

$$k_p = (0.137, 0.321, 0.542)^T \tag{13}$$

(3) Final network of FSRU-LNGC system.

By repeating the weight value determination process for the hazard layer, the following Table 3 is made up from the collected data of our FSRU risk analysis group, illustrating the overall weight value of the identified hazards for the three processes.

Table 3. Overall Weight Values of the Identified Hazards for the Three Processes

Operation Process	Weight Value with Dependencies	Identified Hazards	Priority within the Process via ANP	Overall Priority
Navigation Process	0.137	Collision	0.581	0.0796
		Grounding	0.356	0.0488
		Equipment Failure	0.032	$4.4*10^{-3}$
		Capsizing	0.002	$2.74*10^{-4}$
		Cargo Containment Failure	0.029	$3.97*10^{-3}$
Berthing Process	0.321	Contacting with Jetty	0.621	0.201
		Collision with Tugs	0.064	0.0205
		Contacting with Obstructions	0.223	0.0716
		Grounding	0.092	0.0499
Transferring Process	0.542	Flash Fire	0.503	0.2726
		Pool Fire	0.212	0.1149
		RPT	0.096	0.05203
		BLEVE	0.001	$5.42*10^{-4}$
		Jet Fire	0.122	0.06612
		VCE	0.066	0.03577

As shown above, the priority scores within each process served as indicators to determine the major hazards of the three processes. This paper neglected the hazards with a priority value of priority score under 0.1. Therefore, collision and grounding were determined as the major hazards for the navigation process, while contacting with jetty and contacting with other obstructions were those for the berthing process, and flash fire, pool fire and jet fire were identified for the LNG transferring process.

Then the ship simulator DMU V-dragon 3000A was adopted to find the attributes for the maritime processes, *i.e.*, navigation process and berthing process. Extreme conditions were selected as the input parameters: the wind direction was blowing to the shore; the radius of turning area was set as 500 meter and 1000 meter, respectively; the berthing length was set as 1.2 times and 2 times ship's length overall. Two scenarios were designed to determine the most influential factors:

1. Full loaded, port side berthing with spring tidal current;
2. Full loaded, starboard side berthing with ebbing tidal current.

The failure simulation runs were shown in Table 4.

Table 4. Simulation Results of Ship Simulator for Berthing Process

Number of runs	Wind	Current	Radius of Turning Area	Water Depth	Transverse Wave Height	Berth Length	Consequence
1	N-6	Spring, 0.6m/s	500m	20m	0.7m	2L	Contacting the FSRU
2	N-6	Spring, 1.5m/s	1000m	21m	0.8m	2L	Contacting the jetty nearby
3	N-8	Spring, 0.8m/s	1000m	21m	1.0m	2L	Contacting the FSRU, tugs malfunction
4	N-6	Spring, 0.6m/s	1000m	19m	1.5m	2L	Contacting the berthing ship nearby
5	N-8	Ebb, 0.9m/s	1000m	20m	0.8m	2L	Contacting the FSRU, tugs malfunction
6	N-7	Ebb, 0.7m/s	1000m	15m	0.8m	2L	Contacting with the berth nearby
7	N-6	Ebb, 0.6m/s	1000m	20m	0.7m	1.2L	Contacting with FSRU, failed to get alongside the berth
8	N-6	Spring, 0.6m/s	1000m	20m	0.8m	1.2L	Contacting with FSRU, failed to get alongside the berth

Based on the simulation results by the ship simulator, the most significant parameters leading to collision of LNGC are poor visibility, beam wind frequency and large current; leading factors for grounding are insufficient UKC, inadequate channel width and sharp channel curvature. The magnitude of following current, transverse wave height and water depth of berthing area are the major attributes for contacting with the nearest obstruction; while the attributes for contacting between LNGC and LNG FSRU are berth length, radius of turning basin area and the probability of crossing wind.

For LNG transferring process, the connection flange failure and connection hose failure were identified as major attributes for the identified fires based on the collected data. By considering the correlations and mutual dependency, the final evaluation network is determined, shown as Figure 6.

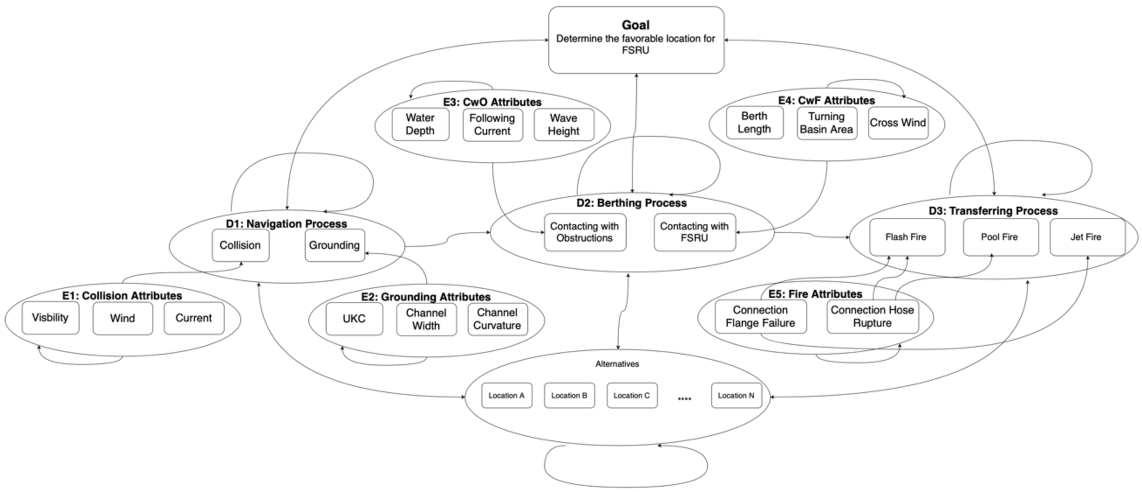


Figure 6. FSRU-LNGC System Evaluation Network of QMNMDA

From Figure 6, we can see that the three processes are set as independent but each of them has dependent elements, and the E level lists the leading factors to the identified events of the D level.

(4) Attribute utility value determination

To analyze the safety performance of proposed FSRU LNGC system, the five scale set is predetermined as V, $V = (v_1, v_2, v_3, v_4, v_5) =$ (favorable, acceptable, moderate, limited acceptable, unacceptable). In order to determine the utility value of each attribute, the FSRU-LNGC risk analysis group must establish an evaluation scale. The group was made up with 30 senior officers of deck department aboard ships, 30 professional pilots and 30 professors from maritime colleges. Based on the opinions of the expert judgment team and previous studies on the marine maneuvering, every individual attribute was evaluated quantitatively based on the safety utility value (SUV) or risk tolerance index, which was distributed evenly from 0 to 1 with the interval of 0.2. Furthermore, safety utility value range from 0.8 to 1.0 means the environment of this location is favorable to locate LNG FSRU, while the value locating between 0.6 and 0.8 means it is acceptable for LNG FSRU; the range 0.4 to 0.6 means moderate environmental conditions for the system; limited acceptable when the SUV is in the range of 0.2 to 0.4; it is unacceptable when the utility value goes below 0.2. The evaluation standards for adopted attributes of navigational and berthing process were established based on the collected questionnaires (see Appendix 1). The total evaluation standards were displayed in the Table 5 by analyzing the collected data for all the attributes of navigational process and berthing process.

Table 5. Evaluation Standard for Each Attribute of Maritime Safety Study

Utility Range / Factors	*Favorable, (0.8,1]*	*Acceptable, (0.6,0.8)*	*Moderate, (0.4,0.6]*	*Limited Acceptable, (0.2,0.4]*	*Unacceptable, [0,0.2]*
Visibility (d/y)	＜15	15～20	20～30	30～40	＞40
Windy Days (d/y)	＜30	30～60	60～100	100～150	＞150
Following Current Prob.	< 3%	3~6%	6~10%	10~15%	>15%
Channel Width	>900	650~900	450~650	300~450	< 300
Channel Curvature	<15°	15°~25°	25°~35°	35°~45°	>45°
UKC	>15m	10~15m	5~10m	2~5m	<2m
Water Depth	>25m	22~25m	18~22m	15~18m	<15m
Following Current	<0.3m/s	0.3~0.6	0.6~0.8	0.8~1	>1m/s
Wave Height	＜0.3m	0.3～0.6	0.6～1.0	1.0～1.2	＞1.2m
Berth Length	>2.5L	2~2.5L	1.5~2L	1.2~1.5L	<1.2L
Turning Basin Area	>1200m	1000~1200 m	800~1000 m	600~800 m	<600m
Cross Wind Prob.	< 1.5%	1.5~3%	3~4.5%	4.5~6.5%	>6.5%

The data collected by the Delphi approach are utilized to establish the evaluation standard, and then the utility value function of E-level elements in Figure 6 are able to be established by statistical tools, see Appendix 2; next, the real observation data and the boundary value of evaluation scale may be used to determine the utility value for the attribute layer. Multiplying the utility values by the corresponding weight factors, the overall utility value for FSRU LNGC system is obtained by the following function.

$$Overall\ Utility\ Value = k_{NP}\sum_{i} w_i A_{NP} + k_{BP}\sum_{j} w_j A_{BP} + k_{TP}\sum_{k} w_k A_{TP}$$

Where k_{NP}, k_{BP}, k_{TP} stand for the weight values of each process, w_i, w_j, w_k are defined as sub-weight factors of each attribute, and A_{NP}, A_{BP}, A_{TP} are described as the utility value of each attribute of navigation process, berthing process and transferring process.

4. Case Study

To assess the safety extent of FSRU-LNGC systems, two locations were applied to carry out case study based on the proposed model. The proposed LNG FSRU for Location A is at the south edge of the coast line and at a near shore area; while the proposed Location B is at the northeast side of the coast line, and at an offshore area, 2300 meters extended from the shoreline. The proposed direction of Location A is 053°～233°, berth length is 446 meters (m); the design direction of Location B is 099°～279° and berth length is 430 m. After the dimension of two proposed locations were determined, the evaluation steps can be processed from LNGC navigating in the inbound channel to the LNG successfully transferring from LNGC to FSRU.

4.1 Maritime Processes

Besides the proposed locations of FSRU-LNGC systems, a common LNGC type, Q-Flex, is applied in this study as the input ship type of the ship simulator by considering the current trend for LNG offshore application, and the dimension of its receiving unit FSRU is predetermined accordingly (Bowen et al., 2008), see Table 6.

Table 6. Parameters of LNGC and FSRU

Parameters	LNGC(Q-Flex)	FSRU
LOA	303	315
Loading Capacity	142933.7 m^3	217000 m^3
Breadth	50	50
Draft	12	12.5

At the left side of the bowtie shown in Figure 4 five scenarios are presented. From those we shall consider here only the flange and hose ruptures. The LNGC or FSRU LNG tank rupture will occur only after a collision incident, where the probability will be a fraction of the collision probability depending on collision speed and location of collision. It will be difficult to estimate the probability with any accuracy, but the frequency may be lower than 10^{-6}/yr, hence rather unlikely. On the other hand, very large LNG clouds resulting from a gaping hole in a tank may travel as a heavy gas over a distance of say 2 kms. In case of delayed ignition, it is not sure what will happen, flash fire or VCE. There remains the re-gasification unit. There is at least one typical accident known on a peak shaving plant that occurred in 2014, at which maintenance work at the unit resulted in an explosion propelling a fragment toward a tank and perforating the wall (Rukke, 2016). Also, here it will be difficult to estimate a failure frequency rate.

Generally, the loading / unloading equipment of FSRU have four liquid loading hoses and two vapor return hoses, each of them has one spare part. Referred from 20, the maximum loading capacity, length of LNG loading hoses and other parameters are listed in Table 7 (Nafta, 2015).

Table 7. Parameters of FSRU's Loading Equipment

Parameter	Value
Maximum Loading Capacity	8000 m^3/h for all loading hoses
Maximum Unloading Capacity	5000 m^3/h for all loading hoses
Number of LNG Loading Hoses	4 (1 spare)
Number of Vapor Return Hoses	2 (1 spare)
Inner Diameter of LNG Loading Hoses	0.254 m
Length for LNG Loading Hoses	18.5 m
Inner Diameter of LNG Loading Hose Flange	0.41 m
Inner Diameter of Vapor Return Hose Flange	0.41 m

Considering the data availability for attributes of collision hazard, the visibility parameter is determined by number of days under poor visibility (visible distance < 4000 m) per year; the wind parameter is determined by number of days under standard wind scale, which is equal to number of days under Beaufort scale 6 and 7 plus 1.5 times number of days under Beaufort scale 8 or more (Ji et al., 2014); and the parameter current is determined by the probability of following current, which is the most difficult situation for ship maneuvering. For grounding hazard, the attribute channel width and channel curvature can be determined directly by the actual channel data, and the minimum under keel clearance (UKC) is equal to the minimum chart water depth minus actual draft of LNGC. For the second process, berthing process simulation, the water depth for the contacting possibility for LNGC and other navigation obstruction is the minimum water depth in berthing area; "Following Current" is the magnitude of following current during berthing operation; while the transverse wave height can be directly obtained from the hydrographic data of two harbor authorities. For the hazard of possible collision with FSRU, the berth length and turning basin area is the values of designed berth length and radius of turning water, and the crossing wind, which is defined as the wind blowing the LNGC toward FSRU side, was evaluated by the wind rose maps of two locations. Therefore, the actual values of navigation process and berthing process related attributes for two alternatives are shown in Table 8. Then the utility values of navigation process and berthing process are calculated by maximum membership functions integrating evaluation scale in Table 6.

Table 8. Values of Maritime Processes Related Attributes for Two Locations

	Channel Width	Channel Curvature	UKC	Windy Days	Following Current Prob.	Visibility	Water Depth	Following Current	Wave Height	Berth Length	Turning Area Radius	Crossing Wind Prob.
Location A	1050m	31°	12m	140	7.6%	22	20 m	0.8m/s	1.08 m	1.5L	1020m	4.6%
Location B	690 m	27°	5m	151	9.3%	30	17m	0.85m/s	0.81 m	1.25L	1260m	3.8%

4.2 LNG Transferring Process

Based on the previous research (D'alessandro et al., 2016; Pitblado et al., 2006), it is a reasonable to simulate this event "LNG releasing on the water" by two scenarios: one is called maximum credible scenario (MCS), which is defined as: an accident that is within the realm of possibility (i.e., probability higher than 1×10^{-6}/yr) and has a propensity to cause significant damage (at least one fatality) (Khan, 2001).; another one is called worst case scenario (WCS), which means the extremely dangerous situation for FSRU LNGC system.

For the two scenarios, the external environment factors for weather data input, wind, air temperature and relative humidity, can be obtained from the meteorological and hydrographic records of two locations, and the input data for MCS and WCS are listed in Table 9.

Table 9. Input Data for Simulation Plans

	Wind	**Air Temperature**	**Humidity**	**Pasquill Stability**	**Estimated Release Volume**	**Hole Size Diameter**
Maximum Credible Scenario (MCS)	Prevailing Wind (A; 8 m/s, N; B:6.7m/s, NE)	Yearly Average (A: 10.5℃; B:15.1℃)	Yearly Average Humidity (A: 69%; B: 75%)	E	1167 m^3	0.2m (Flange Failure)/0.12m (Hose Rupture)
Worst Case Scenario (WCS)	15m/s (A: SE; B: NE)	Highest Monthly Average Temperature (A: 15.1℃; B: 20.6℃)	Highest Monthly Average Humidity (A: 83%; B: 88%)	Loc. A: C; Loc. B: D	2667m^3	0.41 m (Flange Failure)/0.254 m (Hose Rupture)

For maximum credible scenario, the input parameter "wind" was the prevailing wind for two locations. As shown in Figure 9, the wind rose map of location A shows the prevailing wind direction was north wind with the speed of 8 m/s; while the prevailing wind direction of location B is northeast wind with the speed of 6.7 m/s; the air temperature for MCS was the average temperature of one whole year, where 10.5 degree centigrade for location A and 15.1℃ for location B; similarly, the humidity parameter was selected as the average humidity for a whole year, 69% for location A and 75% for Location B.

For worst case scenario, the "wind" parameter was the most hazardous when the wind is blowing toward the pier since the fire may get more assets and people involved. By considering the wind rose map of each location, the most hazardous wind directions were southeast and northeast for location A and location B, respectively and the worst wind speed is 15m/s because it is the maximum speed to allow LNG transferring operation under Chinese regulations (JTS 165-5-2016). Since the air temperature may fluctuate day to day, the WCS air temperature was chosen as the highest monthly average one for a whole year, 15.1℃ for location A and 20.6℃ for location B.

Similarly, the humidity parameter was determined as the highest monthly average humidity for a whole year, 83% for location A and 88% for location B.
The release preconditions, hose loading capacity, leakage time and hole size, were determined as the main parameters to define the exact releasing volume of MCS and WCS. For WCS, the hose loading capacity was referred as the LNG FSRU's maximum loading capacity and the accidental release time was determined as 20 minutes to calculate the simulated release volume for the events as connection hose rupture and flange failure. As shown in Table 5, the inner diameter of LNG loading hose and loading hose flange were 0.254 m and 0.41 m, respectively, so the hole size was determined as the total-damage scenario. For MCS, the hose capacity was determined as the 87% of the maximum loading capacity and the release time was 10 minutes; the holes were determined as 0.2 m for connection flange failure and 0.12 m for connection hose rupture scenario.

The runs were designed in 4 group comparisons with 8 simulations by DNV-GL PHAST software, shown in Table 10. Simulation plan 1, 2, 3 and 4 were taken for connection flange failure. Among these four simulation plans, simulation plan 1 and 2 took place in location A under scenario MCS and WCS, respectively; Simulation plan 3 and 4 took place in location B under scenario MCS and WCS. Meanwhile, simulation runs 5 to 8 were for connection hose rupture, and simulation plan 5 and 6 took place in location A under scenario MCS and WCS; Simulation plan 7 and 8 took place in location B under scenario MCS and WCS, respectively.

Table 10. Outcomes of Designed Simulation Plans

Plan	Location	Scenario	Dia. of Hole Size (mm)	Est. Leakage Volume	Fire Type	Thermal Radiation Distance (m)			Flammability Limits Distance (m)		
						$4kW/m^2$	$12.5kW/m^2$	$37.5kW/m^2$	UFL	LFL	0.5LFL
1	A	MCS	200	1167	Flash				220	794	1590
2	A	WCS	410	2667	Jet	1141	1022	976			
3	B	MCS	200	1167	Flash				194	771	1546
4	B	WCS	410	2667	Jet	1128	1016	976			
5	A	MCS	120	1167	Flash				11	77	277
6	A	WCS	254	2667	Pool	501	302	192			
7	B	MCS	120	1167	Flash				9	70	202
8	B	WCS	254	2667	Pool	722	525	222			

Figure 7 shows the preliminary simulation outputs for two alternatives under the condition of "flange failure with worst case scenario" (simulation plan 2 and 4).

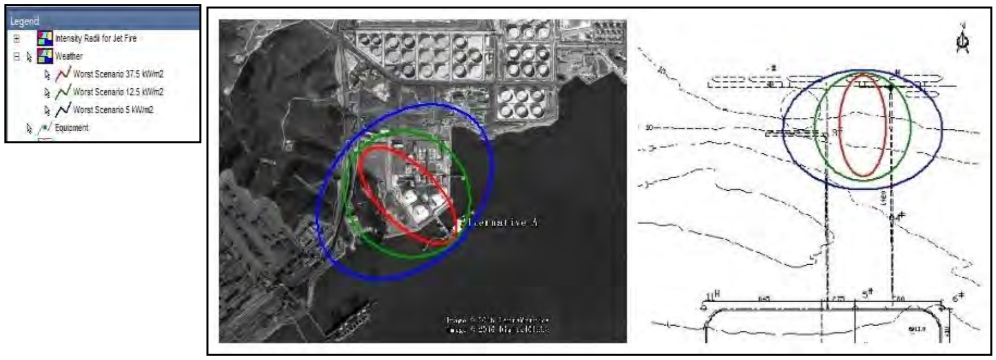


Figure 7. Simulation Outputs for Two Alternatives under WCS for Event A

From Figure 7, on the ***left*** is the simulated thermal radiation influence areas of location A and on the ***right*** that of location B. The red circle is the high thermal radiation area with heat flux 37.5 kW/ m^2, the green one is the thermal radiation intensity of 12.5 kW/c and the blue circle is the range of thermal radiation intensity of 5kW/m^2. Meanwhile, other simulation plans were taken under different input data, and Table 11 shows all simulated outcomes of eight simulation plans. The potential fatalities would be calculated based on the values of thermal radiation distance and flammability limits distance.

4.3 Results and discussions

After the completion of simulation runs for three processes, the utility value should be determined from bottom hierarchy to the top. Navigational process and berthing process, which were called maritime safety study in this research, adopted risk evaluation matrix to determine each utility value; while for chemical process safety part, LNG transferring process was determined by the potential loss of life (PLL), which given the population density is in principle the integral of the societal risk incidents presented as components of the so-called $F–N$ -curve ($PLL = \sum_{i=1}^{n} f_i N_i$). PLL is expressed in fatalities/year; the metric is also called Expected Value (EV) (Hirst and Carter, 2002) and Average Rate of Death (RoD) (CCPS, 2000).

The vulnerable building for two alternatives should be determined to calculate PPL value. Three ranges (500-meter circle, 1000-meter circle and 1500-meter circle) were drawn to show potential damaged buildings for location A and B. On the other hand, the PLL of flash fire was calculated by the distances of LFL and 0.5 LFL. The possibility of fatality was assumed 100% in Zone 1, a defined zone between UFL contour and LFL contour; and 50% for Zone 2, defined between LFL contour and 0.5 LFL contour. Referred by DNVGL MPACT Model (DNVGL, 2016), the heat flux value "4 kW/m^2" could lead to 1% possible fatality, while the value of "12.5 kW/m^2" was 50% and the value of "37.5 kW/m^2" was 100%. As for the range between these three-point values, the lethality ellipse, was employed to calculate the PLL in this study. According to the Table 10, the PLLs of location A and location B under MCS and WCS were calculated shown in below table.

Table 11. Summary of PLL for Simulation Runs

Plan	Loc.	Scenario	Fire Type	Involved Vulnerable Buildings	Potential Involved Personnel	PLL	Thermal Radiation Distance			Flammability Limits Distance		
							$4kW/m^2$	$12.5kW/m^2$	$37.5kW/m^2$	UFL	LFL	0.5LFL
1	A	MCS	Flash	Working stations (7), LNG tanks (3), residential area (1), LNG FSRU system (1), berth (2), office building (1), warehouses (3), storage tanks (15), grocery shop (1), police station (1)	Zone 1:301; Zone 2: 76	339				220	794	1590
2	A	WCS	Jet	Working stations (3), LNG tanks (3), residential area (1), berth (1), LNG FSRU system (1), office building (1)	Red Zone: 694; Blue Zone: 10; Green Zone: 15	706	1141	1022	976			
3	B	MCS	Flash	LNG FSRU system (1), berth (2), pipeline bridge (2), turning basin (1)	Zone 1:78; Zone 2: 38	97				194	771	1546
4	B	WCS	Jet	LNG FSRU system (1), berth (1), pipeline bridge (2), turning basin (1)	Red Zone: 124; Blue Zone: 15; Green Zone: 25	142	1128	1016	976			
5	A	MCS	Flash	Working stations (1), LNG tanks (1), LNG FSRU system (1)	Zone 1:14; Zone 2: 28	28				11	77	277
6	A	WCS	Pool	Working stations (1), LNG tanks (3), LNG FSRU system (1)	Red Zone: 40; Blue Zone: 20; Green Zone: 9	58	501	302	192			
7	B	MCS	Flash	LNG FSRU system (1), pipeline bridge (1)	Zone 1:14; Zone 2: 10	19				9	70	202
8	B	WCS	Pool	LNG FSRU system (1), berth (1), pipeline bridge (2), turning basin (1)	Red Zone: 32; Blue Zone: 17; Green Zone: 35	54	722	525	222			

The probability 10^{-5} per year was usually defined as the boundary of the individual risk of fatality for marine transfer operation (MARIN, 2016). The frequency of each scenario can be obtained from the event tree analysis, so the value of risk can be calculated by PLL timing frequency. Based on the ALARP boundary values (Sames and Hamann, 2009), the safety utility scale was built accordingly. By the calculated weight value of three processes, the total utility value for Location A and Location B under maximum credible scenario can be determined.

The total safety utility value for location A under MCS is:

$$SUV_A = k_{NP} \sum_i w_i A_{NP} + k_{BP} \sum_j w_j A_{BP} + k_{TP} \sum_k w_k A_{TP} = 0.4225 \quad (14)$$

The total utility value for location B under MCS is:

$$SUV_B = k_{NP} \sum_i w_i A_{NP} + k_{BP} \sum_j w_j A_{BP} + k_{TP} \sum_k w_k A_{TP} = 0.5931 \quad (15)$$

Under WCS, $SUV'_A = 0.1212$; $SUV'_A = 0.2036$.

Therefore, location B performs better than location A either under MCS or WCS. Under MCS, they both located in the moderate level, but under WCS, the safety utility value of location A and B were in the limited acceptable range. The calculated results told us the extreme external conditions should be avoided in advance to ensure the safety of the FSRU-LNGC system.

For the navigational process, location A outperformed location B on both “collision” and “grounding”, proving the navigation environment of location A was more reliable for LNG carriers than that of location B; for berthing process, location B had a higher overall score, showing it was less risky for identified contacting with berthing obstructions and LNG FSRU. For LNG transferring process, two events and two scenarios were identified for LNG accidental release, location B performed better than location A on both of the two events as it separated the populated areas with two pipeline bridges so that less vulnerable buildings were involved in the vicinity of location B. Location B outperformed location A in two of three processes, and had a higher score in the total utility value since offshore FSRU is a safer solution, although offshore area usually has a less favorable navigation environmental factors.

5. Conclusion

This research serves as a quantitative way to evaluate the three consecutive processes for an integrated engineering system, FSRU-LNGC system. A QMNMDA model was presented to evaluate the process safety level of the defined system and both ship simulator and consequence analysis were employed to fulfill the research objective. In addition, a real case with two FSRU areas was taken to show the procedures of this safety analysis. During the evaluation process, some may be taken into account to mitigate the systematic risk into an acceptable level. For navigational process, the security zones, both static and dynamic zones, should be set up for large scale LNG carriers, such as Q-Flex and Q-Max, to avoid other traffic interfering LNGC, and this measure has been proved to reduce the occurrence of collision in inbound channels significantly by Ma and Wu (Ma and Wu, 1998); the recommended routes should be always top priority to navigate since the UKC can meet the requirement of safe sailing or large draft vessels may ride on the tide to pass the shallow areas. For berthing process, enough turning basin, especially enough berthing width should be ensured to lower the risk of contact with FSRU or other navigational hazards, and the transverse speed of the LNGC should be observed frequently when it is approaching the LNG FSRU. For LNG transferring process, the emergency plan and procedures should be implemented before the operation begins; the responsible officers should be assigned to ensure every possible contingency could follow an organized procedure; evacuation plans and extreme situation trainings were the key factors to succeed in potential disasters.

This study serves a trial to apply both nautical simulation and chemical process simulation on offshore industry. In the evaluation process, the objective environmental factors were evaluated via simulation and statistical software. However, human factors and other uncertainties are necessary to consider under different hydrographic and meteorological conditions for the FSRU-LNGC system. From the perspective of offshore safety, this data-driven direction would be a right way to establish evaluation scale in a more close-to-reality way. To accomplish this goal step by step, more data sources should be added to monitor LNG operations in different dimensions and more non-linear mathematical models should be applied to build a clearer relationship between raw data and safety performances for both LNGC and FSRU.

Acknowledgement
I would like to pay my highest respect to Dr. Mannan for his great contribution to make this world safer and better. His attitude towards process safety will be always memorized.

REFERENCES

Abbasi, T., Pasman, H.J., Abbasi, S.A., 2010. A scheme for the classification of explosions in the chemical process industry. J. Hazard. Mater. https://doi.org/10.1016/j.jhazmat.2009.09.047

Andersson, H., Christiansen, M., Fagerholt, K., 2010. Transportation Planning and Inventory Management in the LNG Supply Chain. https://doi.org/10.1007/978-3-642-12067-1_24

Aronsson, E., 2012. FLNG compared to LNG carriers. Chalmers Univ. Technol.

Bai, J., 2010. Simulation of Large Vessel Berthing Maneuvering. Dalian Maritime University.

Bowen, R.R., Miller, M., Planteen, J., Tredennick, O., Norman, G., Duke, C.M., Greer, M.N., 2008. LNG Technology Advances and Challenges 1990, 1–9. https://doi.org/10.2523/iptc-12111-ms

CCPS, 2000. Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Ed. AIChE Center for Chemical Process Safety, ISBN 0-8169-0720-X

Chang, D.Y., 1996. Applications of the extent analysis method on fuzzy AHP. Eur. J. Oper. Res. 95, 649–655. https://doi.org/10.1016/0377-2217(95)00300-2

COWI, 2008. Risk Analysis of Sea Traffic in the Area around Bornholm 1–150.

D'alessandro, A.A., Izurieta, E.M., Tonelli, S.M., 2016. Decision-making tools for a LNG regasification plant siting. J. Loss Prev. Process Ind. 43, 255–262. https://doi.org/10.1016/j.jlp.2016.05.012

DNVGL, 2016. Theory MPACT Model.

Finn, A.J., 2002. Effective LNG production offshore. GPA Annu. Conv. Proc.

Fujii, T., Arai, Y., Asama, H., Endo, I., 1998. Multilayered reinforcement learning for complicated collision avoidance problems, in: Proceedings - IEEE International Conference on Robotics and Automation. https://doi.org/10.1109/ROBOT.1998.680648

Fujii, Y., Yamanouchi, H., Mizuki, N., 1974. Some factors affecting the frequency of accidents in marine traffic. J. Navig.

GIIGNL Annual Report, 2019. The LNG industry THE LNG INDUSTRY 1–60.

Hightower, M., Gritzo, L., Luketa-hanlin, A., Covan, J., Tieszen, S., Irwin, M., Kaneshige, M., Melof, B., Morrow, C., Ragland, D., 2004. Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water. Explosion. https://doi.org/SAND2004-6258

Hirst, I.L. and Carter, D.A., 2002. A "worst case" methodology for obtaining a rough but rapid indication of the societal risk from a major accident hazard installation, Journal of Hazardous Materials A92, 223–237

Ji, C., Ahammad, M., Mannan, S., 2017. Facility layout optimization of LNG-FSRU system, in: Institution of Chemical Engineers Symposium Series.

Ji, C., Chen, S., Xie, H., 2014. Research on Feasible Degree of Navigation Environment for CALM Type Single Point Mooring System. J. Dalian Marit. Universtiy 2, 29–32.

JTS 165-5-2016, 2016. Code for Design of Liquefied Natural Gas Port and Jetty.

Keeney, R., Raiffa, H., 1976. Decisions with Multiple Consequences: Preferences and Value Tradeoffs, Cambridge Books. https://doi.org/10.1057/jors.1977.126

Li, S., Meng, Q., Qu, X., 2012. An Overview of Maritime Waterway Quantitative Risk

Assessment Models. Risk Anal. https://doi.org/10.1111/j.1539-6924.2011.01697.x
Liu, Y., So, R.M.C., Lau, Y.L., Zhou, Y., 2001. Numerical studies of two side-by-side elastic cylinders in a cross-flow. J. Fluids Struct. https://doi.org/10.1006/jfls.2001.0383
Ma, H., Wu, Z., 1998. Evaluation and analysis on danger degree of port shipoperating environment by Grey System Theory. J. Dalian Marit. Universtiy.
Macduff, T., 1974. THE PROBABILITY OF VESSEL COLLISIONS. Ocean Ind.
MARIN, 2016. Nautical And Risk Studies for the Delimara LNG Terminal in Marsaxlokk Port, Malta. Item 6: Nautical Quantitative Risk Assessment (QRA) Report.
Martins, M.R., Pestana, M.A., Souza, G.F.M., Schleder, A.M., 2016. Quantitative risk analysis of loading and offloading liquefied natural gas (LNG) on a floating storage and regasification unit (FSRU). J. Loss Prev. Process Ind. 43, 629–653. https://doi.org/10.1016/j.jlp.2016.08.001
Montewka, J., Krata, P., Goerlandt, F., Mazaheri, A., Kujala, P., 2011. Marine traffic risk modelling - An innovative approach and a case study. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. 225, 307–322. https://doi.org/10.1177/1748006X11399988
Nafta, S.K., 2015. REGULATIONS FOR USE OF THE LIQUEFIED NATURAL GAS TERMINAL.
Pedersen, P.T., 1995. Collision and Grounding Mechanics. Proc. WEGEMT'95.
Pekalski, A., Puttock, J., Chynoweth S., 2014. DDT in a vapour cloud explosion in unconfined and congested space: large scale test. X ISPHMIE, Tenth International Symposium on Hazards, Prevention, and Mitigation of Industrial Explosions, Bergen, Norway, 10-14 June, 847-856
Pitblado, R., Baik, J., Raghunathan, V., 2006. LNG decision making approaches compared, in: Journal of Hazardous Materials. https://doi.org/10.1016/j.jhazmat.2005.07.081
Planas, E., Pastor, E., Casal, J., Bonilla, J.M., 2015. Analysis of the boiling liquid expanding vapor explosion (BLEVE) of a liquefied natural gas road tanker: The Zarzalico accident. Journal of Loss Prevention in the Process Industries 34, 127-138.
Rukke, S. (2016). Failure Investigation Report – Liquefied Natural Gas (LNG) Peak Shaving Plant, Plymouth, Washington. https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/FIR_and_APPENDICES_PHMSA_WUTC_Williams_Plymouth_2016_04_28_REDACTED.pdf
Saaty, T.L., 1990. How to make a decision: The analytic hierarchy process. Eur. J. Oper. Res. https://doi.org/10.1016/0377-2217(90)90057-I
Saif, M., Wang, W., Pekalski, A., Levin, M., Radulescu, M.I., 2017. Chapman–Jouguet deflagrations and their transition to detonation. Proceedings of the Combustion Institute 36, 2771–2779.
Sames, P.C., Hamann, R., 2009. Towards Environmental Risk Acceptance Criteria. https://doi.org/10.1115/omae2008-57257
Schleder, A.M., Martins, M.R., Souza, G.F.M., 2011. Bayesian Networks on Risk Analysis of a Regasification System on an Offshore Unit. https://doi.org/10.1115/omae2011-49393
Shapira, A., Goldenberg, M., 2005. AHP-Based Equipment Selection Model for Construction Projects. J. Constr. Eng. Manag. https://doi.org/10.1061/(asce)0733-

9364(2005)131:12(1263)
Simonsen, B.C., 1997. Mechanics of ship grounding.
Winbow, A., 2002. The importance of effective communication, in: International Seminar on Maritime English.
Woodward, J.L., Pitblado, R.M., 2010. LNG Risk Based Safety: Modeling and Consequence Analysis, Wiley. https://doi.org/10.1002/9780470590232
Yang, Y., 1996. Study on mathematical model for simulating ship berthing or unberthing. J. Dalian Marit. Universtiy 4.
Zhang, X., Yin, Y., Jin, Y., 2007. Ship motion mathematical model with six degrees of freedom in regular wave. J. Traffic Transp. Eng. 3.

APPENDIX 1: Sample Questionnaire for Safety Utility Value of LNG FSRU

Evaluation Attributes

Which department are you in?
1. Maritime Institute
2. Pilot Station
3. Shipping Company

How many years have you worked/researched for LNG carriers?
1. Less than 5years
2. 5 to 8 years
3. More than 8 years

The evaluation scale was set between 0 and 1, and five evaluation ranges were determined with the even interval of 0.2 based on the safety level for LNG FSRU system, see table below.

Table. 1-1 Quantitative Value for Safety Qualitative Evaluation

Favorable	Acceptable	Moderate	Limited Acceptable	Unacceptable
[0.8,1]	[0.6,0.8)	[0.4,0.6)	[0.2,0.4)	[0,0.2)

Safety utility value range from 0.8 to 1.0 means the environment of this location is favorable to build LNG FSRU, while the value locating between 0.6 and 0.8 means it is acceptable for LNG FSRU; the range 0.4 to 0.6 means moderate environmental conditions for the system; limited acceptable when the safety utility value is in the range of 0.2 to 0.4.

Safety Evaluation for “Visibility”
Visibility value for LNG carrier is defined as the number of days under poor visibility (visible distance < 4000m) per year. Now please fill the blanks about the relevant values.

Which value do you think is the most appropriate one when safety utility value of “Visibility” is set as 0.2, 0.4, 0.6 and 0.8, respectively? Please fill the blanks.

Table. 1-2 “Visibility” Evaluation Table

	Safety Utility Value= 0.2	Safety Utility Value= 0.4	Safety Utility Value= 0.6	Safety Utility Value= 0.8
Restricted Visibility Days/Yr				

APPENDIX 2: Utility Function Determination for “Visibility” by R

```
> lm.fit=lm(Risk~Vis, data=data1)
> summary(lm.fit)

Call:
lm(formula = Risk ~ Vis, data = data1)

Residuals:
     Min       1Q   Median       3Q      Max
-0.19608 -0.12252 -0.01319  0.12838  0.27082

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  0.8303064  0.0440807   18.84   <2e-16 ***
Vis         -0.0108557  0.0009122  -11.90    7e-15 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.1407 on 41 degrees of freedom
Multiple R-squared:  0.7755,     Adjusted R-squared:   0.77
F-statistic: 141.6 on 1 and 41 DF,  p-value: 7.005e-15
```

Figure 2-1. For “Risk= $\beta_0+\beta_1$Vis”

```
> lm.fit=lm(Risk~log(Vis), data=data1)
> summary(lm.fit)

Call:
lm(formula = Risk ~ log(Vis), data = data1)

Residuals:
      Min        1Q    Median        3Q       Max
-0.115569 -0.060755 -0.001431  0.057830  0.183096

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.93130    0.06452   29.93   <2e-16 ***
log(Vis)    -0.43800    0.01784  -24.56   <2e-16 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.07494 on 41 degrees of freedom
Multiple R-squared:  0.9363,     Adjusted R-squared:  0.9348
F-statistic:   603 on 1 and 41 DF,  p-value: < 2.2e-16
```

Figure 2-2. For “Risk= $\beta_0+\beta_1$In(Vis)”

```
> summary(lm.fit)

Call:
lm(formula = Risk ~ Vis + I(Vis^2), data = data1)

Residuals:
      Min        1Q    Median        3Q       Max
-0.112369 -0.036073  0.004677  0.040416  0.143156

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.251e+00  3.279e-02   38.14   <2e-16 ***
Vis         -3.495e-02  1.637e-03  -21.35   <2e-16 ***
I(Vis^2)     2.555e-04  1.694e-05   15.08   <2e-16 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.05511 on 40 degrees of freedom
Multiple R-squared:  0.9664,     Adjusted R-squared:  0.9647
F-statistic: 575.5 on 2 and 40 DF,  p-value: < 2.2e-16
```

Figure 2-3. For “Risk= $\beta_0+\beta_1$Vis+ β_2Vis^2”

```
> lm.fit=lm(Risk~Vis+I(Vis^2)+I(Vis^3), data=data1)
> summary(lm.fit)

Call:
lm(formula = Risk ~ Vis + I(Vis^2) + I(Vis^3), data = data1)

Residuals:
      Min        1Q    Median        3Q       Max
-0.124696 -0.009811  0.000220  0.012575  0.138456

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.464e+00  4.408e-02  33.224  < 2e-16 ***
Vis         -5.504e-02  3.662e-03 -15.030  < 2e-16 ***
I(Vis^2)     7.492e-04  8.583e-05   8.729 1.04e-10 ***
I(Vis^3)    -3.441e-06  5.918e-07  -5.814 9.38e-07 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.04085 on 39 degrees of freedom
Multiple R-squared:  0.982,      Adjusted R-squared:  0.9806
F-statistic: 709.6 on 3 and 39 DF,  p-value: < 2.2e-16
```

Figure 2-4. For “Risk= $\beta_0+\beta_1$Vis+ β_2Vis^2 +β_3Vis^3”

```
> lm.fit=lm(Risk~Vis+I(Vis^2)+I(Vis^3)+I(Vis^4), data=data1)
> plot(lm.fit)
> summary(lm.fit)

Call:
lm(formula = Risk ~ Vis + I(Vis^2) + I(Vis^3) + I(Vis^4), data = data1)

Residuals:
      Min        1Q    Median        3Q       Max
-0.093642 -0.016540 -0.000006  0.018339  0.132348

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.362e+00  7.141e-02  19.071  < 2e-16 ***
Vis         -4.131e-02  8.437e-03  -4.897 1.83e-05 ***
I(Vis^2)     1.870e-04  3.243e-04   0.577   0.5676
I(Vis^3)     5.337e-06  4.927e-06   1.083   0.2855
I(Vis^4)    -4.588e-08  2.557e-08  -1.794   0.0808 .
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.03973 on 38 degrees of freedom
Multiple R-squared:  0.9834,     Adjusted R-squared:  0.9817
F-statistic: 563.2 on 4 and 38 DF,  p-value: < 2.2e-16
```

Figure 2-5. Risk= $\beta_0+\beta_1$Vis+ β_2Vis^2+β_3Vis^3 +β_4Vis^4

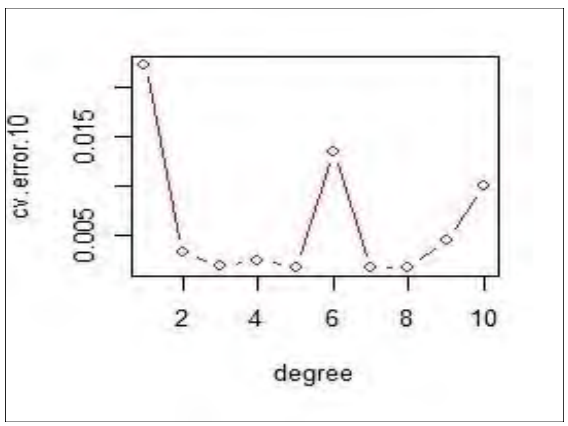


Figure 2-6. K-fold Cross Validation

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

How to Improve the Trust in Safety Related Instruments

Wolter Last*
Hint Americas Inc.
2800 Post Oak Boulevard, Suite 4100
TX 77056, Houston
*Presenter E-mail: wlast@hint-global.com

Abstract

Yearly Instrument Protective Functions (IPF) reports for safety critical elements are common practice in the oil and gas and petrochemical industry. Including mean time between failures (MTBF) calculations and fail to danger/ fail to safe evaluations, they give an overview about the integrity of the installed based instruments and help to define eventual engineering adjustments. However, input information for the IPF reports are often manually entered on paper or in excel sheets which is inefficient, costly and subject to human errors. Plants sometimes cannot retrieve or store the instrument data because the infrastructure is not there to connect to directly.

The method of monitoring process safety and fire & gas instrument within the oil and gas and petrochemical industry needs to evolve. Operators need to be able to trust their instruments and rely on actual, accurate and controlled real-time data.

What if the process safety instrument data were automatically entered in a process safety maintenance management system? IPF reports could be customized and generated any time, instrument maintenance activities could be triggered by predefined conditions, etc. The possibilities are extensive.

By using an automatic process safety maintenance management system, the reliability of safety related instrument can be improved, company risks can be reduced, and the efficiency of testing and can be increased.

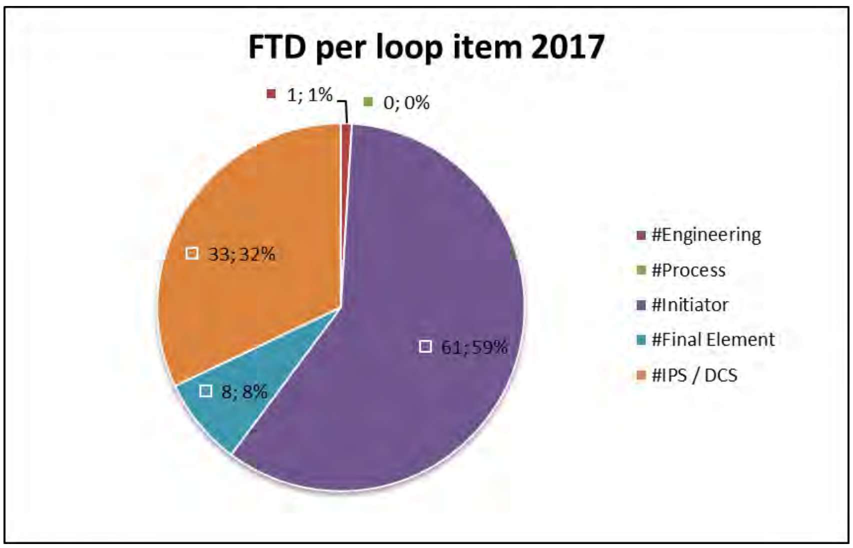
Keywords: Instrument Integrity, Risk Reduction, Process Safety Management System, Instrument Protective Functions, Condition Based Maintenance, Safety Integrity level (SIL).

1 Introduction

Nowadays it is uncommon to wait an extensive period to receive results. If you must wait a week for medical results, you start questioning why it is taking that long. Yet in some parts of the industry it is still acceptable to have yearly intervention moments, instead of real time observation. Instrument Protective Functions (IPF) reports are usually done on a 6- or 12-month schedule. These reports provide results on the reliability of the process safety related instrument. In worst case scenario it would be possible to have a poor performing process safety instrument of nearly a year. Would you trust a doctor that lets you wait months for results?

Process safety reporting should be required by law to obtain and keep the license to operate. There are international standards like: IEC 61511, API, ISA and legislations which outline the requirements to obtain a license to operate. If these requirements are not met, the plant is not permitted to operate. These laws and legislations set a base level of trust in the operations of a plant.

Safety related instruments are the principal contributors to possible failures of most protective functions as shown in below graphic taken from a major oil company's 2017 IPF report.



For this example, the field instruments (initiators + final elements) are responsible for a 70% of the Failure To Danger (FTD's). This means that engineering and maintenance effort should concentrate on the field instruments.

Instruments are evolving from simple 4-20 milliamp transmitters into smart instruments, which don't only transmit the reading, but are also capable of sharing health status information. Example of instruments are temperature, pressure, level transmitters, process safety valves, fire, smoke and gas detectors etc. Testing/validation/calibration can even be done automatically. Yet in IPF reporting it is still common to do manual validations. While doing these validations, the results are written down on paper or in more advance cases logged into a handheld. This process is time consuming and error prone. Within the industry the biggest margin of errors is caused by humans. With the capabilities of smart instrument this process can be automated. The validations from the field can immediately be stored into a database, preventing the human errors in the process.

Manual validations require a person to be present while the validation runs, to observe the results. When using instrument automated validations, the presence of a person is not needed and can be executed remotely. This would mean that 1 person could start multiple validations at the same time and have the results be stored automatically, which saves significant amounts of time.

Being able to remotely trigger the validations can improve the time efficiency even further. Smart instrument can handle remote triggers to start their validations. Considering the process, there is the potential to initiate validations on all the instrument at the same time. A process safety maintenance management system could schedule these triggers and could for example run monthly validation and calculate Key Performance Indictors (KPI's) like Mean time between failure, fail to safe (FTS), fail to danger (FTD), fail to nuisance (FTN), availability rate, etc. If a process safety related instrument is not performing within the process safety criteria they must be replaced.

The logic to determine if a piece of instrument is running correctly can be executed automatically when a new validation result is received. Combining automated judgement with automated scheduled validations would provide insight on the recurrence of the validations and provide way more accurate insight of the performance of the safety related instrument.

Human interaction is needed when validations fail. When validations fail, maintenance is needed to correct or replace the safety instrument. An example of maintenance would be to calibrate a process safety related pressure transmitter to make sure the validations are within expected ranges and that the instrument is working safely with other words e.g. if the pressure comes above HPA the safety system should act accordingly and close the valve.

Live process and diagnostic data create further opportunities to observe and maintain the safety instrument. An experienced technician can judge whether instrument needs maintenance. For example, reading will drop if a filter starts getting plugged. Based on the information retrievable from smart instrument and the experience from technicians, triggers can be designed which indicate when maintenance needs to be done and more specifically which maintenance needs to be done. The maintenance is then instead of corrective or preventive, based on conditions.

2 Trust factors

What determines if a safety related instrument is trustworthy?

- Acts according to designed safety criteria
- Results of gathered data
- Amount of gathered data
- Quality of gathered data
- Method of gathered data

- Frequency of gathered data
- Performance indicators
- Cross comparison

Is a result within its limits trustworthy when a fault signal is active on the instrument? When you have a complex system, is one sample enough to validate the system? Would you rather trust a validation ran in the field over a validation in a controlled laboratory? These questions seem simple but are questions we do not always keep in mind when executing routine tasks. To improve the trust in safety related instruments the correct answers need to be given for these questions every single time.

4 Design

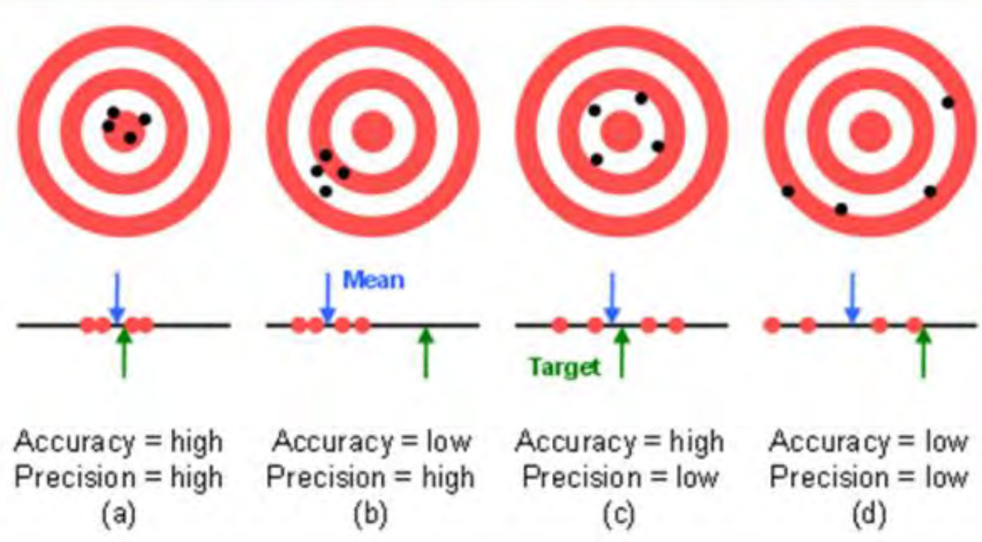
The first and most important part of process safety instruments is if they act according to the design. When a limit is reached an action needs to be taken e.g. set of the sprinkler system, shut a valve or ring the alarm. When doing validations, it is being checked if an instrument runs correctly, but the fail scenario is not continuously tested if an instrument runs correctly. In normal operations these scenarios should be avoided, but when the opportunity is there to test the fail scenarios, it is important to make sure that all systems respond the way they should in case of an emergency.

5 Results

Results are the basis to proof the trustworthiness of an instrument. When the results go out of the preconfigured bounds for a safety instrument an action needs to happen. An alarm needs to be rang in case of a gas detector and a sprinkler system needs to activate in case of an office fire. These systems are to ensure the safety of the people and resources in a certain area and within the industry it safeguard the process operation. It is however very costly when the sprinkler system is triggered incorrectly and destroys all electrical instrument like computers and ruins all documentation. This is the reason why generally for firefighting system initially only an alarm is ringing, and sprinklers are not automatically engaged in an office area. The reason is the risk involved with the potential danger that the office fire has to the people and resources in that moment and place.

6 Amount

Amount of results of an instrument provide information about the precision and accuracy. This information only becomes available when you compare measuring results to previous results. It is comparable to shooting with bow and arrow. one single shot tells you something about your accuracy. It does not give you any information about your precisions, because there is nothing to compare it to. Conclusions can be drawn after a couple of shots:



These extra results provide valuable information which otherwise would not have been considered when only looking at one validation. This extra information can detect if there is a failure upcoming, for example through trend checking.

7 Quality

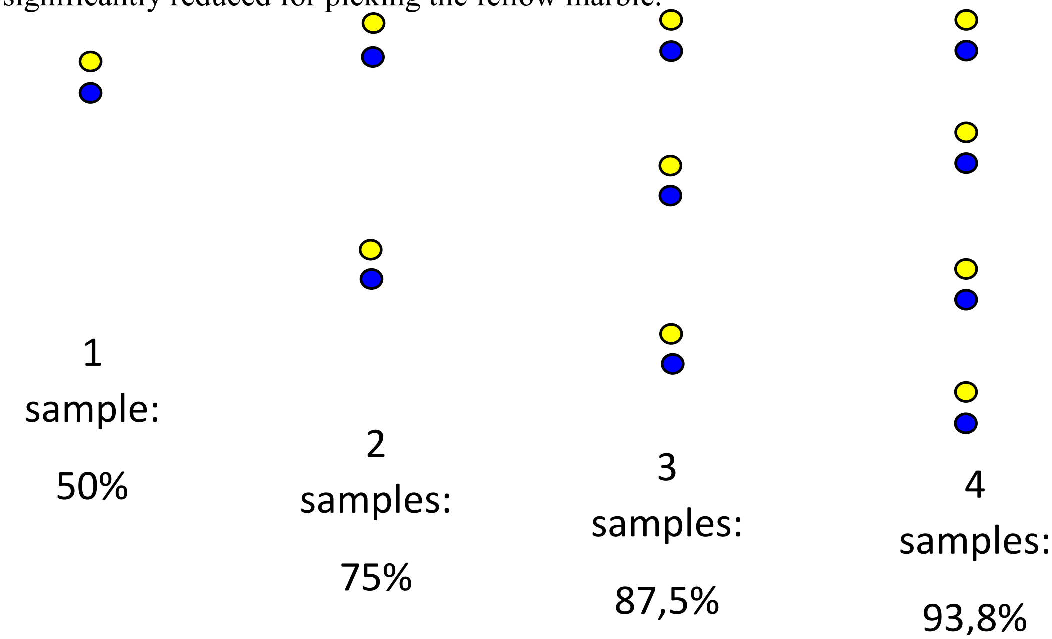
One value by itself often does not tell you the full story of an instrument. For simple analysers there is often a flow switch or some extra signal to tell you that the value is trustworthy. The more complex the instrument is the more information it can provide about its trustworthiness. Combine that extra information with the results gathered in the chapter amount and a system can produce a quality label to inform the investigator about the quality of the instrument at the time of doing a validation. This quality label provides extra insurance that the data received from the instrument is correct.

8 Method

There are different ways and methods to run instrument validations. For analyzers there are reference sample tests, line sample tests etc. and for valves there are bump tests and leak tests. The biggest difference in these options is the amount of human involvement. Systems do not change procedures or execute them partly. Humans do have the tension to change things especially when pressed for time or with a lack of motivation. This inconsistency is a big risk for data gathering. An instrument measuring a value is a process which can be controlled and improved. The process of reading a value and writing it into a system by a human cannot be controlled. Human errors cover a large portion of the errors in our industry and can be prevented. Humans don't like to do the same task repeatedly, even it is their job. Therefore, automated data gathering is preferred over manual data gathering. It reduces costs, it reduces the change of errors, it creates opportunities of gathering more data and created instant evaluations and notifications or alarms. The human can then use all this extra information to judge where actions are needed to correct the instrument and make sure everyone stays safe.

9 Frequency

The importance of frequency can be explained by an example of a bowl or marbles. In case you have two marbles, the chance of picking the yellow marble is 50 precents. Given that the picked marble is put back the second time the chance of getting the yellow marble is 75 precents and the third time 87,5 precents etc. When the bowl of marble contains more marble, the chance is significantly reduced for picking the fellow marble.



The important questions is how confident do you want to be to catch the error or how much assurance do you want that there is no error in the instrument. The more complex the system, the more validations need to be done to ensure that the instrument is trustworthy.

		Marble count				
		2	**5**	**10**	**50**	**100**
Sample count	**1**	50,00	20,00	10,00	2,00	1,00
	2	75,00	36,00	19,00	3,96	1,99
	3	87,50	48,80	27,10	5,88	2,97
	4	93,75	59,04	34,39	7,76	3,94
	5	96,88	67,23	40,95	9,61	4,90
	6	98,44	73,79	46,86	11,42	5,85
	7	99,22	79,03	52,17	13,19	6,79
	8	99,61	83,22	56,95	14,92	7,73
	9	99,80	86,58	61,26	16,63	8,65
	10	99,90	89,26	65,13	18,29	9,56
	20	100,00	98,85	87,84	33,24	18,21
	30	100,00	99,88	95,76	45,45	26,03
	40	100,00	99,99	98,52	55,43	33,10
	50	100,00	100,00	99,48	63,58	39,50
	60	100,00	100,00	99,82	70,24	45,28
	70	100,00	100,00	99,94	75,69	50,52
	80	100,00	100,00	99,98	80,14	55,25
	90	100,00	100,00	99,99	83,77	59,53
	100	100,00	100,00	100,00	86,74	63,40

8 Performance indicators

Another important aspect of the quality label is the performance indicators. Performance indicators can be calculated when then state of an instrument is being recorded. Possible states are utilised, maintenance, faulted and out of service (offline). Calculations that can be made based on those states are mean time between failure, mean time to repair etc. These calculations can be used as a basis for the quality label mentioned in chapter 5.

10 Cross comparison

Instruments can be cross checked to further increase the trust in an instrument. Cross referencing becomes easy when all the data is stored in a database and available through an easy to use application. With cross referencing anomalies can be found like the temperature difference of night and day.

11 Conclusion

The full data spectrum of a process safety related instrument needs attention to gain trust and improve reliability.

1. Make sure the design SIL level is correct and that the instrument still acts accordingly.
2. Verify the instrument by running validations, preferably automatically.
3. Gather enough information to make sure there are no decisions made on random results.
4. Check multiple aspects of the instrument to ensure data quality.
5. Choose the correct method for the validation for quality and efficiency.
6. Plan the frequency of validations based on the complexity of the instrument.
7. Use performance indicators to watch the performance of an instrument.
8. Conduct cross comparisons to find additional improvements.

The goal is to go from paper file to electronic data. Not only the current validation, but also track the history of previous validations. The system stores information of all safety critical instruments like Availability, reliability, MTBF, FTD, FTS, etc. during the life cycle of the installation. Having a real-time system and relational database available which can generate reports of all safety critical instruments instantly. Company risk will be reduced by having a transparent system in place where the evidence is gathered and stored for all safety related instruments and prove that they are performing within the expected design criteria.

Through automation the efficiency of maintaining safety related instruments can be improved, which creates time to look further into the instrument data to further improve the performance and trust in the instruments.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Biocompatible Herder for Rapid Oil Spill Treatment over a Wide Temperature Range

Mingfeng Chen[c], Zhengdong Cheng[a,b,c,*], Dali Huang[a,b,+], Shijun Lei[c], Rong Ma[c], M. Sam Mannan[b,c],Roshan Sebastian[b,+], Abhijeet Shinde[c], Hongfei Xu[b,c], Lecheng Zhang[c]
[a] Department of Materials Science & Engineering, Texas A&M University, College Station, TX, 77843-3122, USA
[b] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX, 77843-3122, USA
[c] Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX, 77843-3122, USA
*Presenter's E-mail: zcheng@tamu.edu

Abstract

Oil spills caused by damaged oil rigs, ruptured pipelines, and tankers can have immediate and long-term detrimental effects on marine systems and aquatic life. Herein we further develop the merit of an oil spill recovery technique called oil herding. A herder is an amphiphilic oil-collecting surfactant which is applied to spray around the oil spill areas and is able to retract oil slicks, transforming them from a large thin layer to a small thick bulk. This herding treatment greatly simplifies further in-situ burning and the recycle process. The natural konjac glucomannan (KGM) material could be functionalized and examined here as an oil herder, which has the great advantage of nontoxicity, biocompatibility, and adaptability. Moreover, functionalized KGM is a non-ionic surfactant with no Krafft temperature. The absence of Krafft temperature gives KGM surfactants the unique ability to retain surfactant ability at temperatures nearing 0 °C. It unlocks a new direction for efficient oil herders within low temperature water areas, especially for oil spills treatment in Arctic waters, in the offshore safety control.

Keywords: Herders, Biocompatible, Oil spill response, Wide temperature range, Functionalized konjac glucomannan, Oil contamination treatment

1. Introduction

Oil spills are environmental catastrophe; oil kills sea flora and fauna, contaminates fragile ecosystems, sea creature nursery areas, and soil beaches, among other destruction (Paine et al., 1996; Peterson et al., 2003). Occurring either accidently or deliberately, oil spills can result from malfunctions at offshore drilling rigs, from pipeline and holding tank ruptures at ports, and well blowout (Iakovou et al., 1997). On the other side, the petroleum products play a pivotal role to help human beings maintain a decent standard of living. The increase in demand for petroleum products engenders an uptick in petroleum exploration, production, and transportation (Brown et al., 1987; Urquhart, 1986). Oil is stored and processed along different nodes at terminals and refineries. Accordingly, an oil spill can take place at any point in these transportation modes, storage or processing locations. **Fig. 1** labelled the 15 largest oil spills in history occurrence in the world up to 2019 (Baffes, 2007; Kaushik, 2019). Oil spills could occur on any continent and in any ocean, in extreme temperature ranges, from Arctic to Equatorial. **Table 1** summarizes the 15 largest oil spills in history corresponding to **Fig. 1**. It is worth noting that large-scale oil spills as shown in **Fig. 1** and summarized in **Table 1** resulted in huge socio-economic impacts and attracted negative media and public attention. Besides of larger oil spills, more than half of the oil spills incidents are smaller in magnitude and are commonly existing, which often evade attention and more difficult to clean up (Blumer et al., 1971; Jesus, 2016). Additionally, The National Science Foundation (NSF) has lately developed a "NSF's 10 Big Ideas" plan, which one of the ideas is named as "Navigating the New Arctic". Energy crisis is not a new topic nowadays while there are around 1/3 of the world's undiscovered gas and $1.68*10^{13}$ gallons of oil in the Arctic area. The energy concerns would be significantly lessened and the reliance on other types of energy would also be reduced. Many countries and oil companies have oil platforms in the Arctic, but the oil drilling also comes out with the oil spill problem. The extreme climate (low temperature of -2 to 2 °C in **Fig. 1**) and Arctic geographic location also play an important role to the spill effect and made the oil spill treatment situation more complicate.

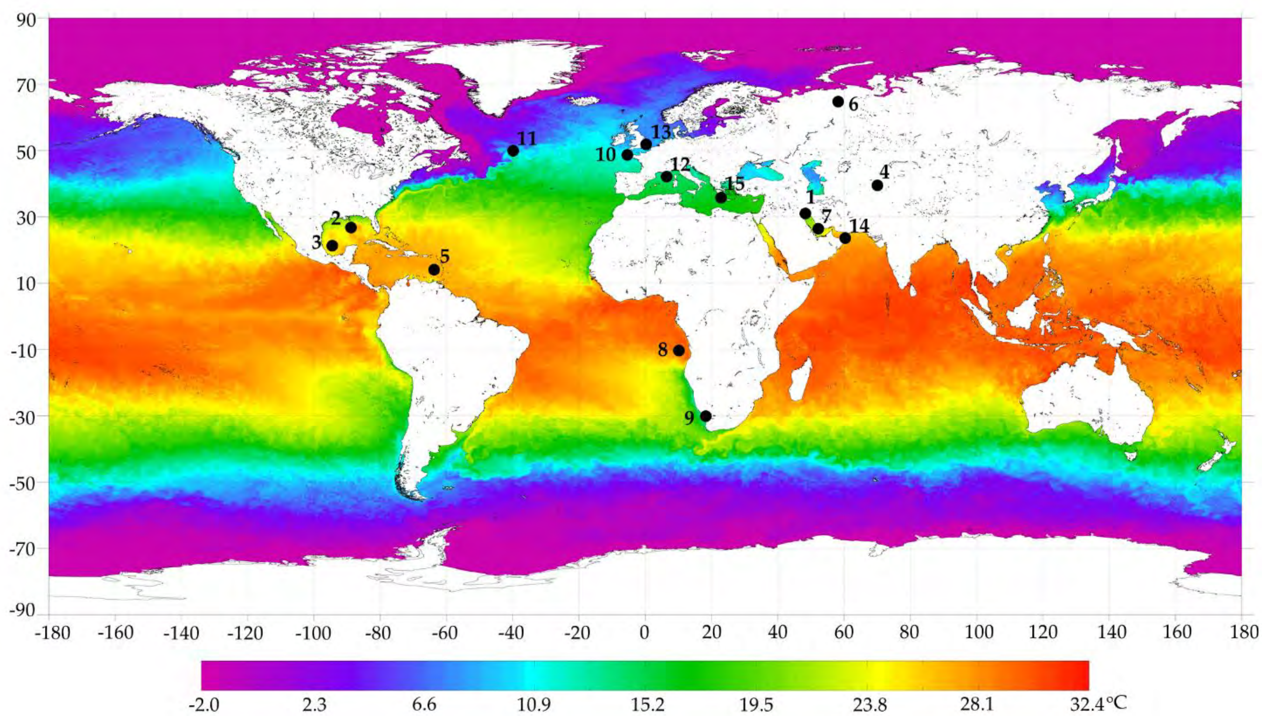


Fig. 1. The world map showing locations of the 15 largest oil spills in history and sea surface temperature (5 kilometers) contour chart. The black dots designate location of oil spills and numbers from 1 to 15 mean the volume ranking of the oil spill.

Table 1 List of 15 largest oil spills in history (corresponding to **Fig. 1**)

Ranking	**Date**	**Cause**	**Location**	**Source**	**Oil spill volume (million gallons)**
1	1991.01.23	Gulf War	Persian Gulf	Oil rig	400
2	2010.04.20	Rig explosion	Gulf of Mexico	Deepwater Horizon oil rig	210
3	1979.06.03	Well blowout	Gulf of Mexico	Ixtoc 1 Oil Well	140
4	1992.03.02	Well blowout	Fergana Valley, Uzbekistan	Oil well	88
5	1979.07.19	Tanker collision	Trinidad & Tobago	Atlantic Empress/ Aegean Captain Oil Tanker	87
6	1994.09.08	Dam burst	Kharyaga, Russia	Oil reservoir	84
7	1983.02.04	Collision	Persian Gulf, Iran	Nowruz Fields Platform	80
8	1991.05.28	Explosion	Angola Offshore	ABT oil tanker	79
9	1983.08.06	Fire on tanker	Cape Town, South Africa	Castillo de Bellver oil tanker	78
10	1978.03.16	Tanker sinking	Coast of Brittany, France	Amoco Cadiz oil tanker	69
11	1988.11.10	Tanker explosion	North Atlantic off Coast of Canada	Odyssey oil tanker	43
12	1991.04.11	Tanker explosion	Coast of Genoa, Italy	MT Haven oil tanker	42

13	1967.03.18	Tanker leakage	Southwest Coast of United Kingdom	Torrey Canyon oil tanker	36
14	1972.12.19	Tanker collision	Gulf of Oman	Sea Star oil tanker	35
15	1980.02.23	Tanker fire	Port of Pylos	Irenes Serenade oil tanker	30

Oil spills in ocean circumstances have resulted in irreversible negative environmental impacts and pecuniary loss (Goldberg, 1994; Silliman et al., 2012). Oil slick would float on the water and spread because of the smaller specific gravity and surface free energy. The spilled oil has capability to affect the delicately poised marine ecosystem and can trigger a domino effect which can have deleterious effects on the coastal belt and human lives. Hence, it is imperative to have in place an effective and rapid oil spill response system.

Oil spill treatment methods have many different classifications and circumscriptions. Here, the commonly used category for oil spill remediation in the aquatic environment includes mechanical, chemical, and biological procedures. The mechanical methods using oil booms, skimmers, barriers or sorbents are the most universal method for dealing with oil spill. Engineers use machines and instruments to physically suck up oil or absorb oil from water surface which needs large manual labor forces and resources. Also, the mechanic recovery would be largely affected by offshore changeable environment. In the chemical treatment, dispersants could be used to break large oil area into small size oil droplets. It would bond with oil and water and it is inevitable that the dispersants have biocompatibility and toxicity problem, which would greatly affect marine system in the oil spill location. Bacteria and microorganisms could eat or break toxic oil components into non-toxic matters. But it is slow in time and not suitable in very low temperature areas or close to coastal. In oil spill accidents discussed in Fig. 1 and Table 1, one method or composite methods were used to handle with oil spill. Regardless of the physical oil booms, barriers and in situ burning, the commonly used oil spill treatment methods for the accidents above was to spray dispersant like Corexit 9500A, Corexit 9527A, JD-2000 or MARE CLEAN 200, which mostly have been reported to have known or unpredictable effect to the marine system.

In this work, we explore an effective chemical herding method. The herders, or called herding surfactants, reduce air-water surface tension and retract the thin spilled oil to form a thick slick layer, which will then favor in-situ burning and recovery. Herder is a surfactant whose chemical structure includes the hydrophobic tail and the hydrophilic head. It is comparatively effective in remote offshore waters, while other mechanical, biological and chemical methods are not that convenient nor efficient to some extent (Aggarwal et al., 2017).

Traditional oil herders have two major shortcomings. One is the toxicity impact and stubborn bio-incompatibility which will make the herding surfactant remain on water body for a long period (Imai et al., 1994; Inácio et al., 2013). The other is that the traditional herders would lose most herding efficiency in Arctic areas due to their intolerance to low temperatures. They suffer from a relatively high Krafft temperature, below which surfactants lose their surfactant property. The definition of Krafft temperature is the minimum temperature for surfactant to form micelles. There is an abrupt large solubility increase above the Krafft temperature (Bakshi and Singh, 2005; Rico and Lattes, 1986).

Our project focused on developing an innovative oil herder from natural plant-based product, konjac. The konjac glucomannan (KGM) is the base material used to develop the proposed oil herder, which is a natural polysaccharide and has flexibility in functionalization (Behera and Ray, 2016; Nishinari, 2000). The easily degraded functionalized KGM materials have both hydrophobic tails to be attached and hydrophilic backbones forming the surfactant structure. The natural KGM material could be functionalized to work as the efficient oil herder. Compared with traditional ionic surfactant, the non-ionic functionalized KGM surfactant does not have Krafft temperature limits and its herding efficiency is not restricted at low temperatures around 0 °C. Results of this study demonstrated that functionalized KGM has great potential to work as an efficient biocompatible oil herder for a wide range of temperatures, especially suitable for oil spills response in Arctic Circle.

2. Results and Discussion

The schematic mechanism of oil herding was shown in **Fig. 2**. When inevitable accidents occur at sea, crude oil leaks out, spreading across the water surface and stabilizing as a very thin layer. After the herder (float on water and surround oil) was spread around the oil, the bulk oil slick started to shrink and become thicker (**Fig. 2(a)**). In the side view of oil herding theory, as shown in **Fig. 2(b)**, initially had the tendency to spread out to become a very thin oil slick surface due to the gravitational force and smaller surface tension. Before herding surfactant was applied, oil on water surface system experienced with three forces, the oil-water surface tension ($\gamma_{O/W}$), the oil-air surface tension ($\gamma_{O/A}$) and the air-water surface tension ($\boldsymbol{\gamma}_{A/W}$). Water is a highly polar solvent and has high surface tension ($\boldsymbol{\gamma}_{A/W}$=72.5 mN/m) (Vargaftik et al., 1983). The $\gamma_{O/W}$ and $\gamma_{O/A}$ majorly depend on oil and water properties and the net sum value ($\gamma_{O/W}+\gamma_{O/A}$) is around 25 mN/m (Gupta et al., 2015; Venkataraman et al., 2013). Higher $\boldsymbol{\gamma}_{A/W}$ made the oil slick quickly spread outside from center until $\boldsymbol{\gamma}_{A/W}$ and ($\gamma_{O/W}+\gamma_{O/A}$) value are the same. At this moment, the oil slick became a very thin layer and reached the equilibrium state. The herder structure in **Fig. 2(b)** consists of a hydrophobic tail (black line) and hydrophilic head (red dot). After the herder was applied to the sea, the equilibrium state of $\boldsymbol{\gamma}_{A/W}$ and ($\gamma_{O/W}+\gamma_{O/A}$) was broken. The hydrophilic head dissolved on the water surface and to form a monolayer, and the hydrophobic tail forms an interface between the air and the water, which in effect greatly reduced the air-water surface tension ($\boldsymbol{\gamma}_{A/W}$<25 mN/m). Higher $\gamma_{O/W}+\gamma_{O/A}$ value motivated oil slick to contract until all surface tensions reach to the new equilibrium. At this moment the oil slick became a much thicker bulk. The oil slick on water was always moving to the direction of the equilibrium state and surface tensions are also adjusting at the same time.

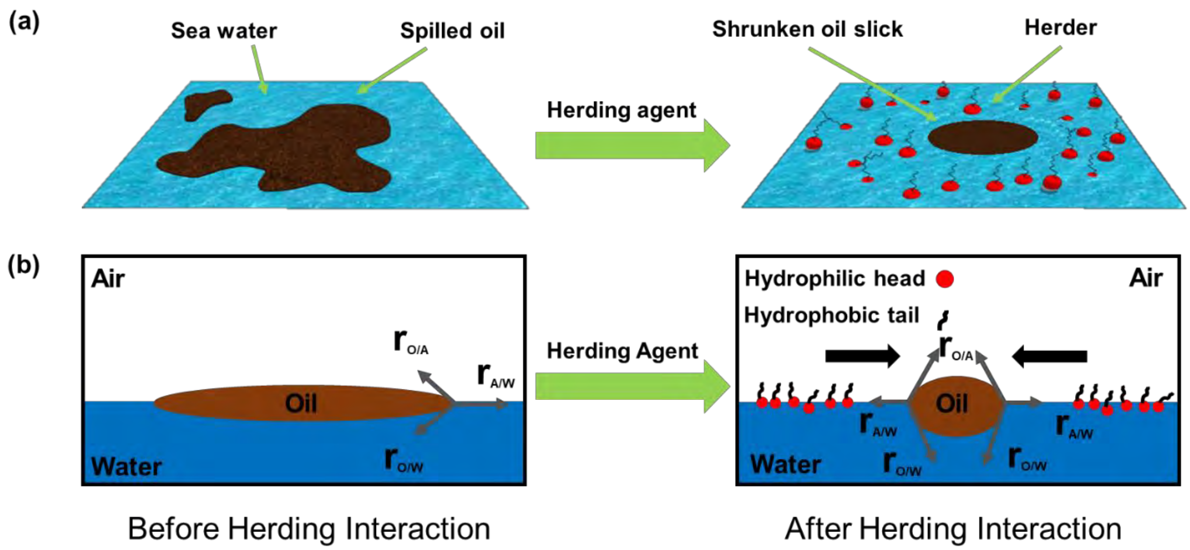


Fig. 2. Schematic illustration for oil herding on the sea surface. (a) General 45° view of herding process before and after addition of the herding agent. (b) Side view of herding mechanism before and after adding herding agent. The hydrophilic head and hydrophobic tail of the surfactant are labeled.

The lab-scale oil herding process experiment was first tested using the configuration shown in **Fig. 3**. The crystallizing dish simulated the sea environment. Artificial sea water was prepared using ASTM International standard protocol (ASTM D1141-98) with deionized (DI) water and dissolved mineral salts. The oil spill was replaced with dodecane ($C_{12}H_{26}$) due to its liquid alkane hydrocarbon characteristic. The water was dyed with water-soluble methylene blue; the oil dodecane was dyed with oil-soluble Sudan IV for easier observation. A portable camera was clamped to a supporting mast and positioned above the crystallizing dish to record changes of the oil slick.

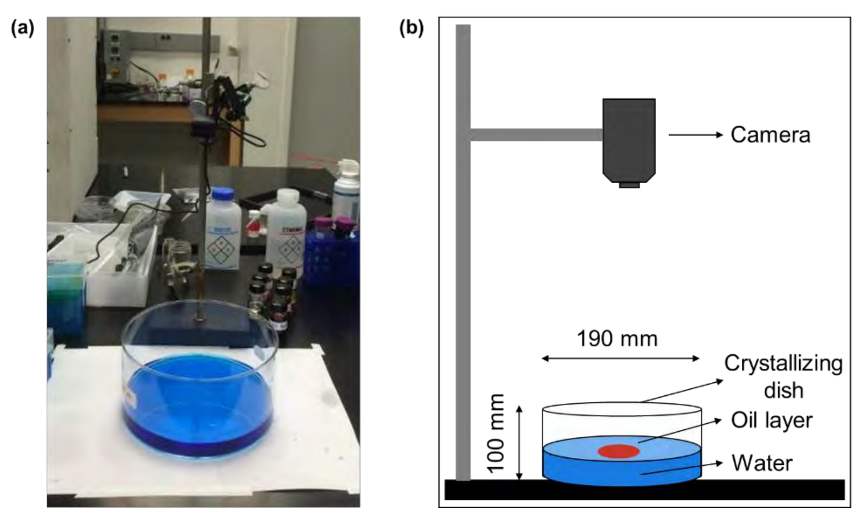


Fig. 3. Experimental setup for oil herding process. (a) Photograph of experimental setup in lab. (b) Schematic illustration of experiment design and instrument.

Herding surfactant is essentially a surface-active agent. To preliminarily investigate the material herding efficiency to oil, suitable polymer surfactants with hydrophobic head and hydrophilic tail (similar to **Fig. 2(b)** surfactant structure) were tested. Polyethylene glycol (PEG) is a water soluble polymer and easy to couple with hydrophobic chain to form surfactant (Komoto and Kobayashi, 2004; Winger et al., 2009). Four common lab PEG derivatives were chosen as herders for testing, as shown in **Fig. 4**. The experiments were performed at room temperature. The slick thickness ratio was defined as below.

$$\text{Slick thickness ratio } (\%) = \frac{Stable\ Oil\ thickness\ before\ herding}{Stable\ Oil\ thickness\ after\ herding} \qquad (1)$$

Higher slick thickness ratio implied better herding quality. From **Fig. 4(a)** and **Fig. 4(b)**, the slick thickness ratio largely increased with herder concentration increment while the oil slick, accordingly, shrunk. The same changes could be also seen from the two insets, which demonstrated that PEG-monolaurate and PEG-monooleate surfactants were efficient in herding. While for **Fig. 4(c)** and **Fig. 4(d)**, the slick thickness ratio remained mostly the same when herder concentration increased, demonstrating that PEG-dibenzoate and PEG-disterate were not suitable for herding oil. The effectiveness of surfactants at herding oil is directly related to the chemical structure of the PEG derivatives. **Fig. 4(a)** and **Fig. 4(b)** showed good herding ability due to their amphiphilic characteristics. The reason of slick thickness ratio curve of **Fig. 4(c)** and **Fig. 4(d)** remained flat were assumed to be its internal chemical structure large benzene rings and two side longer carbon chains. The benzene rings and longer carbon chains affected the steric hindrance of materials and largely restricted the hydrophobic side reaction with oil slick. They could not perform herding effect and thus curves in Fig.4c and 4d remained flat, and the thickness ratio was close to 1.

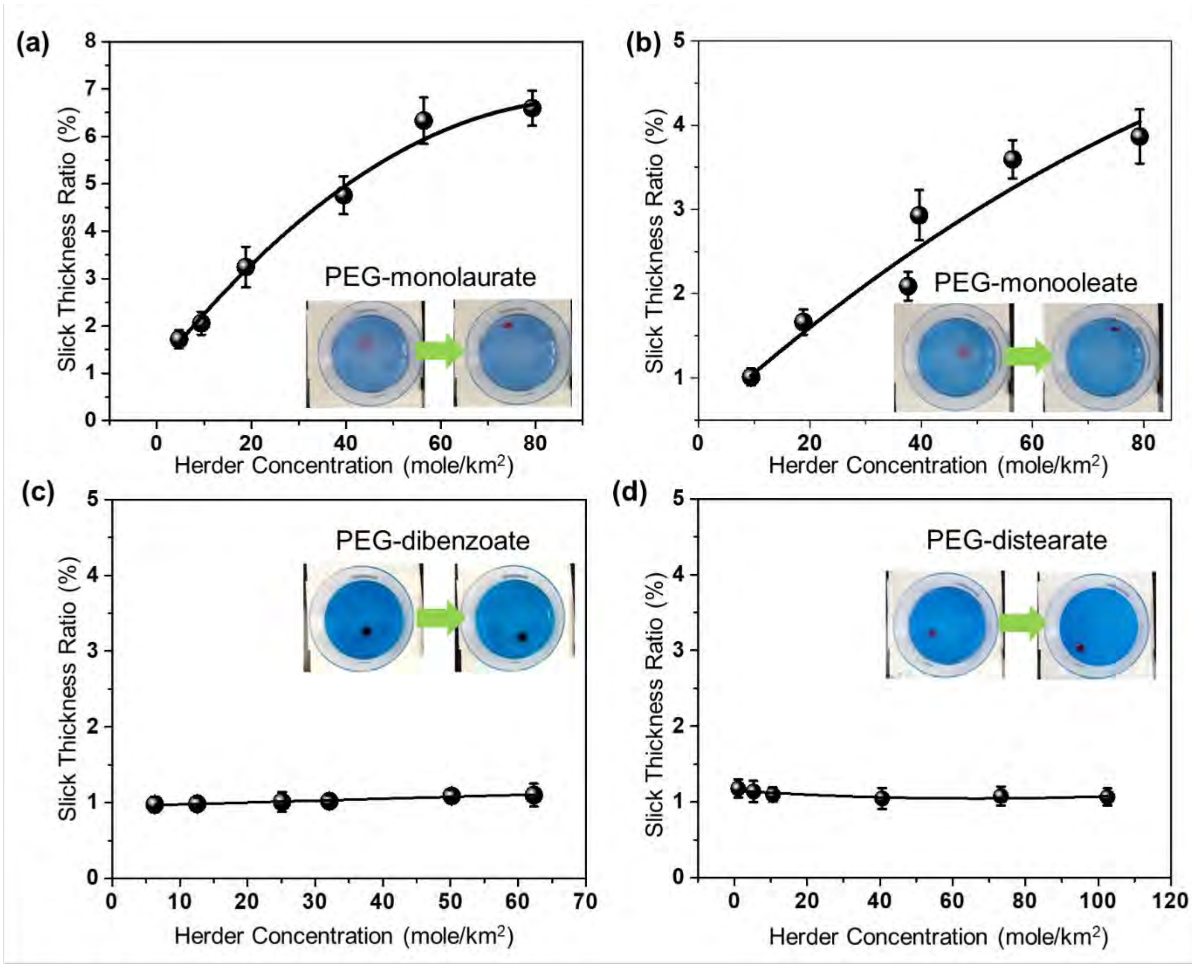


Fig. 4. Lab conventional herding surfactant efficiency evaluation at room temperature. Oil slick thickness ratio changes with the herder surfactant concentration of (a) PEG-monolaurate, (b) PEG-monooleate, (c) PEG-dibenzoate, (d) PEG-distearate. The insets are the photographs of equilibrium state before and after adding herders.

More comparisons were tested to study herder efficiency with different commercial surfactants at varying temperatures and salinity. From **Fig. 5(a)**, both surfactants, Span-20 and PEG-monolaurate, presented good herding ability with large slick thickness ratios at 25 °C. In **Fig. 5(b)**, the PEG-monolaurate retained high herding ability under 25 °C. While temperature decreased to 4 °C, which is close to Arctic Ocean temperature, oil slickness ratio maintained around 1.0, regardless of the herder concentration increment. The results demonstrated that PEG-monolaurate was not a good herder for oil spill response in low-temperature areas. Then herding efficiency of PEG-monolaurate surfactant in saline water and pure DI water was tested. As shown in **Fig. 5(c)**, there was no clear oil slick thickness ratio change between PEG-monolaurate in pure water and 3.5% saline water, meaning the surfactant was not significantly affected by salinity. All the results above urged us to design and synthesize one new herding surfactant to replace PEG-monolaurate for overcoming the low temperature herding defect.

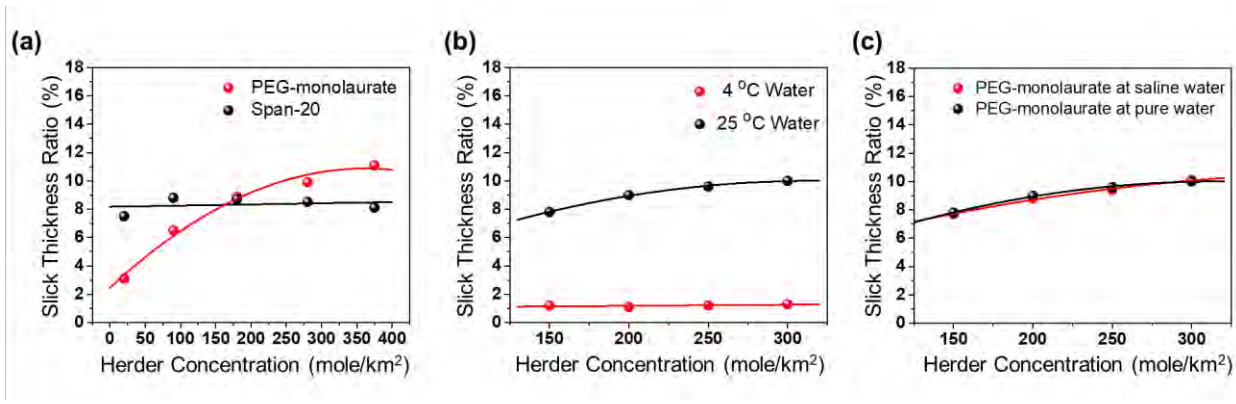


Fig. 5. PEG-monolaurate herding surfactant efficiency evaluation. Oil-slick thickness ratio changes with the herder surfactant concentration. (a) Comparison of herder PEG-monolaurate and herder Span-20 at 25 °C. (b) Comparison of herder PEG-monolaurate at 4 °C water and 25 °C water. (c) Comparison of herder PEG-monolaurate in 3.5% saline water and pure DI water.

Herein, the natural konjac was studied to explore the its possibility to work as oil herders. Similar to PEG, konjac is a water soluble polymer and has more hydroxyl (-OH) group to functionalize as surfactants (Dave et al., 1998; Nishinari, 2000). Konjac naturally contains of great amounts of natural polysaccharide (Katsuraya et al., 2003; Y.-q. Zhang et al., 2005). Its chemical structure is shown in **Fig. 6(a)**. Konjac is grown mostly in Asian countries, including Japan, Korea, China, and southeast Asia countries. The konjac corm is as shown in **Fig. 6(b)**. Konjac is broadly utilized in the food, nutraceutical, and cosmetics industries. The greatest value of konjac corm flour (as shown in **Fig. 6(c)**) is its component konjac glucomannan (KGM). Konjac is the only economic crop that can provide KGM in large quantities. Natural polysaccharides have recently garnered interest in the polymeric surfactants area because of their facile production, environmental friendliness, and non-toxic characteristics(Behera and Ray, 2016; Takigami, 2009; Tester and Al-Ghazzewi, 2016).

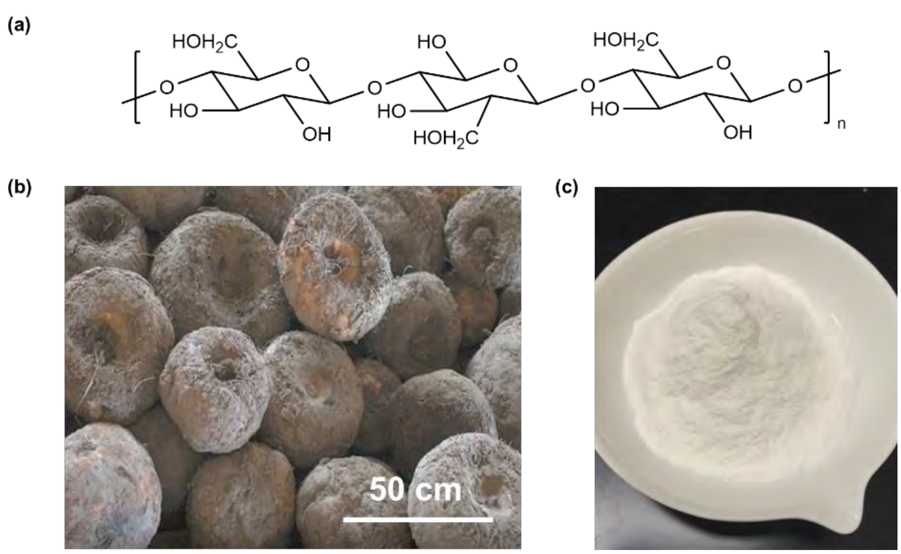


Fig. 6. Konjac glucomannan (KGM). (a) Chemical structure of KGM. (b) Image of konjac corm. (c) Photograph of KGM powder processed from konjac corm.

KGM powder needs to perform the pretreatment before further surface functionalization. The undegraded KGM polymer has large molecular weight and very long hydrophilic backbone which will increase time to form monolayer on water-air surface and further increase the herding time(Luo et al., 2012; H. Zhang et al., 2001). Polymer degradation needs to be taken to shorten the polymer chain length, which could be later testified through molecular weight measurement. Smaller molecular weight suggests shorter polymer backbone chain. The degraded polymer surfactant had shorter chains and required less time for backbone to stretch out to form monolayer for more efficient herding. Furthermore, the degraded surfactant has decreased polymer coil in tendency due to the efficient packing of hydrophobic tails and prevented unnecessary aggregates formation, reducing the invalid polymer aggregate surfactant (Babak and Desbrières, 2004; Henni et al., 2005; Muhd Julkapli et al., 2011).

High energy particle beam like γ-ray or e-beam was already broadly used for polysaccharides backbone chain scission (Gryczka et al., 2009; Woo and Sandford, 2002; Xu et al., 2007). In our work, the long polymeric chain broke down using the e-beam irradiation. The degradation mechanism of KGM by the chain scission of the polymeric chain is carried out by irradiating the KGM samples with radiation doses of 1.21 kGy, 5 kGy, 9kGy and 16 kGy. Gy (Gray) is an SI-derived unit of ionizing radiation and 1 kGy =1000 J/Kg.

The functionalized konjac glucomannan (MKGM) synthesis route was as shown in **Fig. 7**. The detailed synthesis procedure was explained in section 3.2.2. Two chemical functionalized steps were performed. After octadecyl isocyanate (ODI) treatment in step 1, and 1,3- propane sultone in step 2 were chemically grafted, the MKGM surfactant was achieved for use.

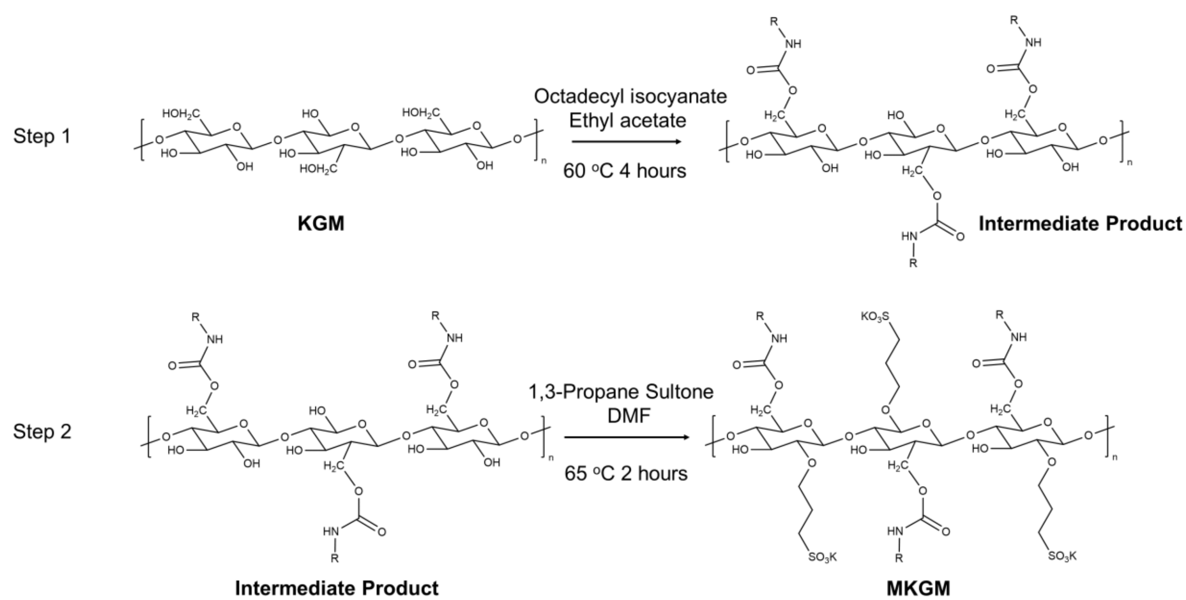


Fig. 7. Functionalized KGM synthesis route.

Fourier transform infrared spectroscopy (FTIR) and gel permeation chromatography (GPC) were investigated for proving surface functionalization of MKGM and the e-beam radiation effect (shown in **Fig. 8)**. Pristine KGM and MKGM was carried out through FTIR. From **Fig. 8(a)**, the peaks for MKGM at 1390 cm^{-1} and at 1650 cm^{-1} represented S=O and C=O groups, while KGM didn't show peak in the same wavelength. This variance indicated the chemical reaction of synthesis, ODI successfully grafted to KGM in step 1 and 1,3-Propane Sultone in step 2 from **Fig. 7**. **Fig. 8(c)** represented GPC molecular weight result related to e-beam radiation. It was clear that the molecular weight of KGM gradually decreased after exposure to e-beam radiation. The molecular weight decreased to 290,000 g/mol at 16 kGy radiation compared with initial 1,000,000 g/mol. As discussed above, the lower-molecular-weight MKGM exhibited better herding surfactant efficiency. Further investigation was undertaken to examine the internal physical structure of pristine KGM and MKGM through scanning electron microscope (SEM). **Fig. 8(b)** and **Fig. 8(d)** revealed that KGM and MKGM exhibited an irregular shape and no clear difference between them was observed, proving that the e-beam radiation and surface functionalization did not break the macrostructure of konjac powder.

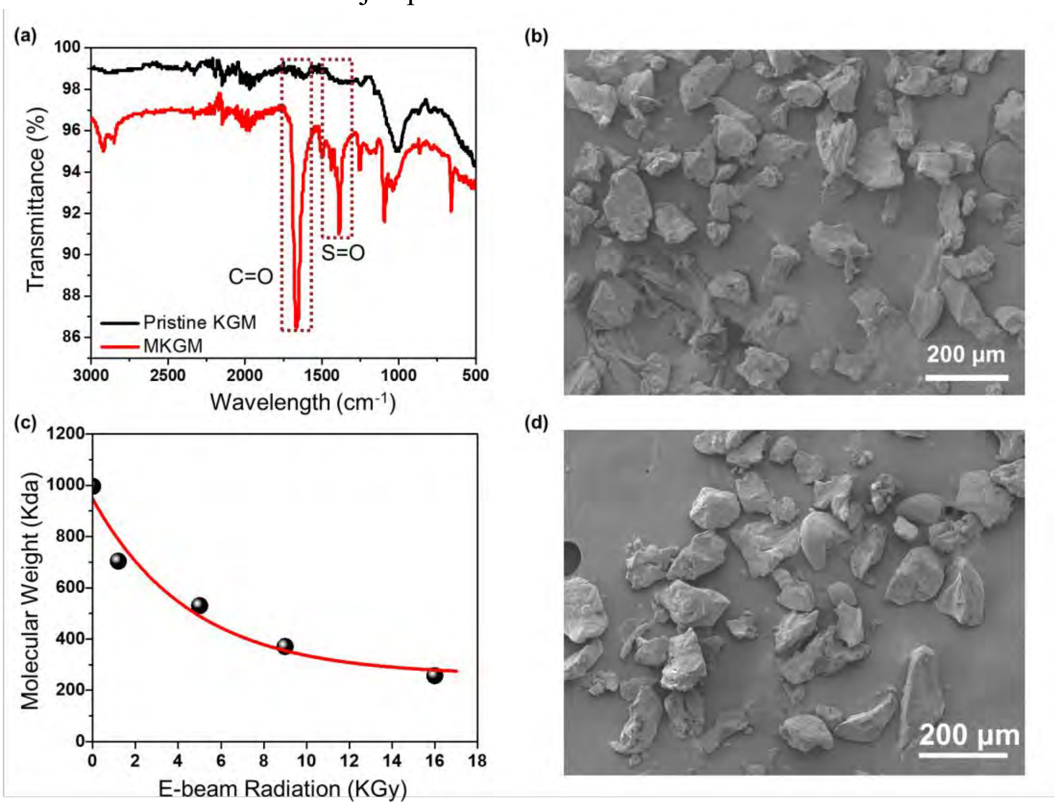


Fig. 8. Chemical characterization of KGM. (a) FTIR spectra of pristine KGM and MKGM. (b) SEM image of pristine KGM powder. (c) Molecular weight of MKGM under various e-beam radiation dosage. (d) SEM image of MKGM at 16 kGy radiation.

The efficacy of MKGM herder in different solvent delivery agents (water and toluene), were investigated. The MKGM tested in this case had been subjected to a 9 kGy radiation dosage.

Fig. 9 showed oil herding through MKGM at 25 °C in water (**Fig. 9(a)** and **Fig. 9(b)**) and toluene (**Fig. 9(c)** and **Fig. 9(d)**) in the crystallization dish. Software ImageJ was used to analyze the images of the oil slick area in different times.

From **Fig. 9(a)**, water was used for the solvent delivery agent. 0.4 ml dodecane (dyed red), simulating an oil spill, was applied to the water surface. Once the oil layer stabilized, 0.25 wt% herder in water (0.2 ml) was spread to the edge of oil layer through a pipette. After 30 minutes of oil herding process, the oil area reached equilibrium and herding process was complete (**Fig. 9(b)**). The herding process was effective but slow. The solvent polarity was assumed to be a factor in the efficiency of the herding process.

It has been reported that toluene could be used as the solvent delivery agent (Gupta et al., 2015). From **Fig. 9(c)**, the nonpolar solvent toluene replaced water in the crystallization dish. Similarly, 0.4 ml dodecane (dyed red) simulating an oil spill was applied on the surface and allowed to reach equilibrium, then 0.25 wt% herder in toluene (0.2 ml) was spread to the edge of oil layer to start the herding process. Time to equilibrium and the herding time decreased to 8 minutes. Water needed to take 2.75 times longer than toluene and toluene proved to be the better delivery agent. The herding improvement might result from the better distribution of the MKGM. Considering the lower density of toluene and its nonpolar characteristics, the MKGM macromolecules dispersed with toluene would form a thin layer in the air-water interface instead of diffusing into water. This behavior would reduce the time for the macromolecules to align the air-water interface and thus reduce the oil herding process.

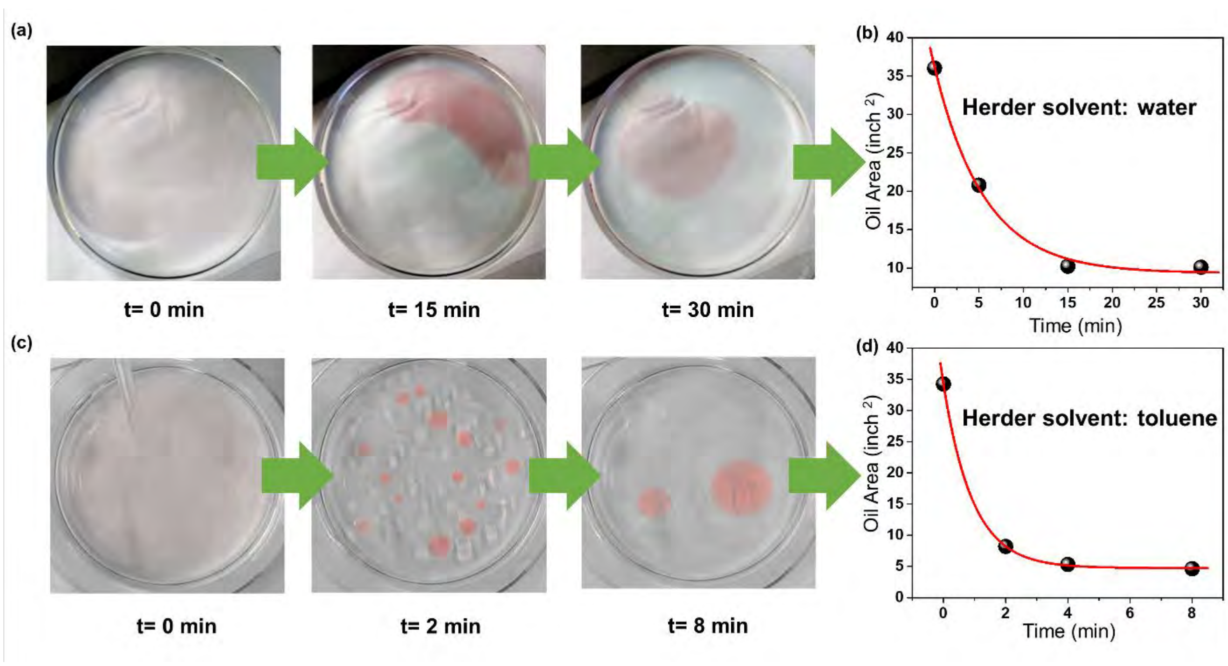


Fig. 9. Oil herding with MKGM surfactant. (a) Photographs of herding process with MKGM herder dispersed in water. (b) Evaluation of herding oil slick area versus time (min) with MKGM herder dispersed in water. (c) Photographs of herding process through MKGM herder dispersed in

toluene. (d) Evaluation of herding oil slick area versus time (min) with MKGM herder dispersed in toluene.

The e-beam radiation dosage of MKGM then was evaluated to affect herding efficiency in low temperature areas. Sea water was cooled to and maintained at 1 °C and the circulating bath flow was set to the bottom of crystallizing dish for maintaining the low temperature environment. **Fig. 10(a)** and **Fig. 10(b)** demonstrated the herding process with MKGM receiving e-beam radiation dosages of 1.21 kGy and 16 kGy. Software ImageJ was used to evaluate the oil slick areas in different times. The oil slick data was as recorded in **Fig. 10(c)**. The oil slick area first decreased and finally stabilized. The herding process was complete at 14 minutes (1.21 kGy) and 10 minutes (kGy). Then all different e-beam radiation dosage of MKMG herding were performed and the herding time was measured as shown in **Fig. 10(d)**. The herding times of 14.5 min, 12 min, 10 min, and 6 min, showed a linear relation with radiation dosage. The results further demonstrated that the lower-molecular-weight MKGM (achieved from various dosing e-beam radiation) exhibited better herding surfactant efficiency.

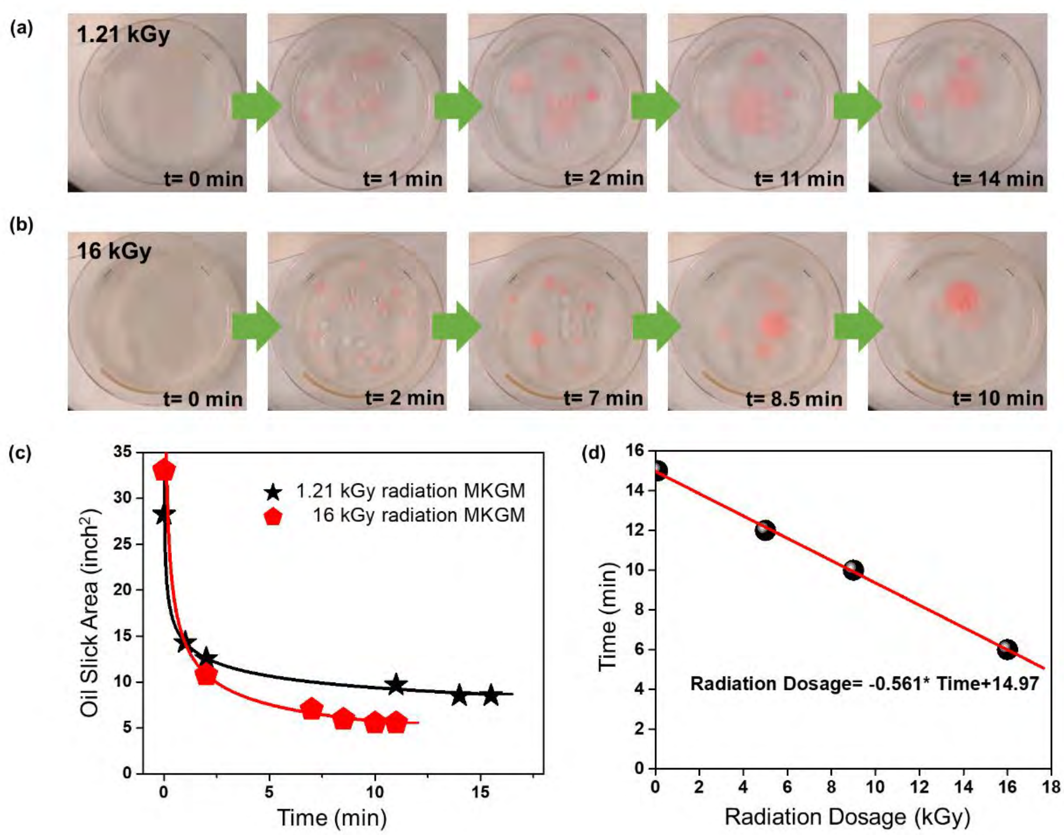


Fig. 10. Oil herding with degraded MKGM with various radiation dosage in low temperature water (1ºC water) The toluene ratio 0.005 (wt/vol) and 0.4 ml of mixture is applied on the 0.4 ml dodecane (oil layer) 1 °C water. (a) 1.21 kGy (b) 16 kGy (c)Time versus radiation (d) Evaluation of herding oil slick area versus time (min) with MKGM herder dispersed in toluene.

Krafft temperature and solubility behavior of the ionic surfactant SDS and the non-ionic surfactant MKGM were detailed discussed in **Fig. 11**. **Fig. 11(a)** and **Fig. 11(c)** were the data of SDS and MKGM conductivity versus temperature, and **Fig. 11(b)** and **Fig. 11(d)** drew the plot of ionic and non-ionic surfactant molecular arrangement. The conductivity measurement was proven to be able to identify the Krafft temperature. Detailed measurement was discussed in section 3.2.3. As discussed above, Krafft temperature is the minimum temperature for surfactant to form micelles. There is an abrupt large solubility increase above the Krafft temperature. Surfactant working temperature should be higher than Krafft temperature for surfactant functioning.

From **Fig. 11(a)**, there was a clear increase in conductivity with temperature. There were 3 parts for the data set. Within the first part (13 °C to 14.4 °C), the conductivity increase in conductivity was slow. In the second part starting from 14.6 °C, there was a sudden large increase in conductivity, which demonstrating that the Krafft temperature and the monomer solubility achieved to critical micelle concentration (CMC). Starting from the second part, the micelles formed while monomers began to decrystallize. In the third part, the conductivity increment speed slowed down and micelles were still forming. Correspondingly, schematic illustration of ionic surfactant molecular alignment with the temperature, was explained in **Fig. 11(b)**. **Fig. 11(b1)** showed the crystallized monomers of the ionic surfactants below the Krafft temperature. Monomers crystallized and have no herding surfactant shape and effect. **Fig. 11(b2)** represented the formation of micelles when the Krafft temperature was crossed and the micelles increase conductivity of the solution. In **Fig. 11(b3)**, there was continuing formation of micelles. From the figure, the ionic surfactant crystallized and had no herding surfactant functionality below Krafft temperature. The ionic surfactant was only working while the atmosphere temperature was above Krafft temperature. This restriction also largely limited the surfactant usage rate.

Different with ionic surfactants, the non-ionic surfactant MKGM exhibited distinct conductivity tendencies versus temperature. In **Fig. 11(c)**, there was a steady decrease in the conductivity of the solution with temperature increment. Unlike SDS, MKGM did not show any abrupt increase in conductivity and did not appear to have a Krafft temperature. The molecular alignment of non-ionic was performed in **Fig. 11(d)**. The hydrophilic polymer chain was stretching in low temperature and will started to coil-in in high temperature to some extent. (**Fig. 11(d1)-Fig. 11(d3)**). The molecular alignment did not affect the surfactant functioning well. The absence of Krafft temperature for non-ionic surfactant is a great advantage in low temperature (0 °C) oil spill treatment environment, while ionic surfactant would crystallize to solid and lost herding efficiency in that temperature range.

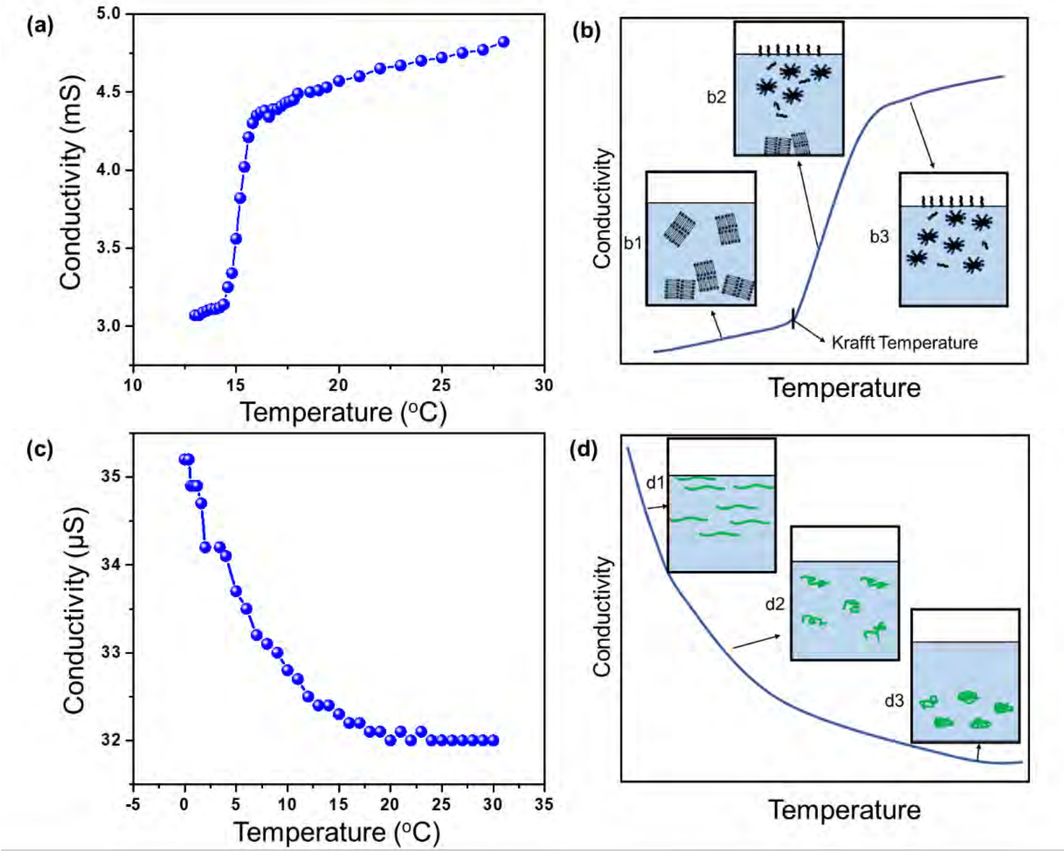


Fig. 11. Comparison of mechanism of ionic and non-ionic herding surfactant efficiency. (a) Ionic surfactant SDS: graph of conductivity of SDS solution in water versus temperature. (b) Schematic illustration of relation with ionic surfactant conductivity versus temperature and resulting molecular alignment. (c) Non-ionic surfactant KGM: graph of conductivity of MKGM in water versus temperature. (d) Schematic illustration of relation with non-ionic surfactants conductivity versus temperature and resulting molecular alignment.

In addition, commercialization potential for the MKGM herder was evaluated. The prices of commercial surfactant PEG-400, PEG-1500 and PEG-Sorbitan derivative are \$39.00/kg, \$83.50/kg and \$64.22/kg from Sigma-Aldrich company. In comparison, the functionalized KGM was calculated to be \$29.00/kg, which proved to be a promising surfactant candidate for oil spill mitigation in industry.

Finally, a simple biocompatibility test was performed for the MKGM herder, as shown in **Fig. 12**. Edible black beans, red beans, and pinto beans were purchased from local supermarket. 12 black beans, 12 red beans, and 9 pinto beans were randomly chosen and set aside in lab atmosphere for 7 days (**Fig. 12 (a)**–**(c)**). All beans did not sprout and kept their original shape. We then separated beans into three plastic petri dishes, into which four black beans, four red beans and three pinto beans each were placed. Three water environments were simulated, and beans were immersed with reference sea water, 0.25 wt% pristine KGM in sea water, and 0.25 wt% MKGM in sea water for 7 days (Fig. **12(d)–(f)**). All beans sprouted in a normal speed. The KGM and Surface modification of KGM in sea water did not affect the growth of the beans, which also proved the biocompatibility of the herder.

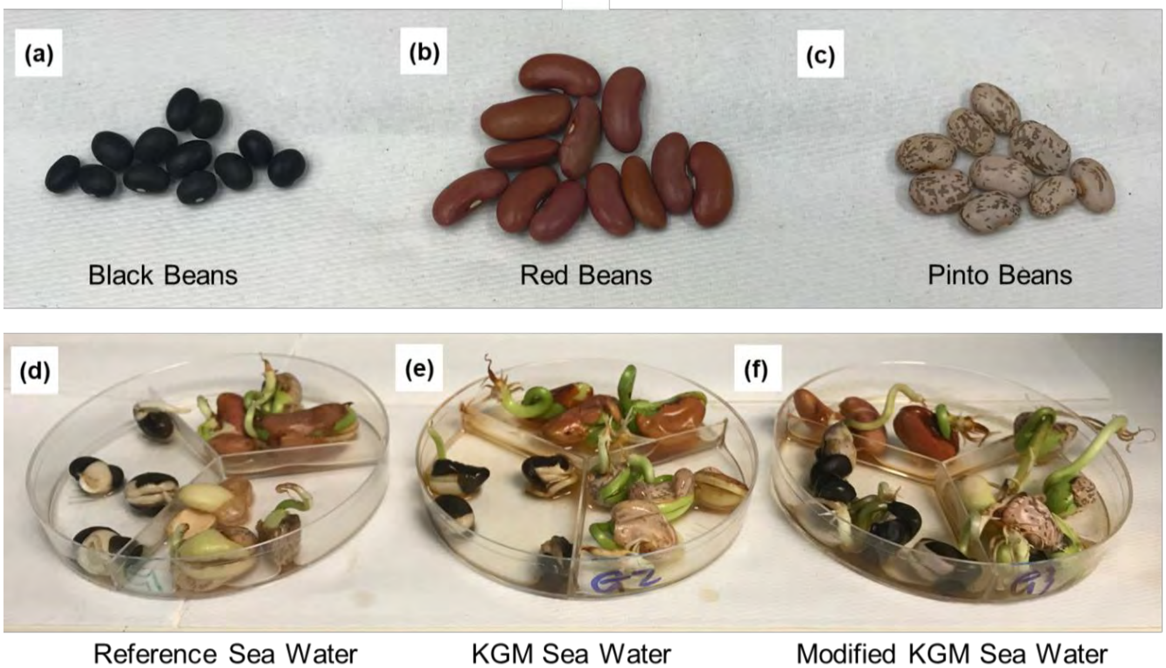


Fig. 12. Biocompatible test for MKGM herding surfactant. Photographic images of edible beans, (a) Black beans, (b) Red beans and (c) Pinto beans. Photographic images of successful bean sprouting in various water environment. (d) Beans in reference sea water, (e) Beans in KGM sea water and (f) Beans in MKGM sea water.

3. Materials and methodologies

3.1 Chemicals and materials

Pristine KGM powder (Ticagel® Konjac High Viscosity) was achieved from TIC Gums company. Octadecyl isocyanate, ethyl acetate, 1,3-propane sultone, potassium carbonate and N, N - dimethyl formamide were purchased from Sigma-Aldrich.

Black beans, red beans and pinto beans were purchased from a local HEB supermarket.

3.2 Experimental Methodologies

3.2.1 Electron beam radiation of KGM powder for degradation

Four laboratory zipper reclosable polyethylene (PE) bags were prepared, and into each was packaged five grams of pristine KGM powders. The dimension of the PE bag was 7.5 cm x 14 cm. The PE bags were separately placed on a conveyor belt and transferred into the e-beam processing chamber. The samples were irradiated at dosages of 1.21 kGy, 5 kGy, 9 kGy and 16 kGy. Gy (Gray) is an SI-derived unit of ionizing radiation. 1 Gy is equal to 1 J/Kg, representing the absorption of 1 joule of radiation per kilogram.

3.2.2 Surface functionalization of degraded KGM

The synthesis route of the herding surfactant was performed in a two-step chemical process as shown in the **Fig. 8**. The first step was hydrophobic surface functionalization of the KGM. The KGM was first dried in a vacuum drier for 24 hours to remove residual moisture. An amount of 5 g of KGM was taken in a 250-ml round-bottom flask, and ethyl acetate (100 ml) was added. The mixture was shaken manually for 1 minute and then sonicated for 15 minutes in VWR Model 50T Ultrasonic cleaner to get a homogenous mixture. The hydrophobization of KGM was carried out using octadecyl isocyanate (ODI). The hydrophobic tail was grafted to the KGM structure. An amount of 1 gram of ODI was added to the round-bottom flask and then sonicated repeatedly for 15 minutes. The chemical grafting took place under continuous stirring for 4 hours at 60 °C. The mixture was then centrifuged in a CL 2 Centrifuge at 3900 rpm for 3 minutes to separate the solvent from the reacted mixture. The residue mixture was again washed in ethyl acetate and re-centrifuged at 3,900 rpm for 5 minutes. The excess ethyl acetate was drained out and the residual mixture was dried overnight in the vacuum pump in preparation for step 2. Step 2 consisted of attaching charges to the polymeric chain. In the second step, a 1 g sample was put in a 250-ml round-bottom flask. Added to the flask were 0.5 ml 1,3-propane sultone, 0.15 g potassium carbonate, and 20 ml solvent N, N - dimethyl formamide, and the mixture was continuously stirred at 70 °C for 1.5 hours. The mixture was centrifuged at 3900 rpm for 4 minutes to separate the solvent. The residue was washed again in acetone and re-centrifuged at 3900 rpm three times for 3 minutes each time. The acetone was drained out and the residual mixture was dried in the vacuum pump overnight to form the MKGM.

3.2.3 Surfactant conductivity measurement

SDS (ionic surfactant): SDS in DI water solution (0.1 mol/l) was prepared in a 200 ml glass beaker. The solution was stored in refrigerator at 5 °C for 24 hours. The SDS surfactant has crystallized below the 5 °C atmosphere. The glass beaker was taken out of the refrigerator and placed on a hot plate stirrer. The conductivity meter probe was immersed into the solution. The dual measuring mode of conductivity meter could measure both the conductivity and the temperature. The solution was slightly heated to remain 0.2 °C/min increase. The measured conductivity and temperature data were drawn in **Fig. 11(a)**.

MKGM (non-ionic surfactant): 0.25 wt% of MKGM (16 kGy) in 200 ml water solution was kept overnight under refrigeration to maintain the temperature at 0 °C. The conductivity meter probe immersed into the solution measured both the conductivity and temperature. The solution was slightly heated to achieve 0.2 °C/min increment. The conductivity versus temperature plot is shown in **Fig. 11(c)**.

3.3 Characterization

The morphologies of pristine and modified konjac particles were imaging at JSM-7500F JEOL field-emission scanning electron microscope (FE-SEM). The molecular weight measurement was performed at TOSOH ambient temperature gel permeation chromatography system (GPC). The chemical structure of konjac particles were tested through Fourier-transform infrared spectroscopy (FTIR). All photographs were taken through Supereyes B007 USB digital microscope portable camera and SONY Alpha a600 camera. The temperature tests in this work were measured with thermometer Omega hh11b. The conductivity was tested with CON 6 hand-held conductivity meter.

3.4 ImageJ Software Analysis

ImageJ was the software for analyzing and calculating the oil slick areas in this work. It is an imaging processing program through Java-based language and could transfer colorful photograph into black & white photograph for pixels analyzing. Through ImageJ, every oil herding picture was transferred into pixels. The crystallizing dish area was known and transferred to pixels. Then the oil slick occupied black pixels were measured and converted to oil slick areas by the crystallizing dish pixels. Thus, the different herding time oil slick areas were achieved.

4. Conclusion

In this work, a novel biocompatible, highly environmental MKGM herding surfactant, was developed for rapid oil spill remediation. The synthesized MKGM surfactant was able to retract oil area efficiently. MKGM's non-ionic surfactant characteristics allows it to function without susceptibility to Krafft temperature, giving MKGM surfactants the unique ability to maintain surfactant function at temperatures approaching 0 °C. The ability to perform unaffected by low temperature is a great advantage compared with traditional ionic surfactant, as most are not able to function under 5 °C. Considering the increasing oil drilling in Arctic areas and inevitable oil spills, it offers a new direction to act as newly efficient oil herders for a wide range water temperature.

Acknowledgements

This research is partially supported by Mary Kay O'Connor Process Safety Center, Texas A&M University. We would like to thank National Center for Electron Beam Research for the KGM e-beam radiation. We acknowledge Materials Characterization Facility at Texas A&M University for performing FE-SEM and FTIR test. We acknowledge Dr. David Truong at Soft Matter Facility at Texas A&M University for GPC measurement.

References

Aggarwal, S., Schnabel, W., Buist, I., Garron, J., Bullock, R., Perkins, R., . . . Cooper, D., 2017. Aerial application of herding agents to advance in-situ burning for oil spill response in the Arctic: A pilot study. *Cold Regions Science and Technology, 135*, 97-104.

Babak, V. G., & Desbrières, J., 2004. Dynamic surface tension of hydrophobically modified chitosans. *Mendeleev Communications, 14*(2), 66-69.

Baffes, J., 2007. Oil spills on other commodities. *Resources Policy, 32*(3), 126-134. doi:https://doi.org/10.1016/j.resourpol.2007.08.004

Bakshi, M. S., & Singh, K., 2005. Synergistic interactions in the mixed micelles of cationic gemini with zwitterionic surfactants: fluorescence and Krafft temperature studies. *Journal of colloid and interface science, 287*(1), 288-297.

Behera, S. S., & Ray, R. C., 2016. Konjac glucomannan, a promising polysaccharide of Amorphophallus konjac K. Koch in health care. *International journal of biological macromolecules, 92*, 942-956.

Blumer, M., Sanders, H. L., Grassle, J. F., & Hampson, G. R., 1971. An ocean of oil: a small oil spill. *Environment: Science and Policy for Sustainable Development, 13*(2), 2-12.
Brown, G. G., Graves, G. W., & Ronen, D., 1987. Scheduling ocean transportation of crude oil. *Management Science, 33*(3), 335-346.
Dave, V., Sheth, M., McCarthy, S. P., Ratto, J. A., & Kaplan, D. L., 1998. Liquid crystalline, rheological and thermal properties of konjac glucomannan. *Polymer, 39*(5), 1139-1148.
Goldberg, V. P., 1994. Recovery for Economic Loss following the Exxon" Valdez" Oil Spill. *The Journal of Legal Studies, 23*(1), 1-39.
Gryczka, U., Dondi, D., Chmielewski, A. G., Migdal, W., Buttafava, A., & Faucitano, A., 2009. The mechanism of chitosan degradation by gamma and e-beam irradiation. *Radiation Physics and Chemistry, 78*(7-8), 543-548.
Gupta, D., Sarker, B., Thadikaran, K., John, V., Maldarelli, C., & John, G., 2015. Sacrificial amphiphiles: Eco-friendly chemical herders as oil spill mitigation chemicals. *Science advances, 1*(5), e1400265.
Henni, W., Deyme, M., Stchakovsky, M., LeCerf, D., Picton, L., & Rosilio, V., 2005. Aggregation of hydrophobically modified polysaccharides in solution and at the air–water interface. *Journal of colloid and interface science, 281*(2), 316-324.
Iakovou, E., Ip, C. M., Douligeris, C., & Korde, A., 1997. Optimal location and capacity of emergency cleanup equipment for oil spill response. *European Journal of Operational Research, 96*(1), 72-80.
Imai, T., Tsuchiya, S., Morita, K., & Fujimori, T., 1994. Surface tension-dependent surfactant toxicity on the green peach aphid, Myzus persicae (Sulzer)(Hemiptera: Aphididae). *Applied Entomology and Zoology, 29*(3), 389-393.
Inácio, Â. S., Costa, G. N., Domingues, N. S., Santos, M. S., Moreno, A. J. M., Vaz, W. L. C., & Vieira, O. V., 2013. Mitochondrial dysfunction is the focus of quaternary ammonium surfactant toxicity to mammalian epithelial cells. *Antimicrobial agents and chemotherapy, 57*(6), 2631-2639.
Jesus, C. D. (2016). Thousands Of "Small" Oil Spills Are Destroying the Gulf of Mexico. Retrieved from https://futurism.com/thousands-of-small-oil-spills-are-destroying-the-gulf-of-mexico
Katsuraya, K., Okuyama, K., Hatanaka, K., Oshima, R., Sato, T., & Matsuzaki, K., 2003. Constitution of konjac glucomannan: chemical analysis and 13C NMR spectroscopy. *Carbohydrate polymers, 53*(2), 183-189.
Kaushik, M. (2019). *11 Major Oil Spills Of The Maritime World*. Retrieved from https://www.marineinsight.com/environment/11-major-oil-spills-of-the-maritime-world/
Komoto, I., & Kobayashi, S., 2004. Lewis acid catalysis in supercritical carbon dioxide. Use of poly (ethylene glycol) derivatives and perfluoroalkylbenzenes as surfactant molecules which enable efficient catalysis in ScCO2. *The Journal of organic chemistry, 69*(3), 680-688.
Luo, X., Yao, X., Zhang, C., Lin, X., & Han, B., 2012. Preparation of mid-to-high molecular weight konjac glucomannan (MHKGM) using controllable enzyme-catalyzed degradation and investigation of MHKGM properties. *Journal of Polymer Research, 19*(4). doi:10.1007/s10965-012-9849-x
Muhd Julkapli, N., Akil, H. M., & Ahmad, Z., 2011. Preparation, properties and applications of chitosan-based biocomposites/blend materials: a review. *Composite Interfaces, 18*(6), 449-507.

Nishinari, K. 2000. Konjac glucomannan. In G. Doxastakis & V. Kiosseoglou (Eds.), *Developments in Food Science* (Vol. 41, pp. 309-330): Elsevier.
Paine, R. T., Ruesink, J. L., Sun, A., Soulanille, E. L., Wonham, M. J., Harley, C. D. G., . . . Secord, D. L., 1996. Trouble on oiled waters: lessons from the Exxon Valdez oil spill. *Annual Review of Ecology and Systematics, 27*(1), 197-235.
Peterson, C. H., Rice, S. D., Short, J. W., Esler, D., Bodkin, J. L., Ballachey, B. E., & Irons, D. B., 2003. Long-term ecosystem response to the Exxon Valdez oil spill. *Science, 302*(5653), 2082-2086. Retrieved from https://science.sciencemag.org/content/302/5653/2082.long
Rico, I., & Lattes, A., 1986. Formamide, a water substitute. 12. Krafft temperature and micelle formation of ionic surfactants in formamide. *The Journal of Physical Chemistry, 90*(22), 5870-5872.
Silliman, B. R., van de Koppel, J., McCoy, M. W., Diller, J., Kasozi, G. N., Earl, K., . . . Zimmerman, A. R., 2012. Degradation and resilience in Louisiana salt marshes after the BP–Deepwater Horizon oil spill. *Proceedings of the National Academy of Sciences, 109*(28), 11234-11239.
Takigami, S. 2009. 32 - Konjac mannan. In G. O. Phillips & P. A. Williams (Eds.), *Handbook of Hydrocolloids (Second Edition)* (pp. 889-901): Woodhead Publishing.
Tester, R. F., & Al-Ghazzewi, F. H., 2016. Beneficial health characteristics of native and hydrolysed konjac (Amorphophallus konjac) glucomannan. *Journal of the Science of Food and Agriculture, 96*(10), 3283-3291.
Urquhart, R. D., 1986. Heavy Oil Transportation - Present And Future. *Journal of Canadian Petroleum Technology, 25*(02), 5. doi:10.2118/86-02-05
Vargaftik, N. B., Volkov, B. N., & Voljak, L. D., 1983. International tables of the surface tension of water. *Journal of Physical and Chemical Reference Data, 12*(3), 817-820.
Venkataraman, P., Tang, J., Frenkel, E., McPherson, G. L., He, J., Raghavan, S. R., . . . John, V. T., 2013. Attachment of a hydrophobically modified biopolymer at the oil–water interface in the treatment of oil spills. *ACS applied materials & interfaces, 5*(9), 3572-3580.
Winger, M., De Vries, A. H., & Van Gunsteren, W. F., 2009. Force-field dependence of the conformational properties of α, ω-dimethoxypolyethylene glycol. *Molecular Physics, 107*(13), 1313-1321.
Woo, L., & Sandford, C. L., 2002. Comparison of electron beam irradiation with gamma processing for medical packaging materials. *Radiation Physics and Chemistry, 63*(3-6), 845-850.
Xu, Z., Sun, Y., Yang, Y., Ding, J., & Pang, J., 2007. Effect of γ-irradiation on some physiochemical properties of konjac glucomannan. *Carbohydrate polymers, 70*(4), 444-450.
Zhang, H., Yoshimura, M., Nishinari, K., Williams, M. A. K., Foster, T. J., & Norton, I. T., 2001. Gelation behaviour of konjac glucomannan with different molecular weights. *Biopolymers: Original Research on Biomolecules, 59*(1), 38-50.
Zhang, Y.-q., Xie, B.-j., & Gan, X., 2005. Advance in the applications of konjac glucomannan and its derivatives. *Carbohydrate polymers, 60*(1), 27-31.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Hurricanes Versus Tropical Storms Impacts – Shut-down? Recovery?

Chris (Kumar) Israni & Yaneira Saud*
ERM
840 W Sam Houston Pkwy N, Houston, TX 77024
*Presenter E-mails: chris.israni@erm.com, yaneira.saud@erm.com

Abstract

During the summer and fall seasons, regions along the US coastline face the threat of being hit by Tropical storms and Hurricanes. While Hurricanes are known for their impacts, the sites are typically well prepared to brace such weather conditions, with adequate planning prior the event occurring, and recovery measures, should the area be hit by the Hurricanes. Often, when forecasts indicate a Tropical storm as opposed to a Hurricane measures, there is a tendency to reduce the preparedness by a few notches as compared to the advent of a Hurricane. Should the storm pass by quickly or its intensity reduces further, the sites are not impacted by this lower level of preparedness. However, in the event of the forecast changing, or the storm gaining intensity or slowing down its progress, often sites will not have enough time to elevate the preparedness, e.g. the pattern of hurricane Harvey and its anomalous intensity, speed and path of progress.

Preparedness during those transition hours, posed further challenges, thereby hampering the recovery measures. At those times, while recovery measures are essentially, sites may often run into the situations of not having the right rescue equipment and other essential supplies. Hence, recovery may now pose additional threats to the people and the process.

This paper will discuss thoughts and views of the authors of how much of the preparedness must be common be it hurricanes or tropical storms, and what challenges will be different. The authors will share their view of what measures are independent of the storm intensity and what measures can be avoided during tropical storms, what becomes essential prior to the storms, and how can the risks to the people and process during the recovery measures be minimized. Key to remember is irrespective of the conditions and planning, the threat will always exist to human lives. Appropriate mitigation measures will weaken the impacts

Keywords: Inclement weather, Emergency Response, Operations Shutdown, Recovery Measures

Introduction

Tropical storms and subsequent Hurricanes [1] are natural phenomena that occur in the North Atlantic Ocean, Caribbean Sea, Gulf of Mexico, and Eastern North Pacific Ocean. When these named storms make land impacts, they bring about a lot of damage to people and property, due to the excessive winds and water. In recent times Hurricanes Katrina, Rita, Harvey, Irma, and Dorian have brought about tremendous amounts of damages to the USA and nearby islands [2,3,4].

Hurricane Dorian

With the onset of such events, one must realize the transient state of such phenomena, where the weather forecast is constantly changing. In the recent times, Hurricane Dorian has been once such classic example. The initial predicted path was to make landfall to Florida, for the USA, after devastating the Bahamas. As it made its progression, the hurricane categories changed from a 1 going up to 5 and then several iterations between 1 and 3, until this got converted into a tropical storm by the east coast of Canada. The figures 1- 3 below, indicate the model predictions, and how the predictions changed based on the storm progression.

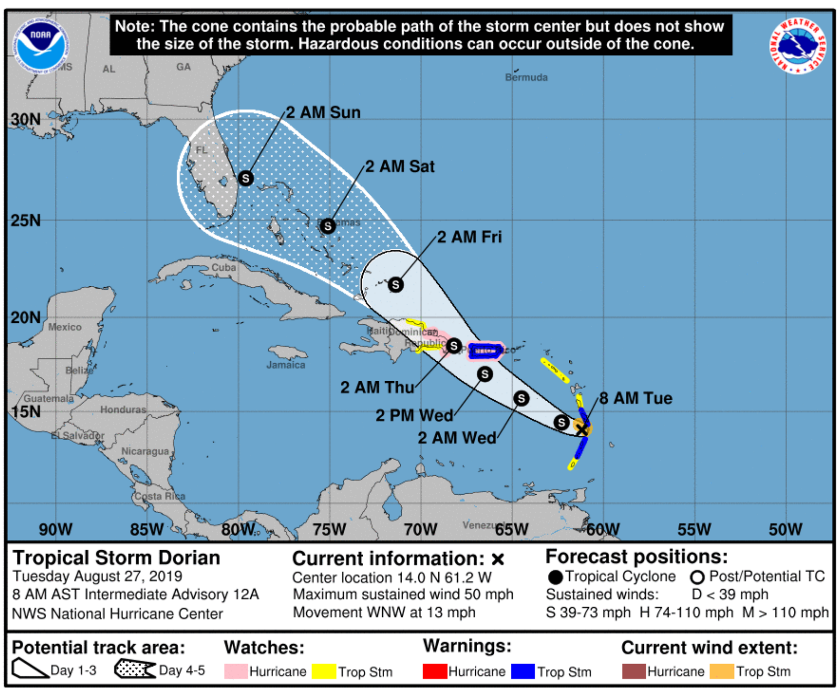


Figure 1. Dorian Projected Path – August 27, 2019 [5]

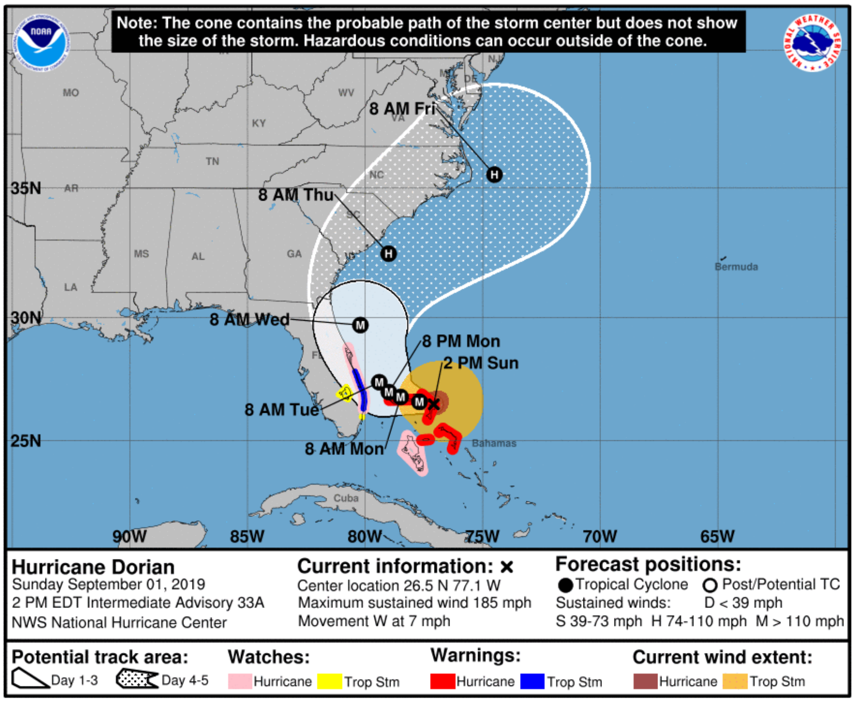


Figure 2. Dorian Projected Path – September 1, 2019 [5]

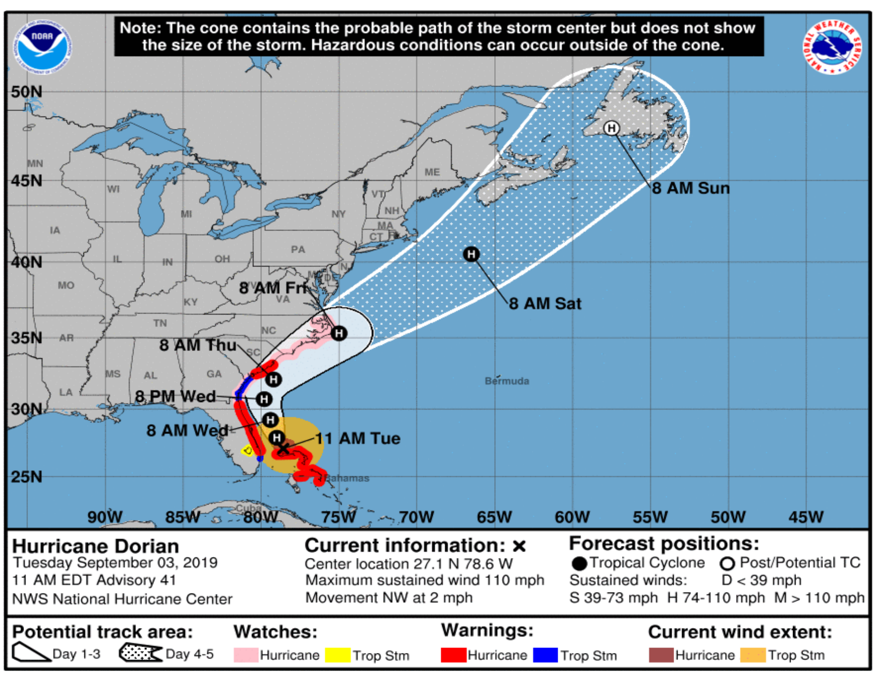


Figure 3. Dorian Projected Path – September 3, 2019 [5]

Weather Forecasting, Preparedness and Aftermath

The above illustration of the recently occurred Hurricane Dorian, indicates how uncertain the paths and the intensity of the storm may be; making it very critical to rely on weather forecasting.

As a precautionary measure, regions in the Gulf coast, East coast and West coast of the USA, have their hurricane preparedness plans initiated, typically by June of each year. Every state comes up with their plan providing the residents suggestions on path forward, in the event of such inclement weather conditions [6 – 9]. These plans get updated on an annual basis, based on the lessons learned of the previous year's conditions and happenings. Hurricanes such as Katrina, Harvey and Irma have been indicative of such changes [2,3].

Industries that fall under such zones also have regulatory aspects, leading to mandatory hurricane preparedness plans as laid down by OSHA [10]. Under these requirements, it is the employers responsibility to ensure that the employees are safe during the occurrence of such events.

Let's take the examples of Hurricane Katrina (occurred in 2005) and Hurricane Harvey (occurred in 2017), that had devastating impacts on the regions of landfall. Each of these events involved massive preparations for the respective cities, towns, and also the industries in those regions. The weather forecast for Hurricane Katrina changed very rapidly [11], and despite the efforts taken the by the respective sites, the aftermath was devastating [12]. Data collected from the event, on the aftermath, also led to additional research by various groups such as [13], to get into more accurate predictions on the commercial impacts to refineries.

Similarly summarizing the formation of Hurricane Harvey [14] which began on August. 17, 2017 as a slow-moving tropical storm in the Gulf of Mexico, weakened to a tropical wave August. 19, 2017. However, this Tropical Depression Harvey reformed on August. 23, 2019. It grew into a Category 1 hurricane with 80-mph winds August 24, 2019 and continued to gain strength as it slowly progressed towards Texas. The National Hurricane Center upgraded the storm to a Category 4 hurricane with sustained winds up to 130 mph Aug. 25. It made the first landfall over, in south-central Texas, late August 25, 2019 as a Category 4. It stalled around southern Texas for days as a weakening hurricane, producing catastrophic flash and river flooding. Harvey then downgraded to a tropical storm August. 26, 2019. By the next day, the winds died down to as much as 40 mph, but the storm dumped a year of rain in less than a week on Houston and much of southeastern Texas. Tropical storm Harvey made its third and final landfall August. 30, 2019 near Port Arthur, Texas, and Cameron, Louisiana, bringing widespread flooding. Tropical Storm Harvey was then downgraded to a tropical depression but it continued to dump large amounts of rain on parts of eastern Texas, Louisiana, and southern Arkansas.

What do we know about Emergency Response ?

Emergency response during such transient conditions as illustrated above with Hurricane Harvey, can we very tricky and challenging, especially for industry sites. A straight-forward conservative approach would mean, a complete shutdown of the site, in anticipation of such inclement weather. The focus here would be protection of human lives, in anticipation of any potential disastrous situations. At the same time this results in downtime, implying drop in production and thereby revenue/profitability.

On the other hand, another approach may be to ignore the potential impacts of an upcoming storm/hurricane. In such cases, evaluating potential financial impacts, a site may be inclined to continue production in a limited but safe manner. These are two ends of a spectrum, and a site may not necessarily resort to either end. Rather the emergency response plan would be based on the assumption, that the existing plan is robust and resilient. Meaning, that the associated hurricane preparedness plan might include various scenarios involving rapid decision making and rapid adaptations to changes in these decisions, due to changing weather conditions.

This challenge is prevalent for all the sites that fall in such hurricane prone regions. However, that is essentially the truth is that the employer is responsible for the safety of their staff while on site [15].

What did we learn from Harvey pertaining to sites?

The intensity of the Hurricane Harvey [14], was every changing. A slow moving hurricane, that was downgraded to a tropical storm, however it continued to move at a very slow pace, and bring a massive downpour of rain along its path. This resulted in severe localized flooding. A key factor that dominates the entire situation here is the ever changing weather condition. For sites in that region, it comes very critical to have rapid decision making for response plans, and communicating that information for a seamless implementation.

For a successful site, its operational excellence (OE) program must be sustainable that is depicted via the model[17] below in Figure 4

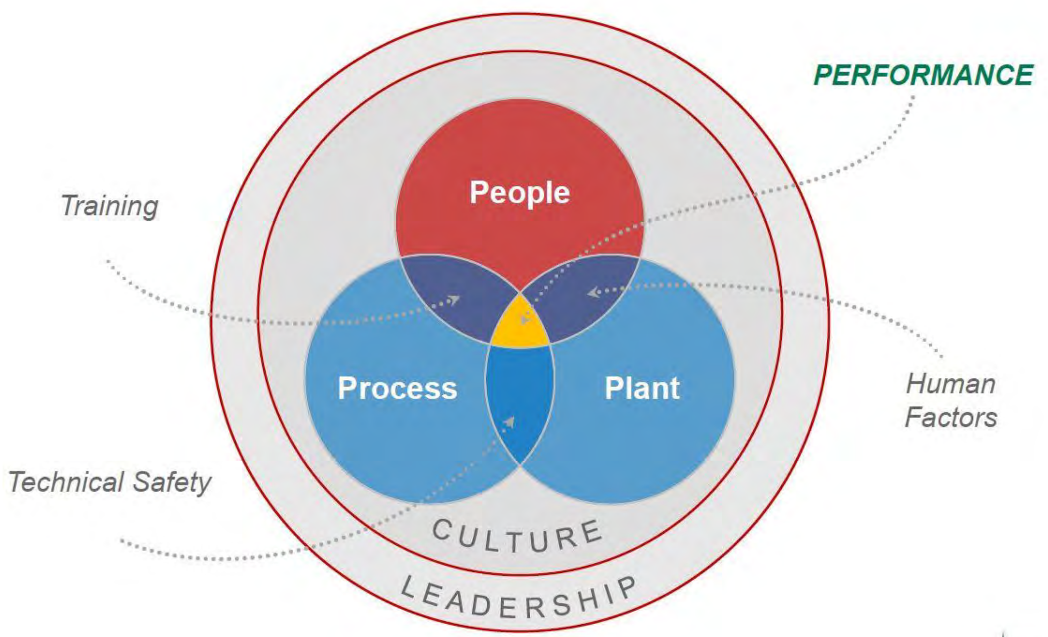


Figure 4. Explanation for Sustainable Safety [17]

This success in OE is also attained when the technical safety involved follows a risk based process safety (RBPS) approach [17]

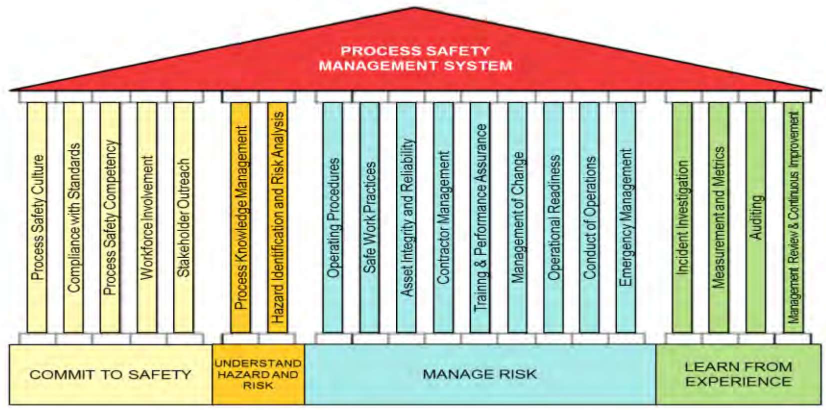


Figure 5. Illustration of Risk Based Safety [17, 18]

While the concepts of OE and RBPS are followed during regular operations, and operational upset conditions such as planned and unplanned shutdowns, the same can be applied evening during pre-disaster and post disaster type of situations as was with Harvey (Hurricane and Tropical storms).

For a site, the decision making is always a challenge as they have to keep evaluating the changing conditions, keeping in mind people safety and production, hazards associated with the shutdowns, startups and recovery (in the event that the storm strikes).

Based on the experience of the authors in assisting sites for assessment of their post disaster reviews, the authors have come up with the following areas that assist in minimal impacts to a site, during such tropical inclement weather. These factors are:

1. Management Systems and Safety Culture: A strong and robust prevalent safety culture helps in the decision making process. This brings about ownership, and involvement of relevant teams, that assist in making the right decisions, constantly emphasizing that it is always people over production.

2. Shutdown and Startup Procedures: The importance of having adequate of shutdown/start-up procedures, decisions, and the execution of such procedures during inclement weather, make the implementation process easy, and eliminate any potential confusion in times of turmoil

3. Hazard Identification & Intervention and Safe Work Practices (SWP): Presence of a comprehensive permit to work (PTW) system that includes a combined hazard assessments, which incorporates maintenance and operations disciplines, helps in such situations. This must also involve field verification of identified safeguards and mitigations before the equipment intervention begins.

4. Hurricane/Tropical Storm Preparedness: While it may seem obvious that sites will have such preparedness plans in place, the key is that these plans be revisited every year, incorporating the principles of lessons learned based on field observations, real-time data and the concepts of

RBPS. Another factor while preparing the sites is to remember that while the typical approach may be to focus only on Hurricanes, it should be noted that tropical storms come with their set of impacts too, that could impair a site.

5. Emergency Response and Recovery Logistics: While updating the preparedness plans, the site must be prepared to handle disasters with recovery measures as well. Take a situation of potential flooding that involves the need of flood response resources being readily available, for example light boats, waders, occupied building unperishable food supply, bedding, standalone kitchen/laundry facilities, clothing changes, and personal hygiene supplies.

6. Emergency Response and Recovery Tactical Communications: While performing emergency response and associated recovery measures, the importance of clear tactical communication is priceless. This helps personnel understand their roles, and the roles of others involved in response measures. It also assists in maintaining and improving morale of the employees, keeps them involved in the decision making process, and helps to improve perceptions.

References

[1] Weather related definitions, https://kestrelmeters.com/pages/weather-glossary , accessed on 24 August 2019

[2] Hurricanes in History, https://www.nhc.noaa.gov/outreach/history/, accessed on 9 September 2019

[3] What was the largest hurricane to hit the United States, https://geology.com/hurricanes/largest-hurricane/, accessed on 15 September 2019

[4] Dorian – Atlantic Ocean, https://blogs.nasa.gov/hurricanes/tag/dorian-2019/, accessed on 15 September, 2019

[5] DORIAN Graphics Archive: 5-day Forecast Track,Initial Wind Field and Watch/Warning Graphic, https://www.nhc.noaa.gov/archive/2019/DORIAN_graphics.php?product=5day_cone_no_line_and_wind, accessed on 16 September, 2019

[6] Hurricanes, https://texashelp.tamu.edu/browse/by-type/naturally-occurring/hurricanes/, accessed on 9 September 2019.

[7] Disaster preparedness guide, Mayor's Office, City of Houston, TX, Office of Emergency Management, 2019

[8] Hurricane preparedness South Carolina, https://www.scemd.org/, accessed on 9 September 2019

[9] Florida Emergency Preparedness Guide, Florida Health Publication, 2019

[10] Occupational Safety and Health Administration. "Emergency Action Plans." U.S. Department of Labor, Occupational Safety and Health Administration. 1910.38

[11] "Service Assessment – Hurricane Katrina Aug 23-31, 2005" U.S. Department of Commerce, NOAA, June 2006.

[12] Case Study – Hurricane Katrina, https://www.metlink.org/other-weather/miscellaneous-weather/case-studies/case-study-hurricane-katrina/ accessed on 15 September 2019.

[13] Park, J; Moore, J and Gordon, P "The regional economic impacts of Hurricanes Katrina and Rita on Oil refinery operations in the Gulf of Mexico, and the rest of the US : Applying a flexible multi regional Input-Output Model " https://www.researchgate.net/publications/242186880, published January 2007.

[14] 2017 Hurricane Harvey: Facts, FAQs, and how to help, https://www.worldvision.org/disaster-relief-news-stories/2017-hurricane-harvey-facts, accessed on 10 September 2019

[15] Emergency Response Plans, https://www.ready.gov/business/implementation/emergency, accessed on 12 September 2019

[16] General Duty Clause, Section 5A OSH Act of 1970.

[17] Israni, C, "Attaining operational excellence via a sustainable approach to safety", presented at MKOPSC, 2018.

[18] CCPS. *Guidelines for Risk Based Process Safety.* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2007.

[19] Process Safety Management, OSHA 3132, US Department of Labor, Occupational Safety and Health Administration.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Exposure of Fabrics used in Personal Protective Equipment to Combustible Dust Flash Fires

Claudio V.B. Favero, Sean C. O'Hern, Alfonso Ibarreta*, Timothy J. Myers, Michael C. Stern, and James Vickery
Exponent, Inc.
9 Strathmore Road, Natick, MA 01760 USA
*Presenter E-mail: aibarreta@exponent.com, cfavero@exponent.com

Abstract

The use of appropriate fabric in personal protective equipment (PPE) garments is essential to protect personnel from injuries caused by flame engulfment, thermal radiation, and burning material during exposure to a combustible dust flash fire. One of the standards available today for evaluating performance of such fabrics, i.e., NFPA 2112 *Standards on Flame-Resistant Garments for Protection of Industrial Personnel Against Flash Fires,* does not account for the heat flux from the burning material that may impinge on the fabric during a dust flash fire incident. In a previous study[1], we exposed different types of fabrics to transient dust and liquid mist fuelled flash fires (an organic dust, a metal dust, and xylene) and qualitatively analysed the performance of these fabrics. Here, we extend the scope of the initial investigation by evaluating performance of fabric when exposed to a flash fire for a longer period of time, as well as exposed to a different incident angle to the flash fire. The time of exposure is important because the fabric becomes less effective over time. The angle of incidence plays an important role on the amount of burning material that can impinge on the fabric. This study is part of an effort to increase the understanding of thermal degradation of fabrics for better selection of material used in personal protective equipment.

Keywords: Combustible dust, fabrics, personal protective equipment, flash fires.

[1] Analysis of Combustible Dust Flash Fires on Personal Protective Equipment Fabrics, Proceedings of the IChemE Hazards27 Conference, Birmingham, UK, 2017.

MARY KAY O'CONNOR
PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Integration of Process Safety into Engineering Design during Offshore Project Execution

Jeff Bryant, Charlie Gerschefski, Edward Liu*, Steven Zhang*
Wood.
17325 Park Row, Houston, TX 77084
*Presenter E-mails: edward.liu@woodplc.com steven.zhang@woodplc.com

Abstract

Process Safety, as part of Technical Safety which also includes Fire Protection, Environmental Protection, and Human Factor Engineering, plays an important role in the life-cycle of the offshore project execution. A well-managed execution of Process Safety in different engineering design phases, from the conceptual design to commissioning phase, can ensure regulatory compliance and efficient improvement in the engineering decision making for project assurance, risk reduction and control.

This paper will present the approach that Wood implements to facilitate the project conceptual design with Project Technical Safety Philosophies, General Arrangement layout studies, (high level) key Process Safety studies, integrated with other Technical Safety considerations. Wood's in-house Process Safety study experience and lessons learned will be presented for the project FEED and DED phases, involving process hazard identification and analysis (HAZID & PHA), Formal Safety Assessments (QRA, FERA, EERA, TRIF, etc.), Functional Safety Assessment (FSA), and Performance Standards. A flowchart of the Process Safety study sequence will be presented with integration of Fire Protection, Environmental Protection, and Human Factors Engineering. The successful implementation of this approach can fulfil the project assurance in safety design and improve the efficiency by applying cutting edge technologies.

Keywords: Process Safety, Offshore Project Execution, Engineering Design

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

A Case Study from a Fire Incident in Naphtha Heater Caused by Sulfidation

Kevin C. P. Wen*
Safety & Health Dept. Advanced Engineer
Nan Ya Plastics Corporation
No.201, Tung Hwa N. RD, Taipei, Taiwan, ROC
*Presenter E-mail: Kevinwen@npc.com.tw

Abstract

On November 19, 2017, a naphtha heater of FPG's ML chemical plant was forced to an emergency shutdown (ESD) caused by an abnormal signal. Following troubleshooting and inspection, the process was restarted on November 21; however, during startup, naphtha heater caught fire that also spread to process equipment. The fire resulted in one week of downtime loss, but luckily there was no casualty.

Background and Analysis:

1. The heater in this case was a vertical cylindrical one with two main components: helical radiation coil and cross-flow convection fin tubes. It has height of 29.87m, OD of 3.378m, and the tubes' was of Cr-Mo steel.
2. Because naphtha contains sulfur and that the temperature of naphtha heater reaches 350℃ when in operation, thickness measurement and steam decoking of the radiation coil were regularly carried out. However, thickness measurement of the convection fin tubes had never been conducted due to its compactness.
3. Investigation of the fire incident revealed a two centimeter hole in the convection fin tube. In addition, the deposits in the tubes were found to contain sulfide (3~5 wt%), while there was dirt on the outside. Also, thickness of the tubes bottom had obviously been thinned. On the other hand, no evidence of creep was found.
4. Cross-referencing the observations with API 573 and API 571, we concluded that the root cause of fire incident was the high temperature sulfidation corrosion on tubes of the convection zone which eventually led to a hole and naphtha leaks.

After the incident, we implemented the following improvements to the naphtha heater:

1. Thicknesses of both the radiation coil and convection fin tubes are to be measured by Smart

Pig (Pipeline Inspection Gauges), the results of which serves as an indicator for decoking and tube renewal.
2. As steam decoking was ineffective, possibly making coking problem worse, it has been replaced by mechanical cleaning (PIG decoking system) .

Keywords: naphtha heater, sulfidation corrosion, convection fin tubes, coking, decoking, radiation coil

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

How to Treat Expert Judgment? With certainty it contains uncertainty!

Hans J. Pasman* and William J. Rogers
TEES Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A & M University, College Station, 77843 Texas, USA
*Presenter Email: hjpasman@gmail.com

Abstract

To be acceptably safe one must identify the risks one is exposed to. It is uncertain whether the threat really will materialize, but determining the size and probability of the risk is also full of uncertainty. When performing an analysis and preparing for decision making under uncertainty, quite frequently failure rate data, information on consequence severity or on a probability value, yes, even on the possibility an event can or cannot occur is lacking. In those cases, the only way to proceed is to revert to expert judgment. Even in case historical data are available, but one should like to know whether these data still hold in the current situation, an expert can be asked about their reliability.

Anyhow, expert elicitation comes with an uncertainty depending on the expert's reliability, which becomes very visible when two or more experts give different answers or even conflicting ones. This is not a new problem, and very bright minds have thought how to tackle it. But so far, however, the topic has not been given much attention in process safety and risk assessment. The paper has a review character and will present various approaches with detailed explanation and examples.

Keywords: Probability, imprecision, expert elicitation, Dempster-Shafer theory, Fuzzy sets, and logic

1. Introduction

It seems so easy: once in case in an analysis, *e.g.*, a LOPA, the complexity of the problem structure has been solved, as a next and final step data must be filled in, such as the probability of failure on demand of a critical component, *e.g.*, a pressure relief valve. However, one knows that manufacturer data are too optimistic, while the OREDA data base [1] may provide an answer not valid under the conditions the valve is applied in an actual process. In the best case, there is in the plant some historical data available on similar valves, but those are of a different brand creating another uncertainty. As a last resort, a few people familiar with the installation and employed already a considerable number of years at the plant may be asked to provide an estimate. This reverting to expert judgment can have different forms. Easiest for the expert may be to give a linguistic grading term (‘high’ or ‘low’) or just a single figure, but knowing there will be uncertainty the interviewer may invite the experts to specify an interval with both a lower and a higher bound. Even more sophisticated is to ask for an estimate of a mean value and a confidence or credibility interval. Experts may also be asked about different information, *e.g.,* whether a run-away in case of a certain batch-process is thought possible or plausible under the expected condition ranges.

In a wider context, questioning experts serves to support optimum decision making. There are many methods developed for that purpose, for example Saaty’s [2] method of Analytical Hierarchy Process (AHP) developed in the 1970s, in which participants must make pairwise selection between alternatives on the basis of a number of criteria. More sophisticated is multi-attribute utility theory to make a decision based on value judgments of multiple, competing objectives. However, this paper will treat the use of expert judgment in risk assessment questions.

Already decades ago, statisticians engaged in intense deliberations on how to deal with uncertainty. It all starts with deep thoughts about the concept of probability. Oldest is the so-called frequentist idea in which an experiment is performed of which the outcome can take different forms or values. A classic case is the throw of a dice, or determining a sample of a large population of red and white balls in an urn and predicting the fraction of red. The objective is to determine a distribution of outcomes enabling prediction of future action outcomes or composition of the population without counting them all. This developed to a collection of distribution functions in which results could be fitted and to significance levels with confidence limits dependent on the variability of draws and the size of the sample. Later, the Bayesian approach gained strength, in which all previous information/knowledge can be cast into a prior distribution, while new evidence is represented by a likelihood function, and the result is an update of the prior to a posterior distribution based on the normalized co-occurence of the prior and the likelihood. The Bayesian model provides many more possibilities in solving problems than frequentist statistics and has become the leading approach for evidence-based testing of a hypothesis or an event.

In many situations, though, when asked in human dialogue to make an estimate or a prediction of the probability of an event occurrence, a person can produce such a probability value based on intuition supported by experience. Such a probability estimate is called a subjective or imprecise probability value. It fits well with the Bayesian approach, which works with information of all uncertainty levels and propagates the uncertainties. With new evidence in the likelihood, the prior is updated to a posterior result with lower uncertainty than the prior. Besides a development of a strict probabilistic approach by Cooke [3] in the 1980s that we shall consider later, in the 1960s and 70s, two different less strict theories evolved dealing with uncertainty:

- Dempster-Shafer theory of evidence, developed by Dempster [4] and later Shafer [5] on belief and plausibility. Also with the Dempster rule, replies from different responders can be combined. Strict probability theory requires that the probability an event will occur and the probability it will not occur, sum to unity, 1. A human making an estimate will often not guarantee, though, that the complement of the answer given, fulfills that requirement. He/she may not know, hence is ignorant, or at least he/she is unsure it will.

- Fuzzy set and logic by Zadeh [6, 7] in which an interviewer will obtain an imprecise, hence fuzzy, answer represented by a membership function with the value 1 at the given estimate and with value zero at a minimum below which and a maximum value above which the estimate value is believed to be not possible. The membership function can have any shape between 0 and 1.

Over the years, these theories have been further developed and applied for various purposes, such as Dempster-Shafer in sensor fusion for target identification in a cluttered environment and Fuzzy set and logic in classification problems. Fuzzy logic enables solving the problem of combining unsharp values of characteristic properties of related items or kinds to a desired final result, such as the known example of food quality wasn't bad, service was perfect, price is okay, hence tip can be decent. Different values of characteristics will infer different outcomes. Both Dempster-Shafer theory and Zadeh's fuzzy set and logic are widely applied to facilitate decision making in uncertain situations.

Uncertainty is usually categorized by two types, although distinction is not always very clear and a variable can contain both types of uncertainty at the same time:

- Aleatory uncertainty, by which due to lack of accuracy/precision of observational means, in general random variability from ranges of conditions, an outcome cannot be established accurately, and,
- Epistemic uncertainty, which is a consequence of lack of knowledge about the subject due to the amount and quality of the data.

In particular, the epistemic uncertainty will be addressed here.

By the end of 1980s, Klir [8] in the Cambridge Debate on Uncertainty, wrote a clear synthesizing paper *against* the claim that probability, as traditionally defined, the standard approach, is the only concept to describe uncertainty. He did this with a counterclaim that one must go beyond only probability. Klir starts off with distinguishing two types of uncertainty:

- Vagueness, encompassing: fuzziness, haziness, cloudiness, unclearness, indistinctiveness, sharplessness and indefiniteness, and,
- Ambiguity, comprising of: non-specificity, variety, generality, diversity, divergence, equivocation, incongruity, discrepancy, dissonance, disagreement.

He continues by mentioning that *imprecision* can relate to both vagueness and ambiguity, while in the latter non-specificity and disagreement are again different. After analyzing the matter in much detail, Klir [8] concludes that probability conceptualizes "uncertainty strictly in terms of conflict among degrees of belief allocated to mutually exclusive alternatives"; in other words, a probability P of an event or quantity intrinsically holds the contrast that the probability the event will *not* occur or the quantity will be different, will be the complement $1 - P$. Hence, the standard approach to probability covers only part of uncertainty.

Uncertainty is also related to less precise information and in that context Zadeh [9], after having launched in 1965 the fuzzy set theory mentioned above, published in1977 the possibility theory. The latter states that where imprecision is inherent to natural language, in case the meaning of information is the objective and not its measure, one can speak of "possibilistics", rather than probabilistics, and even of a possibility distribution as a counterpart to the probability one. All of this found its way to Artificial Intelligence techniques.

More recently in 2011, Helton and Johnson [10] summarized the alternative representations of epistemic uncertainty at increasing structure and quantification as follows: (1) Interval analysis, just providing a low and high boundary with no information in between (uniform distribution with all values equally likely); (2) Possibility theory, consisting of a set of possible elements to each of which a likelihood value can be attached together forming a possibility distribution, which is related to the Fuzzy set approach; (3) Evidence theory (Dempster-Shafer), which specifies a limited number of focal elements, while each element is given a measure of credibility (basic assignments or basic belief assignments summing to 1, confusingly also called basic probability assignment); (4) Probability theory, involving element probabilities in a fully developed structure embodied by a probability density function.

At this probability end of the spectrum, Cooke developed so-called *structured expert judgment* attempting to make the process of interrogating experts on a probability value, in which there will be always disagreement among experts, as transparent as possible. This is realized by introducing a set of strict methodological rules. These rules lead among others to calibration of the experts and to the individually scoring of performance-based weights.

In the remainder of the paper, we shall restrict ourselves to the more practical aspects of expert estimation. In Section 2 we shall describe the Dempster-Shafer approach in more detail, and in Section 3 the Fuzzy set and logic one, both with some examples. In Section 4 Cooke's method will be described, and in Section 5 similarities and differences, also in required effort, will be summarized, followed by Section 6 with conclusions.

2. Dempster Shafer Theory (DST) of evidence

In various publications Shafer [5, 11] explains the original idea of belief functions and evidential reasoning in case a human makes a statement about an event, fact, or value. It encompasses belief, doubt, plausibility, disbelief, and ignorance, all associated with uncertainty. For example, if a person asserts that a certain event took place or is going to take place, it does not mean that there is no space to believe it did not occur or is not going to occur. The statement can gain strength, hence support, by evidence – a Bayesian element[1] -, while the reliability of the person making the statement can be estimated by a different person knowing the one making the statement (where reliability and unreliability sum to 1). This reliability is called weight of rather mass, m. Generalizing and following the practical application to reliability engineering by Rakowsky [13], hypotheses or information pieces of a data source, *e.g.,* experts' estimates on states or events, may constitute a set of elements, A (a frame*,* formally called a *frame of discernment* or of *disjoint states*). For example, suppose the set A contains three of each other independent pieces of evidence or elements A_1, A_2, and A_3, then, the power set[2] Ω of $A = \{\{\emptyset\},\{A_1\},\{A_2\},\{A_3\},\{A_1, A_2\},\{A_1, A_3\},\{A_2, A_3\},\{A_1, A_2, A_3\}\}$. Hence, with n elements the number of sub-sets is 2^n, or with three information pieces or so-called *focal*

---

[1] Dempster and Shafer asserted compatibility of their approach with the Bayesian updating of existing information with new evidence, and Shafer even called their theory a "generalization of the Bayesian theory of subjective probability judgment", evoking interesting and very clear comments by Judea Pearl [12]. The latter was in 2011 awarded with the ACM Turing award in computer science for introducing probabilistics in artificial intelligence and because of his foundational work on causality and on Bayesian networks.

[2] Power set Ω is the set of all sub-sets, mathematically formulated as $A \subseteq \Omega$. The number of subsets is 2^{Ω}.

elements, $2^3 = 8$. Each subset can be assigned a mass, called *basic assignment*[3] or basic belief assignment, depending on judgment of its trustworthiness. Pearl [12] called the assignment the "probability of provability". The sum of masses must be 1 (mathematically, $m : 2^\Omega \rightarrow [0,1]$). The $\emptyset$ null set represents the uncertainty whether any more information on the subject exists; if it is thought certain there is no more, $m(\emptyset) = 0$.

Due to subjectivity, it is uncertain which piece of evidence has the highest reality value. Also, because of multi-value statements and other complications, the explanatory wording by different scholars of the Dempster-Shafer Theory (DST) implied relations that can slightly differ and may confuse. At this stage, the belief function or belief structure shall be introduced. In this, *belief* represents the lower bound of mass associated with a focal element or a collection of those, supporting the expert claim or trustworthiness of the source, and plausibility represents the upper bound. In contrast to many papers, we shall start with *disbelief* in a subset A_i out of set A, or belief in not $\bar{A}_i$. It is easy to see that this is the complement of the sum of all supporting mass or evidence $m(A_j)$ of any focal element A_j intersecting with A_i including A_i itself, hence contributing to the plausibility of A_i, while excluding null sets: $bel(\bar{A}_i) = 1 - \sum_{A_j \cap A_i \neq 0} m(A_j)$ (to be clear j includes i). Thus, plausibility of A_i can be defined as $pl(A_i) = 1 - bel(\bar{A}_i)$. Next will be the definition of belief, or the degree in which A_i is believable: $bel(A_i) = \sum_{A_j \subseteq A_i;\, A_j \neq \emptyset} m(A_j)$, hence the mass of focal elements A_j, which are *subsets* of A_i and A_i itself. Its complement is *doubt* as represented in Figure 1. It always holds that $bel(A_i) \leq pl(A_i)$, while the two are not additive nor add to 1.

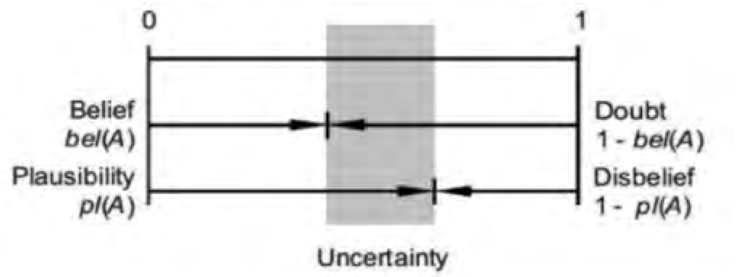


Figure 1. Representation of the various qualifying functions given evidence or data and the margin of uncertainty or ignorance according to Rakowsky [13].

Summarizing, $m(A)$ measures the degree of belief in claim A; $bel(A)$ measures the total degree of evidence support by the non-null focal element subsets of the set of interest A and that of A itself, so it represents a minimum of support, while $pl(A)$ measures the total support of all elements intersecting with A, and not null, hence a maximum of support. The difference represents the uncertainty. In continuation of the example above with j = 1 to 3:

$$bel(A) = \sum_{A_j \subseteq A;\, A_j \neq \emptyset} m(A_j),\ e.g.,\ bel(A_1, A_2) = m(A_1) + m(A_2) + m(A_1, A_2) \quad (1)$$

$$pl(A) = \sum_{A_j \cap A \neq 0} m(A_j),\quad e.g.,\ pl(A_1, A_2) = m(A_1) + m(A_2) + m(A_1, A_2) + m(A_1, A_3) + m(A_2, A_3) + m(A_1, A_2, A_3) \quad (2)$$

[3] Shafer [5,11] and others called m basic probability assignment or *bpa,* but later, *e.g.*, Rakowsky [13] warned that actually it should not be confused with a probability value, so it is preferable to speak of basic assignment.

If a second person confirms the statement made but the reliability of this person is estimated differently, Dempster's combination rule (intersection, AND, joint) to be considered as updating just as in the Bayes theorem, calculates the final weight:

$$m_{12}(A|A \neq \emptyset) = \frac{1}{1-k}\sum\nolimits_{B\cap C=A} m_1(B)m_2(C);\ \ m_{12}(\emptyset) = 0;\ \ k = \sum\nolimits_{B\cap C=\emptyset} m_1(B)m_2(C)$$

where $m_{12}(A)$ is the combined reliability of common focal elements A, $m_1(B)$ is the reliability of focal elements B of the first person and $m_2(C)$ are those of C of the second, while k represents the effect of conflicting elements, hence, those that do not intersect, $B\cap C = \emptyset$. Summing intersecting elements, $B\cap C \neq 0$, though, is often an easier way to derive k via its complement.

Example 1: asking experts about a possibility of event occurrence
Applying the rule is not in every case straightforward. The following is an example inspired by one of Shafer [10] applied to the process safety area of interest. When asking two experts independently of each other whether for a certain batch process a run-away is possible or not, both respond positively. So, in the combination there are two focal elements with a runaway possibility. There is no conflict, but the older expert is estimated to have a reliability m_1 = 0.8 and the younger one m_2 only 0.6. When the joint unreliability (1 – 0.8)(1 – 0.6) = 0.08 is calculated, $k = 0$, as there is no intersection with a null element. Hence, the reliability of the joint opinion m_{12} increases to 1 – 0.08 = 0.92. If conflicting opinions appear and the younger states that runaway is not possible, in the combination will be an intersection with a null set, hence k = 0.8×0.6 = 0.48. The unreliability of the younger person, (1 – 0.6), leaves the possibility of runaway still open, so that the extent of belief m_{12} of the statement runaway is possible decreases to 0.8·(1 – 0.6)/(1 – 0.48) = 0.62, and in analogy, that of runaway will not be possible 0.23. If, for example, probabilities of an event are estimated and two fully reliable experts differ strongly of opinion but coincidentally agree with low probability on the same alternative possibility, the rule no longer provides a correct answer as the rule yields mass = 1 for that low probability; later Yager [14] and others suggested improvements, see for more details also Sentz and Ferson [15].

The above example was on an event possibility, but DST can be applied also to failure rates. We shall follow Rakowsky [13], Simon et al. [16] and Khakzad [17] to see how we can apply DST in daily life of risk assessment to objectivize expert estimates of state probability and belief mass values and using those in fault and event trees, formally modeled in evidential network representing belief and plausibility but solved by Bayesian network algorithms. More reading and applications can be found in [15], [18] and [19]. Although the DST allows analyzing relatively complex situations, as examples the simplest scenarios will be considered here.

Example 2: an expert estimating probability of successful functioning and failure
Assume a component that will have one failure mode, so it has only two states it can be in: functioning successfully (S) or failed (F). The frame of discernment is: $\{\{\emptyset\},\{S\},\{F\},\{S,F\}\}$. The component is either in S or F -state (mutual exclusiveness), so the first and last term can be eliminated as the knowledge with the two middle elements about which state the component is in, is complete; however, if the latter is not the case, the set $\{S,F\}$ will express the epistemic uncertainty or ignorance about the state the component is in. Anyhow, given the expert is fully trusted, the probabilities provided can be taken equal to the masses, because these probabilities

represent the best extent of belief. For example, when asked, an expert estimates the successful functioning probability over the next year to be 0.7, and the failure probability in that same year to be 0.2 (two in ten). The sum of masses over the singletons must equal 1, so the mass of $\{S, F\}$ = 0.1. In this case, $bel(S)$ and $pl(S)$ are equal to 0.7 and 0.8, whereas $bel(F)$ and $pl(F)$ will be 0.2 and 0.3. Simon et al. [16] and Khakzad [17] show how epistemic uncertainty can be propagated as a separate 'state' using the Bayesian network (BN) infrastructure. In Figure 2 an example is presented of a fault tree modeled as a BN.

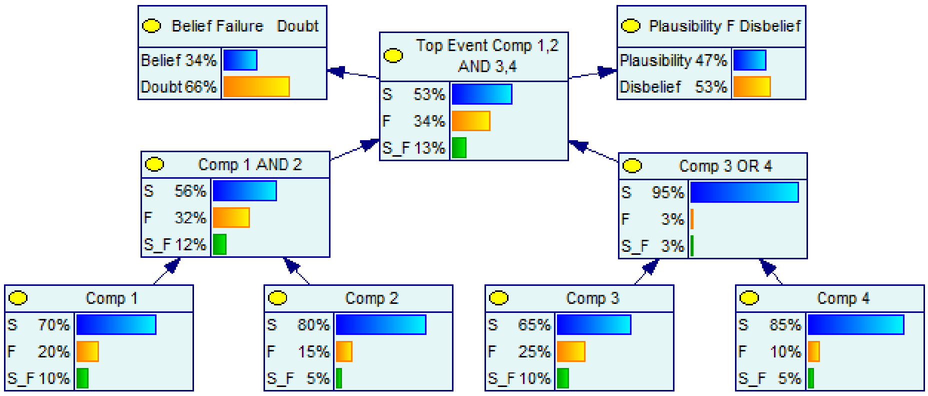


Figure 2. Evidential network showing the result of estimates of functional success probability $\{S\}$ over one year, failure probability $\{F\}$ (for demonstration assumed high) and remaining epistemic uncertainty $\{S, F\}$ of two parallel components in AND and two in OR position solved by Bayesian network (GeNie, BayesFusion LLC), following the reasoning of Simon et al. [16] and Khakzad [17].

Example 3: two (or more) experts are asked to estimate probability values

Alternatively, two experts A and B can be asked to provide probability values. Fusing the values they give, shall be performed using the combination rule as shown by Rakowsky [13]. A simple example is worked out in the following Tables 1-3:

Table 1. Expert focal element input data

	Expert A	*m*	*Expert B*	*m*
$\{S\}$	A1	0.7	B1	0.8
$\{F\}$	A2	0.2	B2	0.15
$\{S, F\}$	A3	0.1	B3	0.05

Table 2. Combination table of singleton intersections

	A1	A2	A3
B1	$\{S\}$	0	$\{S\}$
B2	0	$\{F\}$	$\{F\}$
B3	$\{S\}$	$\{F\}$	$\{S, F\}$

Table 3. Support results for the combined singletons;

$\{S\}$			$\{F\}$			$\{S, F\}$		
R1	A1∩B1	0.560	R4	A2∩B2	0.030	R7	A3∩B3	0.005
R2	A1∩B3	0.035	R5	A2∩B3	0.010			
R3	A3∩B1	0.080	R6	A3∩B2	0.015			
Σ		0.675	Σ		0.055	ΣΣ	=	0.735
$m\{S\}$ = 0.675/0.735 = 0.918			$m\{F\}$ = 0.055/0.735 = 0.075			$m\{S, F\}$ = 0.005/0.735 = 0.007		

The belief and plausibility of the resulting focal elements is: $bel(\{S\}) = 0.675$; $pl(\{S\}) = 0.925$; $bel(\{F\}) = 0.075$; $pl(\{F\}) = 0.082$; $bel(\{S, F\}) = 0.005$; $pl(\{S, F\}) = 1$. This procedure can be applied also if one expert provides interval values instead of point values.

From the above reasoning for a binary system, use can be made to solve more complex situations with multiple modes of failure, such as ternary (Rakowsky [13]) and quaternary systems (Khakzad [17]).

Example 4: different ways to interview experts
DST can also be applied in a slightly different sense. Curcurù et al. [20] describe two examples, both used with respect to failure rates in a fault tree:

- Example 4.1: an analyst sets a basic assignment value for an upper and a lower bound of trustworthiness, whereas experts produce an interval of failure probability values that to their opinion corresponds to the basic assignment bounds.
- Example 4.2 is the other way around: if there are historical data available, the analyst proposes an upper and lower bound value and (two) experts may judge trustworthiness by providing a basic assignment value for applying the data in an actual, concrete case.

Because both cases will be developed similarly, we shall consider example 2 more closely, and select for that the fault tree of two basic components A and B in parallel, connected by an AND gate. In Table 4 the input data of basic assignment values m and corresponding failure probability values for the two components and the two experts are presented. For the failure probabilities Curcurù et al. [20] did not define a time span, which could, *e.g.*, be one year.

In Table 5 the basic assignments of the two experts are aggregated; in Table 6 the AND intersection is realized by solving the interval multiplication. The results of Table 6 are plotted in Figure 3.

Table 4. Input data according to the example given by Curcurù et al. [20], arranged differently.

	Expert 1					Expert 2			
	Lower bound		Upper bound			Lower bound		Upper bound	
m	0.9	0.1	0.9	0.1	*m*	0.7	0.3	0.7	0.3
Comp. A	2E-03	0	4E-03	1	Comp. A	2E-03	0	4E-03	1
m	0.9	0.1	0.9	0.1	*m*	0.6	0.4	0.6	0.4
Comp. B	3E-03	0	5E-03	1	Comp. B	3E-03	0	5E-03	1

0 = component will never fail
1 = it will always fail

Table 5. Application of the combination rule on the m-values: $(1 - (1 - m_1)(1 - m_2))$.

	Expert 1 + 2			
	Lower bound		Upper bound	
m	0.97	0.03	0.97	0.03
Comp. A	2E-03	0	4E-03	1
m	0.96	0.04	0.96	0.04
Comp. B	3E-03	0	5E-03	1

Table 6. AND intersection resulting in probability of failure of the top event

AND gate => Comp. A × Comp. B = interval multiplication:
$[x_1, x_2] \cdot [y_1, y_2] = [\min(x_1y_1, x_1y_2, x_2y_1, x_2y_2), \max(x_1y_1, x_1y_2, x_2y_1, x_2y_2)]$

	Lower bound		Upper bound	
m	0.931	0.001	0.931	0.001
x_1y_1, x_2y_2	6E-06	0	2E-05	1
m	0.039	0.029	0.039	0.029
x_1y_2, x_2y_1	0	0	4E-03	5E-03

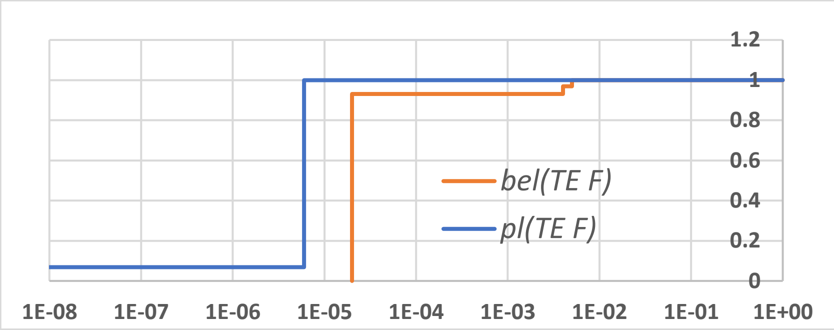


Figure 3. Belief (lower bound) and plausibility (upper) as by Curcurù et al. [20], applying bel and pl definitions (here only plausibility values had to be summed, from the smallest up).

In case of OR-gate failure Component A and B probabilities must be added and their co-occurrence subtracted from the sum. Example 4.1 can be evaluated similarly as example 4.2.

3. Fuzzy sets and logic, type 1 and type 2

Type-1 fuzzy sets

Zadeh's 1965 fuzzy sets and logic [6] for dealing with uncertainty have become quite known, while mid-1990s Klir and Yuan [21] showed their applicability. In the late 1990s and in this century Mendel [22] broadened and deepened the concept. Application is relatively straightforward and wide-spread, and it is used in risk assessment to estimate values or to express even linguistic grades of consequence severity or event frequency. Oldest is what in hindsight is called Type-1 fuzzy set, which originated in classifying types where it is not always possible to sharply describe characteristics or criteria. To use the words of Zadeh: due to imprecision the class will have a "continuum of grades of membership". In other words, the class or fuzzy set A is characterized by a membership function associating each point of A on the real line (X) on which the set extends from the extremes x_a to x_b, with a membership value (μ) in the interval [0, 1]. At x_0, $\mu = 1$, while at x_a and x_b, $\mu = 0$. The membership function can have any shape, but this is often assumed to be a triangle, trapezoid, or Gaussian, see Figure 4. Hence, $A = \{(x, \mu_A(x) | x \in X\}$ or in words: A is a function of x and μ, given variable x is part of the universe of discourse X, or $A = \int_{x \in X} \mu_A(x)/x$, where the quotient symbol or slash means group associating all elements in X with $\mu_A(x) > 0$, and the integral $\int$ can be replaced by a summation Σ in case values are discrete. A horizontal cross-section is called an α-cut, as shown in Figure 4, and is defined as a crisp set (not a fuzzy set) of all membership grades larger than alpha: $A_\alpha = \{x | \mu_A(x) \geq \alpha\}$.

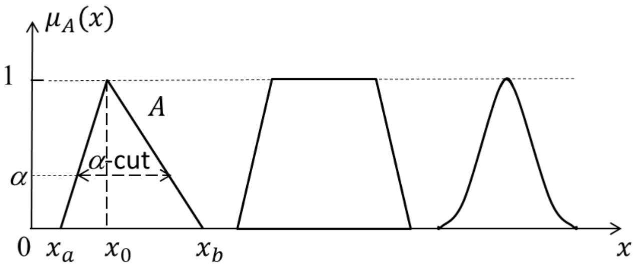


Figure 4. Fuzzy set shapes

It turned out that the approach could be applied to a large variety of problems in which a value, a type of object, a characteristic, or property could not be sharply defined but yet could be expressed as a fuzzy set, called fuzzy number, and processed mathematically. For example, in case of consequence severity and event frequency yielding risk or when the result of failing basic components in a parallel or series configurations must be determined, arithmetic operations on the fuzzy numbers shall be performed. Taking again the fault tree as in the previous section on DST, and calculating the failure probability of the system of two parallel basic components (AND-gate) the fuzzy numbers of experts 1 and 2 (Table 7) must first be averaged (Table 8) and then multiplied (Table 9). In principle, the latter means multiplying the membership values at all α-cut levels, which boils down to multiplying the values of x_a, x_0, and x_b of the respective input fuzzy sets, if these have similar, e.g., triangular shape. Results are depicted in Figures 5a and b. In case of an OR-gate both fuzzy numbers must be added and their product subtracted.

Table 7. Input values of two experts of estimated failure probabilities of components A and B

	Expert 1			Expert 2		
	x_a	x_0	x_b	x_a	x_0	x_b
Comp. A	2E-03	3.00E-03	5E-03	1E-03	3.00E-03	4E-03
Comp. B	3E-03	3.50E-03	4E-03	2E-03	4.00E-03	5E-03

Table 8. Averaged input of failure probabilities

	x_a	x_0	x_b
Comp. A	1.50E-03	3.00E-03	4.50E-03
Comp. B	2.50E-03	3.75E-03	4.50E-03

Table 9. Resulting fuzzy number failure probability top-event in AND-gate configuration of components A and B

x_a	x_0	x_b
3.75E-06	1.13E-05	2.03E-05

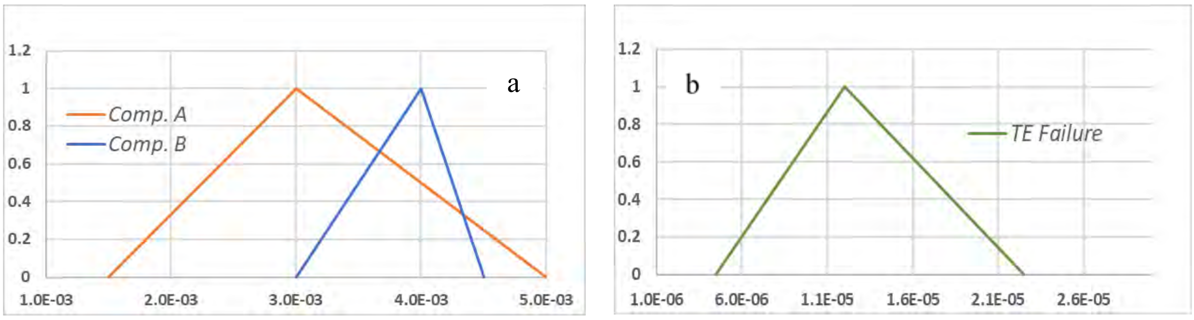


Figure 5a and b. *Left,* the averaged fuzzy sets of the two components A and B, and *right,* the resulting top event fuzzy number in case of AND-gate configuration of the two.

If in contrast inference is required of one or more fuzzy sets on the same or on different universes, rule-based logic must be applied to derive the resulting shape of the inferred fuzzy system or function, *e.g.*, in its simplest form:

IF $x = A$ THEN $z = C$; or more extended: IF $x = A$ AND $y = B$ THEN $z = D$,

where the first is a single-antecedent−single-consequent rule, and the more common second is a two-antecedent−single-consequent rule. The AND connection can also be OR or NOT. Antecedents and consequent can be numeric or also frequently linguistic. If antecedent or their combination is numeric, a numeric consequent can be implied if the result cannot be determined arithmetically. Obviously, the arguments have a conditional relation. If the consequent will be a fuzzy set, the inference procedure has been developed by Mamdani [23], and if it is a function of x and y, or a constant, Sugeno, or more precisely Takagi, Sugeno and Kang [24, 25] inference shall be applied. The Sugeno inference operation increased the applicability of fuzzy sets greatly, *e.g.*, by enabling improved control systems (robots).

Given two AND related antecedent fuzzy sets at the same universe, their intersection/conjunction produces the minimum area they have in common; if their relation is an OR union/disjunction yields the area they have not in common, hence the complement. It shows the min and max principle. Of practical use, *e.g.*, in control, is the case of antecedents not necessarily at the same universe. If a value of both antecedents must be combined to infer a consequent value being a fuzzy set (Mamdani), the smallest antecedent membership grade is implemented as the membership grade of the given consequent (so called t-norm operator) producing the firing level of the rule. The result is the remains of the consequent set below the α-cut at the firing level and the sought value is the centroid of the remaining part, obtained by defuzzification. By defuzzification of the resulting fuzzy set the arithmetic mean position of all the points, the centroid, or any other central measure is computed. In case two rules apply the result can consist of an amalgam of different consequents of which a centroid can be calculated (see Figure 6). Looping through the whole of antecedents in discrete steps is also possible and will construct a complete consequent. Often, inputs are provided in linguistic terms, such as high medium low or good medium bad, or a more extended range of terms. This kind of input but also numeric ones can lead to arrays of fuzzy sets to cover a range (see for an example Figure 7); the finer the higher the 'granulation'. In contrast, for Sugeno inference the consequent in the form of a function or constant is multiplied with the firing level and no defuzzification is needed. In case of an OR-relation the maximum (t-conorm) shall be obtained, so the largest membership grade is selected.

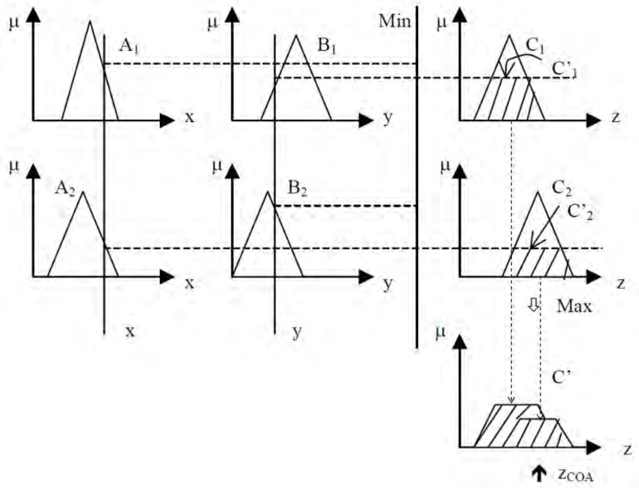


Figure 6. Two rule, two antecedent−single consequent in AND configuration with Mamdani inference as, *e.g.*, occurs in a control situation. Indicated x and y set values 'translate' into z_{coa}, the centroid of area, slightly modified after Castillo and Melin [29].

The above description is a bare minimum in which mathematical equations have been avoided. Wierman [26] or Mendel [22] present details and derive the many equations, which for extended cases tend to become rather complicated. Mendel [22] also suggests software that can be used within Matlab®, which itself has an app for rule-based logic of Type-1 fuzzy sets.

Applications in risk assessment are several, *e.g.*, Markowski et al. [27, 28]. The membership function of values of various types of variables to be used in the assessment, such as consequence severity or event frequency including human factor influences; the latter in many situations must be estimated by experts as proper and sufficient observations are lacking.

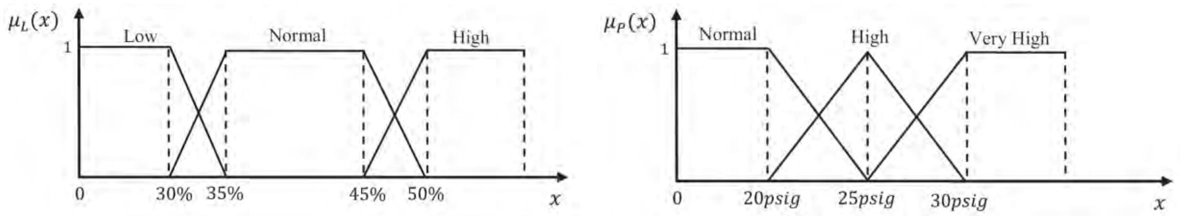


Figure 7a and b. Two example membership function arrays of reactor liquid level (*left*) and reactor pressure (*right*), both based on interviewing operators in order to obtain early warning of a possible run-away through an automated system applying Bayesian network, after Naderpour et al. [30]. Note the shoulder fuzzy sets at both ends.

A limitation of Type-1 fuzzy set is that different responses of the experts must be averaged. The authority of or confidence in experts can be expressed by weight factors, but expert weighting is often not done. Due to all this, uncertainty in inputs will be smaller than when responses are included in full, and uncertainty in the output will be lost when after defuzzification only the crisp value is retained. In part, these limitations can be avoided with Type-2 fuzzy sets.

Type-2 fuzzy sets

After his 1965 announcement of the development of fuzzy sets, Zadeh [7] also proposed in 1975 the concept of Type-2 fuzzy sets. The essence of the concept is that the membership function itself is fuzzy. This opens the possibility of improvement, because the uncertainty in various inputs can be retained and are not in part reduced by averaging. Development of practical implementation of the idea took a long time, see Mendel [22] and his many IEEE articles. Therefore, during the last decade Type-2 fuzzy set quickly became popular as a tool to support multi-criteria decision making. Operations with Type-2 fuzzy sets are not simple. In fact, each input of a Type-1 fuzzy set contains in 2-dimensional form the uncertainty an estimating expert perceives about the subject. In Type-2 fuzzy set an additional uncertainty is added, so the aggregated uncertainty becomes 3-dimensional in representation and evaluation becomes rather intricate. As an in-between concept Interval Type-2 fuzzy set (IT2 FS) has been developed, which allows uncertainty to be modeled 2-D again, because over intervals there is no preference for any value, hence an interval will be covered by a uniform distribution. To represent this uncertainty mean and standard deviation of the uniform distribution are equated to those of a T1 FS triangle. Below it will be explained in more detail how that works. Fortunately, the IT2 FS requirement of estimates to be formulated as intervals $[a, b]$, provides in fact the most convenient way experts can make estimates. In Figure 8a and 8b is shown how individual responses as T1 FSs are wrapped in an IT2 FS upper and lower 'membership function'.

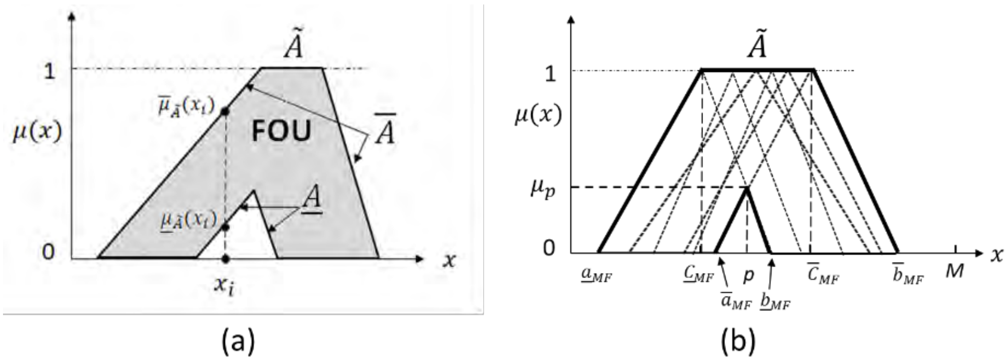


Figure 8a and b. IT2 FS $\tilde{A}$ in case of primary triangular T1 FSs; (a) showing the footprint of uncertainty (FOU) area and maximum and minimum envelope borders $\bar{A}$ and $\underline{A}$; (b) showing a few embedded T1 FSs and all parameter symbols involved; M means here the maximum bound on the value of x (after Liu and Mendel, 2008).

The way this concept can be used in risk assessments will be shown by some examples.

Example 1. Estimating failure rate values.
Although an estimate can be made directly in numerical values, it is often given in linguistic grades, such as '*very high, high, medium, low, very low*' or even wider. Anyhow, in such case the expert must indicate as well on a continuous, usually logarithmic numerical scale (Figure 9) what is meant by these terms.

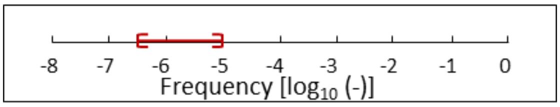


Figure 9. Example of a logarithmic scale of probability values per year (frequency) of an interval [-6.5, -5] or rather [0.32E-06, 1E-05] per year according to the expert equivalent to '*very low*'.

For creating interval fuzzy set the expert generated intervals $[a, b]$ must be converted first into symmetric triangular fuzzy sets. The principle is to equate the mean, $m_{MF} = (a_{MF} + b_{MF})/2$, and standard deviation, $\sigma_{MF} = (b_{MF} - a_{MF})/2\sqrt{6}$, of a T1 FS to the mean, $(a+b)/2$, and standard deviation, $(b-a)/2\sqrt{3}$, of the uniform distribution over the interval (Liu and Mendel [31]). This yields: $a_{MF} = ½(a+b) - (b-a)/\sqrt{2}$ and $b_{MF} = ½(a+b) + (b-a)/\sqrt{2}$. In case of left and right shoulder fuzzy sets, slightly different equations apply.

Table 10 Responses on a pressure relief valve of three experts and the transformed values

Per 10^7 hours		Expert 1		Expert 2		Expert 3	
a, min	**b, max**	**2.0**	**7.0**	**5.0**	**10.0**	**3.0**	**8.0**
a_{MF}	b_{MF}	1.0	8.0	4.0	11.0	2.0	9.0
m_{MF}	s_{MF}	4.5	1.4	7.5	1.4	2.0	9.0
[a, b] in fits		200	700	500	1000	300	800

Suppose we interview three experts about the failure rate of a particular pressure relief valve. Their responses of failure per 10^7 hours (in fits $\times$100) are summarized in Table 10 together with the transformation and aggregation to obtain the FOU. For the aggregation, the maximum and minimum a_{MF} and b_{MF}-values of the three experts are selected. Referring to Figure 8b for the symbols, the C_{MF}-values are obtained as $\underline{C}_{MF} = (\underline{a}_{MF} + \underline{b}_{MF})/2$ and $\overline{C}_{MF} = (\overline{a}_{MF} + \overline{b}_{MF})/2$, while p and μ_p follow from: $p = \frac{\underline{b}_{MF}(\bar{C}_{MF} - \bar{a}_{MF}) + \bar{a}_{MF}(\underline{b}_{MF} - \underline{C}_{MF})}{(\bar{C}_{MF} - \bar{a}_{MF}) + (\underline{b}_{MF} - \underline{C}_{MF})}$ and $\mu_p = \frac{\underline{b}_{MF} - p}{\underline{b}_{MF} - \underline{C}_{MF}}$. This way the full uncertainty implied by the responses is embodied in the FOU. It means that the broader the base of the IT 2FS and the smaller the lower FOU envelope the larger the uncertainty.

Applying the procedure to construct the IT2 FS yields Figure 10. The centroid bounds have been computed according to the Karnik-Mendel method (Mendel [22]) and are c_l = 3.6 and c_r = 8.2 with a mean C of 5.88.

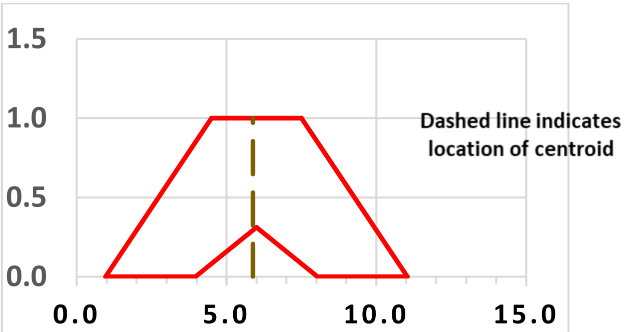


Figure 10. IT2 FS constructed based on the responses of three experts.

Just for comparison, if by means of a Bayesian network the three uniform distributions of the data are convoluted a mean of 5.83 is found with a standard deviation σ of 0.823 (hence 6σ, which covers 99.7% of a normal distribution, would have as bounds 3.4 and 8.3)

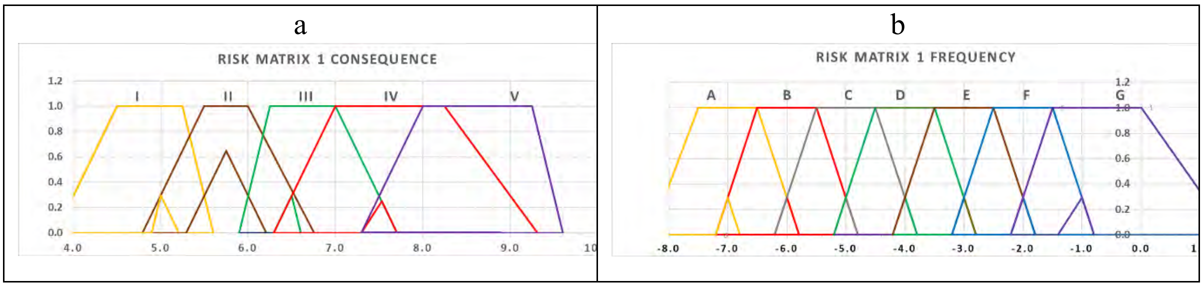
Tables 11a and b. Mock-up response values of three experts

$\log_{10}$ scale **Consequence [$]**	Expert 1 a, min	Interval b, max	Expert 2 a, min	Interval b, max	Expert 3 a, min	Interval b, max
Negligible (I)	5.00	5.50	4.00	5.00	4.50	5.20
Low (II)	5.50	6.50	5.00	6.00	5.25	6.50
Moderate (III)	6.50	7.50	6.00	6.50	6.50	7.50
High (IV)	7.50	9.00	6.50	7.50	7.50	8.50
Catastrophic (V)	9.00	9.50	7.50	8.50	8.50	9.20

log_{10} scale Frequency [/yr]	Expert 1 a, min	Interval b, max	Expert 2 a, min	Interval b, max	Expert 3 a, min	Interval b, max
Remote (A)	-8.00	-6.50	-8.00	-7.00	-7.00	-6.00
Unlikely (B)	-6.50	-5.50	-7.00	-6.00	-6.00	-5.00
Very Low (C)	-5.50	-4.50	-6.00	-5.00	-5.00	-4.00
Low (D)	-4.50	-3.50	-5.00	-4.00	-4.00	-3.00
Medium (E)	-3.50	-2.50	-4.00	-3.00	-3.00	-2.00
High (F)	-2.50	-1.50	-3.00	-2.00	-2.00	-1.00
Very High (G)	-1.50	1.00	-2.00	-1.00	-1.00	1.00

Example 2. Converting a linguistic risk matrix into a quantitative one

Interval Type-2 fuzzy set (IT2 FS) can also be used to convert linguistically graded consequence severity or event occurrence frequency into numerical risk. To that end experts must be asked to give estimates of linguistic terms as intervals on a continuous scale, which due to the wide range covered will be logarithmic. Another more complex case is the conversion of a linguistic risk matrix with given acceptance criteria (acceptable, tolerable acceptable, tolerable not acceptable, not acceptable) into a quantitative one[4]. The procedure creates an array of severity and frequency IT2 FSs, which form the antecedents for a Sugeno inference mentioned earlier. We shall not go into details. For the inference special software has been developed. The inputs are collected in Tables 11a and b, the arrays of IT2 FSs are presented in Figures 11a and b, the original and converted three-dimensional matrix of this example is shown in Figures 12a and b and a projection of the 3-D on the ground plane in Table 12.

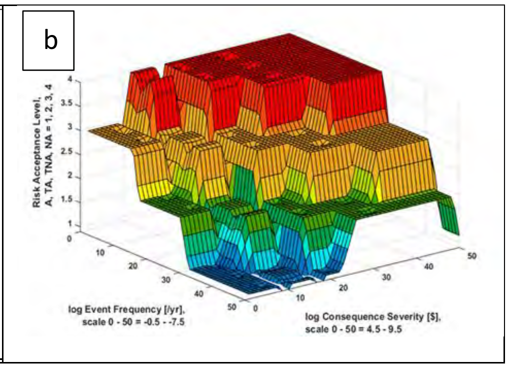


Figures 11a and b. IT2 FSs of consequence severity and event frequency of the three experts.

a

		Consequence				
		I	II	III	IV	V
Frequency		Negligible	Low	Moderate	High	Catastrophic
G	Very high	TNA	NA	NA	NA	NA
F	High	TNA	TNA	NA	NA	NA
E	Medium	TA	TNA	TNA	NA	NA
D	Low	TA	TA	TNA	TNA	NA
C	Very low	A	TA	TA	TNA	TNA
B	Unlikely	A	A	TA	TA	TNA
A	Remote	A	A	A	TA	TA

NA: Not Acceptable; TNA: Tolerable Not Acceptable; TA: Tolerable Acceptable; A: Acceptable



Figures 12a and b. The original linguistic matrix and the converted three-dimensional one.

Table 12. Projection of the converted 3-D matrix on the X-Y plane

log_{10} Consequence [$]	4.50	5.00	5.50	6.00	6.50	7.00	7.50	8.00	8.50	9.00	9.50

[4] This example has been part of a paper submitted to Process Safety and Environmental Protection journal.

$\log_{10}$ Frequency [/yr]					Risk Acceptance Level:		1 = A; 2 = TA; 3 = TNA; 4 = NA				
-7.50	1.00	1.00	0.95	0.86	1.15	2.00	2.00	2.00	2.00	2.00	3.00
-6.80	1.00	1.00	1.00	1.72	2.00	2.00	2.00	3.00	3.00	3.00	3.00
-6.10	1.00	1.00	1.29	1.72	2.00	2.00	2.00	3.00	3.00	3.00	3.00
-5.40	1.00	1.15	1.74	1.72	2.00	3.00	2.99	3.00	3.00	3.00	3.00
-4.70	2.00	2.00	2.00	2.58	3.00	3.00	3.00	4.00	4.00	4.00	2.75
-4.00	2.00	2.00	2.36	2.58	3.00	3.15	3.15	4.00	4.00	4.00	2.45
-3.30	2.00	2.00	2.62	2.58	3.00	4.00	3.99	4.00	4.00	4.00	2.15
-2.60	3.00	3.00	3.00	3.43	4.00	4.00	4.00	4.00	4.00	4.00	2.00
-1.90	3.00	3.00	3.72	3.43	4.00	4.00	4.00	4.00	4.00	4.00	2.00
-1.20	3.00	3.00	3.81	3.43	4.00	4.00	4.00	4.00	4.00	4.00	2.00
-0.50	0.00	0.00	0.00	1.00	1.00	0.96	1.53	1.77	1.73	1.75	1.99

Because the experts provided intervals also at the ends of the ranges, judging the range beyond as unrealistic, there are no shoulder sets. Therefore, the risk acceptance level figures decrease at the edges.

4. Probabilistic approach of expert estimation

Expert elicitation applying a probabilistic approach has a long history. It had already started in the 1970s with trying to solve problems in nuclear risk assessment (Rasmussen [32]). Perhaps the latest is applying it in the field of climate change (Oppenheimer et al. [33]) claiming that *structured expert judgement* is applied "in order to facilitate characterization of uncertainty in a reproducible, consistent and transparent fashion." That is "experts quantify their uncertainty on potentially observable variables of interest", "and on calibration variables from their field whose true values are known post hoc" (seed variables). Hence, the elicitation is on numeric values. The example given is on atmospheric dispersion modeling. One of the co-authors of [33] is Cooke, [3], who is an expert in probabilistic approach to expert elicitation. Cooke calls his method the "classical model", because it is based on calibration measurement and classical statistical testing [34]. The principle is that the experts provide numerical answers at 50% and 5% probability. Oppenheimer et al. [33] summarize characteristics of expert elicitation as follows:

"(i) experts' statistical accuracy and informativeness (the ability to concentrate high probability in small regions) is very uneven, ranging from informative and statistically accurate to very overconfident;

(ii) both equal-weight and performance-based combinations of individual experts' distributions generally result in improved statistical accuracy, and for equal weighting this improved accuracy is often purchased at the expense of very wide confidence bands;

(iii) statistical accuracy and informativeness are often antagonistic - the most informative experts are also the least accurate - although many expert panels contain accurate and informative individuals; and

(iv) performance weighting yields better performance, both in- and out of- sample, than weighting schemes not based on performance."

The procedure described by Cooke and Goossens [35], here summarized and maybe oversimplified, is that experts are asked to provide estimates of ≤5%, >5% and ≤50%, >50% and ≤95%, and >95%, forming 4 inter-quantile intervals (or bins) as an impression of the perceived width of the distribution of answers. If desired, elicitation can be refined by asking more quantile fractions. Each expert will answer N questions. He/she will also be considered as a statistical hypothesis, so that the N realizations will produce for each expert a sample distribution $s(e)$, or rather for each interval, $s_i(e)$. If there is a distribution where $s_i(e)$ can occur with probability p_i, the amount of conditional information[5] received is $NI(s_i(e)|p_i) = -Ns_i(e)\ln(s_i(e)/p_i)$, or the total amount is $NI(s(e)|p) = -N\sum_{i=1}^{4} s_i(e)\ln(s_i(e)/p_i)$.

With large N, $2NI(s(e)|p)$ becomes chi square (χ^2) distributed with 3 degrees of freedom. This can be seen when expanding the natural logarithm in the relation in a Taylor series and focusing on the dominant terms. The operation results in the χ^2-statistic, based on the summed squared differences of predicted and observed values, for goodness of fit of s to p holding for a 'well-calibrated' expert. If the statistic is low, the probability that the fit is good, is high. This probability provides an expert's *calibration score*. When the expert is asked to produce quantiles instead of numbers in a bin, a transformation of the answer is needed to allow for the non-equal masses, but the method remains basically the same.

Besides a calibration score of each expert, an *information score* is determined. Information scores measure the width of the distribution the expert presents. An expert's information score is the average relative information with respect to the background [34], *e.g.*, a uniform distribution of which a relevant so-called intrinsic range is considered. This range is taken such that it spans all quantile answers plus an overshoot. It is selected by the analyst, because it holds for all experts. Information score of expert e is: $(1/N)\sum_1^N I(f_{e,i}|g_i)$, in which N is as before, $f_{e,i}$ is the density of expert e for item i, and g_i is the background density for item i, all under the assumption that variables are independent. Information scores increase when the quantiles become narrower, as an expert can be supposed to be surer of his/her answer. However, if quantiles come very close it may indicate overconfidence.

The 'decision maker' (DM) combines the calibration and the information scores in linear pooling. To do this the best way causes again a number of intricacies, because experts can try to manipulate their quantile distances. The challenge is to find a set of weights, each weight being an expert's product of calibration and information score, such that the linear pool under these weights maximizes the product of calibration and information scores and optimizes performance. The best expert gets weight of 1. The choice is between a *global* weight decision maker (scores global over all seed variables) (GWDM) and an *item* weight (IWDM) discriminating per seed variable, which both should be better than the *equal* weight one (EWDM), which consists of simple averaging. GWDM is proportional to the product of the calibration and the information scores, given that the calibration exceeds a "significance level" cut-off α, below which the expert weight is set to zero. The significance cut-off α is determined by where it maximizes the product scores. In other words, good answers are rewarded and bad ones are eliminated. IWDM does the same but per questioning the item/seed variable. The performance optimized combination DMs often turned out to be better than EWDM [34].

The data base in [34] contains 45 panel runs on different topics and reports the DM performances. The results are obtained using the software EXCALIBUR (which appears not to

[5] This is according to the Shannon entropy theory. Information content I on randomness of random variable x_j representing an observable event j occurring with probability p_j is: $I(p_j) = -\log_b(p_j)$, or if b is taken as the mathematical constant e, base of the natural logarithm, $-\ln(p_j) = \ln(1/p_j)$. If base is e, information quantity is measured in the unit nats (but when $b = 2$ in bits). Derivation is by considering if two independent events occur, the information on the joint probability: $I(p_1p_2) = I(p_1) + I(p_2)$, hence in general, $I(p^a) = aI(p)$ analogous to $\log(p^a) = a\log(p)$. In N repeats, event j will on average occur Np_j times, so total $NI(p_j) = -\sum_1^n Np_j\ln(p_j)$. In case of conditional $I(s|p)$ to be understood as amount of randomness in s given p, so that $I(s|p) = -s\ln(s/p)$. If $s = p$, then $I = 0$, in other words the sample is exactly the value of the true distribution.

be downloadable anymore). Each study takes quite an effort (1 – 3 months). Further cases are described in [35]. Hanea [36] gives a detailed account of applying the method to the problem of escape time from a burning building applying Bayesian network to relate parameters and interviewing four experts each from a different domain: fire prevention, fire development, fire safety of buildings, and people behavior in evacuation. For calibration, 7 questions were asked on fire statistics and 10 on parameter values of interest, such as alarming system reliability, people flow through exits, waiting time, number of exits and distance to exits in public buildings. EWDM appeared to be slightly lower and less informative than the other two DMs. Hanea reports details, achievements, but also encountered problems of various nature. Bolger and Rowe [37] criticize the unequal weighting of the classical model for several reasons, *e.g.*, because of the influence on experts from a psychological behavior point of view and the usual limited set of seed variables, and they would prefer equal weighting. On the other hand, if bias by group think, polarization, failure to share information, dominance, and dogmatism can be reduced by experienced leadership, group discussions (behavioral aggregation) can also help to resolve the problem. This evoked commentary by Cooke [37] and a response by Bolger and Rowe [37], which altogether sharpens the contours of the problem area of applying expert elicitation.

The mentioned climate change study [33, 33A] focuses on Gaussian dispersion modeling and on the uncertainty induced by crosswind dispersion. Eleven experts have been interviewed on 36 calibration variables; the EWDM appeared in this case to be slightly higher than the performance-based ones, though. The combined uncertainty by the experts turned out to deviate significantly from those implied by 5 different choices of crosswind dispersion model parameters, and it therefore gained credibility. The result was used for probabilistic inversion to improve the model.

5. Similarities and differences in methods

The probabilistic approach again shows that when less uncertainty is desired, efforts to delimit uncertainty increase strongly. One does not get more value cheap! In the probabilistic approach with the attempts to 'calibrate' experts, the afore mentioned expert elicitation complexities appear quite pronounced. However, intrinsically in the Dempster-Shafer and fuzzy set approaches of expert judgment, the above observed problems of expert weighting will be present as well. In DST it is the analyst who by assigning mass gives experts a weight, but that weight also is subjective, while in fuzzy set expert weighting is hardly used. It all increases the uncertainty of the results produced by the methods .

It is not easy to make a choice between Dempster-Shafer method and fuzzy set, although for simpler questions regarding reliability and other observable data the more rigid mathematical treatment of information in the Dempster-Shafer approach makes it attractive and preferential over fuzzy set. In case of bowtie causal structure, thanks to the rigor, DST failure data can be propagated in an *Evidential network*, similar to a Bayesian network. For that, the epistemic uncertainty term is treated as an additional mode. Of course, fuzzy set Type-2 is a substantial improvement over Type-1, so it is worth the additional effort, but it remains approximative. Ferdous et al. in [39] and earlier papers compared for bowtie analysis the lack of failure data by having experts cast their subjective linguistic estimates in a Type-1 fuzzy set and in addition in a DST format showing inconsistency among experts and their fractions of ignorance.

Apart from the methods described, there are other less known ones. Much like DST, Credal sets and *Credal networks* try to accommodate imprecise and incomplete probability, see Cozman [40], or more recently Piatti et al. [41]. A credal set concerns a closed convex set[6] of probability measures that must sum to 1, but which can vary within that constraint. In a finitely generated credal set a number of probability value combination sets (each set summing to 1) exist that can be represented graphically by a polytope reflecting the sets of values by its vertices. Credal sets are often applied to binary variables because it can define upper and lower probability set functions, $\overline{P}(A)$ and $\underline{P}(A)$. It can be modeled by networks that are similar to Bayesian networks and Evidential ones but due to the constraint differ on a few fundamental aspects. In a given credal network, there are several credal sets called extensions that meet the constraints set by the network. Inference is possible. Only to a strong extension being still a joint credal set, which forms a joint density distribution over the variables X_i given parents pa as in a Bayesian network, $P(X) = \sum_i P(X_i|pa(X_i))$, allowing directional separation (so called d-separation), the Bayesian network mathematical infrastructure can be applied. Natural extension is the largest set complying with the network and must be solved in a different way (for which also software is available [42]).

In the fuzzy set Type-2 examples the expert was always asked to indicate on a continuous quantitative scale an interval what he/she thought the grading term covered, enabling the fusing with others. Herrera and Martinez [38] developed a method where the linguistic term can be retained and in which by adding a value between -0.5 and +0.5 in a fusing process loss or gain can be accounted for. It offers a solution in highly complex situations of interdependence, cascading, and indirect causation in which even an indication on a quantitative scale is not possible. The extent to which the grading term holds, appears from the value added.

Zadeh [43] is also pioneer of possibility theory. A quotation from [43] is: "A thesis advanced in this paper is that the imprecision that is intrinsic in natural languages is, in the main, possibilistic rather than probabilistic in nature"; and later "when our main concern is with the meaning of information-rather than with its measure-the proper framework for information analysis is possibilistic rather than probabilistic in nature". If something is possible it does not need to be probable. Possibility theory forms an interface with probability theory, DST, and fuzzy set. It all has been formulated mathematically (Zadeh [43] and Klir [8], [44]). A state of affairs and applications are presented by Dubois and Prade [45]. An application in risk assessment is to find bounds on probability predicted by possibilistic considerations. So far, the approach did not result in convincing applications offering more than we have seen earlier with DST and IT2 FS. The same is true for the 2011 Zadeh introduction of the Z-number [46]. This number consists of two elements, in which the first informs about the constraint of a real variable in terms of 'about', 'close-to', etc., and the second on the reliability of the first in terms of 'sure', 'likely' and such like. Thus, a typical expression is: 'the driving time of College Station to Houston downtown is about 2 hrs, usually'. Mathematically, the constraint can be expressed as a fuzzy number and the reliability as a probability value. One recent fault tree application has been published by Yadi et al. [47] in case of elicitationof experts unsure of exact failure rate values as an alternative to methods mentioned before in this paper.

---

[6] A convex set is a set of elements from a vector space such that all the points on the straight line between any two points of the set are also contained in the set: $x = \lambda a + (1-\lambda)b$ for all λ from 0 to 1 (Watkins Th., www.sjsu.edu/faculty/watkins/convex.htm).

All the methods described in this paper have found their way into Artificial Intelligence.

6. Conclusions

Methods are available to objectivize imprecise and subjective estimates of mostly binary variable values that in principle are observable, but because of long observation lead times or other reasons of inaccessibility, must be obtained by interviewing experts and eliciting their opinions.

Most forceful on the experts and at the same time using most of statistical background knowledge is the so-called structured expert judgment using the "classical model". However, the traditional method is effort intensive and therefore costly.

The Dempster-Shafer approach seems for the type of failure data or consequence model parameter value questions we encounter in risk assessment the best option, because epistemic uncertainty thereby obtains as a separate focal element its own more realistic place and can be included in bowtie and other analyses making use of Bayesian network.

In case values of consequences and rates are given in linguistic terms of natural language, fuzzy set is most suitable. When the effect of linguistic graded variables shall be combined through inference of fuzzy sets (type-1 or type-2), it is possible to derive a concluding linguistic graded result ("Computing with words or perceptions" [48]). The same is true if variables are expressed as index values. In contrast to type-1 fuzzy set where expert opinion differences, whether or not weighted, must be averaged, type-2 can retain the uncertainty introduced by the response differences. Processng is effort intensive, though. Additionally, when the variable can be expressed on a continuous numeric scale, such as for consequence severity or event frequency, experts can be asked to indicate an interval (interval type-2) facilitating processing. The result by inference or arithmetic operation will then be numerical

A few other, less often or maybe not yet often applied methods are mentioned, which in specific complex cases can increase considerably the quality of a solution to a problem.

References

1. OREDA, 2015. Offshore and Onshore Reliability Data, sixth ed., SINTEF NTNU. <https://www.oreda.com/>.
2. Saaty, Th.L. Fundamentals of Decision Making: the Analytic Hierarchy Process. RWS 3 Publications, Pittsburgh, PA, 2006.
3. Cooke, R.M., 1991. Experts in Uncertainty, Opinion and Subjective Probability in Science. Oxford University Press, New York - Oxford, ISBN 0-19-506465-8.
4. Dempster A.P., 1967. Upper and lower probabilities induced by a multivalued mapping. The Annals of Mathematical Statistics 38 (2), 325–339.
5. Shafer, G., 1976. A Mathematical Theory of Evidence. Princeton University Press.
6. Zadeh L.A., 1965. Fuzzy sets, Information and Control 8, 338–353.
7. Zadeh L.A., 1975. The concept of a linguistic variable and its application to approximate reasoning. Information Sciences 8, 199–249.
8. Klir G.J., 1989. Is there more to Uncertainty than some Probability Theorists may have us believe, Int'l Journal of General System 15, 347-378.
9. Zadeh L.A., 1978. Fuzzy sets as a basis for the theory of possibility. Fuzzy Sets Syst. 1, 3–28 (reprinted 1999, Fuzzy Sets and Systems, 100 Supplement, 9-34) (1978).

10. Helton J.C., Johnson J.D., 2011. Quantification of margins and uncertainties: Alternative representations of epistemic uncertainty, Reliability Engineering and System Safety 96, 1034-1052
11. Shafer G., 1990. Perspectives on the Theory and Practice of Belief Functions, International Journal of Approximate Reasoning (4) 323-362; and 1992. Rejoinders to Comments, same journal (6) 445-480.
12. Pearl J., 1990. Reasoning with Belief Functions: An Analysis of Compatibility, International Journal of Approximate Reasoning 4, 363-389.
13. Rakowsky U.K., 2007. Fundamentals of the Dempster-Shafer Theory and its Applications to Reliability Modeling, International Journal of Reliability, Quality and Safety Engineering, 14 (6) 579–601.
14. Yager R., 1987. On the Dempster-Shafer Framework and New Combination Rules, Information Sciences 41, 93-137.
15. Sentz K, and Ferson, S., 2002. Combination of Evidence in Dempster- Shafer Theory, SANDIA Report 2002-0835; http://prod.sandia.gov/techlib/access-control.cgi/2002/020835.pdf.
16. Simon C., Weber P., Evsukoff A., 2008 Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis, Reliability Engineering and System Safety 93, 950–96.
17. Khakzad N., 2019, System safety assessment under epistemic uncertainty: Using imprecise probabilities in Bayesian network, Safety Science 116, 149-160.
18. Simon C, Weber P., 2009. Evidential Networks for Reliability Analysis and Performance Evaluation of Systems With Imprecise Knowledge, IEEE Transactions on Reliability 58 (1), 69-87.
19. Ferson S., Kreinovich V., Ginzburg L., Myers D.S., and Sentz K., 2003. Constructing probability boxes and Dempster-Shafer structures, SAND2002-4015, Unlimited Release, www.osti.gov/servlets/purl/809606.
20. Curcurù G., Galante G.M., La Fata C.M., 2012. Epistemic uncertainty in fault tree analysis approached by the evidence theory. Journal of Loss Prevention in the Process Industries 25, 667–676.
21. Klir G.J., and Yuan B., 1995. Fuzzy sets and fuzzy logic: Theory and applications. Upper Saddle River: Prentice Hall.
22. Mendel J.M., 2017. Uncertain rule-based fuzzy logic systems: introduction and new directions. 2nd Edition, Springer, ISBN 978-3-319-51369-0.
23. Mamdani E.H., 1974. Applications of fuzzy algorithms for simple dynamic plant. Proceedings of the IEEE 12, 1585–1588.
24. Takagi T. and Sugeno M., 1985. Fuzzy identification of systems and its application to modeling and control. IEEE Transaction on Systems Man & Cybernetics 15, 116–132.
25. Sugeno M., and Kang G.T., 1988. Structure identification of fuzzy model. Fuzzy Sets and Systems 28 (1), 15–33.
26. Wierman M.J., 2010. An Introduction to the Mathematics of Uncertainty, University of Creighton, https://www.creighton.edu/fileadmin/user/CCAS/programs/fuzzy_math/docs/MOU.pdf.
27. Markowski,A.S., Mannan M.S., Bigoszewska A., 2009. Fuzzy logic for process safety analysis, Journal of Loss Prevention in the Process Industries 22, 695-702.
28. Markowski A.S., Mannan M.S., Kotynia (Bigoszewska) A., Siuta D., 2010. Uncertainty aspects in process safety analysis, Journal of Loss Prevention in the Process Industries 23, 446-454.
29. Castillo O., Melin P., 2008. Type-2 Fuzzy Logic: Theory and Applications, Studies in Fuzziness and Soft Computing, Volume 223, Springer, e-ISBN 978-3-540-76284-3, p.17.
30. Naderpour, M., Lu, J., Zhang, G., 2015. An abnormal situation modeling method to assist operators in safety-critical systems, Reliability Engineering and System Safety 133, 33–47.
31. Liu F., Mendel J.M., 2008. Encoding words into interval type-2 fuzzy sets using an interval approach. IEEE Transactions on Fuzzy Systems 16 (6), 1503-1521.
32. Rasmussen N. C. et al., 1975. Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants WASH-1400 (NUREG75/014), (US Nuclear Regulatory Commission).

33. Oppenheimer M., Little Ch.M. and Cooke R.M., 2016. Expert judgement and uncertainty quantification for climate change, Nature Climate Change, 6, 445-451
DOI: 10.1038/NCLIMATE2959.
Supplementary information can be downloaded at https://images.nature.com/original/nature-assets/nclimate/journal/v6/n5/extref/nclimate2959-s1.pdf
34. Cooke R.M., Goossens L.L.H.J., 2008. TU Delft expert judgment data base, Reliability Engineering and System Safety 93, 657–674.
35. Goossens L.H.J., Cooke R.M., Hale A.R., Rodić-Wiersma Lj., 2008. Fifteen years of expert judgement at TUDelft, Safety Science 46, 234-244.
36. Hanea D.M., 2009. Human Risk of Fire: Building a decision support tool using Bayesian networks, Dissertation TUDelft, Wöhrmann Print Service ISBN: 978-90-5638-227-8.
37. Bolger F. and Rowe G., 2015. The Aggregation of Expert Judgment: Do Good Things
Come to Those Who Weight? Risk Analysis 35 (1), 5-11; with a Commentary by Cooke R.M., idem, 12-15; and a Response by Bolger F. and Rowe G, 2015. There is Data, and then there is Data: Only Experimental Evidence will Determine the Utility of Differential Weighting of Expert Judgment, Risk Analysis 35 (1), 21-26.
38. Herrera F. and Martinez L., 2000. A 2-Tuple Fuzzy Linguistic Representation Model for Computing with Words, IEEE Transactions on Fuzzy Systems 8 (6), 746-752.
39. Ferdous R., Khan F., Sadiq R., Amyotte P., Veitch B., 2013. Analyzing system safety and risks under uncertainty using a bow-tie diagram: an innovative approach. Process Safety and Environmental Protection 91, 1–18.
40. Cozman F.G., 2000. Credal networks, Artificial Intelligence 120, 199-233.
41. Piatti A., Antonucci A. and Zaffalon M., 2010. Building Knowledge-based Systems by Credal Networks: a Tutorial, in: Baswell, A.R. (Ed.), Advances in Mathematics Research, vol. 11. Nova Science Publishers, New York. http://people.idsia.ch/~zaffalon/papers/2010nova-cns.pdf.
42. Cozman F. G. JavaBayes – user manual, http://www.cs.cmu.edu/~javabayes/ .
43. Zadeh L.A., 1977. Fuzzy Sets as a Basis for a Theory of Possibility, reprint Fuzzy Sets and Systems 100 Supplement (1999) 9-34.
44. Klir G.J., 1999. On fuzzy-set interpretation of possibility theory, Fuzzy Sets and Systems 108, 263-273.
45. Dubois D., Prade H., 2011. Possibility Theory and its Applications: Where Do we Stand? Mathware & Soft Computing Magazine. 18 (1), 18-30.
46. Zadeh L.A., 2011. A Note on Z-numbers, Information Sciences 181, 2923–2932.
47. Yazdi M., Hafezi P., Abbassi R., A methodology for enhancing the reliability of expert system applications in probabilistic risk assessment, Journal of Loss Prevention in the Process Industries 58, 51–59.
48. Zadeh L.A., 2002, From computing with numbers to computing with words - from manipulation of measurements to manipulation of perceptions, International Journal of Applied Math and Computer Science, 12 (3) 307–324.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Lessons Learned – How to Make Them Stick

Jack Chosnek*
KnowledgeOne
P.O. Box 451629
Houston, TX 77245
*Presenter E-mail: jc@knowledge1.net

Abstract

After an incident investigation we gather the facts, assign causes and compile a set of lessons that should, if learned well, prevent a similar incident from occurring. If the company has a good process safety management system, a good effort will be made to share the lessons learned with its employees. Unfortunately, too often we see the same type of incident happening, sometimes in the same company that had the original incident, although not necessarily in the same facility, or in a company using the same process technology as the company that had the incident.
What happened? We don't learn by listening to a talk or reading a bulletin, at least not for the long term. Our memory fades with time. Even if not, we still need to relate the incident findings to the planning and execution of our work. Thus, the way to remember those lessons is by incorporating them in our technology and daily operations. When making a change to the equipment, and during the safety study of the change, we need to consider what features we need to add or change in order to address the incident findings. In addition, operating, maintenance, and emergency procedures need to incorporate the incident findings. This can be done during the yearly review of procedures, or if the incident is closely related to the company's operations, as soon as the findings are analyzed.
Of course, a knowledge repository for the company is also necessary as we need to understand as time goes by, the basis for the changes in the technology and procedures. This is important in order not to lose the knowledge gained from the incident and unwittingly reverse the implemented protections.
Other methods, such as reviewing and discussing the finding in safety meetings on each anniversary of the incident, will also be discussed in this talk.

Introduction

Incidents that happened before happen again, showing that we either are not paying attention to incidents or are not learning the lessons from those incidents. On October 1989, Phillips 66 experienced a major explosion during maintenance operations at its Pasadena, Texas, facility which killed 23 people and left more than a 100 injured. This explosion precipitated the enactment of OSHA's PSM Standard, 29 CFR 1010.119 [1]. Among the causes of the incident, OSHA cited faulty maintenance procedures. Ten years later, in 1999, an explosion rocked the same Pasadena facility resulting in two fatalities. Although in this case it wasn't a vapor cloud explosion but a release of molten material, it was again during maintenance operations. And a year later (2000) another explosion occurred in the same facility during maintenance operations, resulting in one fatality and 71 injured. Although the immediate causes for all these explosions were different, the common thread was maintenance operations. In another case, at Hoeganaes Corporation [2], there wasn't even a significant time span before incidents were repeated. In 2011 the company experienced three incidents in the same year: in January (two fatalities), in March (one serious injury) and in May (two fatalities). All three were related to a dust fire or explosion.

Why Are Lessons Not Learned?

Lessons are not learned, not because of not trying. The Global Congress on Process Safety (AIChE) which meets once a year and has an attendance of hundreds of engineers and process safety professionals, has a joint session of all its tracks dedicated to lessons learned. The Center for Chemical Process Safety (CCPS) has published books [3] and maintains a database of incidents for participating companies [4]. Articles continue to be published on lessons learned in process safety [5] and a monthly bulletin provides an account of an incident or near miss from which we can learn [6]. The US Chemical Safety Board publishes online reports of its investigations and offers videos that demonstrate how the incident happened [7].

Companies typically circulate to employees the results of their own incident investigations and the reports are usually available internally. Sharing with other companies is limited due mainly to liability issues. But the lessons from those incidents may get lost, maybe because they don't have immediate impact or because the causes of the incident are not well defined, or because they get forgotten when they should be applied, during process design or a process hazards analysis (PHA). And, although many companies collect information on near misses, they are used as lagging-indicator metrics [8] for gleaning what are the factors that are liable to result in an incident, and mostly not thoroughly analyzed to learn the lessons they could have provided.

In essence, in spite of the wealth of incident information, the task of distilling a lesson from an incident, communicating it, and having people remember it when it's needed, is a very difficult task. Typically, in the long term we retain about 10% of the information we receive during training. And training is much more than sharing information where retention may be less than 1%.

How to Make Lessons Learned Stick

In order to really learn a lesson, the lesson needs to be translated into everyday use. It needs to be woven into the fabric of the company. There are various ways of accomplishing this which will be discussed now.

1. **The Knowledge Repository**. Trevor Kletz, the world renown process safety expert, said that "Organizations don't have memory – only people do" and that is why incidents recur [9]. But, with today's tools it is possible to impart a memory to an organization [10], and part of that memory would be the lessons learned. One of these tools is a knowledge repository. The repository would be organized such that all aspects of the learnings from an incident would be available and be easily searchable [11]. Thus, our loss of memory of learnings from training or information sharing would be compensated by this repository. We would only need to have a vague idea about the incident and find all its details. This knowledge, though, needs to be incorporated into all the functions of a process plant.
2. **Expanding the Process Technology to Include Incidents.** The technology of the process being used would include any related incidents and the lessons learned from them. This searchable knowledge would go into the repository. For example, if the process used a hydrotreater, all relevant information on hydrotreaters would be added to the repository including any incidents, complete with the investigation reports. As part of the duties of the engineer supporting the process, he/she would follow incidents on hydrotreaters that occur in the world, within the company and externally. In addition, vendors would be asked to provide related incident data as part of the technical package. Some corporations have these technology experts that serve as a resource for the company, but it is not necessary to have a dedicated person to the technology since the information is readily available in the knowledge repository.
3. **Integrating Incident Learnings into a PHA**. Although we are required to review the incidents that have occurred between two consecutive PHAs, this review is for awareness that things can occur. It takes some expertise to connect these incidents to potential causes and consequences discussed during the PHA. An experienced facilitator that is familiar with incidents that have occurred in the industry should be chosen. And, since we are required to have "at least one employee who has experience and knowledge specific to the process being evaluated" [12], the process expert mentioned above should be part of the PHA team. If the expert doesn't have the time to participate throughout the length of the PHA, he/she should give a presentation to the team on the incidents related to the process being studied.
4. **Using a Hazards Register**. A Hazards Register is a database that contains all the pertinent information related to the risks assessed during all of the safety studies performed by the company, whether a Process Hazards Analysis, or a Management of Change review, or an incident investigation [13]. The resolution of each hazard would be available in the Register, and not only the latest resolution but also its evolution (history) starting from the original study. The lessons of all these studies are captured in the Hazards Register since it maintains the reasons and assumptions used in them. This solves the problem of the disconnect between recommendations from a safety study and their resolutions. At any time, we can learn why

we use a particular design or operate in a certain way. In order to be effective, the Hazards Register should be easily accessible by all and be fully and effortlessly searchable.

5. **Integrating Incident Learnings into SOPs**. We are required to include the consequences of deviation when the performing of an SOP. This is a good place to add to the consequence a mention of an incident that occurred when not following an instruction. For example, on bypassing an interlock, a note saying "A bypassed interlock using emergency air resulted in an explosion that destroyed the facility and killed five people" [14]. A video or report of the incident should be available in the control room, or at least used in refresher training.
6. **Remembering the Anniversary of an Incident**. If there was a significant incident in the company, the lessons learned from it should be remembered every year. The anniversary of the incident is the right time to do it. The company should send a bulletin to all employees on that day with a summary of the event [15].
7. **Reinforcing Lessons in Safety Meetings**. For safety meetings or "tool box" meetings one of the topics should be the review of an incident, not necessarily something that happened in the company, but of actions that led to an incident. The videos offered by the US Chemical Safety Board are an excellent resource for this type of meeting.

Conclusions

By using the methods described in this paper, lessons are learned through visualization, constant application and reinforcement. Since the lessons become part of the knowledge of the company, and the methods integrate the lessons into everyday activities of the company, these lessons will stick.

References

1. Phillips 66 Company Houston Chemical Complex Explosion and Fire, A Report to the President, U.S. Dept. of Labor, April 1990.
2. U.S. Chemical Safety and Hazard Investigation Board, "Hoeganaes Corporation: Metal Dust Flash Fires and Hydrogen Explosion", Report No. 2011-4-1-TN, Gallatin, TN (Dec. 2011).
3. Atherton, J., and Frederic, G., "Incidents that Define Process Safety", American Institute of Chemical Engineers, New York, NY, and Wiley, Hoboken, NJ (2008).
4. CCPS, PSID Process Safety Incident Database, www.psidnet.com, accessed August 2019.
5. Ness, A., "Lessons Learned from Recent Process Safety Incidents", *Chemical Engineering Progress*, p.23, March 2015.
6. CCPS, "Process Safety Beacon", published monthly in *Chemical Engineering Progress* (CEP) magazine, and by subscription in over 30 languages, https://www.aiche.org/ccps/resources/process-safety-beacon, accessed August 2019.
7. US Chemical Safety and Hazard Investigation Board, www.csb.gov, accessed August 2019.

8. CCPS, “Process Safety Metrics – Guide for Selecting Leading and Lagging Indicators”, April 2018, https://www.aiche.org/sites/default/files/docs/pages/ccps_process_safety_metrics_-_april_2018.pdf, accessed August 2019.
9. Kletz, T., “Lessons from Disaster: How Organizations Have No Memory and Accidents Recur”, Institution of Chemical Engineers, Warwickshire, U.K., pp. 1-3, September 1993.
10. J. Chosnek, “Maintaining the Corporate Memory”, *Journal of Loss Prevention in the Process Industries*, Vol. 23, Issue 6, November 2010, pp. 796–798.
11. J. Chosnek, "Organizing Knowledge for Improved Process Safety", Proceedings of the Mary Kay O'Connor Process Safety Center International Symposium, October 2008.
12. OSHA 20 CFR 1910.119, Section (e) Process Hazards Analysis, part (4), and Section (f) Operating Procedures, part (1)(ii)(A).
13. J. Chosnek, “Lifecycle Management of Risks with a Hazards Register”, proceedings of the 15th Global Congress on Process Safety, New Orleans, LA, April 2019. Also presented at the Mary Kay O'Connor Process Safety Center International Symposium, October 2018.
14. U.S. Chemical Safety and Hazard Investigation Board, “Investigation Report: Vinyl Chloride Monomer Explosion”, Report No. 2004-10-I-IL, Formosa Plastics Corp., Illiopolis, IL (March 2007).
15. J. Forest, Celanese Corp. Process Safety Director, personal communication, March 2018.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Analyzing Procedure Performance using Abstraction Hierarchy: Implications of Designing Procedures for High-risk Process Operations

Nilesh Ade[3], S. Camille Peres[1,2,3], Farzan Sasangohar[1,2], and Changwon Son[1,3]*
[1] Industrial and Systems Engineering Department, Texas A&M University
[2] Environmental and Occupational Health Department, Texas A&M University
[3] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University
*Presenter E-mail: cson@tamu.edu, peres@tamu.edu

Abstract

Standard operating procedures (SOPs) are a vital element of everyday operations in chemical process industries. Incident investigations also indicate that a majority of adverse events in the processing operations are ascribed to issues associated with SOPs. Although there have been continuous efforts to improve informational and perceptual aspects of SOPs, assessing them from a systems perspective remains a persistent gap. As one novel way to address such gap, this study employs an ecological approach to understand the functional structure of the work domain, that is, abstraction hierarchy (AH) and its relations to SOPs and operator performance. First, this study models a 3-phase separation system, a common gas-oil-water separation process, using an abstraction-decomposition space as a work domain of the system. Second, we assess the AH level, one dimension of the abstraction-decomposition space, of the SOPs developed for three tasks in the 3-phase separation system. In order to consider operators' knowledge about the tasks, experience-task familiarity (E-TF) level is also assessed as a combinatory factor. To this end, a two-way analysis of variance is conducted to find out the effect of E-TF level (high vs. low) and AH level of the SOPs (physical vs. functional) on the operator's performance. Results show significant main effects of the E-TF level and AH level on the successful performance of the SOPs. The interaction effect of the two variables is considered marginally significant. Based on the results, several implications for the design of SOPs in relation to the AH of the chemical processing domain are discussed.

Keywords: human factors, standard operating procedure, man-machine interface, system safety

1 Introduction

It is widely accepted that standard operating procedures (SOPs) play a crucial role in achieving the desired level of safety and productivity in chemical process industries. An SOP is defined as a documented step-by-step instruction that guides operators in carrying out a specific task either routinely or non-routinely required [1]. Primary purposes that SOPs serve include: providing consistent, up-to-date, and recommended operation practices; informing operators of hazards associated with a task and pertinent control measures; and thus conducting a task in a safe, efficient, and effective manner. In pursuit of these advantages, statutory safety and health regulations and guidelines such as the U.S. Occupational Safety and Health Administration (OSHA) Process Safety Management (PSM) [2] and Guidelines for Risk Based Process Safety (RBPS) [3] mandate industrial organizations to utilize SOPs in the course of employee training and actual operations.

Issues associated with SOPs are pointed out as one of the major causes of incidents in chemical process industries. From a review of over 60 incident investigations conducted by the U.S. Chemical Safety Board (CSB), problems regarding SOPs were present in approximately 70% of the incidents [4]. The investigations revealed that SOPs were not properly developed, not complete, or not followed as instructed during the course of incidents. Similarly, an analysis of World Offshore Accident Databank indicated that the absence of procedures and inadequate procedures were responsible for over 80% of human-related causes [5]. More specifically, an investigation of 2005 BP Texas City refinery explosion found out several issues with SOPs in the start-up process including operators' deviations from critical steps of the SOPs and insufficient hazard information to be specified in the SOPs [6].

To address the issues associated with SOPs, three approaches have largely been taken towards the better design of procedures: *informational*, *perceptual*, and *ecological* approaches. First, the *informational* approach has emphasized standardizing and delineating information elements of an SOP. In this approach, a major focus is to specify SOP requirements such as purpose, scope, and general description of a task, hazards and precautions, required tools, equipment and supplies, procedural steps to conduct the task, and data and record management [7, 8]. Second, the *perceptual* approach has sought to examine the visual attributes of SOP components in relation to operators' compliance. For instance, recent studies investigated features of a hazard statement including symbols, signal words (e.g., caution, warning), graphic embellishment (e.g., numbering, boxing, filling) [9, 10]. The findings from the informational and perceptual approaches were beneficial to illuminating what components need to be included in SOPs and how they should be formatted. Hence, their primary focus was mostly fixated on tackling task-specific matters with an ideal aim to make operators strictly comply with SOPs. However, other researchers assert that the zero-tolerance adherence to SOPs may be impossible and even deleterious to achieving safety of complex industrial operations due to constantly changing work environments, being often degraded from what was imagined in the SOPs [11, 12]. In addition, it is also suggested that the usage and role of the SOPs should change as the experience and knowledge of operators matures [13]. Recognizing the dilemma that underlies SOPs, the *ecological* approach views SOPs as decontextualized and abstracted artifacts that *guide*, not *dictate*, operators' problem-solving depending on their experience and knowledge regarding the system to be operated [14]. In light of this standpoint, advocates of the ecological approach insist that under constantly changing or unexpected operating conditions, SOPs should be designed in such a way that they support operators to adjust their actions to unstable circumstances in order to accomplish higher system-level goals [15, 16].

The ecological approach has been taken in designing cognitive work and associated information artifacts in safety-critical domains including chemical process industries. One of the principal concepts of the ecological approach is Abstraction Hierarchy (AH) of a system [17-19]. AH is a framework for representing the functional structure of a complex socio-technical system, consisting of several hierarchical levels that are bound in the goal-means relationship [20, 21]. AH principles have been applied to modeling various complex systems [22-25], devising work analysis method [26-28], and developing ecological interface design (EID) [29, 30]. The EID perspective aimed at externalizing operators' mental model has proven to be effective in supporting detection of unexpected situations and adaptive actions to cope with such anomalies [31]. In particular, previous research indicates that operators who were more knowledgeable and experienced about the functional structure of a system better exploited the utilities of the EID in solving unexpected problems and accomplishing given goals [32, 33]. Similar work was conducted for petrochemical industries. For example, work domains of chemical processing systems such as hydrogenation reactor and fluidized catalytic cracking unit (FCCU) were analyzed using the abstraction-decomposition space method [34, 35]. Furthermore, a control operator interface for the FCCU was developed using EID principles [36].

Although AH has been widely embraced in many studies across different domains and provided advantages in understanding and improving complex cognitive work systems, its application to SOPs used in high-risk environments is not existing to date. Also, research efforts that reflect the system's functional structure (e.g., AH) on SOPs are largely absent in the current body of literature. Furthermore, little is known with respect to what roles operators' knowledge of a task would play in relation to the functional structure of the system. As an exploratory effort to fill such gaps, our study aims 1) to analyze the work domain of a 3-phase separation system, a common crude oil refining process, and 2) to assess how an AH level reflected on the SOPs and an operator's experience and familiarity with a task are related to SOP performance.

2 Background

2.1 Abstraction hierarchy and work domain analysis

A work domain is referred to as a system space being acted upon, independent of any particular operator, event, task, or control interface [37]. Analyzing the work domain, namely, work domain analysis (WDA), is conducted to identify the functional structure of the system under examination and thus the first step of cognitive work analysis (CWA) [21]. WDA is aimed at eliciting the functional abstraction hierarchy (AH) and structural decomposition of the system. Combining the two orthogonal dimensions, an abstraction-decomposition space (ADS) is drawn (Figure 1). As described in Table 1, AH typically consists of five levels that are bound with the goal-means relationship in which a lower-level node acts as a means to achieve its immediate higher-level node. In this sense, higher levels of AH denote goals and abstract functions ('why work is done' and 'what work is done') of the system whereas lower levels are concerned with concrete and physical elements ('how work is done'). Decomposition is laid out on the horizontal dimension incorporating a whole system, sub-system or unit, and component levels.

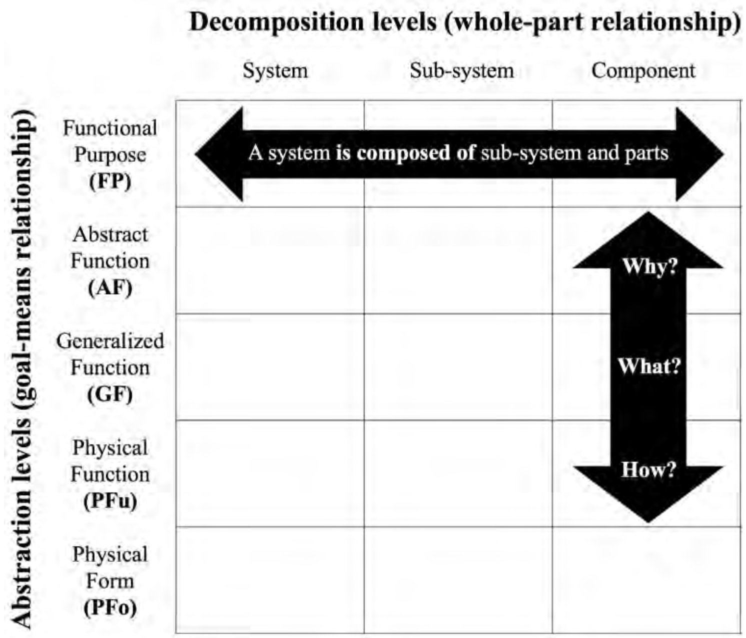


Figure 1. Generic Abstraction-Decomposition Space with two dimensions of abstraction hierarchy and decomposition hierarchy

Table 1. Levels of Abstraction Hierarchy

AH Level	Description
Functional Purpose (FP)	Ultimate goals that a system must achieve
Abstract Function (AF)	Governing laws and principles that constitute the system
Generalized Function (GF)	General processes involved in satisfying the governing principles
Physical Function (PFu)	Capabilities of physical elements to achieve the generalized functions
Physical Form (PFo)	Type, shape, location, and layout of physical elements

2.2 Work domain of 3-phase separation system

2.2.1 A description of 3-phase separation system

A primary purpose of a 3-phase separation system is to separate upstream fluid produced from an oil well into three material components, that is, gas, water, and oil [38]. Of particular importance in the refining process is to completely separate any free water (water not bound to any grains or minerals) because free water is likely to cause corrosion or hydrate formation [39]. As shown in Figure 2, the 3-phase separation system includes several gravity-settling tanks in which heavier molecules (e.g., water, oil) fall down and lighter gases rise over the liquid [38]. After going through multiple separation tanks, each of the components is collected and discharged to respective downstream processes for further treatment.

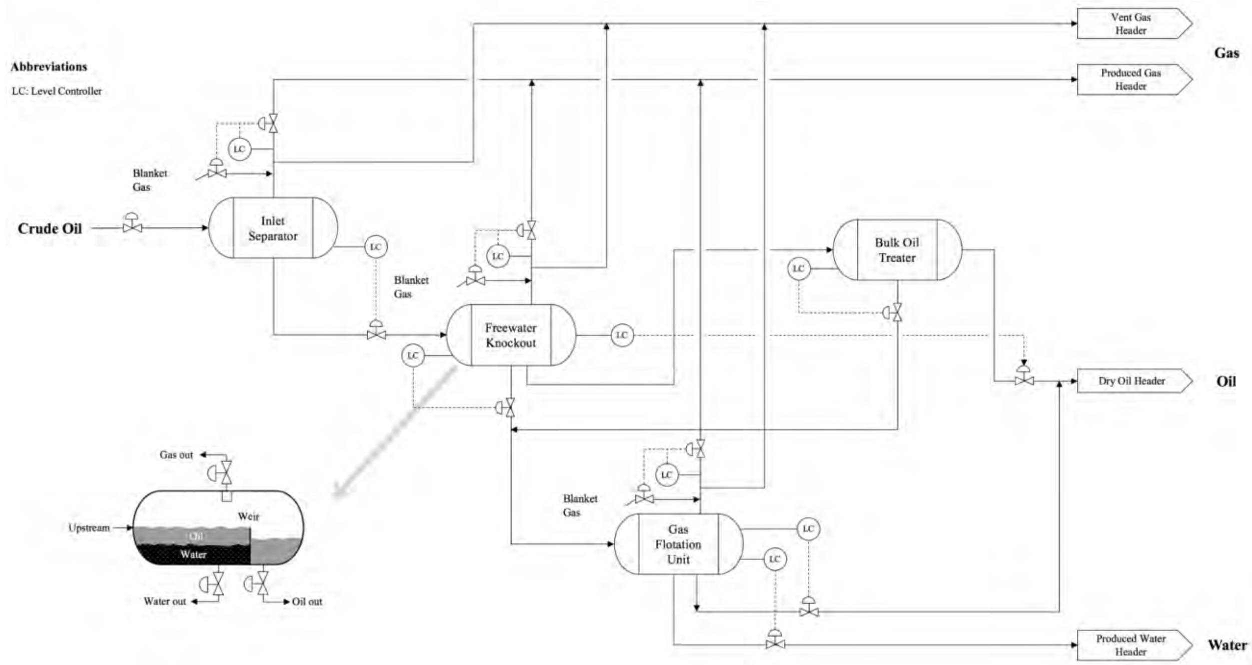


Figure 2. A simplified process flow diagram of the 3-phase separation system

2.2.2 Work domain of 3-phase separation system

As a work domain is independent of operators, tasks, or technical artifacts such as SOPs, we analyzed the work domain of a 3-phase separation system without regard to tasks examined in this study. As the first stage of the work domain analysis, the part-whole decomposition of the 3-phase separation system was conducted (Figure 3). The 3-phase separation system, which constitutes a larger chemical complex by connecting upstream (e.g., crude oil production) and downstream (oil stabilization) processes, is decomposed into multiple units at the sub-system level. The units at the sub-system level provide stream processing functions including fluid input, fluid containment, fluid output, level control, gas releasing, temperature control, pressure control, and energy control. These units are then further decomposed into specific physical functions and components such as fluid feed, pump, valve, separation vessels, and gas, oil, and water outputs.

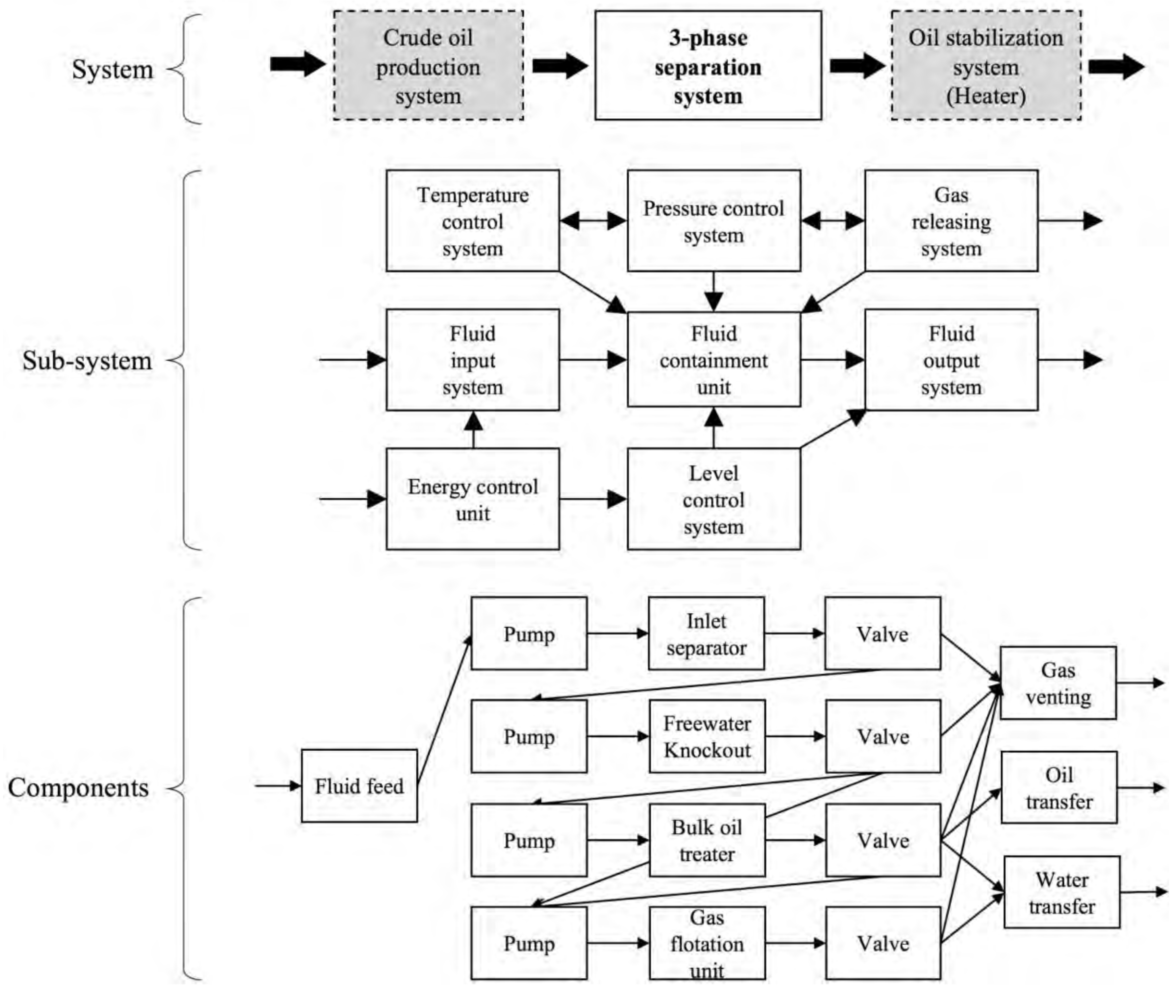


Figure 3. Part-whole decomposition of the 3-phase separation system

Second, the ADS of the 3-phase separation system was generated by adding the AH to the decomposition dimension as shown in Figure 4. At the FP level, the ultimate goals of the system such as production and safety were defined: 'producing oil from raw fluid' and 'securing the safety of separation process'. At the AF level, governing laws of the 3-phase separation system such as maintaining mass flux, separation, pressure, temperature, and energy were identified. At the GF level, generic processes required to satisfy the governing principles of the AF level were modeled. For example, the GF level includes transferring fluid input and output, containing the fluid, releasing gas, removing heat from the fluid, stratifying the fluid, and supplying energy source to enable other functions. As the GF level lies in the interface between functional levels and physical levels, the GFs were also identified both at sub-system and components levels. The PFu level shows capabilities of physical elements of the system such as fluid feed and phase separators, oil and water transfer, and gas venting were identified. Lastly, at the PFo level, specific physical elements such as pumps, valves, vessels, sensors, and topology among them were identified. The line between nodes in the ADS indicates the goal-means relationship in which lower-level nodes are needed to achieve a higher-level node.

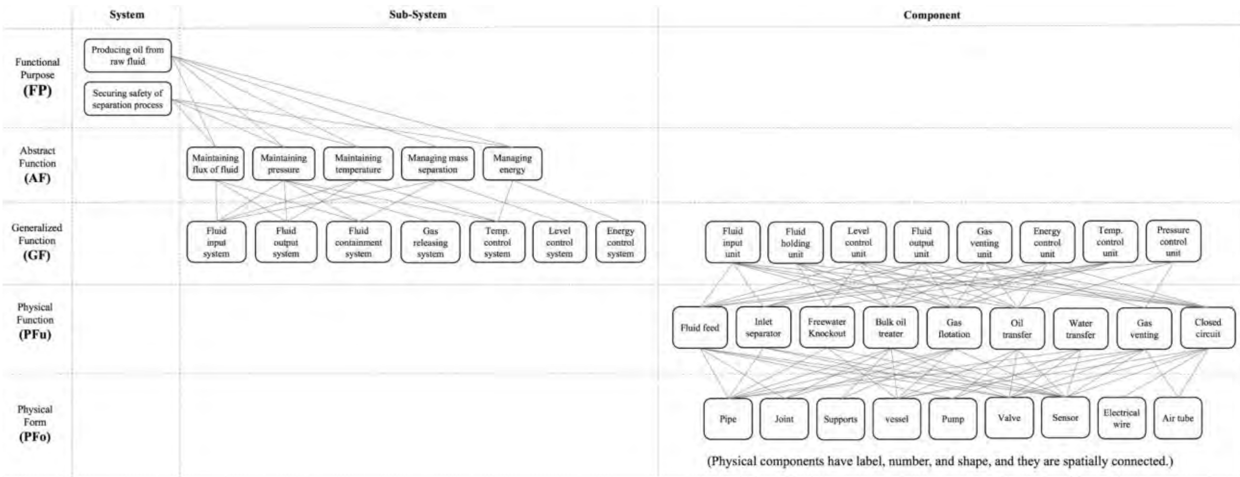


Figure 4. Abstraction-Decomposition Space of the 3-phase separation system

3 Method

3.1 Research setting

To evaluate operators' performance with SOPs in a realistic environment, data for this study were collected in a high-fidelity chemical processing training facility operated by a large petrochemical company located in the south-central U.S. The facility simulates an offshore oil production platform incorporating multiple trains of the 3-phase separation system. To realize the training purpose and eschew any potential risk, the facility uses vegetable oil, running water, and atmospheric air as substitutes for a natural crude oil stream.

3.2 Participants

Participants for this study were recruited via a third-party staffing agency specialized in the oil and gas industry. A total of 25 participants who were active workers in the oil and gas industry were recruited for this study. They were all males and their average age was 40.8 years (SD=12.3, min=20, max=63). The average years of industry experience were 14.3 years (SD=12.2, min=1, max=37). The occupational profile of the participants varied depending on the areas of experience in their career as shown in Table 2.

Table 2. Occupational experience of the participants

Area of occupation in the oil and gas industry	% participants who had experience in the area
Production and transportation	56%
Engineering (e.g., electrical, mechanical)	32%
Installation, maintenance, and repair	28%
Extraction and rig operations	16%
Management and supervisory	8%
Construction	4%

3.3 Tasks and materials

Participants were asked to carry out four tasks: column flushing (CF), level control valve (LCV) replacement, pressure testing (PT), and fluid sampling with a centrifuge (Centrifuge). CF is a task that unloads fluids inside a column attached to a vessel. LCV is a maintenance task that replaces a level control valve that adjusts the fluid level in the vessel. PT is a task that tests high- and low-pressure trips of the vessel. Centrifuge is a task that measures the water content of a sample product. Since Centrifuge is to assess the composition of the product regardless of a processing system type used to separate the stream, it was excluded from the current study.

Prior to conducting a task, participants were given a paper-based SOP prepared by the training facility. The SOP consists of purpose and scope of work, document history, risk information, required permits such Lock-Out/Tag-Out (LOTO), necessary tools and equipment (e.g., PPE), and a series of steps to carry out. An example of the steps of LCV is shown in Figure 5. To record the participants' actions during the SOP implementation, an Akaso Action Camera™ (Akaso Inc.) was attached to a participant's hard hat. Due to technical difficulties associated with the portable video recorders (e.g., inadvertent change of a viewing direction), complete data for CF, LCV, and PT tasks were obtained from 19, 19, 22 participants, respectively.

WORK INSTRUCTION

	Signoff	Operation Step
1.	____	Operator & Craft walk down the equipment to ensure that equipment is ready to be removed from service
2.	____	Notify the Control Room Operator that equipment is ready to be removed from service
3.	____	Perform Job Safety Analysis (JSA) on the task that will be taking place. Check Worksite Hazards, and equipment needed for disassembly and containment
4.	____	Complete a Work Permit
5.	____	Complete a LOTO isolation sheet. Check LOTO points. Highlight points on P&ID's and use for attachment. *Note: Can go to electronic copy and save for reference on LOTO.*
6.	____	Close Manual Valve M101-9
7.	____	Close Manual Valve M101-10
8.	____	Console operator to open LCV-101 to the 100% position
9.	____	Open drain valve upstream of LCV-101
10.	____	Open drain valve downstream of LCV-101
11.	____	Open drain valve downstream of check Valve FSV-M101-29 Trapped pressure may be present. Uncontrolled pressure release could result in bodily injury or death. Wear gloves and safety glasses.

Figure 5. A sample of procedural steps of the LCV task

3.4 Independent variables

3.4.1 Experience-Task Familiarity (E-TF) level of participants

Years of experience may represent an operator's experience in a broad sense. However, the current study considers an individual operator's knowledge as to how to perform a specific task. Therefore, the years of experience may not suffice as a single factor to judge whether or not a participant has adequate knowledge for the task. In addition, the divergence in participants' areas of experience (Table 2) may render the years of experience a less indicative factor. To complement such limitations, participants' experience and task familiarity were incorporated into a matrix as presented in Figure 6. Years of experience were scaled with five-year periods and task familiarity scale was obtained from a post-experiment interview with each participant. A diagonal border that includes either very low experience or very task familiarity was chosen to split a low and a high experience-task familiarity (E-TF) group. Participants having lower than 10 points (white cells in the matrix) were classified into a *low* E-TF group whereas those with equal to or higher than 10 points (gray cells in the matrix) were put into a *high* E-TF group. Based on these criteria, 38% of participants were labeled as a low E-TF group.

	Task Familiarity Scale				
Experience Scale	1 (very low)	2 (low)	3 (medium)	4 (high)	5 (very high)
1 (YE<5)	1	2	3	4	5
2 (5≤YE<10)	2	4	6	8	10
3 (10≤YE<15)	3	6	9	12	15
4 (15≤YE<20)	4	8	12	16	20
5 (YE≥20)	5	10	15	20	25

YE: Years of Experience

Figure 6. Experience-Task Familiarity (E-TF) matrix

3.4.2 AH level of SOPs

As the second categorical factor, the AH level that dominates an SOP was assessed. To do this, individual steps of the SOP was coded either *functional (F)* or *physical (P)* based on the ADS of the 3-phase separation system (Figure 4). To be noted is that the instructions regarding administrative measures such as work permit, LOTO (e.g., steps 1 through 6 in Figure 5) were excluded from the coding because they were considered to be part of another large work system and thus were simulated verbally or virtually.

The coding of AH level was conducted by two of the authors (CS and NA). The average interrater reliability (Cohen's κ) between the two coders for the three SOPs was 0.70, indicating a moderate level of agreement [40]. Finally, the first author's coding was used for analysis. Table 3 presents the results of binary coding (i.e., F/P). Based on the coding, CF and LCV were classified as physical-dominant SOPs and PT as a functional-dominant SOP in a relative sense.

Table 3. Binary (F/P) coding results

SOP (No. of steps)	Physical (%)	Functional (%)
Column Flushing (13)	11 (85%)	2 (15%)
Level Control Valve (16)	14 (88%)	2 (12%)
Pressure Testing (12)	6 (50%)	6 (50%)
Total	31 (76%)	10 (24%)

3.5 Dependent variable: Successful Step Ratio (SSR)

In line with the prescriptive view towards SOPs, a traditional measure of operators' procedure performance was how strictly they comply with procedural steps (e.g., compliance vs. non-compliance) [41, 42]. In addition to this dichotomous measure, we attempted to reflect the ecological approach in the SOP performance measurement. Based on a procedural behavior assessment methodology developed by our research group [43], successful step ratio (SSR) was conceived as an operator's SOP performance measure. SSR considers not only compliant and non-compliant behaviors but also adapted actions from procedural steps and assisted or struggled actions as shown in Figure 7. The logic in this coding scheme enables a coder to label a procedural step whether the step is either compliance (C), adaptation (A), performance with issues (I), or non-compliance (N). When the step was performed correctly without any assistance or struggling, the step was coded as compliance. When the step was performed correctly but with some assistance from instructors or struggling (e.g., spending a long time knowing what to do), the step was coded as performed with issues. When the step was performed correctly but out of order, the step was coded as adaptation. Non-compliance was coded when the step was completely skipped or ended incompletely.

Although non-compliance with procedural steps may be claimed helpful in achieving the goals of a task, it would be an unusual situation such as an emergency event or a highly unstable work environment that warrants the deviation from the SOPs. Considering that the current study was conducted under a relatively stable condition (e.g., no emergency event), steps complied with and adapted were deemed to be successful. To that end, SSR is formulated as a ratio of compliance (C) and adaptation (A) to the total number of steps (Eq.1).

$$SSR = \frac{C + A}{C + A + I + N} \qquad \text{Eq.1}$$

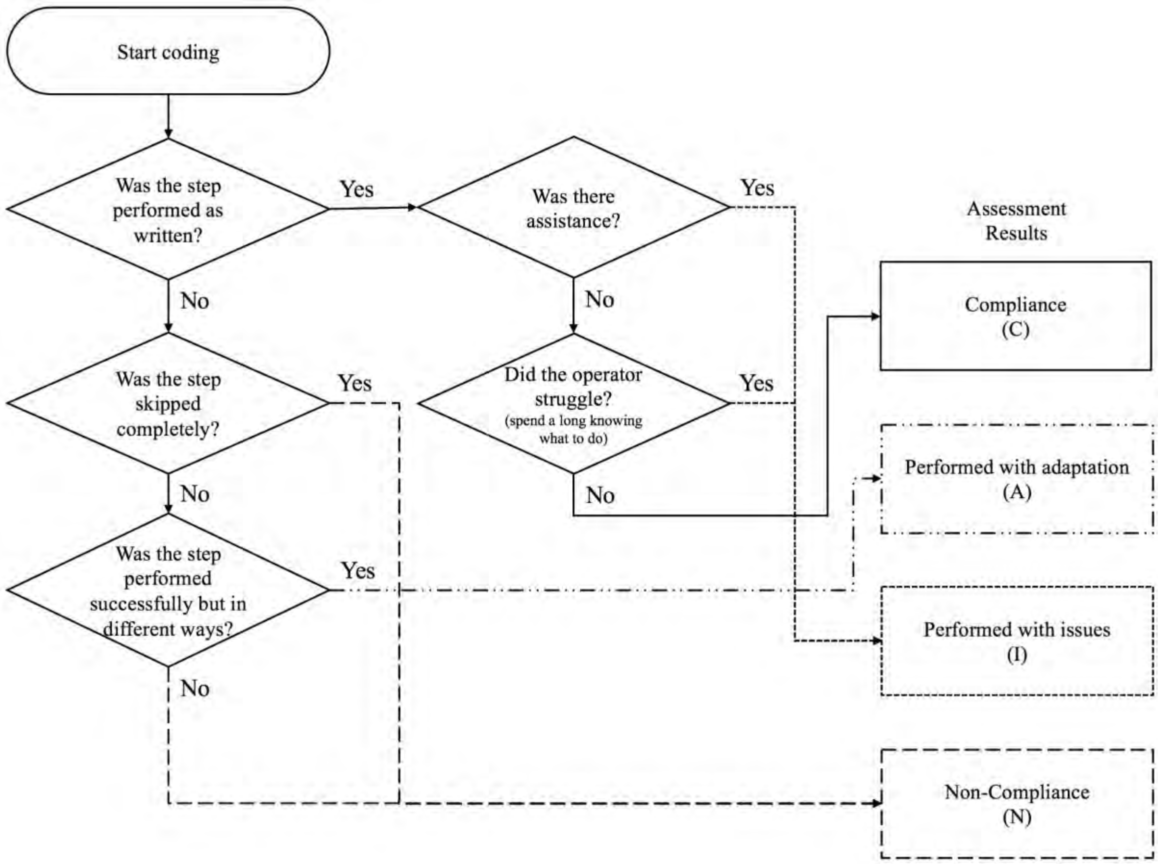


Figure 7. Procedure step performance coding logic (adapted from [43])

3.6 Experiment Protocol

There were six batches of participants with each batch taking two days for data collection. In the afternoon of the first day, a batch of participants checked in to the training facility and was given instructions on basic knowledge of the 3-phase separation process via in-class lecture and a tour to the processing trains in the facility. In total, the instructional session lasted for about three hours. In the morning of the second day, participants came to the facility and were asked to conduct individual tasks. After receiving the SOP for one task, the participant entered the processing trains, located the target equipment, and implemented the SOP. One to two instructors were positioned inside the facility and provided assistance when the participant asked or when the participant's behavior was deemed unsafe. On completion of the task, the participant exited the processing trains and was given another task. An order of assigning tasks to the participants was randomized to control order effects. After all the participants in that batch finished all the tasks, another batch of participants checked in and followed the same protocol. This study was conducted in compliance with research protocols approved by the Institutional Review Board.

3.7 Statistical Analysis

Using the indices introduced in the preceding sections, two-way ANOVA was carried out to examine the main and interaction effects of an operator's E-TF level and AH level of an SOP on

SSR. The assumptions (e.g., normality and equal variance) for ANOVA were found to be satisfied by running Levene's test and inspecting Q-Q plot. Partial eta squared (η_p^2) was used to estimate effect size for the test and reported as being small ($\eta_p^2 < 0.06$), medium ($0.06 \leq \eta_p^2 \leq 0.14$), and large ($\eta_p^2 \geq 0.14$) [44]. All the statistical analyses were performed using JASP [45]. Statistical significance was concluded when $p < 0.05$.

4 Results

4.1 E-TF level and AH level of SOP on SSR

We analyzed how an operator's E-TF level (high vs. low) and AH level (physical vs. functional) of an SOP are related to SSR. As shown in Figure8, the average SSR was 0.66 for the physical-dominant SOPs and 0.35 for the functional-domain SOP in the low E-TF group. Corresponding values for the high E-TF group were 0.85 and 0.74, respectively. Results of the two-way ANOVA indicate that there are main effects of the E-TF level ($F(1, 56)=29.04$, $p < 0.001$, $\eta_p^2 = 0.342$, large effect size) and the AH level (F(1, 56)=15.44, p < 0.001, $\eta_p^2=0.216$, large effect size). There was a marginally significant interaction effect of the E-TF level and the AH level on SSR ($F(1,56)=3.40$, $p=0.071$).

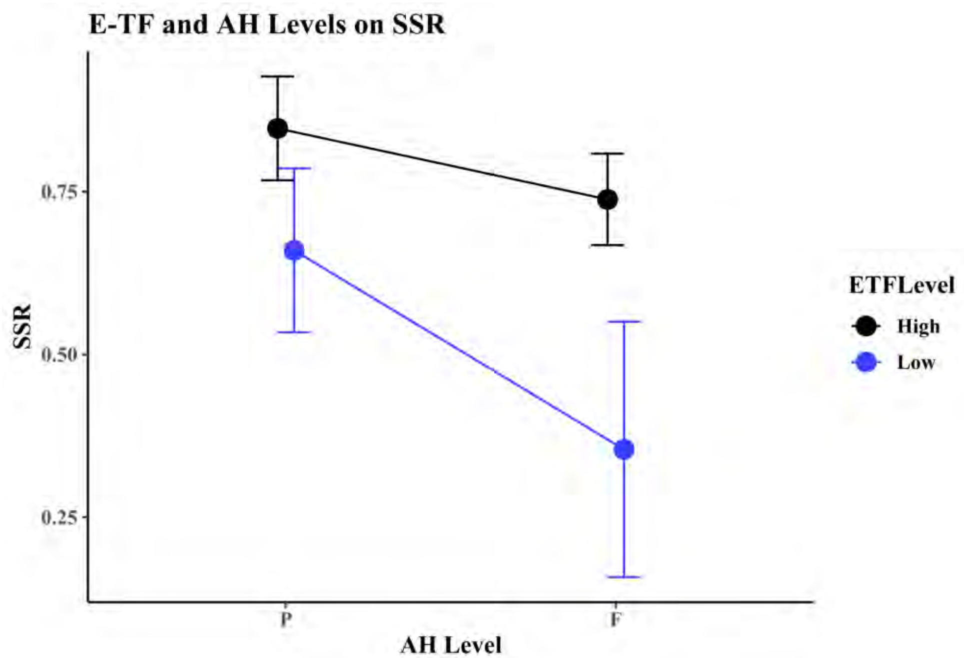


Figure. 8 Successful Step Ratio (SSR) by E-TF level and AH level

5 Discussion

As an exploratory study that embraces the ecological approach towards SOPs, the present study first modeled the work domain of a 3-phase separation system into an abstraction-decomposition space and applied the AH to three SOPs used in the high-fidelity chemical processing facility. We found out that individual steps of the SOPs were representing different AH levels (e.g., physical and functional) of the system. More specifically, our coding results indicated that physical-level steps were more prevalent than functional-level ones. The predominance of physical-level steps appears to be in line with the emphasis on standardization and specification of actions to be taken from the prescriptive approach [3, 4].

Our study then analyzed the relationship among the operators' E-TF level and the AH level of the SOPs, and a ratio of successful steps. The results of the two-way ANOVA first suggest that the more the operator is experienced and familiar with a task, the more successful steps he/she performs. Second, it also indicates that the more physical steps the SOP contains, the more successful steps the operator carries out. Based on this finding, one may insist that the SOPs be designed in such a way that they specify procedural actions at a physical-level and sufficient training be provided to operators so that they become more experienced and familiarized with SOPs for given tasks [41].

While the prescriptive efforts in the design of SOPs may provide some benefits to operators (e.g., gaining experience through training under stable or ideal conditions), it still leaves the SOPs vulnerable to unpredicted and abnormal situations in which the operators have to deviate. To address this *double-bind* issue [46], results of the current study offer an opportunity to exploit the utilities of the ecological approach. As shown in the interaction trend of the E-TF level and AH level, albeit the marginally significant effect, operators with higher experience and task familiarity may have utilized their mental model of the system and thus exhibited comparatively consistent performance in the face of more functional, abstraction step descriptions [32, 33]. This interpretation then implies that SOPs should be designed in a way that they externalize the functional structure (e.g., AH) of the system and thus support operators' goal-achieving behaviors when confronted with unexpected situations [31]. As an example of the SOP reflecting the ecological viewpoint, Figure 9 presents both physical-level actions ('how') and the purpose of doing such actions ('why').

WORK INSTRUCTION

	Signoff	***Physcial Action* Step**	***Purpose***
6.	____	Close Manual Valve M101-9	*To isolate upstream and downstream flow of LCV-101*
7.	____	Close Manual Valve M101-10	
8.	____	Console operator to open LCV-101 to the 100% position	*To release fluid and pressure inside LCV-101*
9.	____	Open drain valve upstream of LCV-101	*To drain the remaining fluid and relieve pressure inside the isolated section surrounding LCV-101 so that removing LCV-101 does not cause bursting pressure incidents*
10.	____	Open drain valve downstream of LCV-101	
11.	____	Open drain valve downstream of check Valve FSV-M101-29 Trapped pressure may be present. Uncontrolled pressure release could result in bodily injury or death. Wear gloves and safety glasses.	

Figure. 9 A sample SOP for LCV that provides both a physical-level description and purpose of actions (changes from the original version, Figure. 5, are italicized)

Notwithstanding the insightful findings presented in this study, limitations of the current study should be acknowledged. First, although the experiment was conducted in a high-fidelity environment, the presence of observers and instructors might have affected participants' behavior representing less of actual operation practices. This limitation can be addressed by conducting similar experiments in real-world work environments. Second, another limitation exists in the design of SOPs used in this study. To maintain the fidelity of the experiment, we used the existing SOPs established by the training facility. Therefore, it was not possible to manipulate the level of AH as indicated in the verdict of PT as a functional-dominant SOP. Hence, in future studies, it is recommend to control the AH levels so that the degree of physical or functional dominance would become more evident. Third, we formulated a couple of novel indices to consider both the operators' knowledge and familiarity with individual tasks (E-TF score) and the variations in the SOP-implementing behaviors (SSR). Due to relatively stable experimental conditions where no adversaries or unexpected situations arose, we found that adherence to the SOP steps largely led to successful outcome although some adaptations were also observed. Thus, future research may consider introducing abnormal or unanticipated events in order to examine how experienced and inexperienced operators comply with or deviate from the SOPs as well as to refine the SOP performance measure in alignment with the ecological approach.

6 Conclusion

As an exploratory research effort, this study employed an ecological approach towards the design of SOPs used in the 3-phase separation system. We found it useful to use AH in modeling a complex chemical processing system and in mapping AH to the steps of the SOPs. By analyzing the relationship among operators' E-TF level and AH level of the SOPs, and the operator's successful step ratio measure, this study identified that the more experienced and familiar with tasks, the more successful steps they carried out, and that the more physical steps the SOP include, the higher the successful step ratio. More importantly, our study results found an interesting tendency that the high E-TF group showed relatively stable performance in the use of the functional-level dominant SOP. To gain more benefits from the ecological approach, future research is warranted to address the limitations of the current study and to design SOPs that support operators' successful performance under variable conditions in high-risk process operations.

Acknowledgement

This research was sponsored by the Next Generation Advanced Procedures Initiative (http://advancedprocedures.tamu.edu/).

References

1. Bates, S. and J. Holroyd, *Human factors that lead to non-compliance with standard operating procedures*. 2012, Health and Safety Executive: Derbyshire, UK.
2. *Occupation Safety and Health Administration Process Safety Management*, U.S. Department of Labor, Editor. 2000.
3. Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*. 2010, Hoboken, NJ: John Wiley & Sons.

4. Baybutt, P., *Insights into process safety incidents from an analysis of CSB investigations.* Journal of loss prevention in the process industries, 2016. **43**: p. 537-548.
5. Christou, M. and M. Konstantinidou, *Safety of offshore oil and gas operations: Lessons from past accident analysis*. 2012, European Commission Joint Research Centre.
6. Holmstrom, D., et al., *CSB investigation of the explosions and fire at the BP Texas City refinery on March 23, 2005.* Process Safety Progress, 2006. **25**(4): p. 345-349.
7. U.K. Health and Safety Executive. *Operating Procedures*. 2019; Available from: http://www.hse.gov.uk/comah/sragtech/techmeasoperatio.htm.
8. Peres, S.C., et al., *A summary and synthesis of procedural regulations and standards—Informing a procedures writer's guide.* Journal of Loss Prevention in the Process Industries, 2016. **44**: p. 726-734.
9. Tharpe, K., S.E. Thomas, and S.C. Peres, *Signal Words and Symbol Designs: Importance in Hazard Statements for Procedures.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2017. **61**(1): p. 1429-1430.
10. Hendricks, J., S.C. Peres, and T. Neville, *The Impact of Hazard Statement Design Characteristics in Procedures on Compliance.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2018. **62**(1): p. 1616-1618.
11. Hollnagel, E., *Safety-I and safety-II: the past and future of safety management*. 2018, Boca Raton, FL: CRC press.
12. Hollnagel, E., *Why is work-as-imagined different from work-as-done?*, in *Resilient Health Care*, R.L. Wears, E. Hollnagel, and J. Braithwaite, Editors. 2017, Ashgate Publishing: Surrey, England. p. 279-294.
13. Sasangohar, F., et al., *Investigating written procedures in process safety: Qualitative data analysis of interviews from high risk facilities.* Process Safety and Environmental Protection, 2018. **113**: p. 30-39.
14. Wears, R. and G. Hunte, *Resilient procedures: oxymoron or innovation?*, in *Resilient health care*, J. Braithwaite, R.L. Wears, and E. Hollnagel, Editors. 2017, CRC Press: Boca Raton, FL. p. 163-170.
15. Wachs, P. and T.A. Saurin, *Modelling interactions between procedures and resilience skills.* Applied Ergonomics, 2018. **68**: p. 328-337.
16. Hale, A. and D. Borys, *Working to rule, or working safely? Part 1: A state of the art review.* Safety science, 2013. **55**: p. 207-221.
17. Rasmussen, J. and K.J. Vicente, *Coping with human errors through system design: implications for ecological interface design.* International Journal of Man-Machine Studies, 1989. **31**(5): p. 517-534.
18. Bisantz, A.M. and C.M. Burns, *Applications of cognitive work analysis*. 2008: CRC Press.
19. Vicente, K.J. and J. Rasmussen, *Ecological interface design: Theoretical foundations.* IEEE Transactions on systems, man, and cybernetics, 1992. **22**(4): p. 589-606.
20. Rasmussen, J., *Information processing and human-machine interaction. An approach to cognitive engineering.* 1986.
21. Vicente, K.J., *Cognitive Work Analysis: Toward safe, productive, and healthy computer-based work*. 1999, Mahwah, New Jersey: Lawrence Erlbaum Associates.
22. Lintern, G., *A functional workspace for military analysis of insurgent operations.* International Journal of Industrial Ergonomics, 2006. **36**(5): p. 409-422.

23. Lind, M., *Making sense of the abstraction hierarchy in the power plant domain.* Cognition, Technology & Work, 2003. **5**(2): p. 67-81.
24. Hajdukiewicz, J.R., et al., *Modeling a medical environment: an ontology for integrated medical informatics design.* International journal of medical informatics, 2001. **62**(1): p. 79-99.
25. Ahlstrom, U., *Work domain analysis for air traffic controller weather displays.* Journal of safety research, 2005. **36**(2): p. 159-169.
26. Bisantz, A. and E. Roth, *Analysis of cognitive work.* Reviews of human factors and ergonomics, 2007. **3**(1): p. 1-43.
27. Jenkins, D.P., *Cognitive work analysis: coping with complexity*. 2009: Ashgate Publishing, Ltd.
28. Naikar, N., *Work domain analysis: Concepts, guidelines, and cases*. 2016: CRC Press.
29. Pawlak, W.S. and K.J. Vicente, *Inducing effective operator control through ecological interface design.* International Journal of Human-Computer Studies, 1996. **44**(5): p. 653-688.
30. Van Dam, S.B., M. Mulder, and M. Van Paassen, *Ecological interface design of a tactical airborne separation assistance tool.* IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2008. **38**(6): p. 1221-1233.
31. Vicente, K.J., *Ecological interface design: Progress and challenges.* Human factors, 2002. **44**(1): p. 62-78.
32. Vicente, K.J., K. Christoffersen, and A. Pereklita, *Supporting operator problem solving through ecological interface design.* IEEE transactions on systems, man, and cybernetics, 1995. **25**(4): p. 529-545.
33. Ham, D.-H., W.C. Yoon, and B.-T. Han, *Experimental study on the effects of visualized functionally abstracted information on process control tasks.* Reliability Engineering & System Safety, 2008. **93**(2): p. 254-270.
34. Miller, C.A. and K.J. Vicente, *Abstraction decomposition space analysis for NOVA's E1 acetylene hydrogenation reactor.* Cogn. Eng. Lab.: Univ. Toronto, Toronto, ON, Canada, CEL-98-09, 1998.
35. Jamieson, G.A. and K.J. Vicente. *Modeling techniques to support abnormal situation management in the petrochemical processing industry*. in *Proceedings of the Canadian Society for Mechanical Engineering Symposium on Industrial Engineering and Management*. 1998. Citeseer.
36. Jamieson, G.A., *Ecological interface design for petrochemical process control: An empirical assessment.* IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2007. **37**(6): p. 906-920.
37. Hajdukiewicz, J.R. and K.J. Vicente, *A theoretical note on the relationship between work domain analysis and task analysis.* Theoretical Issues in Ergonomics Science, 2004. **5**(6): p. 527-538.
38. Sayda, A.F. and J.H. Taylor. *Modeling and control of three-phase gravilty separators in oil production facilities*. in *2007 American Control Conference*. 2007. IEEE.
39. Bilio, M., et al. *CO2 pipelines material and safety considerations*. in *Hazards XXI: Process Safety and Environmental Protection in a Changing World*. 2009. Institution of Chemical Engineers.
40. McHugh, M.L., *Interrater reliability: the kappa statistic.* Biochemia medica: Biochemia medica, 2012. **22**(3): p. 276-282.

41. Park, J. and W. Jung, *The operators' non-compliance behavior to conduct emergency operating procedures—comparing with the work experience and the complexity of procedural steps.* Reliability Engineering & System Safety, 2003. **82**(2): p. 115-131.
42. Basso, B., et al., *Reviewing the safety management system by incident investigation and performance indicators.* Journal of Loss Prevention in the Process Industries, 2004. **17**(3): p. 225-231.
43. Neville, T.J., et al., *Assessing Procedure Adherence Under Training Conditions in High Risk Industrial Operations.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2018. **62**(1): p. 1604-1604.
44. Cohen, J., *Statistical power analysis for the behavioral sciences*. 2nd ed. 2013, New York, NY: Routledge.
45. JASP Team, *JASP*. 2017.
46. Dekker, S., *Failure to adapt or adaptations that fail: contrasting models on procedures and safety.* Applied ergonomics, 2003. **34**(3): p. 233-238.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Relationship between Human-Managerial and Social-Organizational Factors for Industry Safeguards Project: Dynamic Bayesian Networks

Cassio Ahumada[2], Jade Ávila[3], Salvador Ávila[3*], and Beata Mrugalska[1]
[1]Poznan University of Technology, Faculty of Engineering Management, Plac Marii
[2]Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, Texas, USA
[3]Universidade Federal da Bahia, Polytechnic Institute, Industrial Engineering Program, Salvador, BA, Brazil
*Presenter E-mail: avilasalva@gmail.com

Abstract

This methodology intends to identify the Relationship Network between Human-Managerial and Social-Organizational Factors considering the Dynamic behaviour and Work Environment to build preventive actions based on the approximation calculation of the top event. During methodology discussion and testing we can: establish new criteria for Designing Safeguards in the Case of Chemical Industry Control Instrument Interfaces, Regional-Global Culture Features, and Probability Analysis for Human Errors; understand rare event analysis with no history to design possible Future Accident Scenarios; and Identifying, developing and testing safeguards for behaviour adjustment and Culture through Tribal Rituals, Operational Groups, Intellectual Capital for Failure Processes, Human Reliability Factors, Change of Habits, Educational Transformation Programs. This work intends to discuss the new concept of systemic failure (first phase) and related tools for the calculation of reliability. In the new concept, before the fault is active, there is an entire relation-ship between technical, human, social and organizational factors. In a second phase, it is intended to explore the relationships between Human Factors in the work environment indicating what is a safe behaviour and what is the possibility of change over time and environments in routine and emergency. When constructing barriers, and investigating accidents, it is important to explore the role of the leader and the possibility of making the wrong decision. Still in the second phase the socio-functional relations and the possibility of triggering the fault of the operational culture are dis-cussed. The cultural environment has a great influence on the existence of bad habits through rituals of preservation of what is right. It is important for database construction to understand how the executive function works in planning and controlling tasks. The simplicity of analysis of cognitive processing functions and analysis in task planning does not allow advancing the investigation of human error. Phase 3 of research will focus on the analysis of physical-cognitive and organizational criteria that may be the cause of human error or accident or can be barriers to non-existence. In this discussion, we intend to deepen in the subjects: role of the cognitive function in the transformation of the information; evaluate the man-task interface, indicating where the main gaps are; evaluation of the human machine interface by the cognitive side and organizational (stress and leadership); use of the cross matrix to identify barriers in the control panel trying to avoid the failure caused by cognitive gaps due to social phenomena. Finally, in phase 4, a solution is sought for the search for more effective preventive and corrective actions in the current situations of uncertainty through dynamic Bayesian Networks for Human Factors and Human Behaviour.

Keywords: Dynamic Bayesian Networks - Industry Safeguards - Human-Managerial - Social-Organizational.

1 Introduction

The relations between human factors which can provoke events with economic losses must be observed from a nebulous environment (low visibility) and possibility of complex system. Initially, let us go consider that involved factors on accident are multidisciplinary and within a historical existence. These factors can have complex relations that require different measurement methods, some direct on the phenomena in question and some indirect, from some existing variables in the workplace. On this paper, we pretend to provide a methodology for configuration and control of events, with high process losses in the industry with risk activities. This case will be applied to the Chemical Industry.

The operating routine and its deviations can lead to failure and accident [1]. Failure warnings are in the intermediate state, where the process, product, equipment, and staff (or individual) are constant change and can reach the systemic failure state. When this state is established visible consequences occur such as system stop, loss of quality, waste generation, waste of time, reduced billing and others. However, today, in a period of high pressure from society, the sustainability of industrial businesses and critical activities depends on maintaining a positive image.

Therefore, should be avoided the impact of accidents, chemical leaks and incorrect managerial attitudes regarding social responsibility by identifying the relationship network between human-managerial-social-organizational factors, dynamic behavior and the work environment to build preventive actions based on the top event approximation calculation.

Hazard enablers human elements are classified as technological (risk and complexity), managerial (stress and leadership) and behavioral (cooperation, commitment, competence and communication - C4t) [2]. These elements are designed at the beginning of the business and should protect the system from overloading as these elements may degrade over time, it is related to design criteria. Human factors, on the other hand, may be active or inactive, circulating with a certain failure energy and may have economic consequences, it is related with operational routine.

In this context, Human elements are related to *design resistance* while human factors are related to failure or hazard energy during operation, or *operational charge*. This load is dynamic due to the workplace and the types of cultural and behavioral influence within the organizational environment. While resistance is embedded in static patterns that need to be revised due to: the influence of social phenomena, and the degradation of barriers (caused by time and physical attacks). This degradation promotes a new balance of forces for installed safeguards. Unfortunately, the load and resistance is very dynamic.

A research was done by applying questionnaires to operational groups of an industry. The questionnaires were based on principles of risk perception, aspects of cognition, understanding of the workplace and especially knowledge about the human factors in work activities.

1.1 Human Factors Construction

Understanding the implementation of individual or group Human Factors for Routine and Emergency enables effective safeguards to be established to prevent accidents. The Composition of Systemic Failure, depends on active cultural, educational, learning, practice and behavior in transient situations. The dynamics of behavior resulting from these factors are understood and classified to achieve the resilience of the individual under threat can find the solutions. The same can be said of group or organizational resilience, where many other factors are understood, classified and analyzed to result in operational culture [3].

The characteristic human factors for work in routine and emergency situations are constructed by chronological facts in the history of worker, and in respective competence, such as: culture, affection, individual and linguistic, concepts, experience and practices, work, group, work cycle, work organization and maturity.

1.2 Human-Managerial-Social-Organizational Factors

[4] and [5] indicate that human performance factors may cause failure and accident. These factors may be: the interface between worker with equipment and tasks; the relationship between individuals or groups; and the managerial characteristics. [7] discussed about hazard energy but do not formulate devices (doors) that enable the flow of this energy. The model proposed in this work treat the human elements from project and the construction of accident by human factors failures in operational situations. Thus, the human elements enablers flow of hazard energy opening the way toward the accident. This flow comes from a chain of events that occurs from human factors in nine-tier in industry operating, from the influence of culture to failure until the disaster.

The human elements that are part of the project are discussed in the topics organizational culture, safety and technology. These elements may change from design to operational phase, indicating that the energy of the events will or will not go towards the accident, depending on the operating culture installed on the shop floor.

Some structures (social or technical) may degrade and respond differently to each operating situation causing unexpected behavior. In this paper, it is proposed the existence of interconnected human factors that can create hazard energy compared to the projected barriers (human element). Therefore, if during operation some structures are failing, when combined, they can increase the "hazard energy". In this context, it is studied the flow of hazard energy generated, increased or decreased in the human factors, in nine levels passing through the human elements from the project, with or without degradation, allowing or not performing of failure, or accident or disaster.

1.3 Behavior and Dynamic Risk

The subjects discussed here are considered Dynamic Risks based on social culture, technologies, and Industrial Operation. The triggering and development of chain events depend on characteristics installed in the design to avoid the happen of these events. These characteristics dubbed as “resistance” can go into degradation during operations bringing situations where humans initiate and keep the failure cycle.

In the analysis of prediction of team behavior, and technical processes, we should identify which cultural biases and possibilities of human errors that are not avoided. Thus, it is possible to adjust cognitive gaps in order to promote resilience in relation to the dynamic risk to avoid degradation of design barriers (resistance) and the increase of cognitive workload.

The human elements to prevent failure must be reviewed according to environmental threats such as climate and organizational changes. In complex processes and high impact activities, is important to make a careful analysis to write procedures and delimit behavior patterns in Industrial Operation [6]. Analysis of routine abnormal occurrences in chemical (TDI, Polycarbonate, MDI, Sulfuric Acid), Oil and Gas (LPG) industries indicates the need for careful task analysis that goes beyond simply describing the steps with their goals, or only hierarchical analysis with times, auxiliary memory and necessary training [7]. It is necessary to gather the information and requirements of the legislation and analyze the environment of the task.

1.4Workstation

The Workstation project indicates physical, cognitive and organizational requirements to be met. The behavioral variability of the leader and the team is inserted as important information for future human performance, types of decision-action and what knowledge is required. The stability of cognitive-intuitive and emotional functions indicates a prepared structure for decisions under stress and high risks (emergency), as well as decisions and compliance with standards in normal situations [8].

On the one hand are product, process, and operations technology for effective production, on the other are the people and influences of a cultural field with social phenomena in the form of communication, group work, and the relationship of compromises with organizational goals. In the middle are the interfaces, the instruments that translate information and knowledge into action in the field. May be considered interfaces in the production routine: (a) computer screens for process control; (b) written procedures with linguistic symbols and signs; (c) leaders who have the ability to translate group sentiments and information from technology through language dictionaries that attempt to overcome cultural difficulties in carrying out critical activity.

The complexity to discuss the causes of systemic failure, and to perceive human risk, may be high. The lack or decrease of risk perception in the critical task causes ineffective prevention-correction-mitigation actions to avoid the failure or accident.

This event indicates the disruption in the flow of information in the cognitive field (communication and mind map) affecting the accomplishment of the task (failure in equipment or process). Thus, machines, processes and products are not properly controlled because of the lack of attitude or practical-theoretical knowledge to make decisions in standard situations.

The not recognition of an abnormal scenario and the trust on the pre-established pattern may be an indicator of future negative events in the safety (accident) or in the production (plant shutdown). The failure in risk perception can occur in execution (function in routine and emergency), planning (standards and writing procedures) and diagnosis of task. The Regulation of Human Elements in the Project is based on three groups: technology, management and behavior.

The description of the Organizational Standards, Policies and Procedures make up the tools and criteria for measuring, controlling, reviewing and investigating the complexity and causal link of human error and failure. These tools aim to optimize the processes and execution of critical tasks without social and environmental impacts, establishing requirements for Culture, Technology and People.

Workstation complexities vary according to: cognitive relations, visibility of events, and intensity of the risks of unexpected events. We distribute these relations as: (1) Simple activity involving operator and machine in workstation, few people and simple task - cognitive; (2) Integrated manufacturing activities that rely on automated systems (linear manufacturing - cognitive); (3) Industrial continuous processes with recycling and complex relationships, Risks and complexity can be high due to communications and heavy information flow – cognitive and intuitive; (4) network of industrial units where the appropriate culture is fair, no omissions or underreporting occur. Sometimes discussing industry theory 4.0 is easier than practicing since, unfortunately, we have not yet reached this ideal culture level, we still live with the blame culture – cognitive and intuitive.

1.5 Systemic Failure

Organizational Standards, Procedures and Operating Instructions should be structured to avoid trigger situation in routine where systemic failure begins, may to provoke sufficient hazard energy to reach the level of accident and even a crisis by chain reaction.

The study of the task and the analysis of the failure based in the operator's discourse allow us to recognize the current patterns and to estimate new ways of team act. This analysis is presented for groups of operators, and discuss resulting hypotheses from the occurrences investigation in routine identifying cycles of socio-technical events and outliers with projection of future accidents. The variables identified in the routine study through task analysis, failures and occurrence of abnormal events, compose a set of parameters and indicators that represent a certain culture with its informal rules allowing predictive analysis of systemic failure.

On the other hand, as operations can cause a structural high load on the system promoting events that generate accidents or environmental impacts. This discussion is related with the human factors in the operational routine and the possibility of control loss due to failure of barriers, such as procedures or interfaces between men and machines.

The characteristic failure of the socio-technical system, systemic failure, is the result of behavioral heuristics resulted from human errors, incorrect decisions and bad habits related to processes, equipment and products. Thus, the operating culture has relations with the task and the informal rules acquired in the operation.

Knowledge about systemic failure allows integrating the calculation of reliability from factors that connect the different functions (maintenance, operation, process, people, culture and leadership). This systemic failure is constructed as a result of structural design deficiencies or operational.

These deficiencies,

- ✓ are result from improper cultural characteristics and affect safety
- ✓ occur due to individual failure triggers at specific points in the production system.

Management models, that control dynamic risk resulting from human factors, social and climate change, are presented to reduce the probability of failure and energy loss.

The application of task failure analysis [6] techniques in advanced systems increases the identification of the causal nexus, verifies where and how much the hazardous energy flow, analyzes the cost-benefit of installing barriers, and tracks the results.

Therefore, root cause investigation should be considered in complex systems where latent failures occur in the human, managerial, organizational, and technical dimensions. This research recognizes systemic failure and indicates the characteristics that are repeated in the risk installation. The research base material is the shift book that contains process, production, safety, maintenance, environment, and personal data from the work team. After task diagnosis and variables, it is possible to predict the production behavior indicating the revision of barriers from the use of mathematical modeling.

Barriers must be studied to prevent failure, incident, accident and also the crisis caused by a disaster. Thus, it is important to analyze the cognitive gaps for emergency contingency team.

1.6 Reliability Calculation - Systemic Bayesian Network

In complex systems, the quantification of human reliability occurs considering that, the characteristics of the System are connected by energy, mass, flow data that are collected, processed, and represent the current state of each function in reliability. In the event of a systemic failure it must be considered that the individual reliability functions are integrated and what is the level of impact on the top event occurrence [9].

The Bayesian networks based reliability calculation method is best suited because it represents the complex relations between performance factors and events that include modeling uncertainty [10] as well as providing flexibility to the component variables of a system and representing the dynamic nature of the human-machine interface [11]. The discussion on Bayesian Networks of Human Factors and Hazard Energy Enablers indicates which design criteria are involved with human elements, which barriers may degrade over time, and the likely human factors that hazard energy can course through routine structures and processes of critical activity in the industry and highly complex services.

2 Methodology

This experimental methodology develops tests to calibrate a systemic failure model. This model resulted from the discussion of human and technical errors in the execution of the task by authors [4], [5], [12] and from the confirmation of process safety managers and specialists in the Chemical Industry. Model calibration is done as part of an operational mass awareness training on the causes of human error in the dimensions: principles, cognition, work and human factor management. This discussion aims to relate the responses of the operation to the amount of hazardous energy flow. The steps of this methodology are:

(1) Theoretical Systemic Failure Model: life cycle; (2) Identify Operational and Technological Context; (3) Model Adapted to Model Applied in Context; (4) Sensitize and provoke paradigms: concept, scenario, situation and decision-making - risk perception issue; (5) Model Analysis Adapted with Intensity and Visibility of Human Factors; (6) Identify Hazard Enabling Factors and

Failure Processes; (7) Define Specific Bayesian Network Architecture with Intensity and Visibility; (8) Develop Failure Energy Algorithms.

The classification and prioritization of human, organizational, managerial, social and technological factors indicate what are the most important factors and the relationships between them in a systemic failure model. This model that attempts to approach the complexity of multiple dimensions and pathways for energy loss is the starting point for consensus with the shift group to define a more real model of what happens.

This work is initially divided into six levels:
(L1) Project and Product - physical configuration, technology demands and requirements;
(L2) Management Aspects - leadership, work organization, stress level, conflict between policies and practices;
(L3) Safety Behavior (personality, attitude and motivation, dynamic skills, good practices) and C4t (competence, commitment, cooperation and communication).
Nucleation brings together the physical and cognitive interfaces: relationship between human, technical, social and organizational factors bringing effects; human-machine process interfaces in the operational routine, planning and control of the critical task;
(L4) Sociotechnical Culture: organizational, security, global, regional, social phenomenon, just blame, formal and informal workplace rules, information flow;
(L5) Human and social error: deviations, omission, commission, violation, wrong decision, bad habits - rituals, routine and emergency, failure life cycle (feedback);
(L6) Failures and Consequences: routine and emergency, organizational processes and image loss, process losses (time), logistics processes, cost increases, loss of revenue, failure, incident, accident and consequence;

3 Results and Discussions

(1) Theoretical Systemic Failure Model: life cycle

Some assumptions are discussed in the choice of model:

- ✓ we seek the relationships between factors to identify regions with probable human errors, where hazardous energy concentration occurs;
- ✓ the fact that human error exists is not the main problem; the concern is to analyze the impact or intensity to build appropriate barriers that address dynamic threats;
- ✓ by understanding the relationships between factors, it is better to understand how to intervene by changing the form;
- ✓ at high risk learn in practice using simulators for virtual tools;

A Theoretical Model, Figure 1, is suggested for the Chemical Industry indicating types of factors, elements and situations with their characteristics, relationships, visibility and intensity. The human factors and elements that permeate industrial activities are multidisciplinary and dynamic. These factors are directly worker related and include the organization, safety, management and technology dimensions.
Investigating and disseminating knowledge from human error is a form of training adopted by high risk multinationals. The dimensions considered, which is included in the [13] model, and which

are part of the Theoretical Model are: Culture and Organization; Cognition (perception, communication and decision); Technology; Management; Analysis, Measurement and Control of Human Factors and Elements.

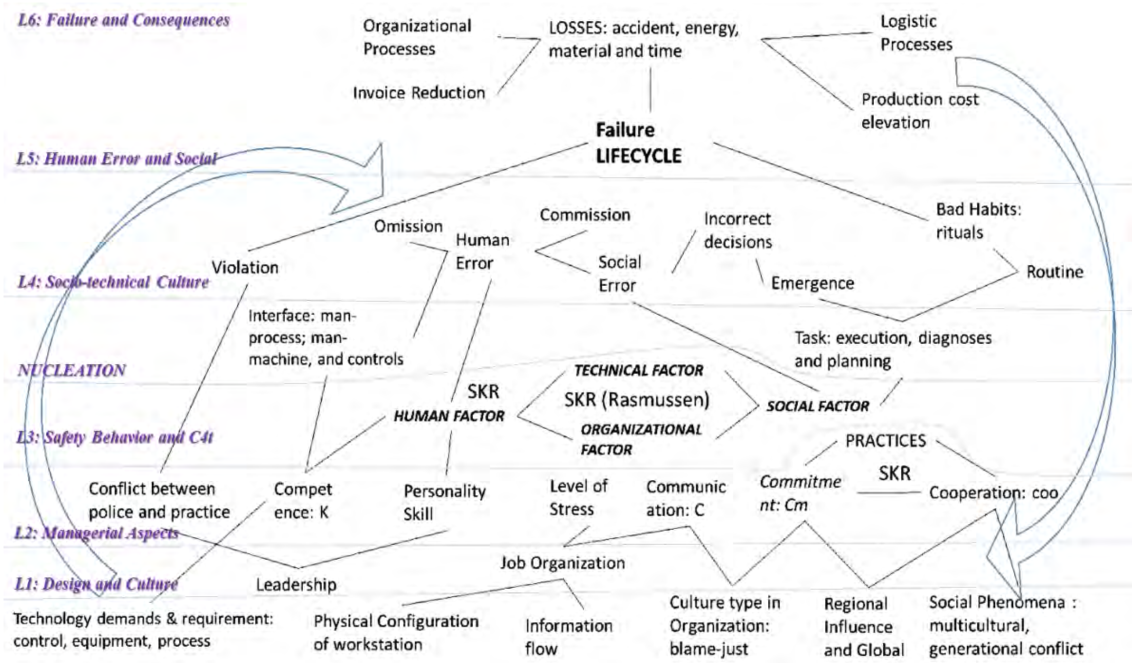


Figure 1 - Theoretical Systemic Failure Model: life cycle

(2) Operational and Technological Context

A questionnaire, visit, reading procedures and reports are conducted to identify the operational and technological context. Context identification is based on plant history, observations, technologies, operation, people, and culture involved in the process.
It is necessary to consult reports, evaluate the workstation and consult manager and operational mass to map the types of failure and cultural aspects of the environment.

TECHNOLOGICAL ASPECTS.
What type of product technology, process technology, process control and process safety? What is the risk level? For the following subjects: product quality, process, activity, billing and accident. What is the complexity of processes, automation, task, recycle - Cognitive effort versus Physical effort by type of function and activity? What are critical technologies and interfaces? Man, process, computer, task and machine?
SOCIAL ASPECTS.
What are the aspects, cultural biases that strengthen or hinder Security? What are the Social Phenomena and Failures that occur in routine with low visibility or evident? Generational conflicts, gender, multiculturalism and others? The type of Linguistics and Communication, underreporting occurs and what is the level of culture of guilt or fair? Analyze accidents and social events. What stress level is installed and why? What type? Physiological or cognitive? How is the team and company compatibility and leaderships regarding the Work Organization? Level of measuring fair culture or guilt: underreporting, omission, commission. What are the impacts of

4Cs: Communication, Competence, Cooperation and Commitment on human error and bad habits. What are the archetypes that reach leaders, supervisors and managers? What is the Leadership style in centralization, listening, determination and resilience? Investigate and describe key Human Factors based on Accident and Failure History - Reporting, Speech, and Observation (operating condition, abnormalities, human factors).

(3) Systemic Failure Model in the Operational Context

According to Figure 1, for analysis of systemic failure, some aspects of the failure life cycle were removed. *We removed:* (L6) invoice reduction, logistic processes (L5) incorrect decisions (L4) violation, emergence (L3) competence (L1) physical configuration of workstation, social phenomena: multicultural, generational conflict.
Because: this chemical industry in analysis is new, the product is new, the managers and supervisors have experience in failure and human errors, the technology is advanced, the best, the team development was harmonized without formation of little politic groups.
We installed: We could install some different facts as excessive discipline in Japanese culture, but it is not the case.
Because: is not the case.

(4) Sensitize and provoke paradigms: concept, scenario, situation and decision making - risk perception issue.

To improve the risk perception was applied a methodology what will be able to make a diagnosis based in principal principles and risk, cognition and practices, workstation and human factors. In the Figure 2, we can map the different question levels involved in this stage. This is the beginning of the Bayesian network construction according to the chemical industry's operating routine.

The questions were elaborated in different dimensions. **The culture**: what are the accepted principles and what are the weaknesses and strengths for security; **The operation**: where cognitive functioning is related to routine practices that can lead to an accident - causes and consequences of risk perception; **The project**: an analysis of what criteria are appropriate for the workstation during the routine including panel and field actions; **The management**: where human factor risks and team and leadership characteristics are discussed by 4Cs, complexity, technology and measurements. Human and organizational factors run through these dimensions and are verified through the response of the provoked situations.

Questions elaborated should be related with failure, risk, culture and human factors. The research is done in all operational mass and the perception on the answer will indicate the energy hazard intensity of human factors (operational charge) or human elements (resistance).

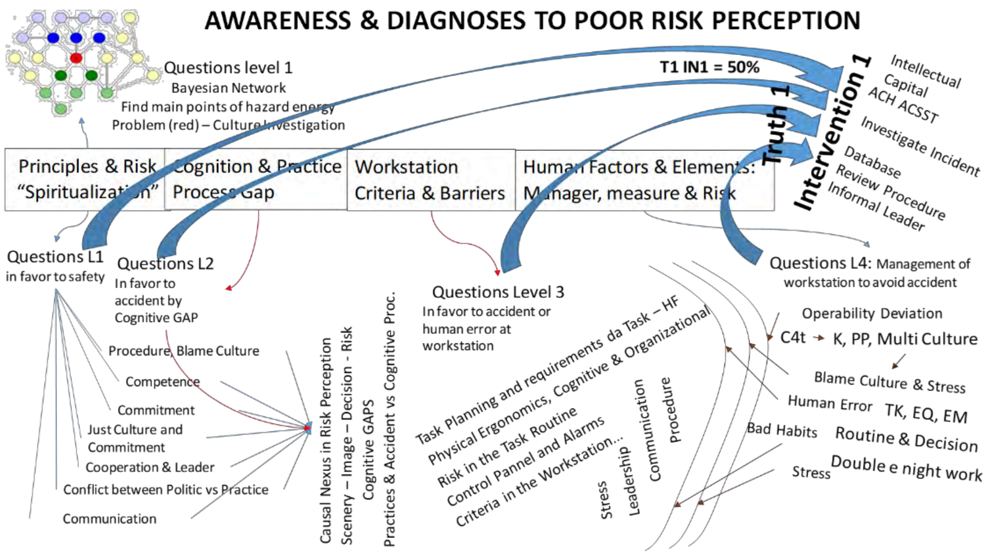


Figure 2 - Awareness & Diagnoses to Poor Risk Perception

(5) Model Analysis Adapted with Intensity and Visibility of Human Factors

Human social and technical organizational factors, raised from the literature review [4], [5], [12], [14] and expert opinion brought a list of factors and elements for the creation of the questionnaire. From this questionnaire (4) the factory factors were raised and measured by the intensity.

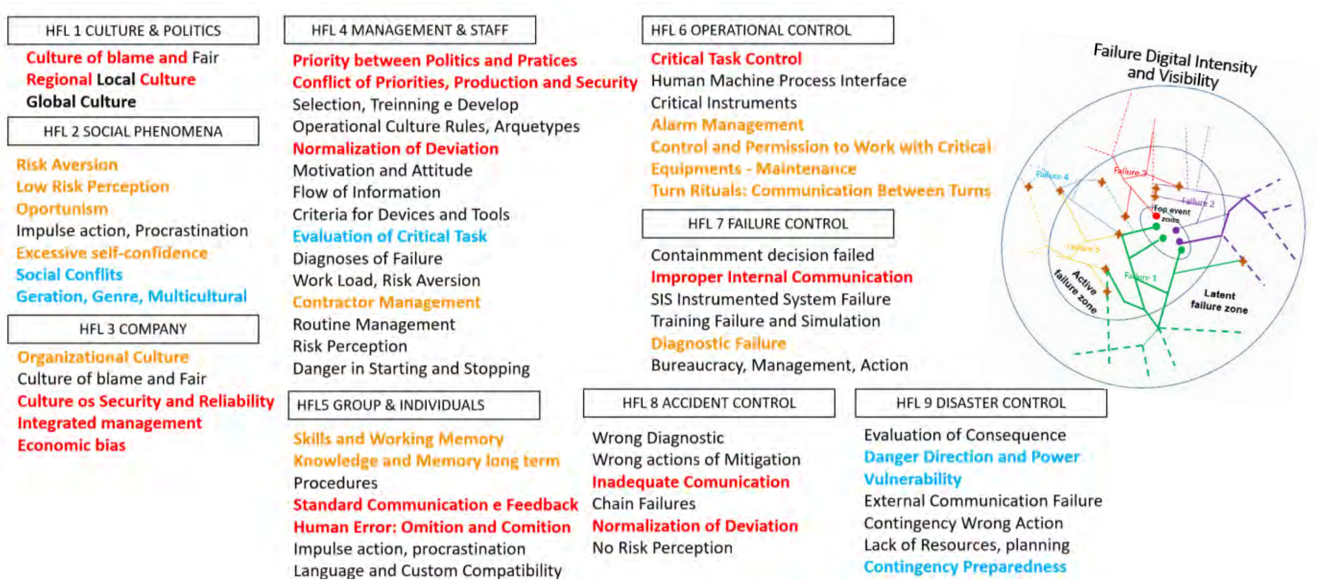


Figure 3 - Model Analysis Adapted with Intensity and Visibility of Human Factors

They were rated for the amount of hazardous energy (operating load) for human factors and their ability to resist the passage of this energy through human elements. Red means low ability to resist hazard energy, orange is intermediate, and blue refers to high resistance. In this way the fingertip of the process failure is represented. At this time the visibility analysis was not addressed.

(6) Identify Hazard Enabling Factors and Failure Processes

After the human factors measurement identification, the hazard enabling Factors are indicated. Each human element is analyzed and applied a filter, how can see on Figure 4. Human factors and elements have inverted colors: high flow of hazard energy by human factors is red, low ability to resist the passage of hazard energy is red.

Human Factors: Competence (Comp); Cooperation (Coop); Risk; Complexity (Cpx); Leader; Stress; Behavior (Bhv); Communication (Comm).

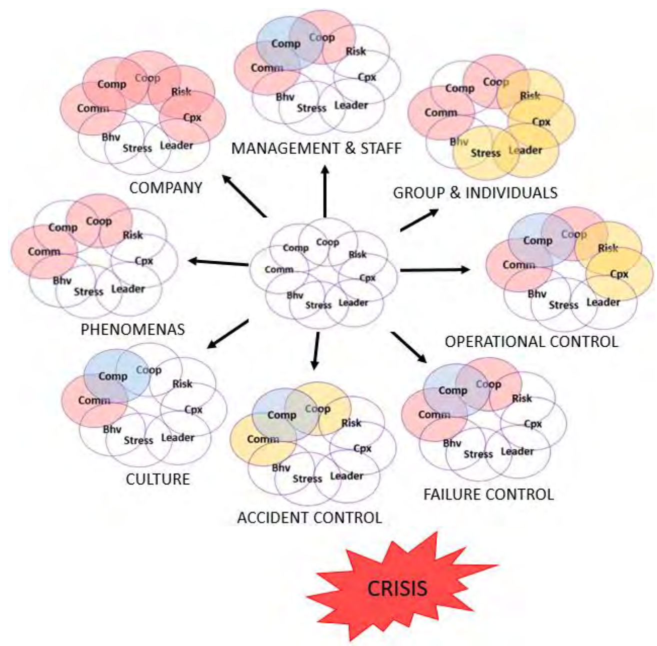


Figure 4 –Hazard Enabling Factors - distribution of resistances or facilities by network level

(7) Define Specific Bayesian Network Architecture with Intensity and Visibility

In this stage is elaborated the Specific Bayesian Network Architecture, Figure 5. In this structure, there are relations and connections between enabling ports.

This setting is dynamic and new factors may disappear or appear and improve or worsen resistance. Aspects such as technological and organizational changes are quite evident for these changes, on the other hand, change of culture and changes of social phenomena in the workplace are not easily visible making it difficult for safety culture makers.

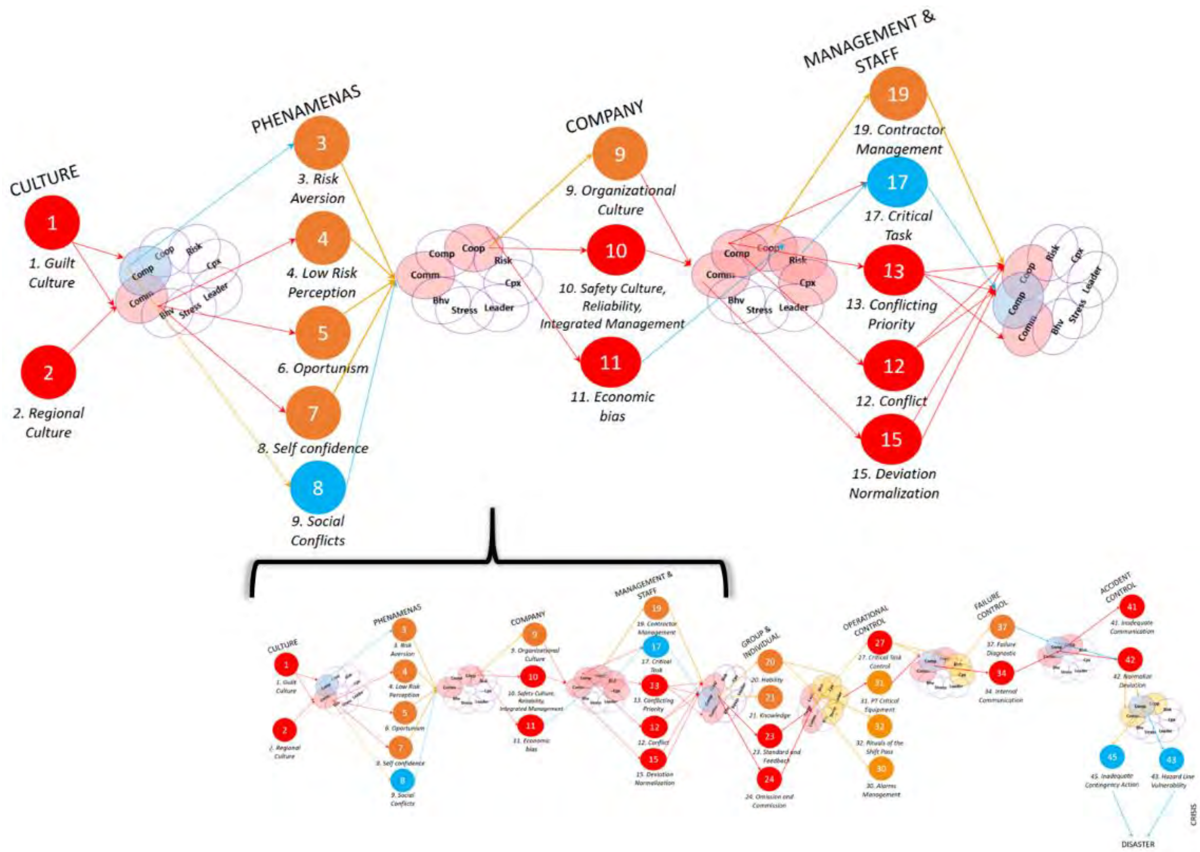


Figure 5 - Specific Bayesian Network Architecture

(8) Develop Algorithms for Failure Energy Calculation between Elements (degraded design) and Factors (operational events);

• Find the relationship between Operation Load and Project Resistance;
• Characterize between impact intensity and factor visibility;
• List project-related issues and operational condition;
• Measuring operator response and through at least 3 ways of addressing the same problem will come interpretations: principle, cognition and practice, job criterion - human errors, human factor management;
• The resultant of resistance to hazardous energy that can be degraded by the environment is the load, or operating pressure to prevent accident;
• Danger Energy Resistance and Load Rating;

Through the answers is indicated how to organize human factors and elements by intensity and visibility, Figure 6.

HUMAN ELEMENT PROJECT		PRINCIPLES*		COGNITION AND PRACTICES		WORKSTATION*		HUMAN FACTOR*	
		VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY
MANAGEMENT	LEADER								
	STRESS								
TECHNOLOGY	RISK								
	COMPLEXITY								
BEHAVIOR	COMPETENCE								
	COMMUNICATION								
	COMMITMENT								
	COOPERATION								
OBSERVATION:									

OPERATIONAL SITUATION HUMAN FACTOR		PRINCIPLES*		COGNITION AND PRACTICES		WORKSTATION*		HUMAN FACTOR*	
		VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY
CULTURE	FAULT								
	REGIONAL								
SOCIAL PHENOMENAS	RISK								
	RISL PERCEPTION								
	OPPORTUNITY								
	SELF CONFIDENCE								
	SOCIAL CONTROL								
COMPANY	ORGANIZATIONAL CONTROL								
	SECURITY CONTROL								
	ECONOMIC BIAS								
OBSERVATION:									

OPERATIONAL SITUATION HUMAN FACTOR		PRINCIPLES*		COGNITION AND PRACTICES		WORKSTATION*		HUMAN FACTOR*	
		VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY	VISIBILITY	INTENSITY
OPERATIONAL CONTROL	TASK								
	EQUIPMENT								
	RITUALS								
	ALARM								
FAILURE CONTROL	DIAGNOSTIC								
	INTERNAL COMMUNICATION								
ACCIDENT CONTROL	INADEQUATE COMMUNICATION								
	DEVIATION STANDARDIZATION								
CRISIS	INADEQUATE CONTINGENCY								
	DANGER LINE								
OBSERVATION:									

Figure 6 - Design: Human Elements & Operation: Human Factors Chosen

4 Conclusions

Human elements are related to *design resistance* while human factors are related to failure or hazard energy during operation, or *operational charge*. This load is dynamic due to the workstation and the types of cultural and behavioral influence within the organizational environment. While resistance is embedded in static patterns that need to be revised due to: the influence of social phenomena, and the degradation of barriers (caused by time and physical attacks).

The operating routine is very dynamic. In this work, the different colors describe the inputs and outputs of the factors in a variable way, since the barriers for the passage of hazard energy interact with each other. Using a qualitative and quantitative methodology with a large challenge due to the dynamism of the process. Thus, for the Bayesian network to function and be validated, the dependence of design elements and human factors must be measured and related.

References

1 Ávila, S. F.; Costa. C. Analysis of cognitive deficit in routine task, as a strategy to reduce accidents and industrial Increase production. Safety and Reliability of Complex Engineered Systemsp. p. 2837-2844. London. (2015).

2 Cerqueira, I.; Drigo, E.; Ávila, S.; Gagliano, M.: C4t: Safe Behaviour Performance Tool. In: Karwowski, W., Trzcielinski, S., Mrugalska, B., Di Nicolantonio, M., Rossi, E. (eds.) Advances in Manufacturing, Production Management and Process Control. AHFE 2018. Advances in Intelligent Systems and Computing, vol .793, pp. 343--353, Springer, Cham (2019).

3 Fragoso, C., Ávila, S. F., Sousa, R., Massolino, C. Pimentel, R., Cerqueira, I. (2017). Blame Culture in Workplace Accidents Investigation: Current Model Discussion and Shift Requirements for a Collaborative Model. In: P. Arezes (ed.), Advances in Safety Management and Human Factors, Advances in Intelligent Systems and Computing 604, DOI 10.1007/978-3-319-60525-8_33. Springer International Publishing.

4 Ávila, S. F. Emergency Decision Model: Accident Analysis of History. In: 8th Center for Chemical Process Safety – CCPS. Universidad Católica Argentina, (2018).

5 Lorenzo, D.K: API 770 – A manager's guide to reducing human errors: improving human performance in the process industries. API Publishing Services, Washington (2001).

6 Ávila, S.; Sousa, C. R.; Carvalho, A. C.: Assessment of complexity in the task to define safeguards against dynamic risks. In: 6th International Conference on Applied Human Factors and Ergonomics (AHFE) and the Affiliated Conferences, Las Vegas. Conference Proceedings; International Conference on Applied Human Factors and Ergonomics, (2015).

7 Embrey, D. Preventing human error: developing a consensus led safety culture based on best practice. London: Human Reliability Associates Ltd. 14p. 2000.

8 Ávila, S.; Mrugalska, B.; Wyrwicka, M.; Souza, M.; Ávila, J.; Cayres, E.; Ávila, J.: Cognitive and Oganizational Criteria for Workstation Design. In: 10th International Conference on Applied Human Factors and Ergonomics (AHFE) and the Affiliated Conferences, Washington D.C. Conference Proceedings Springer; International Conference on Applied Human Factors and Ergonomics, (2019)

9 Ávila, S.; Dionízio, J.: Systemic Fault Analysis to calculate the approximation of the top event (near miss evaluation system): NEMESYS. In: 27th European Safety and Reliability Conference (ESREL). Portoroz, Slovenia (2017).

10 Song, L.: A Bayesian networks approach to build human -machineergonomic risk assessment model for construction workers. MEIE 2018. IOP Conf. Series: Journal of Physics: Conf. Series 1074 (2018) 012151. (2018).

11 Yuan, C.; Lim, H.; Lu, T.: Most Relevant Explanation in Bayesian Networks. Journal of Artificial Intelligence Research 42 (2011) 309-352. (2011).

12 Boring R, Blackman H. The origins of SPAR-H method's performance shaping factors multipliers. Idaho – EUA. August (2007)

13 Reason, J.: Human error. Cambridge University Press, Cambridge (2003)

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Exploration of relationships between safety performance and unsafe behavior in coal mining processes

Trent Parker*[b], Ruipeng Tong*[a], Qingsheng Wang[b], Xiaoyi Yang[a], and Boling Zhang[a]
[a] College of Emergency Management & Safety Engineering, China University of Mining & Technology (Beijing), Beijing 100083, China.
[b] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843, USA.
Presenter E-mails: tongrp@cumtb.edu.cn, qwang@tamu.edu

Abstract

It is well known that safety performance is differentiated to two components, namely, safety compliance and safety participation. However, relationships between safety performance and unsafe behavior were barely explored. In this work, the scales for safety compliance and safety participation were slightly revised for usage in coal mining processes, and job burnout scale was developed on the basis of MBI-GS. Then, structural equation model was employed to investigate the interaction of these factors using samples of 367 front-line coal miners in large state-owned mining companies in China. The results show that individual unsafe behavior could not be diminished significantly by only focusing on these two dimensions of safety performance. Compared with safety participation, safety compliance has more significant influence on unsafe behavior, and job burnout is an indispensable moderator between these two components and unsafe behavior. More importantly, it is vital to pay close attention to employees' occupational psychological health problem for improving organizational safety management and promoting personal performance.

Keywords: Safety compliance, safety participation, unsafe behavior, job burnout

1 Introduction

Safety compliance and safety participation are two widely approved dimensions of safety performance, which introduced by Neal et al. [1,2] on the basis of work performance theory [3]. These two dimensions are different with each other remarkably, for safety compliance refers to the core activities related to safety which need individuals to perform on the purpose of maintaining the safety in their workplace, such as wearing safety equipment. And safety participation refers to individuals voluntarily participating in activities related to safety, that is beneficial to the development of a safety-supportive environment and do not contribute to their personal safety directly, such as helping coworkers [2,4]. The relationship between safety compliance, safety participation and accidents, injuries are explored in various industries. Beyond all question, workers' high level of safety compliance and safety participation will predict a low rate of accident and less injuries. However, the relationship between these two dimensions and employees' unsafe behavior, to the authors' knowledge, has not been investigated. It is unwise to make a hasty conclusion that if one conduct safety compliance and safety participation, then he will not commit unsafe behavior. Thus, the mechanisms by which these two dimensions affect unsafe behavior disturb us a lot. Another question bothered us is which dimension, that is, safety compliance or safety participation, contribute more to the diminishing of workers' unsafe behavior.

Furthermore, by inference, we could infer that safety compliance or safety participation will contribute the reduction of unsafe behavior. The reason may be listed as, on the one hand, as abovementioned, these two dimensions will forecast less accidents and injuries. On the other hand, unsafe behavior is the immediate and primary cause of these safety outcomes. However, on the ground of job demands-resources (JD-R) theory [5,6], safety compliance and safety participation belong to motivation factors, and unsafe behavior pertains to organizational outcomes [7]. The interplay between these two dimensions and unsafe behavior may be impacted by strain factors. Strain factor refers to causes that could undermine employees' energetic resources to reach their work goals, which mostly pay attention to psychological health factors in workplace, for example, job-related anxiety and job burnout [6]. And job burnout is the most representative factors, which belongs to employees' psychological syndrome related to work and has been widely discussed in various groups, such as teachers, nurses. Also, mainly front-line manual workers, for example construction worker and coal worker, suffer from this syndrome [8]. Nahrgang et al. [9] and Tong et al. [7] have reported job burnout could influence workers' unsafe behavior. However, what's the role that job burnout plays on the relationship between safety compliance, safety participation and unsafe behavior, which is barely explored and is another problem interested us a lot. To sum up, what we want to reveal is the interrelationship among safety compliance, safety participation, unsafe behavior and job burnout associated with front-line workers, which on the basis of the industry we have been focused on, that is, construction industry, a pure high-risk and labor-intensive industries.

As one of the high-risk industries worldwide, construction has the characteristics of unique, complex and dynamic [10,11]. Its complex and hazardous project site conditions, dynamic resources involved staff, equipment and materials, combined with the millions employment opportunities it provided differentiate construction from other industries [12,13]. Thus, construction has obtained a lot of attention, also the safety management related to it and the health and well-being of its workers [14]. To improve the safety management, many researches related to various aspects have been conducted, among which included the works associated with employee' safety compliance, safety participation and unsafe behavior, especially for the front-line workers. And lots of efforts have been devoted to investigate variables which influence the abovementioned factors [15], also, the relationships between these factors and accidents and injuries have been explored. However, the relationship between safety compliance, safety participation and unsafe behavior, resemble other industries, has been ignored. What more, the job burnout gets more and more attention in this industry recently, some valuable works have been done [16-19]. But these mainly focused on project managers or site engineers, the special empirical study for construction workers related to their job burnout was lacked, let alone the role burnout plays on the relationship between these two dimensions of safety performance and unsafe behavior.

Therefore, with this background, focusing on construction workers in the Chinese context, at first, the interaction among the aforementioned factors are identified and the hypotheses are presented on the ground of literature reviewing. Then safety compliance and safety participation scales are slightly adapted, and job burnout scale are developed for use in the worker's sample. Third, a survey is performed that sampled construction workers and based on which a quantitatively analysis is conducted to examine our hypotheses. Further, an in-depth discussion is performed and some recommendations are provided to effectively manage employees' unsafe behavior and improve their safety, health and well-being.

2 Literature Review and Hypotheses

2.1 Safety compliance, safety participation and unsafe behavior

Safety performance was traditionally measured by accident rates, fatality rates or TRIFR (total recordable injury frequency rate) [20]. However, these measures are all lag indicators and have been blamed because they are reactive naturally, "insufficiently sensitive, of dubious accuracy, retrospective, and ignore risk exposure" and cannot provide early warnings of injuries or accidents [21,22]. Thus, leading indicators are introduced to better measure safety performance [23]. Among which, safety compliance and safety participation are useful indicators and have been widely approved [1,2,24].

Having a review to the works related to these two dimensions, we can find that, safety compliance and safety participation are generally treated as mediators and outcome variables. Either they are proposed as mediators or outcome variables, the predictors mainly focus on safety climate and safety leadership, both of which will contribute to workers' favorable performance [25-27]. And it is worth mentioning that the researches related to safety leadership primarily pay attention to transformational and transactional styles. When they are treated as mediators, the safety outcomes mainly focus on accidents and injuries, and as mentioned, safety compliance and safety participation are the useful antecedents of the reduction of these two undesirable results.

Apropos of unsafe behavior, the fact that it is the immediate and primary cause of accidents and injuries is beyond any doubt. Combined with the reviewing back of safety compliance and safety participation as abovementioned, we could forcefully deduce that both of these two dimensions would have a negative effect on unsafe behavior. Thus, hypothesis 1 and 2 could be formulated and presented as followed.

Hypothesis 1: Safety compliance of construction workers is negatively related to their unsafe behavior.

Hypothesis 2: Safety participation of construction workers is negatively related to their unsafe behavior.

Then, considering the characters of construction workers, they consist basically of migrant workers who come from countryside, poorly educated, unskilled and inexperienced. And the general pattern of their families is the male labor force comes out alone and is hired as construction worker to win the bread of his family, leaving other family members home. Thus, the burden of raising the whole family is extremely heavy which make them deem very highly of the financial payback, and the more schedules they finish the more wages they will get. Therefore, it is not uncommon for these workers to scarify the voluntary safety activities (i.e. safety participation) to a larger degree than the core safety activities (i.e. safety compliance) for the duration of finishing the work schedules, combined with safety compliance is generally required and always directly related to intangible (e.g. verbal praise or abuse) or tangible (e.g. bonus or fine) reward or punishment, especially the latter, hence hypothesis 3 could be formulated and listed as followed.

Hypothesis 3: Compared with safety participation, construction workers' safety compliance is more significantly related to their unsafe behavior.

2.2 The role of job burnout

To describe the psychological syndrome that employees prolonged response to chronic emotional and interpersonal stressors on their job, job burnout was coined, and it is predominantly defined by three main components, that is, exhaustion, cynicism and low professional efficacy [28,29]. The first component refers to employee's feelings of being overextended and depleted of his or her emotional and physical resources, and this component pictures the basic individual stress dimension of job burnout. And the second component refers to employee responses to his or her job in a negative, hostile, or an excessively detached attitude, also a loss of idealism is often included, and this component pictures the interpersonal dimension of job burnout. Then, the third component refers to employee declining feelings of competence and productivity at his or her work, and this component pictures the self-evaluation dimension of job burnout.

It is reported that construction workers [30] suffered from job burnout and burnout would contribute to their unsafe behavior [9]. Nahrgang et al affirmed that the correlation relationship between compliance (which was defined equal to safety compliance), engagement (equal to safety participation) and burnout was negative [9], but the specific relations among these factors and unsafe behavior were not mentioned. However, what we attempt to discover, which is also unclear and barely delved, is the specific role job burnout plays on the relationship between safety compliance, safety participation and unsafe behavior. There are two roles job burnout may act, that is, mediator and moderator. A mediator refers to a variable which explains the relationship between a predictor and an outcome, and a moderator refers to a variable which alters the strength or direction of the relationship between a predictor and an outcome [31,32]. It is inescapably clear that job burnout cannot be a mediating role either between safety compliance or safety participation and unsafe behavior. Thus, job burnout could be conjectured act as a moderator between these two dimensions and unsafe behavior. To be detailed, the negative effects between safety compliance or safety participation and unsafe behavior would be intervened by job burnout, and the moderator effect may depend on the significant of job burnout. Due to these, hypothesis 4 and 5 could be formulated and presented as followed. What's more, in contrast to the justifications we proposed hypothesis 3, we formulated hypothesis 6, which is also presented as followed.

Hypothesis 4: As for construction workers, all the three components of job burnout, namely, exhaustion (4a), cynicism (4b) and low professional efficacy (4c) significantly moderate the relationship between safety compliance and unsafe behavior.

Hypothesis 5: As for construction workers, all the three components of job burnout, namely, exhaustion (5a), cynicism (5b) and low professional efficacy (5c) significantly moderate the relationship between safety participation and unsafe behavior.

Hypothesis 6: Compared with the relationship between safety compliance and unsafe behavior, the relationship between safety participation and unsafe behavior is more significantly influenced by all the three components of job burnout, namely, exhaustion (6a), cynicism (6b) and low professional efficacy (6c).

The theoretical model which could illustrate these relations are showed as Figure 1. It presents the influence of two antecedents, namely safety compliance and safety participation on unsafe behavior. Also, it shows the moderator between these two antecedents and unsafe behavior, that is job burnout.

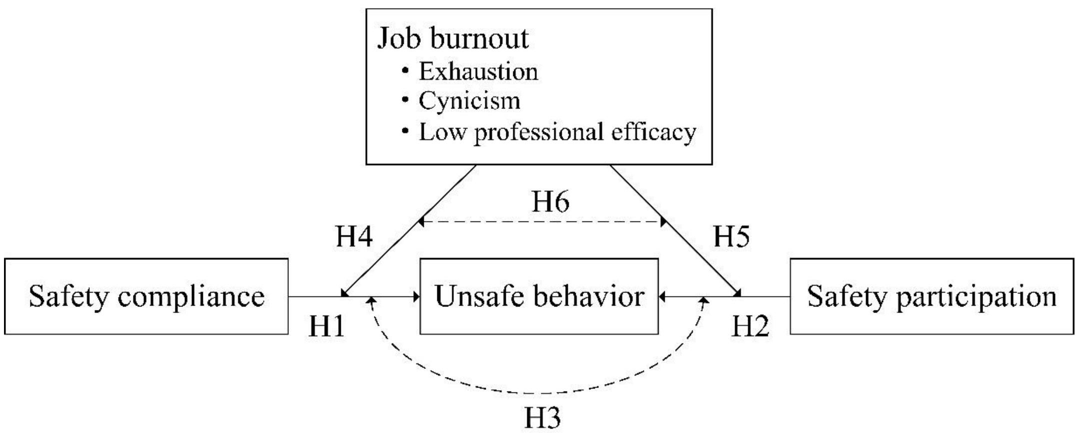


Figure 1- The theoretical model in this study

3 Methodology

3.1 Measures and instruments

The scales and questionnaires include safety compliance and safety participation scales, job burnout scales, and unsafe behavior scales, based on which the questionnaires were developed. A 5-point Likert scale was adopted, which scored from 1 (completely disagree) to 5 (completely agree).

3.1.1 Safety compliance and safety participation

To assess safety compliance and safety participation, several peers had developed scales, such as Neal et al. [1,2], DeArmond et al. [33] and Guo et al [23], among which the scale developed by Neal et al. is the most widely employed. Generally, this scale was revised for use in the participants which were sampled. Considering the participants which we sampled, to suit construction workers' characteristics and real scene, also the Chinese culture, the scale adopted in our work was also revised.

Firstly, the draft scale, which involved the contents and substance of safety compliance and safety participation, was obtained based on Neal et al. [1,2]. And secondly, this initial scale was discussed with 10 squad leaders and 5 full-time safety inspectors who came from two ongoing construction projects which belonged to Crland company and sited in Beijing, China. Crland is a large state-owned real estate enterprise, which employs at least 30, 000 staff and has more than 229 projects sited in 60 cities in China by the end of 2017. The former, who also is one of the members of his team and may come from the same rural area with the other co-workers, is generally responsibility for the work safety and acts as a front-line safety supervisor, and is in charge of the work schedule as well. While, the latter is employed to supervise construction workers, including the squad leaders, and their only duty is to ensure work safety. The common ground is both of them are familiar with the safety and the group of workers. And two-thirds them are construction worker. All of these was to insure the effective of these discussions, and some value information were got, hence to ensure the revised scale was readable, having good face validity and friendly.

Then, according the advices we obtained, all the items of safety compliance and safety participation were weighed and some revises were conducted, for instance, some words were replaced and some examples were given to make the expression clearer. After finishing this, on the purpose of examining the available and quality of the scale, a sample of 100 construction workers from the same two projects which we invited squad leaders and safety inspectors, each project provided half the samples, were invited to perform a pilot survey. Finally, a total of 87 responses and 79 valid responses, which respectively account for 87.0% and 90.8%, were received. Once again, the items were slightly altered and the item-to-total correlation of all the items exceeded 0.40 on the basis of examination of reliability and correlations [24], the employed scale was presented in Table 1.

Table 1 The scale of safety compliance and safety participation

Components	Items	
Safety compliance	SC-1	I use all the necessary safety equipment to do my job, such as keeping safety helmets even if it feels uncomfortable
	SC-2	I follow the required safety rules and procedures to carry out my job, such as safety operational instructions
	SC-3	I ensure the highest levels of safety when I carry out my job, such as checking the environment to before doing my work
Safety participation	SP-1	I always point out to my squad leader or safety inspector if any safety related matters are noticed
	SP-2	I put in extra effort to improve the safety of my work, such as reforming the way the job is done to make it safer
	SP-3	I voluntarily carryout tasks or activities that help to improve workplace safety, such as attending non-mandatory safety-related meetings

3.1.2 Job burnout

To assess job burnout, there are also several scales, such as MBI (Maslach Burnout Inventory) [34], OLBI (Oldenburg Burnout Inventory) [35], BM (Burnout Measure) [36] and S-MBM (Shirom-Melamed Burnout Measure) [37]. Among which the serious of MBI are the most popular and widespread, and this instrument involves 3 distinct versions and can be further differentiate to 5 specific versions [34]. To be detailed, the MBI-HSS (Human Services Survey) which for healthcare professionals and MBI-ES (Educators Survey) which for teachers were initially developed, then focusing on general occupations, the MBI-GS (General Survey) was developed. Afterwards, MBI-HSS was further revised and MBI-HSS(MP) for Medical Personnel was introduced, and MBI-GS was revised for students, the MBI-GS(S) was introduced.

Employed MBI-GS, many researches related to job burnout have been performed in different occupations. However, it was recommended that this instrument which surely was a perfect fundamental scale to measure burnout should be further developed on the basis of characters the specific occupation, especially for construction [19]. Yang et al. have developed an occupation-oriented burnout scale for Chinese construction project managers based on MBI-GS [19]. However, focusing on construction workers in China, to our knowledge, there isn't the special scale to assess their job burnout. Thus, on the same ground of we revised the scale of safety compliance and safety participation, the job burnout scale was developed based on MBI-GS.

Firstly, 10 squad leaders and 5 construction workers were invited to respectively discuss their experience and symptoms of job burnout and each interview lasted for about 1 to1.5 hours. After finishing the interview, the three components of burnout and all the items of MBI-GS were showed to them to have another discuss. The education level of the participants was junior high school or high or technical secondary school, and their work experience varied from 10 to 20 years with an average of 12.5. Hence, we could make sure that their education level can represent the level of their group and they can grasp the purpose of the interview and hence provide some valuable suggestions. Also, their work experience in this industry could ensure them in-deep understanding the particular of this industry.

After finishing these interviews, a total of 37 symptoms which were related to their job burnout and 9 suggestions which were advised to revise the items of MBI-GS were earned. To have an in-depth analysis of these results, it was found that construction workers' symptoms were well covered by the three components of job burnout, that is, exhaustion, cynicism and low professional efficacy. Thus, the draft scale of job burnout for construction worker were developed, which contained 19 items. In order to cover all the symptoms related to burnout experienced by the workers, 3 items were extracted from OLBI, BM and MBI-HSS. Due to the gaps of different culture and linguistic expression, all the items were revised to make them more readable and intelligible to construction workers in China.

Then, a pilot survey was conducted to examine the available and quality of the scale, same to safety compliance and safety participation, the sample of 100 construction workers from two projects were invited. And a total of 87 responses and 76 valid responses, which respectively account for 87.0% and 87.4%, were received. Based the survey, the exploratory factor analysis was performed, in other words, the principal component analysis was conducted to get the factor-loading matrix, which employed SPSS 24.0. And the Kaiser-Meyer-Olkin value, which was 0.887, was got to insure the appropriate of the analysis. To obtain the final scale, four principles were followed, which also adopted by Yang et al. [19].

It showed that to assess the three components of job burnout, that is, exhaustion, cynicism and low professional efficacy, 5, 6 and 5 items were needed, respectively. Therefore, a total of 16-item scale which aimed to measure job burnout of Chinese construction worker was obtained. And it accounted for 82% of the total variance. Apropos of the reliability index, the Cronbach's alpha (α) was got, which was 0.863, and we obtain the Rotated Component Matrix, which was showed in Table 2.

Table 2 Rotated component matrix of the job burnout scale for construction worker

Items		Components		
		EX	**CY**	**LPE**
EX-1	I feel tired and fatigued after work	0.889	—	—
EX-2	When I get up in the morning and have to face another day with my job, I feel exhausted before I've even started	0.866	—	—
EX-3	My job makes me feel emotionally drained	0.831	—	—
EX-4	Working all day is really a strain for me	0.829	—	—
EX-5	I am so weak and susceptible to illness	0.757	—	—
CY-1	I always express negative emotions at work	—	0.861	—
CY-2	The meaning of my work is doubtful	—	0.841	—
CY-3	My job bored me a lot	—	0.839	—
CY-4	I feel less and less interested in my job since I was employed	—	0.752	—
CY-5	I have become more cynical about whether my work contributes anything	—	0.703	—
CY-6	I just want to finish my work and not be bothered by other co-workers or things	—	0.702	—
LPE-1	I am able to effectively solve the problems in my work	—	—	0.769
LPE-2	I feel I am making effective contributions to what my company does	—	—	0.698
LPE-3	I am good at my job	—	—	0.689
LPE-4	I feel exhilarated after I dispose of the problem in my work	—	—	0.677
LPE-5	I will feel comfortable when I complete the task effectively	—	—	0.675

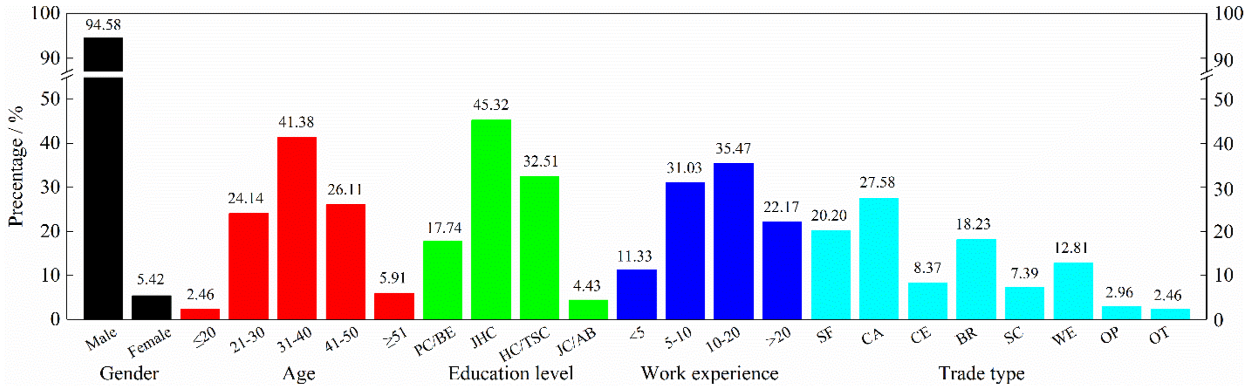
Note: EX: Exhaustion, CY: Cynicism, LPE: Low professional efficacy

3.1.3 Unsafe behavior

To assess unsafe behavior, according to the method provided by Stride et al. [38], the self-report method was conducted, that is to say, construction workers' experiences of unsafe behavior were asked to recall with a span of the recently four weeks. There are two questions related to their unsafe behavior were asked, showed as "In the past four weeks, how many times unsafe behavior of yourself can you recall when you conduct your job" which related to themselves, and "In the past four weeks, how many times unsafe behavior of your co-workers can you recall when they conduct their job" which related to others. It is worth mentioning that a period of four-week was selected was suggested by Warner et al. [39] and Landen and Hendricks [40]. To meet the 5-point Likert scale, the results of unsafe behavior were standardized, to be detailed, 1 to 5 point represent the times respectively were 0 to 10, 11 to 20, 21 to 35, 36 to 50 and above 50.

3.2 Participants

The construction workers of the two ongoing construction projects were invited to participate in our empirical study, and finally 287 questionnaires were distributed. After finishing the survey, 236 responses and 203 valid responses, which respectively account for 82.2% and 86.0%, were received. The demographic distribution of the samples was showed in Figure 2. Almost all the respondents were male with the age of 20 to 50, and the education level of them were junior high school or high or technical secondary school. Most of them, which accounted for about 80%, had approximately more than 5 years working experience, and almost all the types of workers were included.



Note: PC/BE: Primary school or below, JHC: Junior high school, HC/TSC: High or technical secondary school, JC/AB: Junior college or above
SF: Steel Fixer, CA: Carpenter, CE: Cement worker, BR: Bricklayer, SC: Scaffolder, WE: Welder, OP: Operator of tower crane, OT: Other

Figure 2 - Demographic characteristic of the participants (N=203)

4 Results and Analysis

4.1 Statistical analysis

A confirmatory factor analysis was conducted to test the reliability of the hypothetical model. As illustrated in Table 3, all the values of factor loadings and Cronbach's alpha (α) exceeded 0.6. Thus, it showed that all the factors and dimensions, which involved in the hypothetical model we developed, were considered reliable.

Table 3 Confirmatory factor analysis of the factors in this study

	Safety compliance	**Safety participation**	**Job burnout**		
			Exhaustion	Cynicism	Low professional efficacy
Loading	0.817	0.826	0.821	0.793	0.765
α	0.805	0.809	0.801		

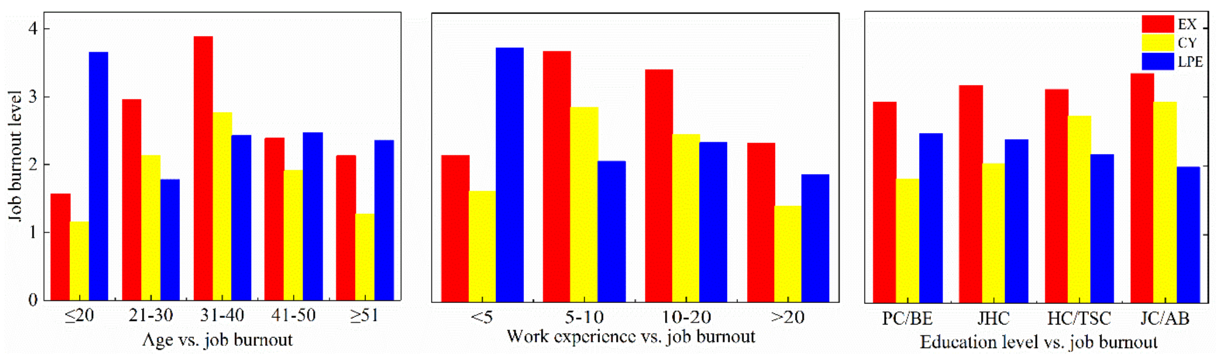
When it comes to the level of safety compliance, safety participation, unsafe behavior and job burnout, they were all presented in Table 4. We could find that construction workers have a high level of safety compliance and a medium level of safety participation with the values of 3.84, 2.49 respectively. The higher value of safety compliance indicated that it is the core safety activities in some degree, which is in consist with the previous works [2,15,41]. And according to the construction workers' self-report, the level of their unsafe behavior was relatively high with an average of 3.12, which means their unsafe behavior times were about 30. But it is noteworthy that this may be biased, to be detailed, it may be lower than their real level, the reasons may be listed as, on the one hand, they may conceal the truth for fear of being punished, on the other hand, they may forget or ignore some types of unsafe behavior.

Based on the recommendations provided by Maslach [42], the average item score of each component related to job burnout was employed to represent the level of construction workers' burnout. Maslach also pointed that a value exceeds 2.70 and 1.80 for exhaustion and cynicism are high, and a value less than 3.30 are low [42]. When it comes to construction worker, these three values were respectively 3.11, 2.26 and 2.31, which showed actually high level of job burnout.

Table 4 The level of the factors in this study

	Safety compliance	Safety participation	Unsafe behavior	Job burnout		
				Exhaustion	Cynicism	Low professional efficacy
Observed	3.84	2.49	3.12	3.11	2.26	2.31
Level	High	Medium	High	High	High	Low

Further, the relationship between construction workers' age and their job burnout level were compared, as showed in Figure 3, also the work experience and education level, which were showed in the same illustration. As we can see, workers between 21 to 50 years, who were the main body of construction workers, had the higher level of burnout, among which workers between 31 to 40 years had the highest level of exhaustion and cynicism, and the workers between 21 to 30 years had the lowest level of low professional efficacy. We could also find that workers who had an experience of 5 to 20 years had the higher level of burnout, and these who had a 5 to 10 years of experience had the highest level of exhaustion and cynicism and the lowest level of low professional efficacy. However, there was no significant difference between education level and job burnout.



Note: EX: Exhaustion, CY: Cynicism, LPE: Low professional efficacy
PC/BE: Primary school or below, JHC: Junior high school, HC/TSC: High or technical secondary school, JC/AB: Junior college or above

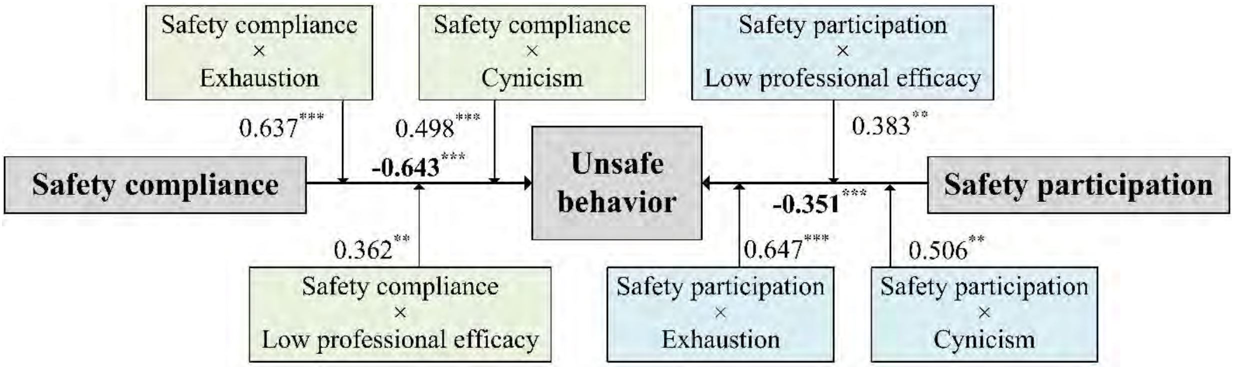
Figure 3- The relationship between age, work experience, education level and job burnout

4.2 Hypotheses testing and analysis

A regression analysis was performed to examine the hypothetical model employed SPSS Amos 24.0, hence the accepted model was obtained and showed as Figure 4. To test the hypotheses, the significant levels were also present in Figure 4. Then, in order to test the fitness of the model, the fit indices were got, as illustrated in Table 5, which showed a relatively high level of fit.

Table 5 Fit indices of the accepted structural equation model

Index	GFI	RMR	RMSEA	AGFI	NFI	CFI	IFI
Value	0.902	0.074	0.087	0.876	0.887	0.893	0.892
Evaluation	Good	Moderate	Moderate	Good	Good	Good	Good



Note: **P<0.01, ***P<0.001

Figure 4 - The accepted hypothetical model in this study

4.2.1 Relationships between safety compliance, safety participation and unsafe behavior

Hypothesis 1 and Hypothesis 2 proposed that construction worker' safety compliance, safety participation should be negatively related to their unsafe behavior, respectively. To the former, the results strongly supported it, because safety compliance was significantly related to unsafe behavior. Also, the results supported the latter, but the significant was a little low. Then, comparing the negative effect of these two dimensions on unsafe behavior, we could find that safety compliance contributes more to the diminishing of worker' unsafe behavior, thus Hypothesis 3 was supported. To sum up, the results were supportive of Hypothesis 1 to Hypothesis 3.

To some degree, this result echoed the previous works which explored the relationship between safety compliance, safety participation and accidents and injuries, such as Clarke [43] and Hon et al. [41]. In high-risk industries, the construction included, both safety compliance and safety participation are critical to organizational safety management [44]. And these two dimensions are related with each other, the former is workers' in-role, mandatory performance and directly associates with the health safety themselves, and the latter is workers' extra-role, voluntary performance and can supports organizational overall safety [2,15]. Thus, both of them can block employees commit unsafe behavior.

However, the negative significant of safety compliance and safety participation on unsafe behavior is different. The reason may be listed as, on the one hand, firstly, although these two dimensions are related, they are inherently distinct [2]. Based on the work performance theory, similar to task performance, safety compliance is formal required, thus, with specified requirements, which make this activity be understood and undertaken easily by employees. On the contrary, similar to contextual performance, safety compliance is informal required, hence, without clear requirements [2,15]. Then, employees' compliance activities are generally monitored by their supervisors, while their participation activities are mainly discretionary. Thirdly, the former is directly related to workers' health and safety, more importantly it associated with their salaries, while the benefits brought by the latter for workers are always indirect and ambiguous [1].

On the other hand, first, given the context of construction, some factors which may impact workers' activities related to compliance and participation are intrinsic and cannot be abated, such as poor workplace environment, risks and hazards, high work pressure. Second, due to safety measures may entail modest benefits while immediate costs, unsafe behavior occurs [41]. Third, which is more significant, unsafe behavior is naturally strengthened, which may attribute to individual tends to deem very highly of short-term results, in orders words, the fruits of taking a shortcut is immediate and motivating, for instance, conducting the jobs with less time and efforts [41]. Therefore, construction workers perform a higher level of safety compliance, which consistent with the previous studies, for example Xia et al. [15] and Lyu et al. [45]. Further, these can explain why safety participation has lower effect on unsafe behavior, which in a sense conform with Hon et al. [41] and DeArmond et al. [33] as well.

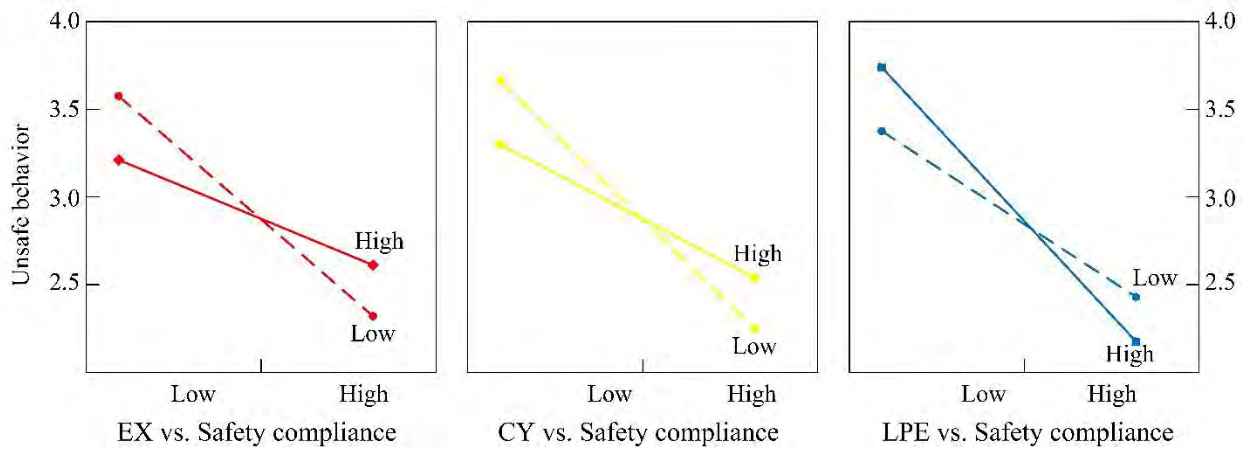
4.2.2 The moderating role of job burnout

Hypothesis 4 and Hypothesis 5 predicted that the relations between construction workers' safety compliance, safety participation and unsafe behavior were moderated by their job burnout. As showed in Figure 4, all the three components of job burnout had significant influence on the relationships, thus Hypothesis 4 and Hypothesis 5 were supported. However, the difference between these two moderate effects were insignificant, which demonstrated Hypothesis 6 was rejected, that is to say, workers' job burnout had the same influence on altering the strength between the two dimensions of safety performance and unsafe behavior.

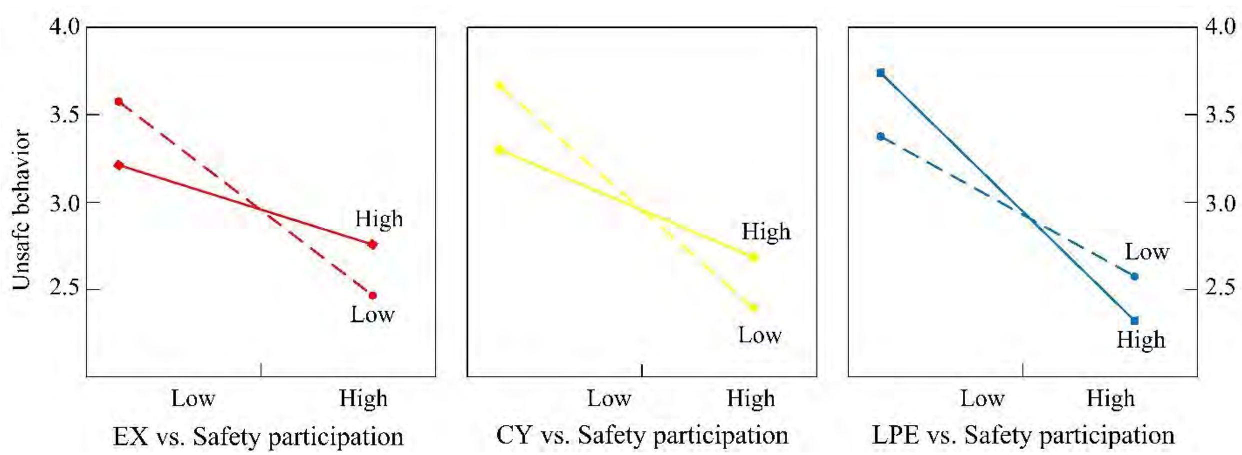
To have an in-depth exploration of the moderating role that job burnout plays, the simple slopes which could present the moderating effect of the three components involved in job burnout on the relationship between safety compliance and unsafe behavior were depicted in Figure 5 (a). As can be seen, in pace with the ascending of construction workers' safety compliance, their unsafe behavior descended. However, the downtrend was undermined by workers' job burnout, firstly, under conditions of high burnout, to be detailed, high level of exhaustion and cynicism and low level of professional efficacy, construction workers exhibited relatively higher unsafe behavior. Secondly, compared the downtrend, it could be found that the slopes related to exhaustion were the slowest, then that related to cynicism followed, and finally was slopes related to low professional efficacy. Then, it could be found that the slopes related to high job burnout tend to have slower downtrend when compared these two slopes associated with the same components of burnout. Also, the resemblant phenomenon could be found in Figure 5 (b), which presented the moderating role of job burnout on the relation between the other component of job performance on construction workers' unsafe behavior.

Furthermore, compared the slopes in Figure 5 (a) and (b), it could be found that, under conditions of the same job burnout, in the wake of the rising of construction workers' safety compliance and safety participation, the slopes related to their participation present higher level of unsafe behavior, and these slopes showed slower downtrend. As the abovementioned which compared the difference of safety compliance and safety participation and their effect on workers' unsafe behavior, these findings were also the evidence. Moreover, these were supportive of Hypothesis 3 in a sense.

As an "occupational phenomenon", which specifically refers to employees' psychological syndrome in the occupational context [46], job burnout will impact workers' job outcomes, for instance, absenteeism and turnover intention, also workers' safety outcomes. Thus, the relationships between construction workers' safety compliance, safety participation and job burnout were undermined by their burnout. The mechanism may be described as the characteristics of the construction industry, such as the prolonged monotonous jobs and high work intensity, would make the worker undergo exhaustion and energy depletion, then, their mental distance to the job would increase and they may feel negativism or cynicism, and their professional efficacy would be lower and lower with this syndrome worse and worse. Combined with the aforementioned, briefly, both the intrinsic factors of this industries and the naturally reinforced unsafe behavior, these all cause the strength between construction workers' safety compliance, safety participation and their unsafe behavior was abated by their job burnout. What's more, the reasons why the difference of the moderating effect of burnout on the above two relationships was no significantly may be the same causes as well.



(a) The effect on the relationship of safety compliance and unsafe behavior



Note: EX: Exhaustion, CY: Cynicism, LPE: Low professional efficacy

(b) The effect on the relationship of safety participation and unsafe behavior

Figure 5 - Moderating effect of job burnout

4.3 Overview

Based on the analysis of the fore, we could confirm that workers' unsafe behavior cannot decline effectively if the attentions only pay to their safety compliance and safety participation, because they also suffer from job burnout, which is at a really high level and this factor act as a moderating role. To be detailed, the positive relationship between worker' high level of compliance, participation and their low rate of unsafe behavior will be undermined by their poor occupational psychological condition of job burnout. Thus, the question which was proposed in the beginning could be answered.

In retrospect, to achieve the goal which we initially set, the scales for safety compliance and safety participation were slightly adapted for apply in our targeted samples, which both retained their original items. More importantly, the job burnout scale was developed for construction worker in China, which contained 16 items and changed relatively larger, but it was confirmed that the three components of job burnout, namely, exhaustion, cynicism and low professional efficacy covered their symptoms perfectly. Then, according the survey which sampled construction workers' in Beijing, China, five in six hypotheses we formulated were supported, and the rest one was rejected. And the results were analyzed from the characteristics of the factors, that is, safety compliance, safety participation, unsafe behavior and job burnout, and the samples we invited, also the industry we focused. Furthermore, it is worth noting that the terrible symptom related to construction workers' job burnout reflects their condition of occupational psychological health, which need urgent attention [7], especially in the era of industry 4.0 [47]. Hence, an in-depth discussion was conducted and some management advices concerning workers' behavior intervening were provided in the next section.

5 Discussion

5.1 In-depth analysis

To effectively prevent and control unsafe behavior, on the ground of the results above, not only construction workers' safety compliance and safety participation, but their job burnout should all be concerned. More in-deep considering, the former belongs to traditional factors which could contribute to the mitigation of employees' unsafe behavior, other factors, take safety climate, safety leadership for instance, are also such classes. And the latter, according to occupational health psychology, belongs to occupational psychological factors, other factors, take job security and psychological capital for example, are such classes as well. It is indubitable that traditional factors should be concerned, such as promoting compliance and participation, building positive climate and improving leadership which all related to safety. More importantly, construction workers' occupational psychological factors and occupational psychological health condition should also be taken into account when intervene their unsafe behavior, which is what we want to argue.

The reason may list as, firstly, as we can see in this empirical study, construction workers suffered a high level of job burnout, which severely undermined the mitigation mechanism of their safety compliance and participation on their unsafe behavior. Beyond that, secondly, employees were reported undergo other occupational psychological health problems and some other negative occupational psychological factors were approved had negative influence on their safety outcomes in workplace, give an example, high-speed railway drivers were reported suffered job insecurity which was affirmed negatively related to their compliance and participation [48], psychological distress [49] was another example. And, thirdly, which may be more important, contrary to these adverse problems and factors, employees would also have heath occupational psychological conditions and there are positive psychological factors which could promote safety outcomes. For instance, both psychological capital and psychological contract were all confirmed would contribute to construction workers' safety compliance and participation [4,50]. Consequently, with the development and maturity of occupational health psychology, there is an increased emphasis recently on considering employees' occupational psychological factors when conduct safety management [48,51], also when intervene unsafe behavior [7]. The consensus that employees' occupational psychological health condition and occupational psychological factors should be taken into account when manage safety in workplace has emerged and is strengthening. Hence, for construction workers, it is advisable to consider the issues associated with their occupational psychology when intervene their behavior. What's more, not only the negative issues, but the positive should both be concerned.

To achieve this, the "dual process management" method and "environment/organization-occupational psychology-behavior" processes which were proposed on the ground of JD-R theory [7], could be followed. For construction workers, to be detailed, to control their unsafe behavior and shape their safety behavior, both the factors related to their occupational psychology which are workers' intrinsic psychological variables, and the factors come from environment and organization which are external workplace variables, should be focused on. According to their effect on workers' behavior, these factors can be categorized as two, one will block construction workers occur unsafe behavior and shape their safety behavior, and the other will lead to their unsafe behavior. And these two factors mainly have two pathways, namely positive and negative, to achieve their influence on workers' unsafe behavior.

Thus, some recommendations for intervening construction workers' behavior were provided as following. First, construction workers' occupational psychological state should be assessed regularly, and some attentions should be paid to the related factors. Such factors involve their job burnout, job insecurity and psychological capital, and so on. And some efforts should be conducted to buffer or enhance these factors. Targeting this, second, as the abovementioned, measures should be taken to improve or strengthen traditional factors which is the predictor of workers' occupational psychological health condition. Such measures include improving the environment of their workplace, strengthening the support of their supervisors and developing smooth channel of communication and feedback for workers' and their managers, and so forth. Apart from that, third, some factors mainly belong to their job characteristics which will also predict construction workers' psychological condition in workplace should be concerned and adjusted, such as work pressure, role overload and complexity of their work. Also, other factors, such as work-family conflict and job autonomy should be considered. What's more, not the factors and the path that contribute to the diminish construction workers' unsafe behavior, but that lead to their unsafe behavior should all be focused.

5.2 Contribution of the study

From the perspective of theoretical literature, three are four aspects this study could contribute to its development. Firstly, the relationships between safety compliance, safety participation and unsafe behavior were detected, and it was verified that worker's unsafe behavior cannot be effectively diminished only focus on their compliance and participation. Secondly, the role job burnout acts as was investigated, it was found that this factor was a moderator on the aforementioned relationships, which indicated workers' burnout should be managed when intervene their behavior. Thirdly, based on the results this study showed, combined with theoretical analysis and literature review, the suggestion that workers' occupational psychological health condition and the related factors should also be considered when conduct researches was proposed. Finally, the scale for construction workers focus on their job burnout in the Chinese context was developed and verified available, which is a reference for peers.

From the perspective of safety management practice in organizations, especially the high-risk industries, take construction for example, there are four aspects this study could contribute to its improvement. At first, another viewpoint for managing workers' unsafe behavior was pointed, that is, making efforts to maintain the health and stable of their occupational psychological condition, and taking their occupational psychological factors into account when conduct management. Then, the "dual process management" method and "environment/organization-occupational psychology-behavior" processes were recommended to achieve this and conduct safety management for preventing and controlling workers' unsafe behavior. Third, some specific advises were provided for safety managers in construction industries. Fourth, construction worker' safety, health and well-being will improve if their occupational psychological condition was concerned.

5.3 Limitations and future research

Three limitations in this work should be mentioned and the corresponding directions for future research are pointed. First, essentially, the data for examining the hypotheses is cross-sectional. Given that safety management in the sampled construction projects is a process rather a static variable, thus, a longitudinal research should be conducted for further investigating the causal relationship among the variables. Second, only construction workers' job burnout was explored, more research should be performed to explore other factors related to their occupational psychological health and job characteristics, also the interrelations among these factors and workers' unsafe behavior. Third, some empirical study should be executed to verify and renovate the dual process management method for intervening workers' behavior in construction industries, because it was proposed on the basis of meta-analysis [7].

6 Conclusions

This work was motivated to investigate safety compliance, safety participation with unsafe behavior and the role job burnout plays, because so much evidence has indicated the importance of its revealed among high-risk industries workers, such as construction in China. The results showed that workers' compliance and participation certainly contribute to the decrease of their unsafe behavior, but the mitigation mechanism was undermined by their negative occupational psychological condition, that is the symptom of job burnout, which was confirmed a moderator. Then, the present work proposed employees' health of their occupational psychological condition and the related factors should be included when take measures to intervene their unsafe behavior. To achieve this, the "dual process management" method and "environment/organization-occupational psychology-behavior" processes were proposed for referring. In addition, the job burnout scale was developed specially for Chinese construction workers. The findings could contribute to the development of theoretical literature, and were useful for construction managers to improve safety practice, particularly workers' behavior management.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 51674268).

Reference

1 Neal, A., Griffin, M. A., Hart, P. M., The impact of organizational climate on safety climate and individual behavior. Safety science, **34**(1-3), (2000) 99-109.

2 Neal A., Griffin M. A., A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels. Journal of applied psychology, **91**(4), (2006) 946-953.

3 Borman W.C., Motowidlo S.J., 1993. Expanding the criterion domain to include elements of contextual performance. In: Schmitt N., Borman W.C., Associates (Eds.), Personnel Selection in Organizations. Jossey-Bass, San Francisco, 71–98.

4 Wang D., Wang X., Xia. N., How safety-related stress affects workers' safety behavior: The moderating role of psychological capital. Safety science, **103**, (2018) 247-259.

5 Bakker A.B., Demerouti E., 2014. Job demands–resources theory. In: Cooper C., Chen P. (Eds.), Wellbeing: A Complete Reference Guide. Wiley-Blackwell, Chichester.

6 Bakker A. B., Demerouti E., Job demands–resources theory: Taking stock and looking forward. Journal of Occupational Health Psychology, **22**(3), (2017) 273-285.

7 Tong R., Yang X., Li H., Li J., Dual process management of coal miners' unsafe behaviour in the Chinese context: Evidence from a meta-analysis and inspired by the JD-R model. Resources Policy, **62**, (2019) 205-217.

8 Ahola K., Honkonen T., Isometsä E., Kalimo R., Nykyri E., Koskinen S., Aromaa A., Lönnqvist J., Burnout in the general population. Social psychiatry and psychiatric epidemiology, **41**(1), (2006) 11.

9 Nahrgang J. D., Morgeson F. P., Hofmann D. A., Safety at work: a meta-analytic investigation of the link between job demands, job resources, burnout, engagement, and safety outcomes. Journal of applied psychology, **96**(1), (2011) 71-94.

10 Li X., Yi W., Chi H. L., Wang X., Chan A. P., A critical review of virtual and augmented reality (VR/AR) applications in construction safety. Automation in Construction, **86**, (2018) 150-162.

11 J Jin R., Zou P. X., Piroozfar P., Wood H., Yang Y., Yan L., Han, Y., A science mapping approach based review of construction safety research. Safety science, **113**, (2019) 285-297.

12 Alruqi W. M., Hallowell M. R., Techera U., Safety climate dimensions and their relationship to construction safety performance: A meta-analytic review. Safety Science, **109**, (2018) 165-173.

13 Soltanmohammadlou N., Sadeghi S., Hon C. K. H., Mokhtarpour-Khangha, F., Real-time locating systems and safety in construction sites: A literature review. Safety science, **117**, (2019) 229-242.

14 Mohammadi A., Tavakolan M., Khosravi Y., Factors influencing safety performance on construction projects: A review. Safety science, **109**, (2018) 382-397.

15 Xia N., Griffin M. A., Wang X., Liu X., Wang D., Is there agreement between worker self and supervisor assessment of worker safety performance? An examination in the construction industry. Journal of safety research, **65**, (2018) 29-37.
16 Lingard H., The impact of individual and job characteristics on 'burnout' among civil engineers in Australia and the implications for employee turnover. Construction Management and Economics, **21**(1), (2003) 69-80.
17 Poon S. W., Rowlinson S. M., Koh T., Deng Y., Job burnout and safety performance in the Hong Kong construction industry. International Journal of Construction Management, **13**(1), (2013) 69-78.
18 Enshassi A., El-Rayyes Y., Alkilani S., Job stress, job burnout and safety performance in the Palestinian construction industry. Journal of Financial Management of Property and Construction, **20**(2), (2015) 170-187.
19 Yang F., Li X., Zhu Y., Li Y., Wu C., Job burnout of construction project managers in China: A cross-sectional analysis. International Journal of Project Management, **35**(7), (2017) 1272-1287.
20 Hinze J., Thurman S., Wehle A., Leading indicators of construction safety performance. Safety science, **51**(1), (2013) 23-28.
21 Glendon A. I., Litherland D. K., Safety climate factors, group differences and safety behaviour in road construction. Safety science, **39**(3), (2001) 157-188.
22 Guo B., Yiu T.W., 2013. How traditional construction safety performance indicators fail to capture the reality of safety. In: Yiu T.W., Gonzalez V. (Eds.), The 38th Austrlasian Universities Building Education Association Conference, Auckland, New Zealand.
23 Guo B. H. W., Yiu T. W., González V. A., Predicting safety behavior in the construction industry: Development and test of an integrative model. Safety science, **84**, (2016) 1-11.
24 Vinodkumar M. N., Bhasi M., Safety management practices and safety behaviour: Assessing the mediating role of safety knowledge and motivation. Accident Analysis and Prevention, **42**(6), (2010) 2082-2093.
25 Smith T. D., DeJoy D. M., Dyal M. A., Pu Y., Dickinson, S., Multi-level safety climate associations with safety behaviors in the fire service. Journal of Safety Research, **69**, (2019) 53-60.
26 Clarke S., Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. Journal of occupational and organizational psychology, **86**(1), (2013) 22-49.
27 Fernández-Muñiz B., Montes-Peón J. M., Vázquez-Ordás C. J., The role of safety leadership and working conditions in safety performance in process industries. Journal of Loss Prevention in the Process Industries, **50**, (2017) 403-415.
28 Maslach C., Leiter M. P., Early predictors of job burnout and engagement. Journal of Applied Psychology, **93**(3), (2008) 498-512.
29 Maslach C., Leiter M. P., 2016. Burnout. In: Stress: Concepts, Cognition, Emotion, and Behavior. Academic Press, 351-357.
30 Bowers J., Lo J., Miller P., Mawren D., Jones B., Psychological distress in remote mining and construction workers in Australia. Medical Journal of Australia, **208**(9), (2018) 391-397.

31 Frazier P. A., Tix A. P., Barron K. E., Testing moderator and mediator effects in counseling psychology research. Journal of counseling psychology, **51**(1), (2004) 115-134.
32 Gao Y., Fan Y., Wang J., Li X., Pei J., The mediating role of safety management practices in process safety culture in the Chinese oil industry. Journal of Loss Prevention in the Process Industries, **57**, (2019) 223-230.
33 DeArmond S., Smith A. E., Wilson C. L., Chen P. Y., Cigularov K. P., Individual safety performance in the construction industry: Development and validation of two short scales. Accident Analysis and Prevention, **43**(3), (2011) 948-954.
34 Maslach C., Jackson S.E., Leiter M.P., 2017. Maslach Burnout Inventory Manual. forth edition. Mind Garden.
35 Demerouti E., Bakker A. B., Nachreiner F., Schaufeli W. B., The job demands-resources model of burnout. Journal of Applied psychology, **86**(3), (2001) 499-512.
36 Pines A.M., Aronson E., Kafry D., 1981. Burn Out: From Tedium to Personal Growth. Free Press, New York.
37 Melamed S., Kushnir T., Shirom A., Burnout and risk factors for cardiovascular diseases. Behavioral medicine, **18**(2), (1992) 53-60.
38 Stride C. B., Turner N., Hershcovis M. S., Reich T. C., Clegg C. W., Murphy P., Negative safety events as correlates of work-safety tension. Safety science, **53**, (2013) 45-50.
39 Warner M., Schenker N., Heinen M. A., Fingerhut L. A., The effects of recall on reporting injury and poisoning episodes in the National Health Interview Survey. Injury Prevention, **11**(5), (2005) 282-287.
40 Landen D. D., Hendricks S., Effect of recall on reporting of at-work injuries. Public health reports, **110**(3), (1995) 350-354.
41 Hon C. K. H., Chan A. P. C., Yam M. C. H., Relationships between safety climate and safety performance of building repair, maintenance, minor alteration, and addition (RMAA) works. Safety science, **65**, (2014) 10-19.
42 Maslach C., Jackson S. E., Leiter M. P., 1996. Maslach Burnout Inventory Manual. third edition. Mind Garden.
43 Clarke S., The effect of challenge and hindrance stressors on safety behavior and safety outcomes: A meta-analysis. Journal of Occupational Health Psychology, **17**(4), (2012) 387-379.
44 Didla S., Mearns K., Flin R., Safety citizenship behaviour: A proactive approach to risk management. Journal of Risk Research, **12**(3-4), (2009) 475-483.
45 Lyu S., Hon C., Chan A., Wong F., Jave A., Relationships among safety climate, safety behavior, and safety outcomes for ethnic minority construction workers. International journal of environmental research and public health, **15**(3), (2018) 484.
46 WHO - World Health Organisation. Burn-out an "occupational phenomenon": International Classification of Diseases, 2019. Available at: https://www.who.int/mental_health/evidence /burn-out/en/
47 Badri A., Boudreau-Trudel B., Souissi A. S., Occupational health and safety in the industry 4.0 era: A cause for major concern? Safety Science, **109**, (2018) 403-411.

48 Guo M., Liu S., Chu F., Ye L., Zhang Q., Supervisory and coworker support for safety: buffers between job insecurity and safety performance of high-speed railway drivers in China. Safety science, **117**, (2019) 290-298.
49 Siu O., Phillips D. R., Leung T., Safety climate and safety performance among construction workers in Hong Kong: The role of psychological strains as mediators. Accident Analysis and Prevention, **36**(3), (2004) 359-366.
50 Newaz M. T., Davis P., Jefferies M., Pillay M., The psychological contract: a missing link between safety climate and safety behaviour on construction sites. Safety science, **112**, (2019) 9-17.
51 Smith T. D., Hughes K., DeJoy D. M., Dyal M. A., Assessment of relationships between work stress, work-family conflict, burnout and firefighter safety behavior outcomes. Safety science, **103**, (2018) 287-292.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Reduce Human Error: Mistake-Proof Procedures and Create an Effective PPE Grid

Nicole Loontjens*
Americas Styrenics
Coventry, RI
*Presenter E-mail: nbloontjens@amsty.com

Abstract

One of the most problematic root causes in investigations is "human error". All humans err; that's never going to stop. We have to ask ourselves, "WHY did the human err?" What was it about the environment, the communication, the culture - that contributed to someone making a mistake? Unless those conditions are perfect, it's likely not legitimate to identify human error as a root cause.

This paper will discuss two practical tools that can be implemented to help humans do the right things. The first is mistake-proofing procedures (we call it "poke-yoke"). The second is a graphical personal protective equipment (PPE) grid.

You cannot poke-yoke a procedure with one person. Gather a small group and go through the procedure at the table. Make sure everyone understands the purpose of the procedure. Note anything that you might want to check in the field. For example, if the instructions indicate to "slightly open the valve", you'll want to observe the operator in the field and try to quantify "slightly" or provide visual indication on the valve itself of the appropriate position. In that example, you would want to calibrate one operator's "slightly" against other operators' "slightly". You'll want to see if equipment required to be used or manipulated in the field is adequately labelled. From the description in the procedure, can the operator easily identify the equipment? Are the steps in the correct order? Does it say when to don or doff PPE? Does the operator need to reference additional information that is not included in the procedure? Is the language unambiguous?

Next, bring the procedure in the field and observe an operator completing the task. They may alternatively walk the group through the task. If *you* had to complete the procedure, could you? You also want to look for opportunities to improve the tasks associated with the procedure. These improvements may cost money, and you want your management to be aware and supportive of

that possibility. For example, if you notice someone tends to climb over a dike wall because the stairs are on the other side of the dike, you may want to add stairs. If a valve needs to be opened but is uncomfortably high, can a step be installed? Are samples being taken from a valve or an engineered sampler? When the operator goes to get PPE, is it available and clearly labelled, or are they making do with something unsuitable?

The second tool is the graphical PPE grid. We want to make it easy for the operators to know what PPE is required for a specific task. I think this is brilliant and I invite you to steal it at will. This grid is set up to divide the tasks in a variety of ways – either by the task, or by the chemical. Each task clearly shows a picture of the kinds of PPE required, as well as options (when applicable). Each picture corresponds to a specific make and model of PPE, shown on the reference table. The grid is plotted out on a large format printer and hung in vertical poster files in the control room along with other important reference documents.

Keywords: Human error, Procedures, PPE, Human reliability

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Beyond Participation—A Case Study for Driving Employee Engagement in Your Process Safety Program

Tony Bocek*
Operations Technician
BP-Cherry Point Refinery
Blaine, Washington USA
*Presenter E-mail: tony.bocek@bp.com

Abstract

Employee Participation, as we know, is one of the 14 process safety elements required by 29CFR1910.119 and an essential part of any process safety program. Ensuring compliance with this requirement is a clearly defined task. However, when seeking to develop and maintain a robust process a safety culture, basic compliance with the requirements of the employee participation element is not enough. The process safety culture of a site is dependent upon field-level employee engagement in the process safety program. Detailed policies, procedures, and practices, while critically important, may not equate to site safety if the employees are not engaged in the program. Operators and Maintenance Technicians must not only believe in the site's process safety program, but champion it. So, to achieve sustainable process safety excellence, the question is: How? How do you engage your Operations and Maintenance work force in your site's process safety program?

BP's Cherry Point refinery has implemented a model for PSM employee participation that provides ownership of the process safety program to Operations and Maintenance Technicians. This model provides for the employee engagement necessary to sustain a high-performing process safety culture. Developmental roles, intended to increase process safety competence in field technicians, provide an opportunity for Operators to take shared ownership of several PSM elements such as MOC, operating procedures, and training while also serving as key operations contacts for Process Hazard Analysis and incident investigation. Additionally, similar developmental roles offered to Maintenance technicians provide personnel with experience in lifecycle management of safety-critical equipment while sharing ownership of the mechanical integrity program at their site.

My presentation outlines this employee engagement model and provides examples of how it is applied to various PSM activities, all from the perspective of a Process Operator. This will provide a case study which other sites can consider while determining how to enhance employee engagement and strengthen their site's process safety culture.

Keywords:
Operational Excellence, Process Safety Culture, Employee Engagement, Employee Participation

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Options for teaching Operational Process Safety

Trish Kerin*
Director
IChemE Safety Centre, Melbourne Australia
*Presenter E-mail: TKerin@icheme.org

Abstract

Over several years the IChemE Safety Centre (ISC) has been working with universities around the world to drive improvement in how process safety is taught. This has seen the ISC release guidelines on desired learning outcomes for graduate engineers. This introduced the need for operational experience, which has received some challenge from universities, as they felt academia was not an operational environment. This led to the development of some useful materials for use by universities to assist their education needs. One part of this was to develop a simplified process safety management system (PSMS) that could be applied to university laboratory activities, highlighting operational process safety requirements. The PSMS is written to fit within existing university safety management systems, which often focus on occupational health and safety. This paper will discuss the development of the PSMS including specific details of elements, and how they can be applied. This PSMS will be freely available to any university who would like to access it.

Keywords: Initial training, safe practices

1 Introduction

It is widely accepted that the academic environment is quite different to an operational environment. Academia is a place of research and learning, an operational environment is a place that aims to produce a product safety and consistently, around the clock. When a student graduates university and enters an operational environment they can often experience a culture shock due to the constant demands of operations. Often accompanying this is the significant safety demands put on employees, which may be very different to their academic experience. For example the new employee may need to do a task in the field that requires a permit to work to be issued. This may be their first experience of these systems, and this can create frustration as they work through what appears to be a bureaucratic system. This may then lead to thinking that safety systems do not always add value, sometimes they get in the way of the "real job". It is because of these experiences that the ISC developed a simplified PSMS (ISC, 2019) that can be applied to university laboratory work, highlighting the application of safety as part of the "real job". It is believed that this will produce more rounded graduates who have an emerging practical understanding of operational safety.

2 Developing the simplified PSMS

A working group of academics, process safety specialist from operating companies and consulting engineers came together to define the requirements based the ISC Guidance document 'Undergraduate Learning Outcomes' (ISC, 2018). This document described the following learning outcomes for the 'Process Safety in Practice' element:

- Apply, adapt and/or create Process Safety Management System (SMS) elements as part of laboratory, practical or pilot plant activities.
- Research, investigate and summarise the application of Process Safety Management System elements as part of industrial training placements.
- Develop and apply regulations, standards, risk assessments, inherent safety techniques and risk-based decisions during Design Projects.
- Identify and evaluate causal factors in process safety incident case studies.

The PSMS was designed to address the first item in this list. Other resources are available or being developed for the remaining three elements.

As a starting point for development the working group considered by the Center for Chemical Process Safety Risk Based Process Safety Guidelines (CCPS, 2007) and the Energy Institute Process Safety Framework (Energy Institute, 2010). From these two resources a list was made of the most applicable elements that could be applied in the academic environment of the laboratory. While the overall structure of the existing management systems is logical when applying it to a workplace, it was determined that a modified structure would assist in the use at an academic institution and better align with the stated learning outcomes in the 'Undergraduate Learning Outcomes' (ISC, 2018) document. For this reason the sub-elements were grouped under the following elements:

- Induction and competency.
- Risk identification and management.
- Operations.
- Review.

3 Overall structure of the PSMS

Within the four elements of the PSMS, there are 17 sub-elements. The PSMS is laid out as shown in Table 1.

Element	**Sub-element**
Induction and competency	Culture
	Standards
	Workforce involvement and working with others
	Introduction to procedures
	Training in equipment use
	Emergency response and preparation requirements
	Incident reporting requirements
Risk identification and management	Hazard identification
	Risk assessment and identification of controls
	Implementation of controls and control validity
	Management of change
Operations	Working with procedures
	Safe work practices – Permit to Work
	Safe work practices -Isolations
	Pre-start up safety review
	Handover and logging
Review	Post activity review

Table 1. Elements and sub-elements of the PSMS

To support the application of the PSMS, a series of examples have been provided in appendices. These serve to show how the system can be used and what should be included in the elements if they are to be adopted. They are not comprehensive lists but show how the information could be used. The examples for each element are listed below in Table 2.

Element	**Example**
Induction and competency	Example health safety and environment policy
	Example laboratory safety rules
	Example take 5 or hazard identification card
	Example induction checklist
	Example applicable standards list
	Example applicable legislation list
	Example chemical inventory and safety data sheet register including infographic of incompatible materials
	Example organisation chart showing responsibilities
	Example position description for students

	Example procedures register
	Example training register
	Example emergency response plan
	Example emergency response evacuation diagram
	Example incident report
	Example incident database
	Example root cause analysis
Risk identification and management	Example hazard identification methods
	Example infographics to show the hazards
	Example risk matrix
	Example team-based risk assessment forms
	Example management of change process
	Example management of change form
Operations	Example management of a procedure
	Example procedure review checklist
	Example permit to work procedure
	Example permit to work checklist
	Example isolation procedure
	Example isolation sign off form including P&ID
	Example infographic showing different isolation equipment available or use
	Example pre-start up safety review form
	Example of a safety moment, including notes and presentation materials
	Example process log
	Example handover checklist
Review	Example post activity review

Table 2 Example materials included in the PSMS

4 How the PSMS can be adopted

The PSMS is available as a free download from the IChemE Safety Centre website (https://www.icheme.org/knowledge/safety-centre/publications/publications/) and written so that users can review what is contained in the document and see examples of how to apply it in practice. While the ISC does not warrant the information, it is copyright free and designed for open access. It contains a section describing how to use the document. This is quoted below (ISC, 2019):

"This document can be used in whole or in part, depending on the needs to the university. It is important to note that the resources contained here are examples only for the university to use for structure, not necessarily accurate details for direct application.
The following steps offer a guide to using this document:

- perform a gap analysis between the current management system in place and the suggested sections in this document. Note: some aspects may be addressed in different ways, the outcome need not be achieved by following this model rigidly
- determine if the gaps that emerge need to be closed
- develop an action plan to close the gaps. This may include:
    - determine which documents or systems need to be developed
    - prioritise the actions
    - develop necessary documents or systems based on the resources in this document, the resources here are templates only and not comprehensive examples
    - implement the systems or documents, including training of personnel as required and
    - review the implementation periodically to ensure it is still functioning and providing the desired outcome"

5 Additional resources

To support the release of the PSMS, the ISC has also developed a case study on laboratory incidents. This follows the same format at the previously released ISC Case Studies, where a story is told from the beginning without disclosing the actual outcome. The participants then make decisions based on the information that have been given. This case study starts following a demonstration of the rainbow experiment, then moves to an experiment performing impact testing on an explosive and finally an experiment using a pyrophoric chemical. The decision points in between focus on what elements of the PSMS may be useful to improve safety where these experiments are being undertaken. The final video in the case study discloses the actual outcomes from the incidents discussed. This case study, along with the PSMS is available as a free download from the IChemE Safety Centre website. The production of this case study was generously funded by Saudi Aramco.

6 Conclusion

Implementation of a PSMP will not achieve an improvement in laboratory safety and teaching of operational process safety on its own, but it is a useful tool to assist in this endeavour. Helping to show students that the use of a management system is standard in the workplace will aid in their introduction to their first role after university. Following defined processes and taking into account standard risk management practices and systems may also assist in producing safer laboratories for all concerned. This is because the hazards will be better understood and managed. It is for these reasons that the PSMS has been created and made freely available to universities around the world.

The next challenge to is assist the university lecturers in how to implement the elements they need. This may require education for the educators. An excellent way this is currently being done is through the American Institute of Chemical Engineers CCPS Faculty Workshops (CCPS, 2019). When we have an opportunity to engage with local faculty, as industry people we should always seek to assist and share our knowledge and experience.

7 References

CCPS. (2007). Risk Based Process Safety Guidelines. New York: Wiley.

CCPS. (2019). https://www.aiche.org/ccps/resources/conferences/events/faculty-workshops. New York: AIChE.

Energy Institute. (2010). Process Safety Framework. London: Energy Institute.

ISC. (2018). Undergraduate Learning Outcomes. London: IChemE.

ISC. (2019). ISC Guidance Sample University Laboratory Process Safety Management System. London: IChemE.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Operator Error or Management Failure? Management's Role in Maintaining Operator Discipline

Marc J Rothschild*, P.E.
Livent Corp.
*Presenter E-mail: marc_rothschild@yahoo.com

Abstract

CCPS defines Operational Discipline as "the execution of operational and management tasks in a deliberate and structured manner." Put more succinctly, operational discipline can be defined as doing the right thing when no one is looking. While Operational Discipline applies to facility personnel across the board, this paper focuses on o*perator* discipline, which this author defines as the requirement to explicitly follow written procedures. The only exception would be if the operator believes that doing so would create harm, in which case the operator should stop all work and only deviate from the procedure with expressed approval from his superiors. This deviation should be processed through the management of change procedures.

Failure to follow procedures has caused incidents and near misses throughout the processing industries. It may be tempting to classify these failures as "operator error" and then reprimand the operator. While this may address the symptom, it most likely would not get to the root of the problem. In order to eliminate these failures, it is important to understand and correct underlying causes. For example, are the procedures accurate and clear? Do the operators have the tools and training necessary to carry out the procedure as specified? Has failure to follow procedures occurred previously and, if so, were actions taken by management in response?

This paper presents a case history of an industrial accident – a refinery hydrocracker explosion – to illustrate how management failure had led to a failure to follow procedures.

Keywords: Operational Discipline, Procedures, Unsafe Practices, Normalization

Introduction

CCPS defines Operational Discipline as "the execution of operational and management tasks in a deliberate and structured manner" [1]. DuPont has offered up this definition for Operational

Discipline: “the deeply rooted dedication and commitment by every member of an organization to carry out each task the right way every time” [2]. While Operational Discipline applies to facility personnel across the board, this paper focuses on o*perator* discipline, which this author defines as the requirement to explicitly follow written procedures. The only exception would be if the operator believes that doing so would create harm, in which case the operator should stop all work and only deviate from the procedure with expressed approval from his superiors. This deviation should be processed through the management of change procedures.

Failure to follow procedures has caused incidents and near misses throughout the processing industries. It may be tempting to classify these failures as “operator error” and then reprimand the operator. While this may address the symptom, it may not get to the root of the problem. In order to eliminate these failures, it is important to understand and correct underlying causes. For example, are the procedures accurate and clear? Do the operators have the tools and training necessary to carry out the procedure as specified? Has failure to follow procedures occurred previously and, if so, were actions taken by management in response?

This paper presents a case history of an industrial accident – a refinery hydrocracker explosion – to illustrate how management failure had led to a failure to follow procedures.

Hydrocracking Process Incident

On January 21, 1997, a refinery hydrocracker unit experienced a runaway reaction, which caused a pipe to fail, resulting in a vapor cloud explosion. One operator was killed, and 46 others were injured. The information given about this accident was obtained from an EPA Chemical Accident Investigation Report [3].

Hydrocracking is a refinery process that breaks apart, or “cracks” larger molecules into smaller ones and saturates the chemical bonds with hydrogen. The process is exothermic, and therefore excess heat must be removed to maintain a constant reaction temperature. The reaction rate increases dramatically with increased temperature, with a 20°F increase resulting in a doubling of the reaction rate. Therefore, it is critical that the temperature be monitored and controlled to prevent a potential runaway reaction.

Figure 1 shows the temperature profile in Reactor Bed 5 at the time of the incident. At 7:34 pm on January 21, 1997, the inlet to Bed 5 showed a rapid increase in temperature, with the temperature exceeding 8008°F. Shortly after this sudden increase, the temperature just as suddenly decreased back to a more normal range. The No. 2 Operator went outside to the temperature panel at the reactor to get confirmation of the temperatures. A few minutes later, the reactor temperatures spiked upwards, dropped to zero and then shot up to nearly 1400°F. This excessive temperature caused a line to fail, resulting in a release and subsequent explosion and fire at the unit. This explosion killed the No. 2 Operator, who was standing at the temperature panel, and injured 46 other personnel. Figure 2 shows this failure point and Figure 3 shows where the No. 2 Operator was located at the time of the incident.

The cause of the runaway reaction is complex and is not included in this paper but is discussed in the EPA report [3]. This paper focuses on the fact that this runaway reaction could have easily been stopped had the operators activated the emergency depressurization system, as instructed in the emergency procedures. This emergency depressurization system was installed in 1986 to prevent a runaway reaction. The emergency procedures specify that the depressurization is to be activated upon reaching reactor temperatures in excess of 800°F. Nevertheless, the temperature exceeded this threshold two times, yet the operators failed to activate this system. The question is, why did the Board Operator fail to follow the emergency procedure and depressurize the reactor?

Operator Error or Management Failure?

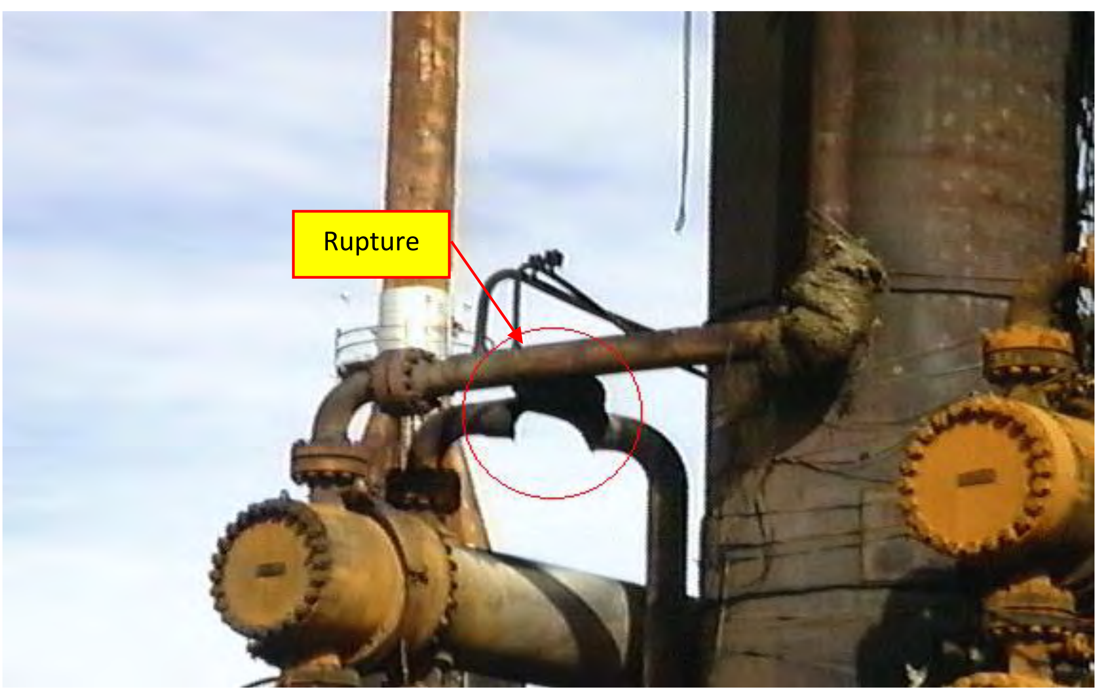
Unreliable Temperature Readings

The first temperature excursion was brief, and the temperature quickly dropped back down to a more normal operating range. The plant had experienced many problems with the temperature recording system, including false readings the previous day. Because of this history, the operators had little confidence that the temperature readings were accurate. The fact that the temperatures returned to normal supported this view. A few minutes later, the temperatures again spiked, this time to 1200°F, but then immediately dropped to zero. In the EPA investigation, it was reported that the operators were not aware that a zero reading indicated an off-the-scale reading, and instead they interpreted a zero as a faulty reading, confirming their suspicions. So, right up to the point of the rupture, the operators did not believe that they had a runaway reaction on their hand.

Although instructed in the procedures to activate this depressurization, the operators are very aware that such action has serious ramifications. The Hydrocracker is a key processing unit and shutting it down would result in significant loss of production, with a corresponding major loss of revenue. Given this consequence of a shutdown, the operators want to be sure that there really is a problem before taking such drastic action.

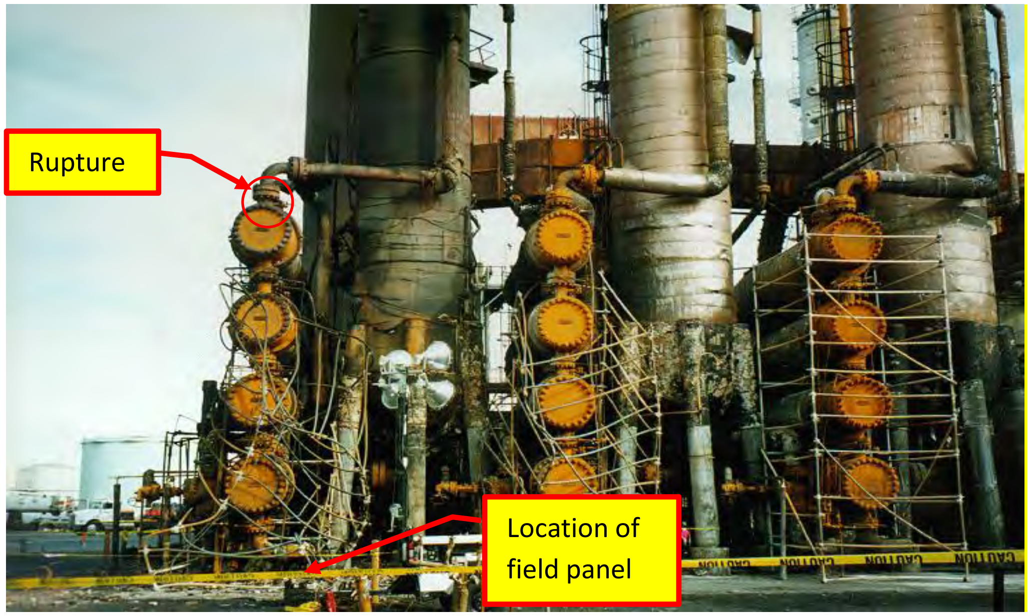
Figure 1 Temperature Profile in Hydrocracker Reactor

Figure 2 Line Rupture



Picture from EPA report

Figure 3   Location of Temperature Panel



Picture from EPA report

Procedural Issues

The operating procedures for this unit had several deficiencies:

- There were inconsistencies regarding the stated upper safe operation temperature, ranging from 690°F in one procedure to 1,000°F in another.
- The procedures were found to be inconsistent on the safe temperature differentials across and between the reactor beds.
- The procedures were out of date. For example, in February of 1996, the catalyst in all top beds of Stage 2 was replaced with a more reactive catalyst. However, no changes were made to the written operating procedures to reflect the catalyst change and the increased risk of temperature excursions due to increased reactivity.
- Some of the procedures were contradictory and could not be followed. For example, the SOP stated that the quench valves should not be opened more than 50%, while this same procedure also specified that the operators are to maintain a flat temperature profile across the beds, which required additional quench flow beyond a 50% valve position.
- The procedures specified that the outlet bed temperatures were to be the same, but that often was not possible at the desired high throughput due to the limiting capacity of the trim furnaces.

Considering these deficiencies in the procedures, it is possible that the operators did not have confidence in them and therefore did not directly refer to them when operating the unit.

Culture of Production over Safety

Perhaps the biggest reason that the operator did not activate the emergency depressurization is that, as reported in the findings of the EPA report: "*An operating environment existed that caused operators to take risks while operating and to continue production despite serious hazardous operating conditions.*" The Production Area Supervisor stated that failure to use the emergency depressurizing system for a temperature exceeding 800°F would be considered a serious matter and could be subject to disciplinary action. Despite these words, there had been several occurrences over the past several years where the reactor temperature exceeded 800°F and the emergency depressurization system was not activated, yet no disciplinary action was ever taken. Moreover, management never even investigated why the operators failed to depressure the unit, as required. In those situations, rather than depressurizing the reactor, which would shut down the unit, the operators instead brought the reactor under control by adjusting operating parameters. This failure to take corrective action by management to enforce the compliance with the procedures gives a clear message to the operators that they acted appropriately in maintaining operations.

The failure of management to recognize the seriousness of the failure of the operators to shut down the unit may be attributed to what is known as "normalization of unsafe practices." Unsafe practices can become part of the normal and accepted way of accomplishing tasks if nothing bad happens as a result of these practices. The space shuttle Columbia disaster is a well-known example of this phenomenon. NASA's original specification for the space shuttle had zero allowance for any foam loss as any loose debris could seriously impact the very delicate thermal protection system. However, despite this very tight specification, nearly every space shuttle flight prior to and including the Columbia disaster experienced some foam loss. As reported by the Columbia Accident Investigation Board: "With each successful landing, it appears that NASA engineers and managers increasingly regarded the foam-shedding as inevitable, and as either unlikely to jeopardize safety or simply an acceptable risk." [4]

The root of normalization of unsafe practices can be found in the relationship between safety and operations. While it is often stated that process safety and operations are on the same side, the truth is that these two elements are almost always in conflict with each other. That is because the benefit of unsafe behavior is immediate and tangible, whereas the potential benefit of safe behaviors is long term and results in an intangible non-event. Had the operators shut down the hydrocracker unit, as instructed, the refinery would have taken a significant financial hit. Consequently, the operators would likely have faced second guessing as to why they didn't try to keep the unit online, especially when considering that they were previously able to keep the unit online under similar circumstances.

We are not able to make decisions based on hindsight, but we are able to evaluate the risks of an adverse event and make informed decisions based on those risks. This was done by the refinery. In 1986 the refinery identified the risk of a runaway reaction and, in response, installed a means to immediately depressurize the unit and established conditions where the operators were to activate it. While the risk of the event remained unchanged, the *perception* of the risk did change.

One factor that influences risk perception is known as "melioration bias," which is the tendency to assign greater weight to short term results, and to underestimate the potential for the occurrence of a negative event. If the unsafe behavior does not result in an incident or accident, and if the unsafe behavior results in positive outcomes, then positive reinforcement increases the strength of the bias. Other factors that affect the perception of risk include rare event and optimism bias. Rare event bias is the tendency to under evaluate or minimize the likelihood of being adversely affected by a negative event that is known to occur only on rare occasions. Optimism bias results in the perception that one is less likely to experience a negative event compared to others in a similar situation.

These shifts in risk perception are revealed in a press release produced by the refinery, following this accident. In their statement, the refinery reported that they "found the incident to be highly unprecedented in the 34-year history of the hydrocracker unit, outside the realm of its experience in the refining industry, and that of the qualified operators on duty the night of Jan. 21" [5]. The implication of this statement is that this was a freak event and that they could not reasonably have prepared for its occurrence. Of course, this is difficult to accept, as the refinery did acknowledge the potential for this event, installed a safety system specifically to address it, and provided instructions to the operators to activate the safety system upon reaching specific operating parameters. From a mathematical perspective, 34 years is not statistically significant compared to the "expected" frequency of a line rupture – which is on the order of once every 10,000 – 100,000 years. However, if the statement accurately reflects the sentiment of the refinery management, it can only be concluded that the management's perception of risk has been reduced due to 34 years of success at being able to maintain unit operations despite occasional temperature excursions.

Management's Responsibility in Maintaining Operator Discipline

As shown in this case study, management needs to make sure that the operating procedures are clear and accurate and that the instrumentation and controls are reliable. In addition, management needs to be unambiguous regarding the importance of safety and that their actions are consistent with this message.

Specific measures that management can take to bolster safety include the following:

- Ensure that employees are aware of the hazards of the process and are aware of the consequences of failure to follow safe operating practices;
- Give operators written authority to stop or shut down the process if they believe that harm may occur;
- Enforce a policy of not allowing deviations from established safety standards without first conducting a Management of Change;
- Implement a policy of zero tolerance for willful violations of process safety policies, procedures and rules;
- Investigate all abnormalities as "near-misses";
- Share findings of incident investigations, including similar incidents in other industries.

Conclusion

In this case study, the runaway reaction could have been stopped had the operator activated the emergency depressurization system, as specified in the emergency procedure. However, in the EPA report, it was concluded that an operating environment existed that encouraged operators to take risks while operating and to continue production despite potentially serious hazards. Management is responsible to ensure that the operators have procedures and instrumentation that they can trust, and Management must give a clear and consistent message regarding the importance of process safety in operations.

References

1. Center for Chemical Process Safety, “Guidelines for Risk Based Process Safety,” 2007.
2. Rains, Brian D., “Operational Discipline – Does Your Organization Do the Job Right Every Time?” Mary Kay O’Connor Process Safety Center International Symposium, College Station, TX, 2011.
3. U.S. Environmental Protection Agency, “EPA Chemical Accident Investigation Report - Tosco Avon Refinery - Martinez, California,” 1998.
4. Columbia Accident Investigation Board, Report Volume 1, Chapter 6, page 122, August 2003.
5. Business Wire Report, “Tosco releases report on Jan. 21, 1997 accident investigation,” May 29, 1997.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

The Future of the U.S. Chemical Safety and Hazard Investigation Board (CSB): Opportunities and Challenges[1]

Rick Engler*
Board Member, CSB[2]
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue, NW
Washington, D.C. 20006, USA
*Presenter E-mail: rick.engler@csb.gov

Abstract

Major, preventable chemical incidents in the United States continue, many of which have caused injuries, fatalities, community harm, and damage to industrial infrastructure. Since 1998, the U.S. Chemical Safety Board (CSB) has investigated more than 130 such incidents across the nation and has issued many recommendations that, once adopted, have led to safety improvements. At the same time, CSB faces ongoing challenges concerning funding, staffing, and how to best address underlying organizational causes of incidents.

Keywords: CSB, safety recommendations, organizational causation

As a Member of the United States Chemical Safety Board (CSB), I talk with the families of loved ones who have lost their lives in horrific chemical disasters. Families want to know what caused their loss. And they often want to discuss how to prevent future tragedies.

These conversations prompt reflection on the major national changes needed to achieve CSB's vision of "a nation safe from chemical disasters".

Thus, my purpose today, is to address some central challenges for chemical safety -- and how CSB is addressing them.

[1] References available upon request. Find CSB investigation reports and recommendations at www.csb.gov.

[2] Disclaimer: The views and opinions expressed herein are those of the author, and do not necessarily reflect the views of the U.S. government, or any agency thereof, including the U.S. Chemical Safety Board. This document is a work product of CSB Board Member Rick Engler and is not an official publication of the US CSB.

The concept of an independent federal agency to investigate the causes of major chemical incidents was prompted by horrific disasters, among them the 1989 Phillips incident in Pasadena, Texas in which 23 people died and more than 300 were injured.

Congress created CSB in 1990 "…to investigate accidents and recommend measures to reduce the risk of catastrophic events." Presidents Bush and Clinton, however, opposed its funding, claiming that its role was duplicated by OSHA and EPA. After efforts by labor unions, environmental organizations, some corporations, and eventually from industry trade associations, CSB was finally funded and began operating in 1998.

CSB conducts investigations of chemical releases into the air from industrial facilities. The most comprehensive CSB investigations address multiple incident causes and circumstances, including physical factors such as equipment failure, as well as gaps in industry consensus standards, management systems, and government regulations.

CSB is not a regulatory agency and does not issue violations, consent orders, or financial penalties. CSB issues *recommendations* and their strength rests with our work's scientific integrity and effective advocacy.

During the CSB's 21-years we have issued a total of about 100 reports, interim reports, bulletins, and case studies. We've made 841 safety recommendations to facility management, trade associations, standard setting groups, unions, and regulatory agencies. And we have produced many videos on specific incidents.

Safety accomplishments catalyzed by CSB recommendations include:

- After a fertilizer grade ammonium nitrate storage facility incident that killed 15 and injured 260, the Federal Emergency Management Agency created a training program on this hazard for emergency responders.

- After an incident that injured 36 people, including six fire fighters, New York City revised its outdated fire prevention code for hazardous materials.

- After an explosion that killed six workers at a natural gas facility, the National Fire Protection Association and the International Code Council developed codes to prohibit flammable gases for use in "gas blows" to clean piping.

- After an oil refinery disaster that killed 15 contract workers and injured 180 others, many refineries removed temporary contractor trailers that were close to operating units.

- After an explosion that killed four workers at a laboratory, the Accreditation Board for Engineering and Technology, Inc. (ABET) revised the chemical engineering curriculum to include components on process safety and reactive hazards. After a graduate student was severely injured in a laboratory explosion, the American Chemical Society published guidance to prevent hazards in research labs.

- After a refinery incident that led 15,000 residents to seek medical evaluation, CSB urged California to strengthen its PSM rule for its 14 refineries. California then adopted the most comprehensive refinery safeguards in the nation, which can offer valuable lessons for reforming the federal PSM standard.

CSB videos have been viewed more than 17 million times on YouTube, where we have over 80,000 subscribers. They are widely used in training in the U.S. and internationally. Recent videos depict the impact of increasingly extreme weather on a chemical plant and the hazards of unregulated onshore oil and gas drilling.
CSB faces major external challenges, among them that:

1) There is no data base for recording chemical incidents. Thus we cannot understand incident trends.
2) Industry is under intense production pressures that can continue to undermine safety; and
3) Necessary public safeguards are under assault.

I'll talk about each of these challenges – and what CSB can do to address them.

CHEMICAL INCIDENTS CONTINUE WITHOUT KNOWLDEGE OF TRENDS

The primary challenge for the CSB is that chemical incidents are frequent. Many cause deaths, injuries, environmental impacts, and significant property damage. We can investigate a small subset of these incidents given that CSB is a very small agency, with about just 40 staff positions. Currently, we have 10 open investigations.

Incidents occur at small, little known firms, such as at Midland Resource Recovery in Phillipi, WV, where three people were killed in 2017 in explosions involving reactive chemicals. The founder and president of the company, which decommissions odorant equipment used in natural gas service, was a victim. They also occur at huge multinational corporations, such as DuPont, Chevron, and ExxonMobil.

At DuPont's La Porte, TX facility in 2014, four workers died and three other workers were injured from their exposure to methyl mercaptan. Two workers were killed when the chemical drained from open valves, filling a room with vapor. One of those workers made a distress call, and two more workers died while responding. DuPont, a firm with a worldwide safety reputation, has had multiple process safety incidents. This suggests that other major firms, not just supposed "outliers", are vulnerable.

While we definitively know that incidents continue, there is no contemporaneous, comprehensive, and publicly accessible database of major chemical incidents at industrial facilities. The EPA's Risk Management Program (RMP) data base, which includes about 12,000 facilities, shows continuing chemical incidents, many with offsite impacts (see table on page 10).

Unfortunately, this EPA data does not accurately show whether the number of these incidents are increasing, decreasing, or staying the same relative to the number of covered facilities.

According to EPA's 2018 Regulatory Impact Analysis, "Although the accident histories submitted with RMPs have shown a reduction in the frequency of accidents since the beginning of the program, there continue to be serious chemical releases. RMP data for 2004 through 2013 show that each year there are an average of approximately 150 accidents with reportable impacts."

Yet EPA also maintains that there is now a "…low and declining accident rate at RMP facilities…" EPA also notes, however, that "Past experience with RMP facility accident reports suggests that following the next 5-year reporting wave… the current 2014, 2015, and 2016 accident totals will increase."

Moreover, EPA explains only the year and number of accidents occurring in that year (and some totals and averages). Their analysis does not indicate a rate calculation – the number of accidents that occurred in a year divided by the number of facilities that could have had an accident during the year. EPA uses only the static number of reporting facilities from the 2015 RMP database without updating this number, which fails to account for manufacturing plant closings.

> One opportunity for CSB is to issue an incident reporting rule, as directed by our enabling law. On February 4, 2019, a U.S. District Court judge ordered CSB to issue, within one year, a regulation requiring facilities to report chemical incidents to CSB. This regulation and the resulting data base can help everyone, over time, understand chemical incident trends.

ONGOING PRODUCTION AND COMPETITIVE PRESSURES

Corporate leaders truly want safe operations and zero incidents. Most, however, face enormous bottom line production pressures. Often, meeting obligations to stockholders is paramount.

It's common knowledge that corporate leaders control investment decisions. They decide what products are made and where they are produced, the choice of technologies, production targets, preventive maintenance allocations, staffing levels, and workforce training. They choose their facility and enterprise levels of risk tolerance and allocate budgets for safety. In a challenging economic environment, they make key decisions that determine safety outcomes.

Executives themselves are concerned. Three of every four executives felt operational risks in their companies were inadequately managed, according to a 2018 report by DuPont Sustainable Solutions. Their report also found that "process safety" was one of the least discussed topics at Board meetings.

> An opportunity for CSB stems from our in investigation of the 2010 Macondo well disaster in the Gulf of Mexico when the Deepwater Horizon rig blew out, leading to explosions and fires that killed 11 workers and massive marine and costal damage. A CSB recommendation to the Bureau of Safety and Environmental Enforcement (BSEE) in the Department of

Interior called upon the agency to draw upon the best available global standards and practices and develop guidance addressing the roles and responsibilities of corporate board of directors and executives for effective major accident prevention.

After BSEE rejected CSB's recommendation, CSB committed to issuing this important and broadly applicable guidance. This guidance could urge offshore oil and gas operators and contractors to adopt effective process safety systems, ensure board competency and training, enable reporting by employees of incidents, near misses, and "what could go wrong" to top executives, build strong worker participation programs, assess executive compensation programs that incentivize production over safety, and address other critical matters.

Hearing the views of corporations, unions, standard setting organizations and others with serious commitments to process safety will be important for issuing the best possible CSB guidance.

THE SAFEGUARDS THAT PROTECT ALL OF US ARE UNDER ASSAULT

Since their adoption, federal regulatory safeguards to prevent chemical incidents have not been fully modernized. And even modest improvements are now threatened**.**

After the 2013 West Fertilizer Company disaster, President Obama issued an Executive Order mandating federal agencies, including OSHA and EPA, to "…consider whether to pursue an independent, high-level assessment of the U.S. approach to chemical facility risk management to identify additional recommendations for all levels of government and industry to reduce the risk of catastrophic chemical incidents in the future". This order, however, did not prompt serious debate about major reform.

The Executive Order led to forward steps, most notably a revised EPA RMP rule that was issued in the last days of the Obama Administration. Today, reforms to OSHA's Process Safety Management (PSM) standard languish on OSHA's regulatory agenda for "long term action".

Now the EPA is moving to dismantle even the modestly improved 2017 RMP rules. They plan to issue a final rule, currently under review at the Office of Management and Budget that rescinds provisions on safer technology and alternatives analyses, third-party audits, incident investigations, and public access to information. EPA's own analysis admits that their rule will have a disproportionally negative impact on people of color and low income communities nearby industrial facilities.

Unfortunately, dismantling these steps forward has received total support from industry trade associations.

> As an independent agency, CSB's opportunity is to continue our work based on a solid scientific and analytical footing -- and to urge effective government regulation when needed. CSB has called for a stronger, not weaker, RMP and PSM rules. Our recent reports continue to call for other sensible safeguards, such as new regulation of the onshore oil and gas drilling industry that was exempted from PSM.

Continuing disasters, intense corporate bottom-line pressures, and threats to public safeguards, means that CSB's work is as important as ever.

CSB is moving forward to issue an incident reporting rule, produce guidance for corporate boards and executives in the offshore oil and gas industry, and to call for needed safety rules.

In addition to these actions, please consider four additional proposals. All four reforms would increase the authority of those with safety responsibilities.

First, chemical engineers and other safety professionals need greater influence, as suggested by our investigation of the 2012 incident at Chevron in Richmond, California where the requests of company engineers to prevent corrosion were not heeded before a loss of containment led 12,000 residents to seek medical evaluation. HSE professionals should have clear lines of reporting to top executives and greater authority over safety decision making.

Second, corporate Boards should have at least one member with professional expertise and experience and a clearly defined role to receive reports of incidents, near misses, and process safety risks and power to bring these issues to the attention of the entire board. This was a CSB recommendation to BP after the 2005 Texas City refinery disaster which killed 15 contract workers.

Third, according to a recent CSB Safety Digest, "worker participation is essential to improving process safety and preventing incidents at facilities with hazardous chemicals." These facilities should have, by law, a safety, health, and environment committee with equal representation by management and workers. In union represented facilities, to comply with the National Labor Relations Act, unions must select the employee committee members. Committees should have authority to investigate hazards, incidents, and near misses, to help develop stop work authority programs and other policies, and to participate in all aspects of chemical safety. There are clear precedents for worker engagement. The 2017 California OSHA PSM standard covering oil refineries offers opportunities for worker participation in all aspects of the standard. Sixteen state laws require safety committees. Some labor-management contract agreements establish full-time worker safety and/or process safety representatives.

And fourth, Local Emergency Planning Committees (LEPCs) deserve what they need to do their jobs to help prevent incidents, not only respond to them. The Emergency Planning and Community Right to Know Act was enacted to help accomplish this – but Congress provided no funding or funding mechanism. LEPCs should have a budget to hire experts, train their members, audit plants, and expand public engagement, including with workers and the low income and communities of color so often disproportionately harmed by hazardous releases.

CSB's investigation of the 2013 West, Texas ammonium nitrate disaster, which killed 12 volunteer firefighters, underscores the urgency of providing our responders adequate resources.

I hope the CSB will consider these four proposals in the future, whether as relevant recommendations stemming from incident investigations or through new safety studies of key issues.

I encourage you to consider and debate these proposals, as well as your own ideas.

Achieving any major changes will be hard. It will take time. But the alternative – more preventable disasters – is unacceptable.

In closing, thank you again for your support of CSB. It's made a huge difference. And please…

- Sign up to get the latest information at csb.gov
- Read our investigation reports and watch our videos
- Share them with colleagues, executives, and your workforce;

And

Be an engaged stakeholder – if you have a suggestion or see a need for CSB action – make sure CSB Board Members hear it.

Finally, thank you for what you do every day to protect workers, our communities, and our industries -- and for debating what it will take to achieve a nation safe from chemical disasters.

EPA RMP Reportable (Impact) Accidents by Year 2004-2016

Year	Impact Accidents
2004	197
2005	152
2006	140
2007	204
2008	168
2009	149
2010	128
2011	138
2012	118
2013	123
2014	128*
2015	113*
2016	99*
Total (2004-2013)	1,517
Total (2005-2014)	1,448
Total (2006-2015)	1,409
Total (2007-2016)	1,368
Average/Year (2004-2013)	152
Average/Year (2005-2014)	145
Average/Year (2006-2015)	141
Average/Year (2007-2016)	137

*May increase after the 2019 RMP reporting wave occurs.

Source: Regulatory Impact Analysis Reconsideration of the 2017 Amendments to the Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act, Section 112(r)(7) U.S. Environmental Protection Agency (EPA) Office of Land and Emergency Management (OLEM) Office of Emergency Management (OEM), April 27, 2018, page 34 (Exhibit 3-7).

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Unravelling Reactive Chemicals Mysteries: Experiences in Reactive Chemicals Incident Investigations

Rob Bellair*
Dow
*Presenter E-mail: RJBellair@dow.com

Abstract

How do you determine the root cause of an incident where a chemical containing vessel violently ruptured and the only witness of what happened was fatally injured? What do you do when all of the witnesses of an incident have unclear memories of what occurred, or if the accounts conflict with what science says is possible? There are many potential traps, pitfalls, red herrings, and wrong turns that can occur in challenging incident investigations and it is of critical importance that investigators tirelessly work toward identifying the true root cause. It can be argued that misidentification of a root cause can result in a more hazardous environment than never performing the investigation at all. In this presentation, highly valuable learnings and examples from investigations are discussed, where a single piece of overlooked evidence unlocked the path to a root cause, when a red herring was prematurely accepted as a root cause, when conflicting evidence threatened to make a conclusion impossible, and where confirmation bias drove an investigation far down the wrong path.

MARY KAY O'CONNOR
PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

We Don't Learn Enough from Incidents: the Roots of Human Errors

Mónica Philippart*, PhD
Ergonomic Human Factors Solutions
Austin, TX 78733
*Presenter E-mail: monica@ergohfsolutions.com

Abstract

Process Safety aims to prevent and control incidents that have the potential to release hazards that could result in serious undesired outcomes. It has been widely agreed for some time now that human error is a causal factor in most accidents. Therefore, adequate human error management is indispensable for comprehensive Process Safety Management.

Regulatory requirements to consider human factors in Safety and Environmental Management Systems have motivated companies to address human error; and so, efforts dedicated to the analysis of human factors in investigations have been increasing. However, these efforts are generally not effective at reaching the root causes of the errors, leaving organizations with the false sense of security that human error is being adequately managed. We are not learning enough, particularly from offshore incidents, and as a result, we keep having incidents that would have been preventable and organizations are not able to continuously improve. Human factors needs to be taken more seriously as a discipline that requires not just a basic understanding and some tools with guidance, but competency; i.e., deep knowledge and skills that have been developed through effective practice.

This paper provides an overview of the incident investigation process, and overview of the fundamentals of human error, and discusses why, in the experience of the presenter, many organizations, while investing time and effort, don't learn enough from incidents.

Keywords: Continuous Improvement, Human Error, Human Factors, Incident Investigation, Process Safety, Root Cause Analysis.

Introduction

Specific numbers vary depending on the research, but it is generally agreed that human error is one of the main causes of industrial incidents. Some have found that 90% of the accidents that occurred in the workplace are due to human error, while others argue that 99% of accidental losses (excluding natural disasters) begin with human error (M. Made, R.S. Taufik and Gustiyana T., 2018).

As defined by the American Institute of Chemical Engineers (AICHE), “Process Safety is a disciplined framework for managing the integrity of operating systems and processes handling hazardous substances”; i.e., Process Safety aims to prevent and control incidents that have the potential to release hazardous materials or energy through the management of relevant systems and processes.

Bridges and Tew explain that Process Safety Management in general focuses on maintaining human errors at a tolerable level because even the premature failure of equipment is caused, if investigated deeply enough, by human error. Multiple management systems are used to control human error and limit its impact on safety, environment, and quality/production (2010). Hence, comprehensive Process Safety Management requires adequate human error management.

The author of this paper has two decades of experience conducting, overseeing, evaluating and teaching incident investigation and Root Cause Analysis (RCA) in the aerospace and petroleum (conventional and unconventional drilling including both operators and drilling contractors) industries. This experience has motivated the attempt to bring to light a shortfall commonly found in investigations, even in those conducted by organizations highly motivated and committed to continuous improvement, which is that they do not uncover important lessons that could be learned were more thorough analyses completed. The author has witnessed in every case the use of renowned methodologies and tools; therefore, this paper does not offer recommendations on which to use. Also, every investigation observed was performed by sharp individuals who participated to the best of their abilities and were interested in delivering a thorough investigation; therefore, the author does not doubt that those assigned to incident investigations are interested and sharp individuals.

The objectives of this paper are to help organizations:

- realize that the incident investigations they are conducting may not be as effective as they intend and, more importantly, as they assume;
- understand what they can do to improve their investigations;
- and to encourage those who need it to make the changes necessary to maximize the benefits of their investigation efforts.

The goal is to improve the robustness of process safety and risk management, and enable more efficient continuous improvement.

The paper first provides an overview of the incident investigation process, then offers an overview of the fundamentals of human error, and finally explains the reasons why many investigations observed in the past two decades did not uncover the root causes of the incidents.

Overview of the Incident Investigation Process

Development of incidents

For the purpose of this paper, an incident refers to an event or result that is unwanted and that the organization wishes to investigate. Incidents are usually the result of a series of events that took place under certain conditions.

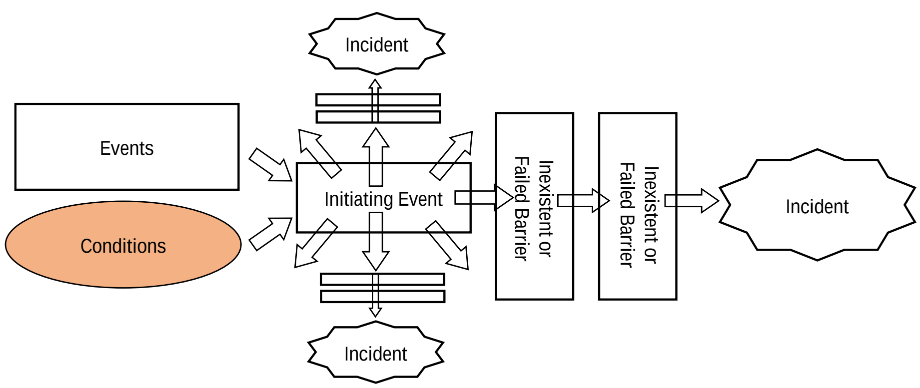
Events are occurrences describing discrete actions related to the incident. They include failures, malfunctions and errors. Initiating events are those that release a hazard. There are four types of events:

- Correct actions.
- No action when action is required.
- Incorrect actions (including actions that are not required)
- Failures, such as something buckling.

Conditions are inactive situations or circumstances that enable the events related to the incident. Examples are equipment that does not meet specifications, a wet surface, small font or ambiguous instructions.

Barriers are defenses against hazards and can be engineered or administrative. Engineered barriers automatically perform their function; however, administrative barriers rely on human action and compliance to prevent, detect and/or correct problems.

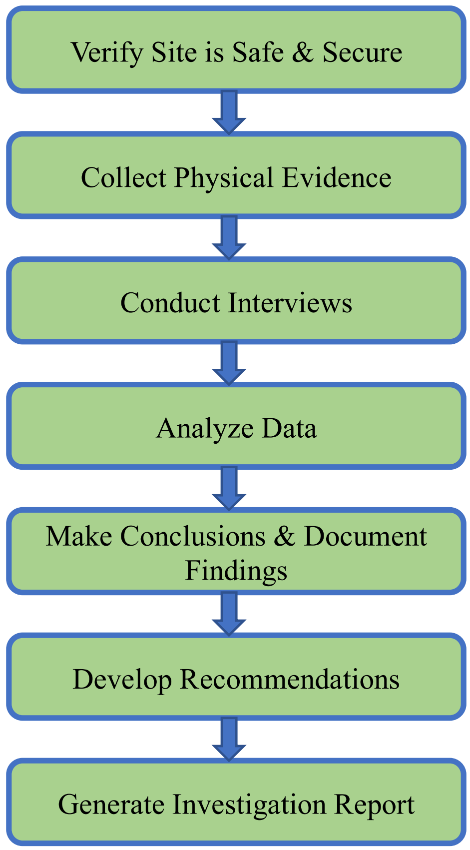
Figure 1. is a simplified representation illustrating that Events and Conditions lead to Initiating
lt is
l be
ould
dent



The investigation process

The purpose of investigations is to determine the causes of incidents to enable the development of recommendations that will prevent future incidents. Investigations contribute to Continuous Improvement.

Generally, the phases of an investigation are:



The steps in t
analysis.

<u>Root Cause A</u>

The incident
incident) to u
most organiza
Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) in 2016, the organizations "urge employers (owners and operators) to conduct a root cause analysis following an incident or near miss at a facility" and define root cause as "a fundamental, underlying, system-related reason why an incident occurred that identifies one or more correctable system failures." The document further states that "By conducting a root cause analysis and

addressing root causes, an employer may be able to substantially or completely prevent the same or a similar incident from recurring."

RCA is a systematic and structured evaluation methodology that helps identify the immediate, intermediate and root causes of an incident. Identifying immediate causes is necessary to prevent the incident from reoccurring; but identifying root causes is necessary to eliminate or modify systemic problems so that future related occurrences may be prevented, thereby helping organizations improve their management system. Though by addressing immediate causes an organization improves, by addressing root causes the organization improves more efficiently. As Bridges and Tew affirm, "Management systems control the interaction of people with each other and with processes. [...] If management systems are weak, then layers of protection will fail and accidents will happen" (2010).

RCA helps determine:

The interactions between human activities, system organization and equipment have become more complex, and therefore the technical analysis of incident sequences have also become more difficult, requiring multidisciplinary interventions to identify the root causes.

Overview of Human Error and Contribution of its Analysis to Investigations

Human events and conditions

A human event is one in which the human performed the action in an event relevant to the incident. A human condition describes the physical, mental or emotional state of a person when that person contributed to the incident. Some human No Action and Incorrect Action events are intentional and therefore do not qualify as errors. These can then be categorized as horseplay, violations or sabotage.

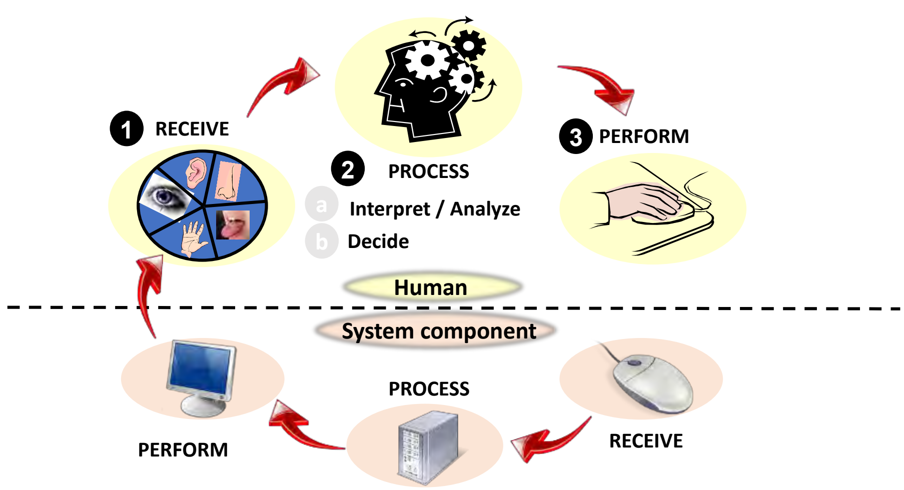
When No Action or Incorrect Action events are not intentional, the events are classified as Human Error. The key is where there was intent. A person can unintentionally not perform an action that was required, unintentionally perform an action incorrectly, unintentionally perform an action that was not required, or intentionally perform an action but with unintended consequences.

For the purpose of this paper, Human Error is defined as an unintended action or the failure to perform an action as required, thereby not producing the anticipated results and potentially leading to an incident.

Human Factors discipline and basic concepts

In order to understand human error, one must first understand some basic concepts of the Human Factors discipline. Human Factors is the application of knowledge about human capabilities and limitations to system, equipment, job or environment design and development to achieve efficient, effective, comfortable and safe performance with minimum cost, manpower, skill and training.

Figure 4 illustrates how humans interact with a system. We receive (or fail to receive) information;



all of this happens in the context of an environment which may make it more or less difficult for these interactions to occur.

Human error can occur at any of the stages of the human- system interaction, and while interacting with anything; from interactions with tools and machines to interactions with other people, computer software, while reading documents… There are factors that make it more or less likely that these interactions are successful. These can be individual physical or mental attributes of the person relevant to the human event, or factors external to the person. Therefore, there are a myriad of sources of evidence, countless opportunities for error, and much human error evidence to collect and evaluate for possible contribution to an incident.

Human Factors contribution to investigations

As stated earlier, the incident investigation process evolved from finding fault (what caused the incident) to understanding why (Gambetti F., Casalli A. and Chisari V., 2012). Similarly, while human error used to be seen as a the cause of incidents, today it is recognized that human error is not a cause, but a symptom of underlying system management failure (Dekker, 2002), eventually leading to the realization that most incidents are in fact caused, on some level, by human error as today's complex systems often surpass the capabilities of the people who operate within them.

Future performance can be improved by understanding the reasons past incidents occurred and applying the lessons learned. In order to understand how an incident developed, it is necessary to understand the perspective of those who were involved; i.e., what led people into thinking or behaving the way they did. This requires the analysis of the human-system interactions, including the internal and external factors that influenced them – Human Error Analysis.

It is also necessary to evaluate the barriers that failed to prevent the incident. As explained earlier, administrative barriers rely on human action and compliance to prevent, detect and/or correct problems. But even engineered barriers depend on people at one point or another (in the design, selection, maintenance, installation, etc.) For these analyses too is necessary the application of human factors.

Human Factors is also valuable for the development of recommendations, particularly when attempting to prevent specific human events. Some errors can be prevented, while others can only be detected and corrected before they create incidents. Therefore, the application of human factors and thorough human error analyses are imperative for more effective prevention of incidents.

Why We're Not Learning All We Could

Though it is a generally recognized that human error plays a large role in causing process plant accidents, in contrast to the nuclear and aerospace industries, very little human error analysis is carried out in the petroleum, petrochemical and chemical industries (Taylor, J. R., 2013). Taylor believes that the main reason for this is that "it is quite hard to do, requiring considerable effort from already hard pressed engineers."
Following are explanations of what have been observed over the past two decades to be key reasons why organizations are not learning valuable information from incidents.

Inadequate use of the Human Factors expert

The Human Factors investigator should have the following specific responsibilities, in addition to any other requested by the investigation chair:

1. Identify human events and conditions that may have caused or contributed to the incident.
2. Identify and collect relevant evidence.
3. Determine why human events and conditions occurred (identify cause-effect relationships).
4. Evaluate barriers and determine why they failed or were exceeded.
5. Generate recommendations to prevent similar occurrences.

These responsibilities span all phases of the investigation process; therefore, the Human Factors investigator should participate in the process from the beginning and remain as part of the core team through the development of recommendations.

Many organizations consider the Human Factors investigator an "add on" to call upon on an "as needed" basis, which often happens after the evidence has already been collected. In some cases, the Human Factors investigator is not called at all because the team members deem that they are sufficiently capable of performing the necessary analyses.

Sometimes the Human Factors investigator never really joins the investigation team but instead is given the "relevant" information and asked to perform an analysis on specific errors (as identified by the investigation team) on the side and then submit the results to the team. There are several shortfalls with this approach, for example those related to the qualifications the people deciding a) the human events that are to be analyzed and b) the "relevant" information to provide to the Human Factors investigator. Just as in a drilling-related incident a drilling specialist would not be called in only to provide expertise for the drilling portion of the sequence of events but instead is a major participant in the investigation, knowing that human error is a main contributor to all incidents justifies the Human Factors investigator to be part of the core team.

Considering that evidence could be necessary from any of the human-system interactions potentially related to the incident, including the internal and external factors that influenced those interactions, and considering the extent and level of knowledge necessary to be able to identify such evidence, without involving the Human Factors investigator from the beginning it is unlikely that sufficient evidence is collected and therefore, no matter how good the Root Cause Analysis with the rest of the evidence, it is unlikely that the investigation arrives at the most helpful conclusions.

Unqualified Human Factors investigator

Some organizations do not assign a Human Factors expert to their incident investigations but instead either require the investigation team to consider Human Factors, or assign someone that role – usually someone with either some familiarity or interest in the Human Factors field. Senior management has been heard making comments such as "We have smart engineers. A "lunch & learn" is enough to prepare them for investigations." But performing human factors analysis not only requires considerable effort from already hard pressed engineers; it also requires deep specialized knowledge.

Human factors is considered by some in management positions as a skill that almost anyone can apply with just a bit of training or reading if just supported by good tools. This is an appealing thought, as it would enable analyses to be performed more routinely in their organizations. There are in fact very good tools aimed at helping Human Factors investigators, but with the proper background. Those aids are not adequate substitutes for properly trained Human Factors experts knowledgeable in the necessary aspects of the discipline. Human Factors is a discipline that requires a college degree, and requiring someone without the necessary knowledge to practice it, no matter how bright the individual, is not only unfair but ineffective. The risk of having unqualified people use those support tools is that the product looks good (with classifications, nomenclature, etc.), but is likely not thorough or perhaps even correct.

It has also been observed that a person has become a "Human Factors expert" in an organization simply because he or she has been performing that role for many years; but again, without the adequate background from the start. Those individuals now feel comfortable with the terminology and tools, and confident about their expertise, and the organization has become accustomed to seeing their product; and so neither has a doubt about the quality of the investigations.

Even those with a Human Factors degree are not necessarily qualified for what should be the Human Factors investigator role inherent responsibilities. Consider the medical field; as expansive and multifaceted as the intricacies of the human body, in which each medical specialty fits to serve the needs of a particular realm of care. Specialties range from allergy and immunology, anesthesiology and dermatology through diagnostic radiology and internal medicine all the way to Urology. All of them are doctors; however, a dermatologist would probably not be able to adequately diagnose a liver problem. Similarly, human factors is a systems-oriented discipline which extends across all aspects of human activity. The discipline promotes a holistic approach in which physical, cognitive, social, organizational, environmental and other relevant factors are taken into account and, therefore, is a combination of numerous disciplines, including psychology, sociology, mechanical and industrial engineering, biomechanics, industrial design, physiology, anthropometry, interaction design, visual design, user experience, user interface design, information design, kinesiology, cognitive psychology, industrial and organizational psychology, space psychology and more. Consequently, there exist domains of specialization within the discipline which represent deeper competencies in specific human attributes or characteristics of human interaction, and so, human factors practitioners come from a variety of backgrounds.

No single person can be expected to be knowledgeable in all aspects of human factors, but in order to adequately accomplish their responsibilities, human factors investigators should have basic knowledge of human physical and psychological processes, capabilities, skill levels, and limitations and, in order to effectively apply this knowledge to incident investigations, knowledge of the methods to:

- identify human events and conditions
- identify errors and types of errors
- identify factors that affect performance

- interview witnesses
- identify cause-effect relationships among events and conditions
- create timelines
- perform Root Cause Analysis
- perform barrier analysis
- draw conclusions
- generate recommendations that will reduce human error or mitigate the negative consequence of human actions.

Simply providing tools to someone with only familiarity of the Human Factors discipline cannot replace an adequately qualified person.

Ending RCA prematurely

Organizations such as the Center for Chemical Process Safety and OSHA agree that root causes of accidents are management system weaknesses, which lead to human error, which lead to accidents (Bridges, W. & Tew, R., 2010). RCA seeks more than just preventing recurrence of the exact scenario under investigation.

Most investigations (see Figure 5):
- Identify the part or individual that failed (Top dart).

be properly

e We Here?

part or individual that
dart).

type of failure (Did not

asic event or condition that
failure (RCTDH could not
cleaned and lubricated on

alysis.

is approach:
ng causes may
roduce problems, not
he same way or in the

Failure to Release Top Dart

Dart Release Valve Malfunction

RCTDH Improperly Clean & **Lub'd**

Unable to Properly Clean
& Lubricate on Rig

Shenzi G1-4 - Cement Head

After pumping 80bbls of 12.5ppg spacer and 589bbls of 16.4ppg cement, the top dart could not be released.

The problem with this approach is that we stop before we learn information that can help us address the underlying causes and therefore continue to have problems (not necessarily the same way or in the same areas). The analysis should continue until one the following is reached:

- an organizational factor that has control over the design, fabrication, development, maintenance, operation, or disposal of the system related to the incident. This would be a root cause.
- A problem out of the control of the organization.
- Insufficient data to continue.
- An event or condition that is not a problem.

Not analyzing near misses

Near misses are evidence of management systems weaknesses. Many organizations choose not to thoroughly investigate near misses, and so, with only a superficial investigation, only the immediate and intermediate causes of those events are identified. This results in:

- the root causes (the management system weaknesses) continue to exist,
- the organization continues to be unaware of the system weaknesses, since they were not uncovered by the investigation,
- and, perhaps more importantly, the organization now believes that the problem(s) that caused the near miss has been addressed.

Human Factors seems commonsensical

Though most engineers don't necessary feel qualified to conduct a human factors assessment, many do feel like they could at least notice if a human factors assessment is nonsense. We are human after all, so we must be able to understand how one could have made a mistake if we just look at the evidence calmly and after the fact (hindsight is 20/20, right?) In fact, what is quite easy is to unknowingly make a poor human factors assessment, and for such assessment to appear thorough and of high quality.

Human Error is popular enough that many can use the language and propose hypotheses that sound plausible and logical. Human Factors investigators who were not adequately qualified in the investigations observed were always able to produce work with which they were satisfied (i.e., they were confident that they did a great job). The results were also accepted by the rest of the investigation team and management, who were unable to realize what incorrect assumptions were made and what factors and evidence were omitted. As stated earlier, these were all sharp people genuinely trying to achieve the best result; but one doesn't know what one doesn't know.

Yes, immediate and intermediate causes are often identified and addressed (we are eliminating mosquitoes), but if we are not identifying the source of the problem (the proverbial pond), then we'll keep having incidents.

Conclusion

This paper provided an overview of the incident investigation process and an overview of the fundamentals of human error in order to provide sufficient background. The purpose was to be able to explain why many investigations do not reveal enough about what caused the incidents, even when conducted with the best effort and intentions. The objectives are to help organizations first realize that they may not be obtaining the expected outcomes from their investigations, second, understand the reason for the weakness in their investigations so they can make the necessary changes, and finally, to encourage organizations to make the changes they need.

It is not unusual to point out that investigations often address symptoms rather than problems; however, this paper intended to be more specific. For example, rather than warning "Don't make a mistake on your paper!", the aim was to specify "Check the punctuation and spelling" and then point out common punctuation and spelling mistakes.

By assigning an adequately qualified human factors investigator and having this person be part of the investigation team from beginning to end, together with an understanding that the investigation needs to arrive at causes at the organizational level (root causes) the quality of investigations can be improved and much more insight can be gained from the effort. Corrective actions will be more effective and address a broader range of issues than simply the immediate cause(s) of the incident under investigation.

The hope is that this paper opens the eyes of those who instinctively believe that by assigning a "Human Factors expert" and/or using Human Factors investigator aids they are adequately managing Human Error, and is seen as an opportunity to improve, to maximize the benefits of their investigations and make them more effective, enhancing process safety, risk management, and continuous improvement.

Bibliography

Bridges, W. & Tew, R. (2010). Human Factors Elements Missing from Process Safety Management (PSM). Process Improvement Institute, 6th Global Congress on Process Safety and the 44th Annual Loss Prevention Symposium, 01-24

Dekker S.W.A., 2002, Reconstructing human contributions to accidents: The new view on error and performance, Journal of Safety Research, 33, 371-385.

Gambetti F., Casalli A. and Chisari V., 2012, The human factors in process safety management, Chemical Engineering Transactions, 26, 270-284 DOI: 10.2202/CET1226047

M. Made, R.S. Taufik and Gustiyana T., Fatigue and Human Errors Analysis in Petrochemical and Oil and Gas Plant's Operation. Proceedings of the International Conference on Industrial Engineering and Operations Management Bandung, Indonesia, March 6-8, 2018

NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping, Office of Safety and Mission Assurance, NPR 8621.1C

OSHA EPA Fact Sheet, The Importance of Root Cause Analysis During Incident Investigation, DOC FS-3895 10/2016

Taylor, J. R. (2013). Incorporating Human Error Analysis into Process Plant Safety Analysis, AIDIC, 31, 301-306. Available: DOI: 10.3303/CET1331051. ISBN 978-88-95608-22-8; ISSN 1974-9791

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Managing Tanks as a Portfolio of Assets

Phil Beccue[1], Dan Brooks*[2,3], and Philip Myers[2]
[1]White Deer Partners Decision Consulting
[2]PEMY Consulting
[3]Arizona State University
*Presenter E-mail: phil@pemyconsulting.com

Abstract

The capital investment in tank storage is a critical component of most energy companies' business model. Decisions managing these assets are driven by the organization's overall performance objectives, business policies, balancing the risks and returns associated with different resource allocations. The discussion that follows in the body of this paper has two objectives: The first is to describe a foundation for evaluating decisions about managing tank risk that takes into account all the risk assessment techniques traditionally used but adds to this a way to incorporate these findings into a decision context that also views tanks as part of an organization's overall business model and managed as part of the organization's overall portfolio of assets supporting its business model. The second objective is to show there are basic analytical tools that add precision to the perspective described in the first objective through straight-forward quantification.

Background

Managing significant asset investments based solely on compliance requirements, the recommendations of risk assessments output by QRAs, PHAs, or other risk assessment methods ignores the central role these assets (including their risks) play in creating value for the organization. Compliance guidelines provide boundaries on the range of decisions that are allowable, but compliance guidelines by themselves fall short of assuring good or even reasonable value-based and business-model driven investment decisions. This paper describes the way in which tank management can use traditional inspection results or risk assessment results such as probability risk assessments (PRAs) or layers of protection analyses (LOPAs) in a basic portfolio structure that links tank management decisions to the organization's business model and economic objectives at the corporate level.

An organization's overall business model and value-creation objectives should play the fundamental role in managing its portfolio of tanks. This decision context allows the organization to invest in the creation, maintenance, replacement or retirement of tankage based on the ways market conditions, technology, regulatory guidelines, and the organization’s business objectives and strategies are changing.

Viewing the management of investments in the tank portfolio as primarily a matter of regulatory or internal corporate compliance is as ineffective as viewing compliance as the basis for the organization’s investment in any other asset – personnel, real estate, financial instruments, marketing, logistics, acquisitions, or any other key component of the business model.

This paper describes an energy company’s tankage as a portfolio of investments that play a key role in achieving the organization’s business objectives. Investments in that portfolio, therefore, would be, within regulatory guidelines, driven by the degree to which those portfolio investments aid achievement of those objectives, balance risk and reward consistent with the organization’s policies, and increase the overall value of the organization to shareholders and stakeholders.

Investments at the organization level functions something like bets: the forecasted benefits are compared to the forecasted costs and resources are allocated according to the organization’s appetite for risk and the expectations of shareholders or owners. Investments in tanks have basically the same structure at the individual tank level. Inspections are conducted, risk assessments are performed, and estimates of various characteristics of the tanks are used to determine the level of further investment that is warranted. Industry guidelines play a key role in the subsequent tank investment decisions following inspections and risk assessments. This paper shows how tank investments can be viewed as a portfolio of investments serving the organization’s business objectives.

Mission-based perspective of tanks as a portfolio of assets

Overview

Energy companies provide crucial products and services to any economy: they create and distribute stored energy in the form of fuels. Storage capacity is central to both the creation and distribution of fuels, so investments in tankage is key to mission success. The Department of Energy maintains strategic storage of hydrocarbons to help balance global shortages that could threaten the economic stability of a country or region.

The “mission” of an organization is the set of fundamental objectives or goals of that organization; the set of objectives that describe what the organization values, wants to accomplish, and uses as performance metrics for their operations. Energy company business plans typically include both tangible and intangible objectives; there are clear financial performance targets, but also efforts and investment toward achieving environmental sustainability, an injury-free workplace, satisfied customers and a respected corporate brand and reputation.

This means in practical terms that the organization’s mission statement and corporate objectives need to be translated into explicit and measurable guidelines for managers making resource allocation decisions in the various divisions and business units.

Storage decisions considered at the "mission" level of an organization entail a number of strategic considerations. The list can be long or short, but often includes consideration of such things as overall capacity, capacity by product type, location, network connectivity (piping and manifolds), clustering in tank farms, right-of-way and transportation issues, environmental and regulatory considerations, investment and maintenance costs, estimated revenue and profit contributions, and more. Investments in creation and maintenance of storage should be considered in light of alternative investments in other aspects of the organization's business model, as well, but the complexity of technical management and local decision making make these comparisons rare and difficult to characterize. For example, how do returns on investments in maintenance of current storage capacity in some region compare to investments in new types of storage in new locations, or expansion of the organization's business model into new products or partnerships or alternative transportation modes? Since the business consequences of investments in tanks are often left unspecified, these types of business comparisons do not occur.

Consideration of corporate business-model concerns has become particularly important for energy companies over the past ten years and expectations are that shifts in overall business focus for many, if not most, large legacy energy companies will be shifting even more in the next ten years.

Signals of a fundamental and long-term shift in energy company business models include some of the following. In the late 1980s and early 1990s, six of the 10 largest organizations in the S&P500 list were energy companies. Now, only one is. Wall Street analysts used to value energy companies by giving significant weight to the size of their reserves because the organizations were considered to be something like utilities in terms of their ability to generate returns for investors over the long term. Now Wall Street evaluates energy companies more like speculative investments and values them increasingly based on their ability to generate profit for investors. This change in energy markets has shifted energy company business models to focus more on the bottom line and margins. In other words, it has changed the meaning of "risk" for these companies. The companies vary in size, market, operating expenses, capitalization, and other key features of their various business challenges.

In this changing economic environment, basing investments solely or even heavily on generic industry-wide compliance guidelines that are typically business-model agnostic and ignore an organization's specific competitive landscape may not be as helpful as it has been in the stable past for maximizing returns to those investments.

In summary, if tanks are viewed as a portfolio of capital assets and key contributors to the organization's overall business model, then decisions about investments in this portfolio of assets should be considered in light of the organization's overall business objectives and return on investment in storage compared to comparable investments in other aspects of the organization's overall business.

This might mean that, similar to other business units, investments in tank storage are viewed on a spectrum from speculative investment in high-risk, high-return ventures all the way to divestiture and abandonment of localized or regions unproductive business operations.

There would typically be a fairly wide range of tank investment decisions based on the organization's business model and the role that each tank or set of tanks plays in achieving the business objectives of the organization. For illustrative purposes, business-model decisions are consolidated in the remainder of this paper to four common types. These are tank investment decisions motivated by:

- Pursuit of new business opportunities
- Growth of existing business
- Sustaining current business
- Abandonment or divestiture of current business

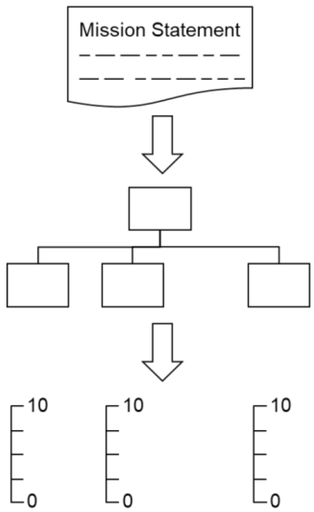
It's important to note that while these decisions are based on the organization's business model (that is, business purposes at the corporate level), the activities funded specifically at the tank or set of tanks level. So, for example, pursuit of new business may mean more frequent use of certain tanks that are in highly sensitive areas and are used for persistent or more toxic products. So more thorough and extensive investigations of risks associated with low probability but high consequence outcomes may be warranted. Is this level of investment a good idea? Figuring that out must include explicit consideration of the business opportunities presented by safely operating tanks – if the business opportunities are small, perhaps not, but if they are strategic, long-term, and large-scale plus are part of the organization's overall shift in business objectives, those investments may be very worthwhile when considered from the corporate point of view.

This example of evaluating an investment in sophisticated risk assessment illustrates the importance of viewing tank storage viewed as a *portfolio* of capital assets. Such an investment isn't an investment in one or two tanks but part of the investment in tankage overall and the role it plays in the business model. Should the portfolio be rebalanced? Should other tanks get less investment as strategy shifts to other parts of the business model? This is consideration of how to optimize the whole of investment in tankage, not just the last or incremental dollar. This is different from a tank-by-tank decision process where each tank is viewed in light of some combination of compliance requirements or location-specific risks or current business uses. Portfolio considerations include the overall role of tankage at the organization level and looks to maximize the total return to investment with respect to that business model, not just the individual benefits of tank-by-tank compliance.

Portfolio analysis can be conducted at many levels of sophistication. What follows is a basic approach that can be tailored to an organization's business environment and situation.

Conceptual approach

Translating an organization's mission into practical guidelines for decision making is key to prioritizing resource allocation, as illustrated in the figure below.



Mission:

- Achieve financial success

Objective:

- Maximize net pre-tax profit

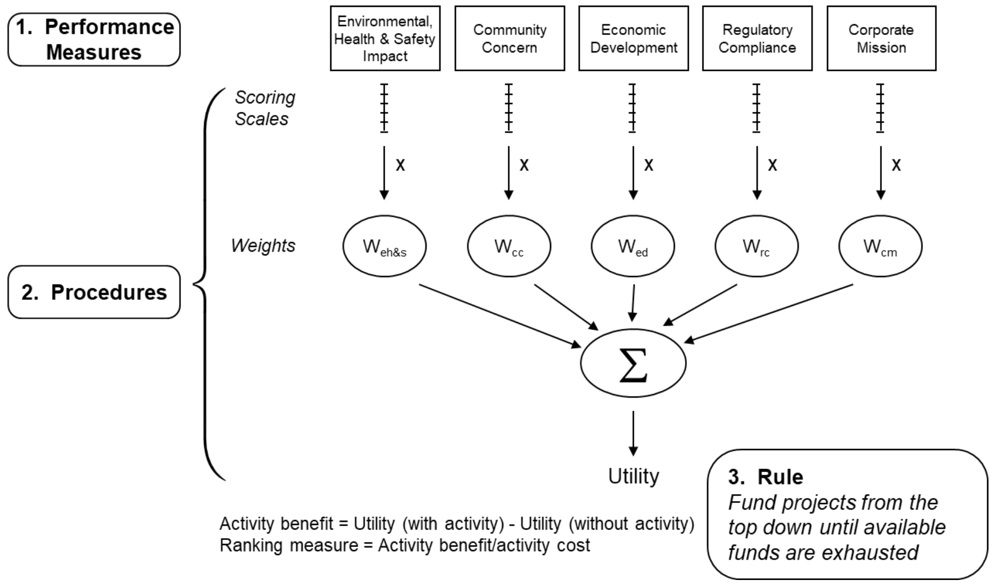
Performance Measures:

- Expected annual revenues
- Expected annual expenses

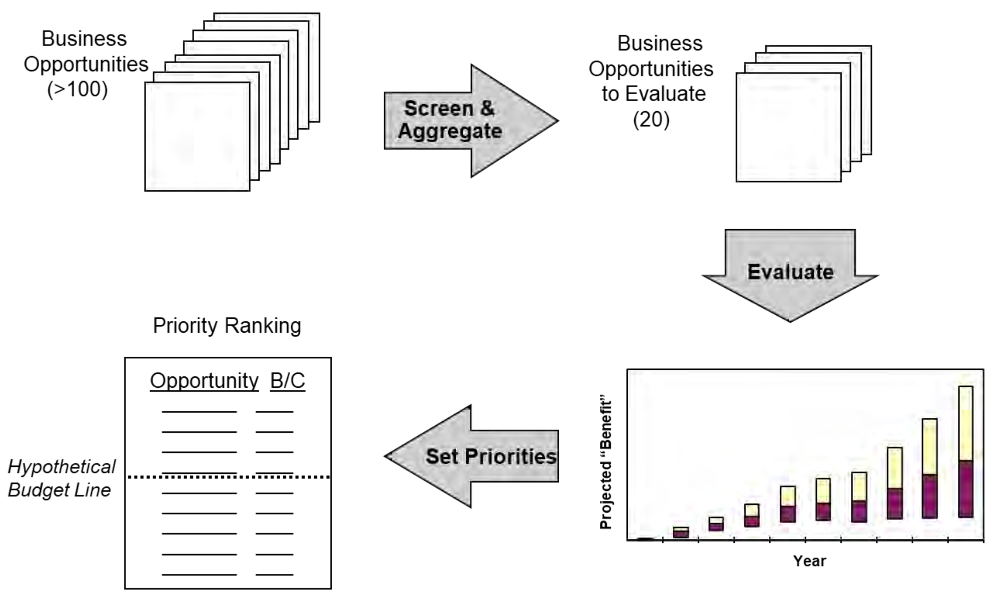
The goal of priority setting is to use limited resources in a way that maximizes the attainment of the organization's mission goals. If resources and time are unlimited, there is no need to set priorities, of course, but given resource constraints, investment decision making attempts to allocate them in a way that yields the most "benefit" to the organization.

"Benefit" is defined here as the degree of achievement of the fundamental goals of the organization as a whole, not the specific benefit to local operations of investment in tankage, maintenance or otherwise. In addition, the portfolio approach takes into account the timing of investments, the expected returns, and the expected risk consequences. Since these are spread over future years, the present value (or net present value) may be managed more precisely through manipulation of investment and risk prevention spending.

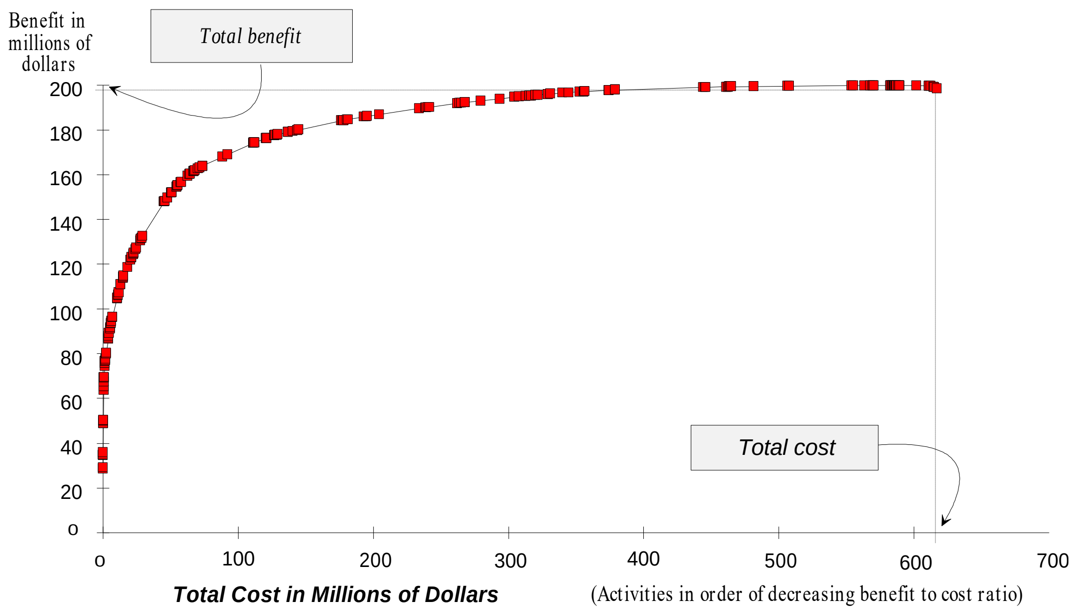
Translating the organization's mission and business model into constituent objectives and performance measures is the basis for estimating the "benefit" of an investment in any project. The diagram below illustrates this process for system designed to prioritize investments in risk-reducing activities for an organization. In addition to financial performance, there may be other key corporate objectives and the value of achieving these objectives can be monetized so that benefits and costs can be compared in monetary terms as a guide to resource allocation.



Once the "benefit" of an investment has been estimated quantitatively using defined performance measures, and the cost of the investment has been estimated using cost accounting, this investment can be compared to any other investment the organization is considering. The diagram below illustrates one way to organize these investment options for comparison relative to their achievement of the organization's mission.



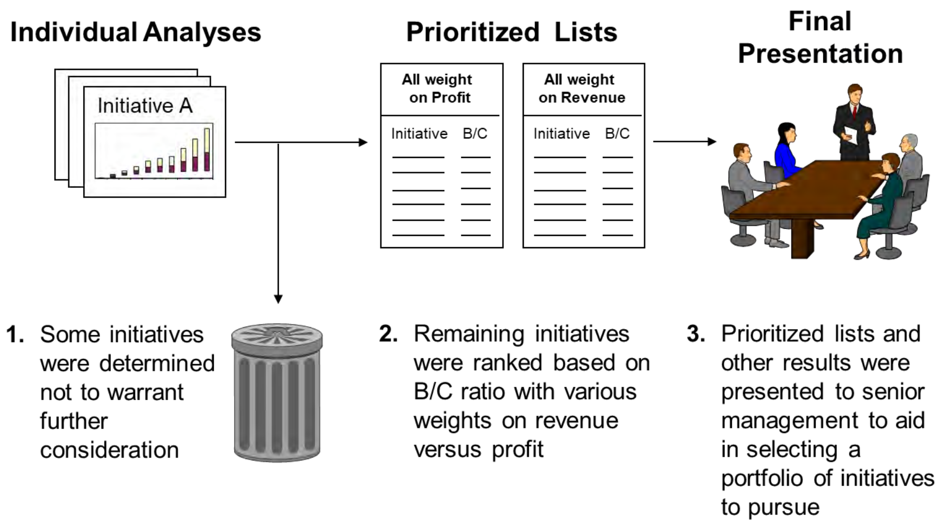
The optimal allocation for any given funding level might look something like the graph shown below. In that diagram, investments in different projects are prioritized based on the benefit-to-cost ratio, so that the incremental dollar is invested in the project with the next best return on investment. This maximizes the return on the marginal or incremental investment. The benefit-cost curve shown in the diagram below is from another prioritization project and some of the projects are investments in preventative and mitigating measures for large-scale risks. By assessing expected present value costs and benefits, these projects could be included in the overall budgeting decisions with other corporate investments.



This approach to prioritizing investments maximizes project-by-project investment decision returns, but it misses the portfolio effects and, in that way, can lead to suboptimal allocations. The remainder of this paper shows how analysis of decisions at the individual tank level can be combined into portfolio decisions that maximize the portfolio investment, not just tank by tank allocations.

"Portfolio" considerations can be included in various practical ways. For example, viewed qualitatively, if investments in tank maintenance are to be based on consideration of risk reduction, revenue maximization, and profit maximization, then performance measures for each of these considerations would be developed similar to the diagram showing performance measures above. Investments (purchase, out-of-service, maintenance, etc.) in specific projects would be evaluated in each of these areas (risk reduction, revenue, profit) at the organization level. Those scores would be combined based on the portfolio priorities of the organization: for example, suppose the financial weighting guidelines were 60% for risk reduction, 15% for revenue growth, and 35% for profit maximization. The combined weighted scores provide a basis for prioritizing investments for this portfolio weighted objective.

A first pass on identifying a portfolio of investments either across the organization or within a business unit (say, within storage management) follows this basic logic.



The overall benefits from a set of investment opportunities can be evaluated at different levels of investment, as illustrated in the next section.

There are challenges to changing the management of storage from a regulatory-driven, bottom-up, risk-driven transactional decision-making basis to incorporating it into the broader mission-driven decision making of the organization based on its mission and business model. There are, after all, many operational benefits and efficiencies to using compliance and broad industry guidelines as the basis for tank-specific decision making. This paper focuses, instead, on potential benefits of considering the portfolio of tanks as a corporate asset. The rationale for investing time in this pursuit with a more critical eye toward compliance-based decision making is similar to Thomas Paine's argument (in Common Sense), that "perhaps the sentiments contained in the following pages are not yet sufficiently fashionable to procure them general favor; a long habit of not thinking a thing wrong gives it a superficial appearance of being right and raises at first a formidable outcry in the defense of custom."

There is inertia and status-quo processes in every business process that make daily operations efficient, and these are necessary. But as technology, regulations, business models and economic markets change, these changes present opportunities for re-evaluation of approaches to decision making. The changes in energy markets over the past decade have brought new value to more integrated and rigorous resource management decision. Management of storage – and management of storage maintenance in particular – is an arena of opportunity because it has so long been left primarily to outside decision criteria in the form of regulatory and event specifics. As Paine said, a long habit of not thinking this was wrong has given it a superficial appearance of being right. That is an expensive assumption to make in today's markets given the alternatives.

A well-designed portfolio management system

There are a wide range of project portfolio processes, models, and systems available ranging from simple "rank and add" valuations to proprietary "black box" simulations to LOPA and other company-specific techniques, to, finally, formal portfolio optimization models that are rigorous and complex.

What considerations are most important when deciding on how to prioritize investments in storage? In addition to the list presented earlier, special attention should be paid to the *performance* characteristics of the decision-aiding system.

An important consideration is whether the investment decision process provides useful and accurate assessments of the value of various competing investments? Just because a process has been around or used for a long time or because it is well-known or endorsed by well-known sources does not always mean the system is appropriate for the purposes of prioritizing storage investments. There are many approaches that combine relatively ad hoc scoring procedures with ad hoc decision rules to identify "best investments." The degree to which these measures accurately capture the true future performance of the investments being evaluated is questionable.

There is a wide range of commercially available approaches that use score cards, group consensus procedures, voting, value hierarchies and other guides for working toward an investment choice. But energy companies are typically held to a higher standard in the decision approach they take because, as the National Academy of Sciences recommends, decision processes addressing risk in the public interest should provide decision insights that are methodologically based, appropriate in their application, and provide timely and useful insights for decision makers.

Finally, decisions made at the *portfolio* level must take into consideration how decisions made at the *unit* level interact with each other, how they are combined, whether there are combination effects, and other system considerations. This includes the full range of routine tank management decisions such as risk assessment investments or risk management scaling.

The structure of decision analysis modeling meets these requirements for a sound decision support system and the way it can be used at the individual tank and the portfolio of tanks levels is shown in the next sections.

Portfolio considerations

Treating a set of assets such as tanks as a portfolio is different from considering these same assets as a collection of similar individual assets. In particular, viewed as a portfolio allows evaluating decisions at a different level and using more appropriate evaluation criteria for those investment decisions.

Sometimes the word "portfolio" is used to describe what is really just a collection of similar projects. The individual projects are evaluated one-by-one independently and the results of different allocations at the project level are aggregated into what are called "portfolio" returns but are often just the addition of the expected returns to the individual investment decisions. Sometimes there is additional sensitivity analysis that shows best-case/worst-case ranges of expected returns but the total returns are driven by the individual decision making. These decisions are often, in the case of tankage, the result of industry guidelines or best practices that ignore company specific financial and business issues and, worse, can be behind current technology and economic trends.

The result is that there can be significant impacts to the overall benefits of this collection of investments at the portfolio level, not at the project-by-project level of evaluation. Ignoring these portfolio-level impacts is a business risk that is often not even thought of, let alone taken into account.

For example, in a portfolio of similar assets – tanks in this case – there are the risks from fluctuations in the individual costs and business returns from each asset, but there may be portfolio-level risks if a large group of the assets are related to each other (for example, all are used for the same large customer so subject to a single-point market impact, or are all for the same product or use the same design or are the same age and condition so may suffer failure rates at the same time, or are all dependent on some market condition or single supplier, creating large-scale business impacts for the organization.

In the same way, a large energy company can benefit from considering investments in their storage portfolio not only at the individual storage device but also at the portfolio level. Portfolio risk and return evaluations are more accurate when used for a group of tanks that serve a key customer or tanks that pose risks for a single important environmental asset or tanks that are all impacted by a change to a particular regulatory requirement or availability of a particular product.

The next sections discuss the first objective of this paper: a description of a way to think about an organization's tankage that uses all the tools of tank risk assessment but also provides a basis for using the financial analyses associated with the organization's business model. In particular, the section discusses how investments – including acquisition, divestiture, maintenance, use plans, and more – in an energy company's storage units can be considered at both the unit and portfolio levels in a sound, practical, useful, and timely fashion with regard or the organization's overall business model, corporate returns and corporate risks.

Analysis first on a tank-by-tank basis where required

Using principles from decision analytics and predictive modeling, decisions about design and monitoring can be evaluated on a tank-by-tank basis, combining the inputs from the business demands, risk assessment findings, subject matter experts on tanks, and project management overseeing budgets and work structure.

The case illustrated below involves a decision on the design of a new tank and the type of leak monitoring system that would be most cost effective given the location, contents, and size of the tank.

The design options may be well-defined but how best to monitor for leaks may require some discussion and thought about different ways that could be implemented. The diagram below shows a strategy table that can be helpful to group discussion and combining different technical expertise into a single overall strategy.

Each column represents an aspect of the leak monitoring system that is a decision variable for the tank team. The lists below the column headings are the different options available for that characteristic of the monitoring system.

Different strategies can be considered by looking at different combinations of these various decision variables. Not all combinations make sense, but the strategy table still provides a proven useful took for keeping a larger number of alternatives actively in discussion before jumping right away to one or two alternatives to pursue in depth.

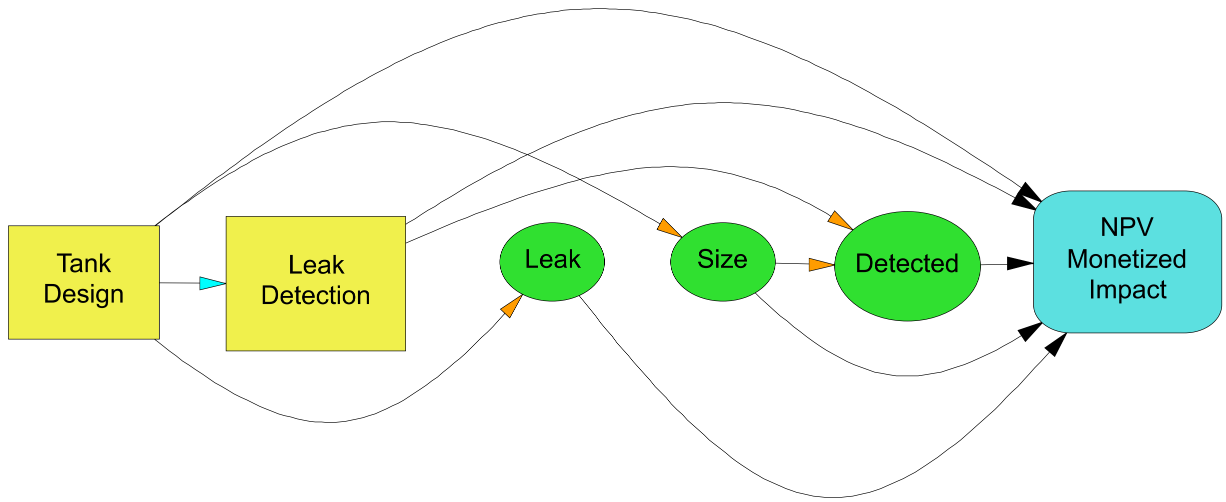
Strategy Generation Table

Strategy	Frequency (per yr, per tank)	Frequency variation	Tank use	Type of testing	Test precision	Test-data use
Base case	0	Uniform	Demand driven (no testing)	None	N/A	N/A
Minimum	1	By tank		Tightness	Low (20K gal)	Individual test
Medium	2	By tank location	Testing driven by tank demand	Inventory: level	Medium (10K gal)	Test averaging
Thorough	3	By tank contents		Inventory: mass		Test trending
Aggressive	4		Tank use linked to testing		High (3K gal)	Process control stats
	6	By tank history		Soil vapor		
		By tank features	Driven by testing schedule	Integrated combo		

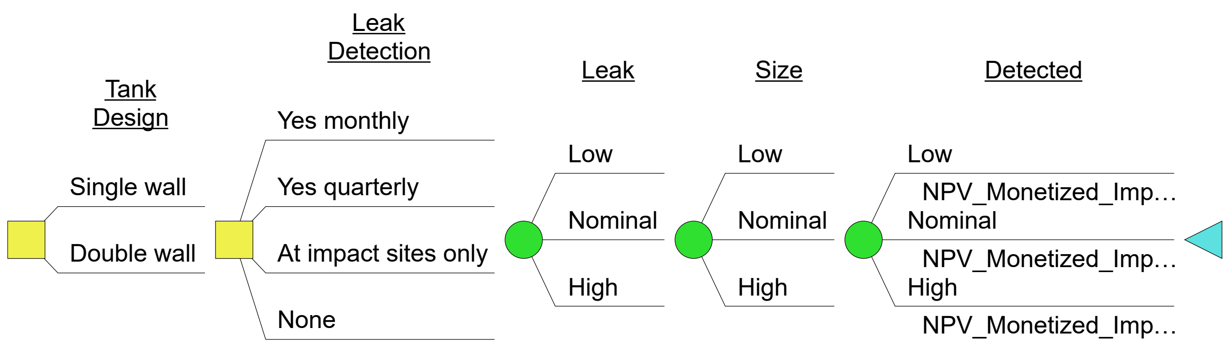
The color-coded combinations represent different monitoring strategies. The table is a template for 6 x 6 x 4 x 6 x4 x 5 or more than 17,000 different combinations. No one would ever look through all those, but the idea is to aid collaboration across disciplines, skill sets, experience, and points of view to find those combinations that might be appropriate for further investigation.

The three strategies identified as examples here are a “Base case” which is to do no systematic or prescribed testing for leaks and only check driven by demand. The “Minimum” strategy is drive by demand at the tank by checking inventory levels with high precision and using test averaging. The “Thorough” strategy tests quarterly by both tank contents and tank history, both by level and by mass, and a high level of precision and includes both test averaging and trending.

These strategies cost different amounts, have more or less disruption on tank use, and provide different levels of protection against undetected and expensive leaks. Using economic analysis from both the costs of testing and the costs of undetected leaks and remediation, estimates can be made of the best overall (in this case, the lowest expected cost) alternative for both design and leak monitoring. The influence diagram below shows the relationship between decision variables (yellow rectangles), uncertainties (green ovals or “bubbles”) and the payoff metric (blue rounded rectangle). The arrows show “influence” of the source entity on the target entity.



The decision tree version of the influence diagram above is shown below where the specific alternatives for each node are shown. The blue triangle at the end represents the summary calculation, in this case the expected net present value over ten years of tank life.



The decision tree structure shows, in addition to the two decision variables, three uncertainties explicitly modeled in this example:

- The probability of a leak, labeled here as low, nominal, or high, (where leak probabilities are inserted for each) where these probabilities are influenced by the tank design used, so two conditional distributions;
- The size of the leak, with three possible levels, each with an associated probability based on the tank design and empirical data for the tank, age, contents, weather and whatever other considerations are included in the analysis;
- The probability of detection, which is influenced by the leak monitoring strategy employed and the size of the leak.

Using a set of hypothetical values motivated by an actual application, the decision tree is used to compute the following values:

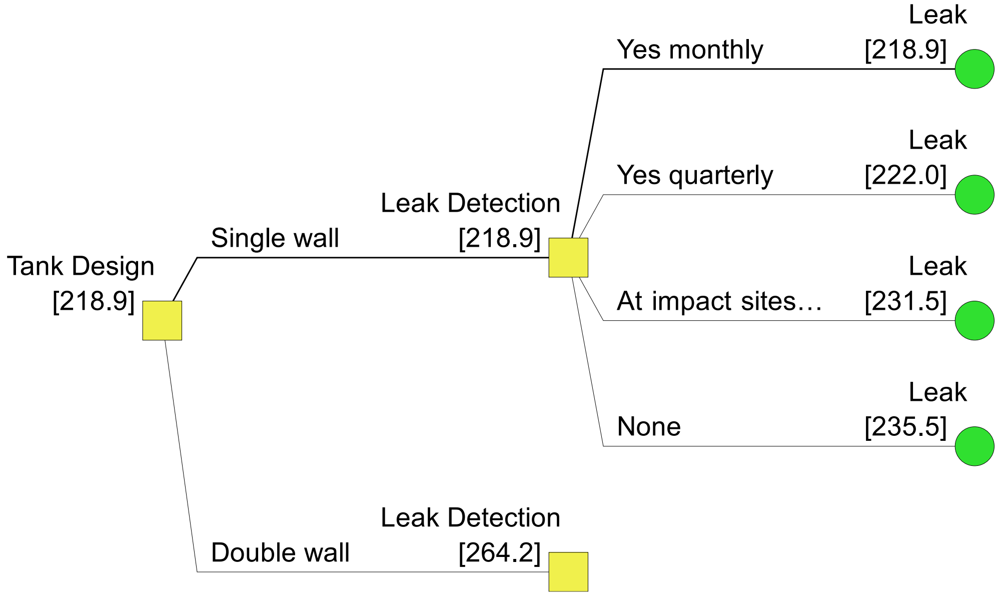
- Monetized values

- NPV of design choice
- NPV of lead detection policy first ten years
- Expected present value of a leak impact to
- People
- Environment
- Assets
- Reputation

- Probabilities, conditioned as shown in the influence diagram

The expanded decision tree below shows the expected values for each strategy combination in square brackets.

This analysis shows that the lowest expected present value cost for the near-term life of the tank is to use a single-wall construction and test monthly using the combination taken from the strategy table. This is better than double-wall no matter what testing is conducted, including "none." Interestingly, the "none" monitoring approach has the highest expected cost due to the impact of an undetected leak. Although these are hypothetical numbers, the motivating example was a large tank location above an aquifer and water system supply reservoir for a city, so the potential for consequences of an undetected leak were significant.



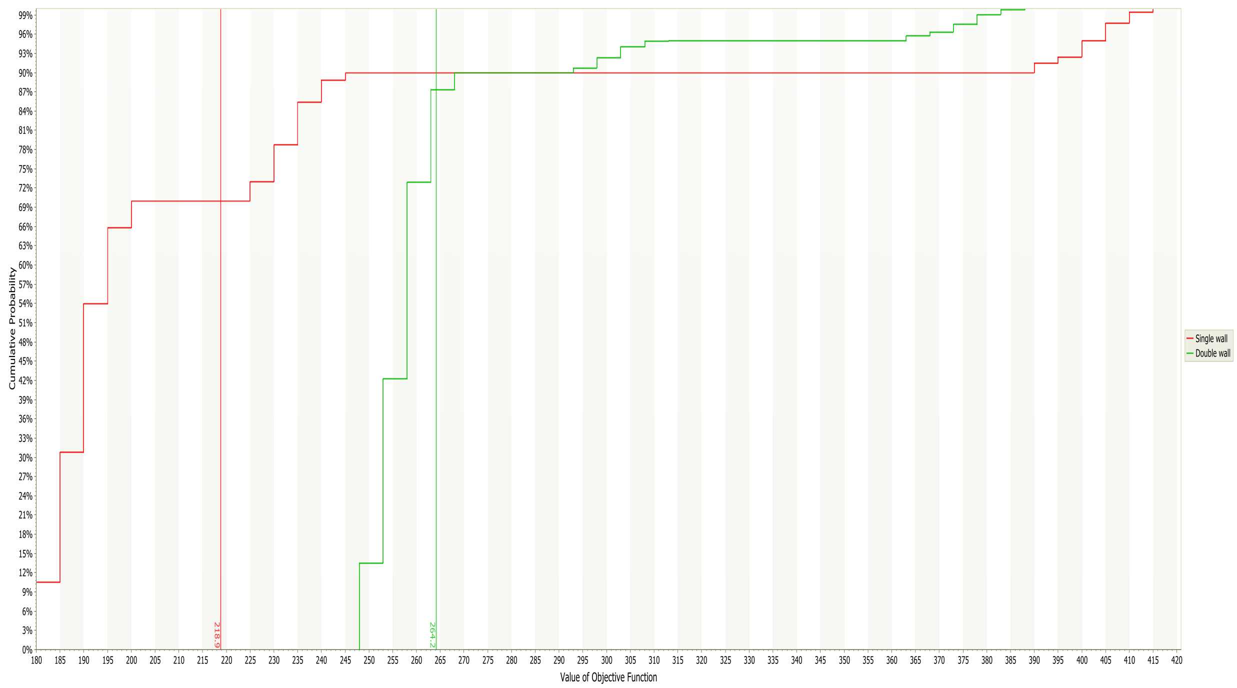
The preferred strategy is a single wall, leak detection monthly. The numbers in brackets are expected NPV in millions over first 10 years of the tank life.

A more detailed assessment of the expected costs can be obtained, if desired, by considering the cumulative probability distributions of the two main design options, as shown in the figure below.

The red line is the cumulative probability of the single wall design and monthly testing. The green line is the cumulative distribution of the double wall design and optimal monitoring strategy for that design.

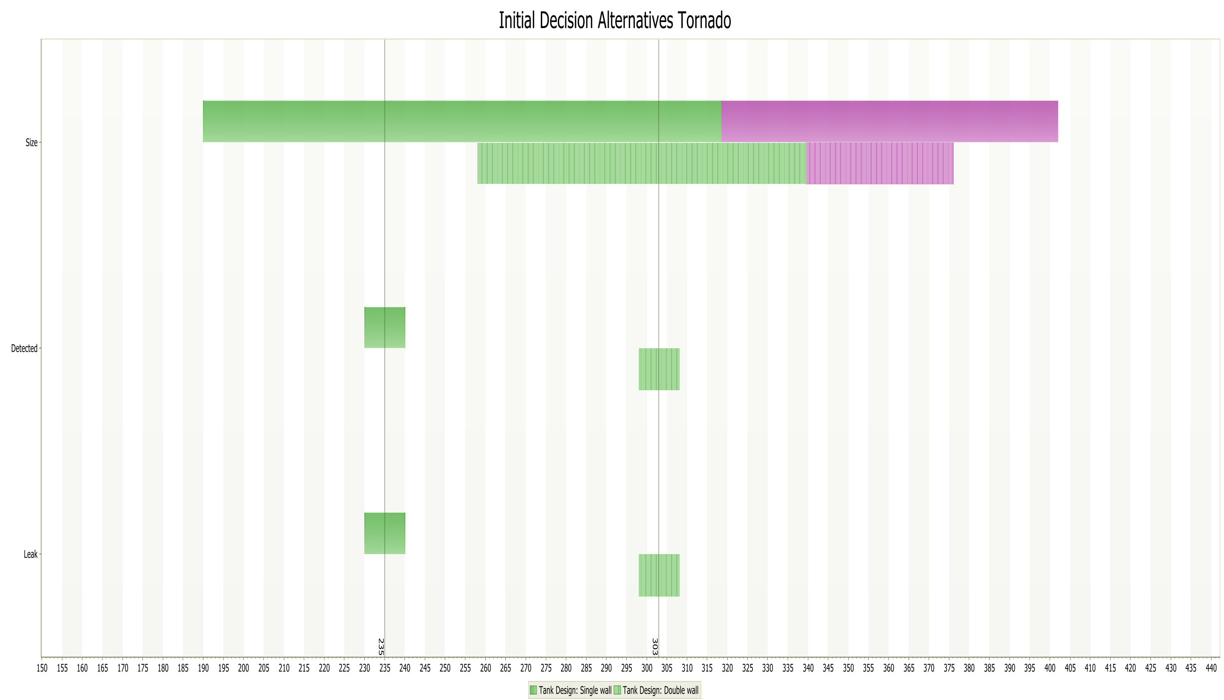
From this, for example, the analysts can see that there is about a 75% chance the actual cost will be less than the expected value (shown by the red vertical line) and a 25% chance it will exceed the expected value with the potential of being a large multiple of that cost, though with only about a 15% chance of a very high cost.

This kind of information can aid re-design considerations or financial planning or insurance coverage decisions.



The cumulative distributions on NPV for each of the alternative designs. Single wall stochastically dominates double wall for these made-up numbers.

This is quite a bit of uncertainty in the actual cost that the tank owner is exposed to. It might be useful to understand what about the tank and the monitoring system is driving this high degree of uncertainty. The tornado diagram below answers that question; the driver on uncertainty in cost is uncertainty about the size of the leak. A large leak can incur a lot of cost before it is detected. In fact, for the larger amounts of leak sizes, the double wall design would actually be the preferred design option, as shown by the change in color to purple.



The tornado diagrams (one for each of the initial design alternatives, single or double wall) for these hypothetical numbers shows that the biggest contributor to uncertainty in the NPV of costs is uncertainty about the size of the leak. If this probability estimate is refined, the uncertainty in future costs will be reduced.

To repeat, a key finding of this sensitivity analysis is that if the chances of a large loss of containment are high enough, the optimal design changes to double wall instead of single wall. This finding may motivate the analysis group to refine the probability estimates to make sure the chances of a large leak are below those cut-off levels. Also note that the risks associated with serious event risks (fire, explosion, over-fill, etc.) are grouped with large-scale business risks such as loss of a key customer, a significant new competitor or regulatory constraint. All of these ultimately matter to the organization at the corporate level and now can be compared directly to each other.

Tanks as a portfolio of financial assets

The previous section illustrates detailed analysis at the individual tank level. Once these financial estimates are acquired for each tank, the next level of decision making is to evaluate the allocation of resources across all tanks.

This section addresses the second objective of the paper: a description of how to think about tanks as a whole and their fit in the organization's business model and strategies. To do this effectively, the tankage should be viewed as a portfolio of investments. There are a number of initial steps in the portfolio approach that are skipped over here due to length constraints. These include consideration of combinations and dependencies in tankage due to business lines, common customers, refinery needs, product and supplier types, and more. Once these dependencies are known and included, they determine the realistic combination of different portfolio options that are available to the organization’s management.

Employing a portfolio approach and making decisions at the portfolio level for tanks routinely faces several organizational challenges, some of them hurdles to that management:

- No repair guidelines (at corporate level)
- Localized and disparately-located knowledge
- Localized priorities for project managers
- No best practices at corporate level
- No common objectives
- Questions about applicable specs
- Reason for repairs
- Level of effort: maximum, minimum, satisfactory, local decision?
- Interaction of repairs proposed and impact on which specs become applicable

Making decisions about tank maintenance projects can often end up being governed primarily by considerations not only outside an organization’s business model and business objectives but by considerations completely outside the organization: industry guidelines, compliance requirements, “best practice” summaries that come from very different business environments, and other outside sources.

Not only does this reliance on outside guidelines often ignore particular business or economic issues specific to an organization, industry standards routinely lag economic changes, regulatory adjustments, and the necessities of staying competitive in energy environments that are encountering new competitive, now customer demands, and shifting international barriers to free trade.

Viewing tank maintenance projects as investment decisions moves them from being viewed primarily as compliance expenditures to being evaluated in terms of their contributions to the overall performance of the organization in terms of the organization’s business model and business objectives.

This implies that business-model based guidelines should be employed when determining what investments should be made in managing storage assets. This has several benefits to the business unit within which the storage assets are located but also to the organization more generally. For example, this approach motivates a reassessment of the overall benefit of the business operations supported by storage, it improves tracking the relationship between investments in storage maintenance and repair to the overall corporate business objectives.

Viewing tank investments in terms of corporate return on investment to business objectives enables project managers and subject-matter experts to more effectively collaborate with their respective skill sets. SMEs can provide insights on the most effective repair strategies for achieving the organization’s business objectives which the project managers provide guidance and management for efficiently implementing those repairs or other investments.

Budgets are influenced much more transparently by the expected return to business objectives for specified levels of investment than the tank-by-tank compliance approach that often is most influenced by getting the necessary repairs done within budget using industry compliance guidelines. In this way the organization's overall business model direction business decisions regarding repair expenditures, additional investments in capital assets, operations, on-going maintenance, and metrics for performance of these various expenditures.

Viewing tankage as a portfolio of asset investments views future investments in tankage through the lens of investment decision making:

1. Not all tanks are the same
    - In terms of importance to overall business model
    - In terms of the risk posed to achieving business model objectives
2. Not all investments in tank management are the same
    - Value (importance) of tanks vary
    - Need for repair varies
    - Like all capital investments, the range of "repair decisions" can be large:
        - Repair like new (most stringent specs)
        - Minimal repairs (least stringent specs)
        - Take out of service temporarily
        - Remove from service permanently
        - Remove and replace

Since tank value is based on an organization's business objectives, it motivates explicit consideration of such things as their location in the business network, the customers served, the risk posed to business objectives under different levels of investment and the overall benefit to cost comparison at different levels of investment.

Different approaches to tank maintenance include regular budget allocations (such as a fixed annual percentage of total spend) versus "bandaid" fixes all the way up to expansion and business development investments. Examples of organizational business objectives serving portfolio investment guides include some of the following:

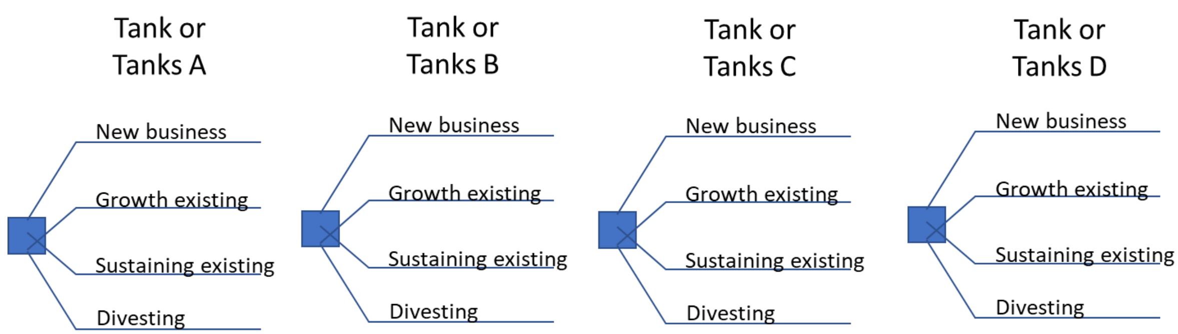
- Example business *objectives*
    - Financial
        - Contribution to revenue stream now (e.g., approximate NPV past five years)
        - Contribution to revenue stream future (e.g., approximate or probability-weighted NPV next five years)
    - Customers served
        - Level of importance to business model now
        - Level of expected importance to business model future
    - Costs of operations
        - Level of operating costs now (e.g., NPV past five years)
        - Level of expected operating costs future (e.g., NPV next five years)
    - Technology age for role
        - Legacy technology and adequacy now and near future

- Example business *contributions* (and risks to business objectives)
    - System importance
        - Role in overall management of product inventory
    - Item importance
        - Overall importance to product or customer service

It is possible to include monetized versions of investments in safety, health (employees, contractors, the public), environmental enhancement, regulatory rapport, corporate citizenship and other relevant business objectives valued by the organization.

Portfolio investment evaluation

Consider, for example, investment decisions for four tanks (or tank groups), as shown below. The specific tank decisions from the previous section have been conducted and now the tanks are being looked at from the perspective of the organization's business model and where those tanks fit into that business model. This may be a time of market stagnation, tight capital, or a time of growth or expansion – whatever the current business emphasis is at the organizational level, that is translated into tank usage. For illustrative purposes, the investment options are reduced to the four alternatives described in the earlier section.



Note that the decisions are not characterized in terms of the activity itself (maintenance, take out of service, etc.) but the *purpose* or business objectives of the organization motivating the activity. This means that the role of the tank in the overall business model has been considered. For the simplified example here, each tank set (A, B, C, D) represents storage capacity that is serving a business purpose and investment in that storage is seen in light of the four objectives shown (assumed here the same for each of the tank sets):

1. Investment in new business opportunities
2. Investment in growth of existing business activities
3. Investment in sustaining current levels of business activity
4. Investment in divesting the storage assets

The range of tank investments might include traditional maintenance or upgrades, but would obviously be broader in that they would include adding new tanks, renting excess storage in another area, joint ventures, or other more complicated business investments revolving around storage management.

When viewed as a connected set of decisions about this portfolio of storage assets, there are 4 x 4 x 4 x 4 ways to combine these sets of alternatives, or 256 different *combinations* of investments options for this portfolio of tank sets. The organization would want to pursue the best possible strategy for a given level of total investment, considering the portfolio as a whole.

One way to approach this would be to consider each option for each tank (or set of tanks) in terms of the investment required and the expected benefit from that investment over the decision horizon that is being considered. So, for example, the organization might consider the present value of the investment, considering the next five years, and the expected net present value of the benefit over the next five years achieved by that investment.

Quantifying benefits can be in terms of financial considerations alone or may include intangibles such as customer support or environmental sustainability objectives. If intangible objectives are included, their value has to be monetized in some fashion. There are a number of broadly accepted ways to do this, both by government agencies as well as investments in the private sector.

To maximize the overall value of this portfolio investment, the organization would compare the expected net present value of returns from the investment to the size of investment required for the various combinations of portfolio investment.

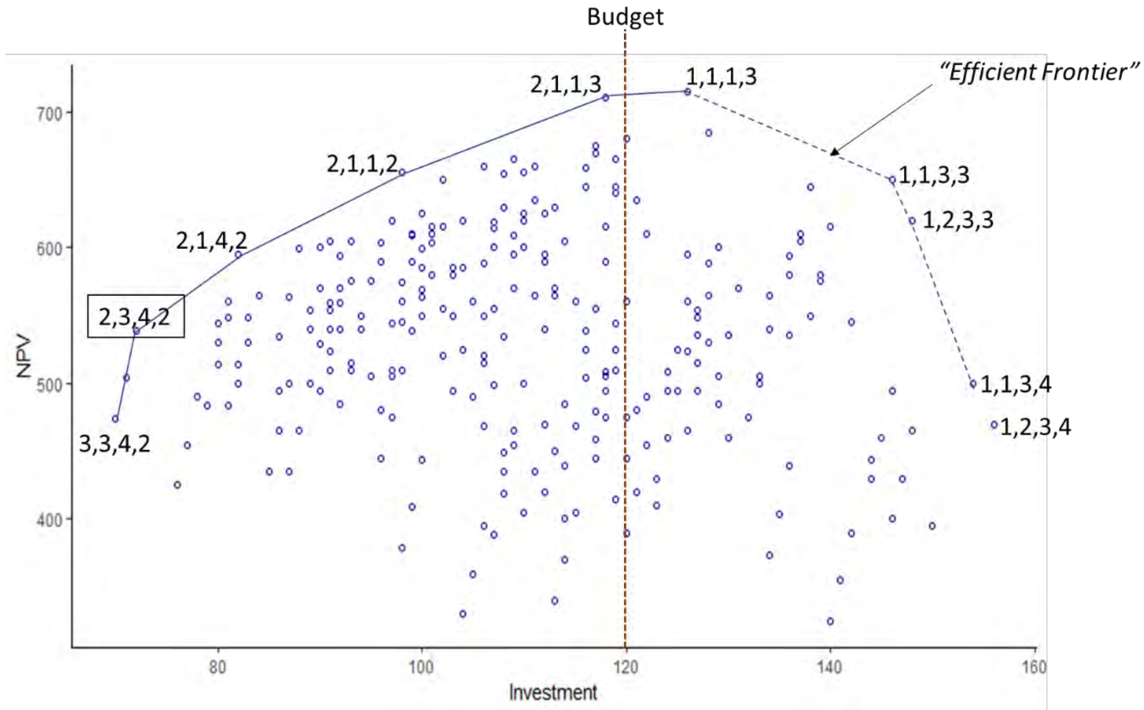
To illustrate the process, consider the following examples of investment and expected NPV for each alternative for each tank set.

Tank set	Alternative	Expected investment	Expected NPV	Expected benefit-to-cost ratio	Priority
A	1	20	150	7.5	
	2	12	145	12.1	x
	3	10	80	8.0	
	4	11	110	10.0	
B	1	22	180	8.2	
	2	24	150	6.3	
	3	12	124	10.3	x
	4	18	75	4.2	
C	1	40	200	5.0	
	2	33	150	4.5	
	3	60	135	2.3	
	4	24	140	5.8	x
D	1	35	140	4.0	
	2	24	130	5.4	x
	3	44	185	4.2	
	4	52	35	0.7	

The “x” in the chart above shows the investment with the greatest return *rate* on investment for each tank viewed independently. These tank investments and returns can also be combined to create different “portfolios” representing different alternative investments in these storage assets as a combined business asset group, as shown below.

Portfolio alterna-tives	Tank investment choices / alternative				PV of Invest-ment	Expected NPV
	A	B	C	D		
1	1	1	1	1	117	670
2	1	1	1	1	106	660
3	1	1	1	1	126	715
4	1	1	1	1	134	565
5	1	1	1	2	110	620
6	1	1	1	2	99	610
.	.	.	.	.	.	.
.	2	2	2	2	93	575
.	.	.	.	.	.	.
256	4	4	4	4	105	360

The portfolio alternatives can be plotted to show the cumulative benefit and cost of each combination of tank investments, as shown in the figure below.



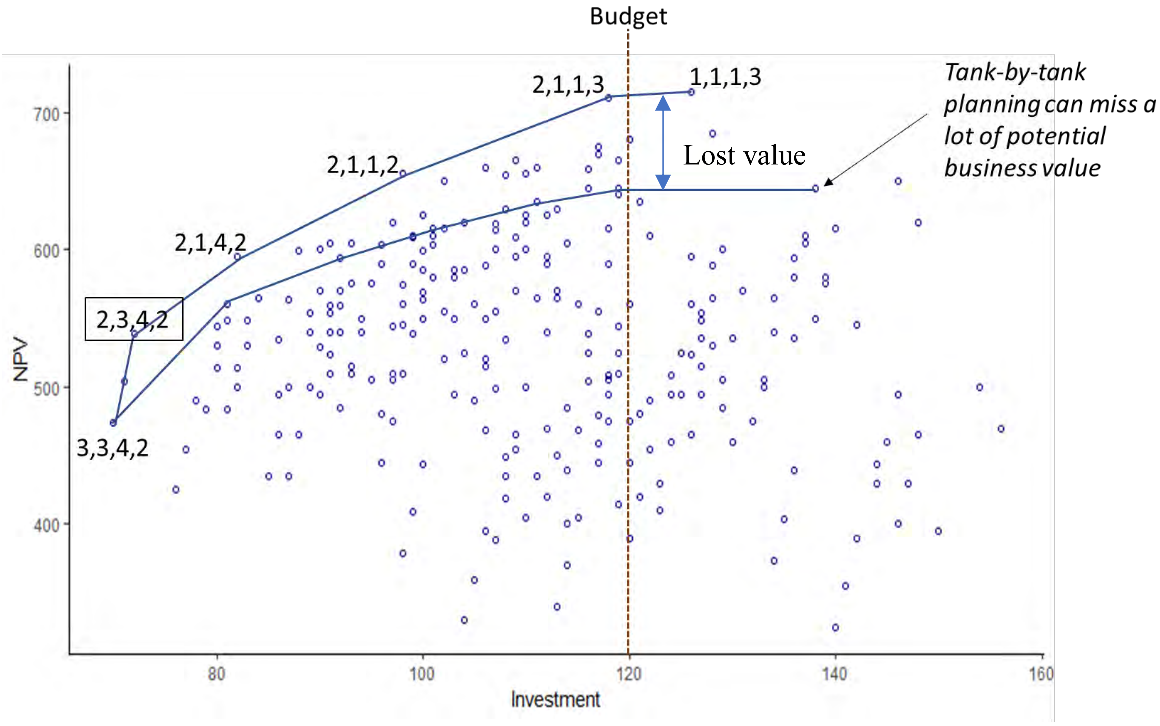
The graphic above shows all 256 portfolio investment alternatives (each characterized by a different combination of investment alternatives in the four tank sets) in terms of the total expected investment on the horizontal axis and the total expected NPV return (on the vertical axis).

A portfolio on the "boundary" of efficient frontier of this collection of portfolio investments shows the greatest return (expected NPV) that can be obtained for a specified level of investment. The hypothetical budget line gives business planners direction in prioritizing the allocation of resources.

Using these example investments and returns, the plot shows that for an investment of $98,000 (if dollar units are thousands for this example), the largest return that can be obtained is $655,000 and that is obtained by investing in alternative 2 for Tank set A, alternative 1 for Tank set B, alternative 1 for Tank set C, and alternative 2 for Tank set D. That is, for this level of expenditure, the best investments are to grow Tank sets A and D and invest in new opportunities for Tank sets B and C. Total return starts to drop for investments above about $130,000, so it would make no sense to invest in these portfolios.

The portfolio shown in a "box" on the graph is the combination of highest return rate on investment for each Tank set – this portfolio has the steepest slope (return rate per dollar invested). However, if the organization is pursuing a growth strategy and is willing to invest more, there are portfolio investments that have greater than even return. The efficient frontier aids the business unit and the organization in setting budgets and allocating resources across business units.

This financial analysis of the tank portfolios can be used to compare investment in storage to investments and expected returns from investment in other parts of the business or other business units or divisions within the organization. So an overall optimal strategy can be designed at the organizational level by combining portfolio investment analyses from these business units or divisions.



Tank-by-tank planning, as illustrated in the graph above, is less effective than portfolio prioritization of investments because the decision framework ignores comparisons of all possible combinations of asset alternatives when considering how to allocate resources. The result is that the organization can be very effective in local decision making yet leave substantial amounts of potential gain on the table.

Additional valuation capabilities

This portfolio structure provides the organization with a number of ways to make more specific investigations of tank investments. For example, sensitivity analysis is now possible at the portfolio level so that the impact of uncertainty about either investment amounts or expected returns can be easily incorporated into the evaluation process.

Because the individual tank investment decisions are characterized in a decision tree structure, tornado diagrams or other sensitivity analyses can identify key uncertainties. The organization can use these insights to pursue possible new efficiencies or evaluate the "value of information" more precisely to spot areas where additional testing is warranted. The "value of control" can be estimated in the same way, where additional investment can reduced uncertainty in either total costs or assure less variability in expected returns.

The value of flexibility – "option valuation" of a type – can be estimated. This may show approaches to tank investments that is conducted in stages where the degree of investment in each stage is determined based on the findings obtained in the previous stage of maintenance. These kinds of 'sequential' maintenance strategies have been shown to sometimes provide a much more tailored and cost-efficient approach to managing tanks in service where the primary cost of maintenance is sometimes opportunity costs of being off line.

The description of portfolio evaluation is illustrated in this paper using a basic model of interactions. There are easily available software platforms that allow the analysts to fully integrate the risk assessments and decision analyses that are applied to each tank or set of tanks and include it directly in the portfolio analysis treating all the tankage as a portfolio of investments so that correlations between uncertainties, common vulnerability and more can be included in the investigation of how best to invest in the organization's storage assets in light of the tanks' conditions and the business objectives.

Summary and examples

The two objectives of this paper were, first, to describe a way of viewing tanks as both individual assets and also as a part of the organization's portfolio of assets used to achieve its business objectives. The second objective was to describe basic and easily employed analytical tools that add precision to these points of view through quantification. Together, these two points provide a valuable aid to those making very practical and sometimes vexing decisions about how to allocate scarce resources in an increasingly competitive business environment.

One important follow-on to this approach is that this structure buckles the information gathering associated with risk assessment directly to the decision making regarding how to allocate scarce resources at the corporate and business model level. The decision on what to do or not to do with a tank one the risk assessment has been completed should be made in a way that maximizes the value of the overall portfolio of tanks to the organization's business strategy. In the same way that risk is diversified by portfolio thinking with other capital assets and investments, risks should be managed both at the tank and at the portfolio level of tank management for corporate risk management to be as effective as possible.

To summarize, these are the basic steps outlined in the preceding discussion:

1. Tanks: The first level of analysis is the individual tanks. This evaluation can use traditional decision analysis tools to develop a set of strategies based on the age, content, condition, location, and other relevant tank attributes, as illustrated in the leak monitoring example. This analysis aids both project managers and SMEs in determining the timing of inspection and the alternatives that should be considered in managing the tank.
2. Tank sets: Tanks can then be grouped based on dependencies. For example, if the configuration of tanks requires that tank X by taken out of service of tank W or manifold Z are out of service for maintenance then those assets would be combined into a "tank set" as illustrated in the portfolio section.
3. Cost estimates: The result of activities 1 and 2 provides the tank managers with estimates of the potential cost of either inspection or maintenance (or both) activities. These estimates may include more rigorous risk assessments using PRAs or LOPAs as guidelines as well as industry guidelines and regulatory requirements.
4. Value estimates: The organizational business model is now used as the basis for estimating the business value of the tank or tank set. That is, based on the organization's current

business strategies and practices, the contribution of the tank to that business plan is monetized. There are numerous ways this is done; the main point here is that this step links the tank or tank set to the organization's (or business unit's) business plan by quantifying its contribution financially.

5. Cost and value in common units: The expected net present value of the costs associated with different levels of maintenance or other alternative investments and the expected net present value of financial contribution from the tank are put in common units so they can be meaningfully compared.
6. Valuation of final tank alternatives: The final set of alternatives for tank management decision at this budget planning point are finalized and predicted values for costs and contribution finalized.
7. Portfolio valuation step: All combinations of tank or tank set alternatives are constructed, as illustrated, for each portfolio (by region, by business unit, or by other relevant organizational business model structure).
8. Efficient frontier of tank investments: All the combinations of tank alternatives are valued in terms of total expected cost and total expected value gain and plotted. The efficient frontier of portfolio investments is identified.

The efficient frontier of portfolio investments is a useful guide for prioritizing investment in the organization's storage capacity and capabilities. Factors outside the portfolio analysis play a role in determining the ultimate priority of investments, but the efficient frontier is an aid in planning by providing an optimal reference point.

Example applications

The following scenarios illustrate situations where tank management decisions might be aided by portfolio considerations that link these decisions to the organization's business objectives:

Example 1: Tank inspection programs. Companies with hundreds or thousands of tanks apply significant resources to programs where the decision rule for resource allocation is strictly time based using the guidelines of industry standards such as API 653, API 510, or other similar approaches. At first glance it may seem that these approaches are the only way to be "good corporate citizens" because the approach is clearly defined by the industry guidelines. On further consideration, it is always possible to reduce or increase the inspection intensity based on both the tank condition and the degree to which the tank supports the organizations objectives.

Example 2: Tankage obsolescence: Tanks are "wasting assets" and are affected by both age related and event driven damage. Age related deterioration has fairly good guidelines in the industry standards. However, traumatic damage such as natural disaster effects (e.g., hurricane, settlement, flood, seismic, lightning) are often subjected to a "repair or replace" objective. Industry standards such as API 579 have been developed which tell an owner if and whether a tank can reasonably continue to operate in its damaged state. But these standards are applied in a one-off approach. Few companies have developed universal approaches that provide guidelines that generally apply to dealing with these assets at the portfolio level.

Example 3: Capacity expansion and business growth: Acquisition of tank facilities of one organization by another is a common happening in the oil industry. These transactions often involve large transfers of oil storage capacity. Because the acquired assets almost always have guidelines and standards for their storage that will differ significantly from the acquiring organization, the condition and costs to either upgrade the facilities to the acquiring companies standards is an ideal application of portfolio theory. On the one hand, by acquiring storage and letting it run for a while to see how it performs has the benefit that it is simpler to do, takes less work than the alternative, and maintains status quo. However, applying the portfolio approach during or after the acquisition allows management to plan changes for the new assets in a way that are going to provide longer term benefits that support the corporate mission and objectives.

Example 4: Market shifts: As markets change the profitability of the various stored petroleum products changes as well. Decisions about adding storage capacity (or reducing it) are often considered within the local business unit but not constrained by the overall framework of an overall corporate portfolio approach to storage.

Example 5: Almost everyone in the storage business has heard of the Buncefield or Caribbean Petroleum tank overfill disasters. New API standards have even been issued that attempt to reduce this potential. What these standards cannot do is to provide the optimal path forward in adoption of new technology for companies that have large portfolios of diverse tank storage systems. Decisions about how to reduce risk in the context of potential risk reduction projects such as the use of safety instrumented systems, how fast to upgrade tank overfill control systems or whether or not and on which tanks these upgrades should be made cannot be addressed by industry standards. The portfolio approach is the optimal approach to answering these questions.

Concluding comments

Tankage and other storage capacity are important capital assets supporting an organization's business model. The way in which they support the organization's business objects can change as the business model of the organization shifts in response to new technologies, regulations, market competition, economic factors, and other influences. Viewing tankage through the same lens as other capital investments provides a basis for evaluating investments in maintenance, expansion or divestiture in light of the degree to which that contributes to the current business model objectives.

There are software packages that support both the detailed risk assessments at the individual tank or set of tanks levels as well as the portfolio allocations that are best. Syncopation software's Enterprise and Portfolio models can be used to support decisions made at the tank level, including constrained optimization, uncertainty and risk analysis, and the value of building flexibility and options into the investment strategy so that changes can be made as "learning" occurs during the assessment stages of tank investment..

The portfolio approach to evaluating investments alternatives in tankage opens the door to inclusion of other investment evaluation techniques. Common and sound approaches to evaluating portfolio management decisions include the following theory-based approaches. These have been helpfully grouped in a book on risk analysis by Lee Merkhofer:

1. Decision analysis including tree structures, influence diagrams, uncertainty and utility modeling, and value of information analyses
2. Multiattribute utility analysis, a special application of decision analysis used to evaluate decision alternatives when value or success entails simultaneous consideration of the achievement of multiple objectives.
3. Financial portfolio optimization
4. Financial and real options valuation

The employment of these and related evaluation techniques enables energy companies to allocate resources in the most effective ways as their business environment continues to change. It also provides a context for more efficient and effective collaboration of skills both within and between different business units.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Building Siting Screening Criteria for Structural Failure Hazards to Occupants

Johnny Waclawczyk*, Mark Whitney
ABSG Consulting, Inc
140 Heimer Rd Suite 300 San Antonio, TX 78232
*Presenters E-mails:jwaclawczyk@absconsulting.com

Abstract

Evaluation of occupied buildings for accidental explosion hazards at petrochemical facilities is a vital part of a process safety program and is a key element of facility siting. In some cases, buildings may be screened out prior to performing structural blast evaluations due to minimal exposure to blast loading. Defining a minimum blast load in which a specific type of building may be screened without structural assessment is left to the owners or their engineering consultants. Determining when a structural assessment for blast hazards is necessary is a critical safety decision.

Currently, API-752 does not include a blast load value that can be used for screening out building types without the requirement for structural assessment. Other publications provide pressure-based benchmarks for screening either for buildings in general or for specific types of buildings. This paper reviews industry guidance and makes recommendations for building blast-screening for consideration in the next revision of API-752.

Keywords: Risk Assessment, Quantitative Risk Assessment, Consequence Techniques, Explosions, Building Screening, Blast Assessment, Minimum Blast Load Hazard, API-752

1 Introduction

Ensuring protection of personnel in the event of an accidental explosion is paramount in a blast hazards assessment. Physiologically, humans can withstand higher blast pressures (e.g. 99% survivability with overpressure < ~1.9 Bar and threshold of eardrum damage ~5 psi [[1]]) than many structures. Pressure in these range can cause significant structural damage to conventionally constructed buildings resulting in severe injuries and fatalities due to structural failure and debris. Thus, evaluation of occupied buildings for accidental explosion hazards at petrochemical facilities is a vital part of a process safety program and is a key element of facility siting.

There are three traditional methods of evaluating of buildings for blast hazards; detailed finite element analysis (FEA), basic dynamics (single and multi-degree of freedom systems), and screening based on blast loads. Building screening is sometimes applied and performed by defining a minimum blast load in which a specific type of building(s) may be considered adequate for personnel protection prior to performing structural blast evaluations due to minimal exposure to blast loading. Screening policy and definition of acceptable blast load criteria are left to the owners or their engineering consultants to perform.

Various industries and government agencies have provided varying levels of regulatory requirements, recommended practices, guidance documents and minimum standards regarding blast evaluation of buildings and screening limits.

American Petroleum, Institute (API) API-752 [2] is a recommended practice for accidental explosions in the industrial facilities. Currently, API-752 does not include a blast load value that can be used for screening out building types without the requirement for structural assessment. Other publications provide pressure-based benchmarks for screening either buildings in general or for specific types of buildings. This paper reviews industry guidance, examines difficulties and challenges for screening evaluations, and makes recommendations for building blast-screening for consideration in the next revision of API-752.

2 Building Screening for Blast Hazards

Screening level analysis is intended to establish the adequacy of a building to perform at or better than a specific level of response without performing structural calculations. In most cases, a blast pressure value is referenced in which a building would be expected to sustain a particular level of damage. If blast loads on the building are predicted to be at or lower than the screening value no additional structural analyses are necessary, and the building is considered adequate to withstand structural failure hazards. Non-structural hazard screening criteria (e.g., window fragments, falling overhead lights, overturning equipment racks) may still require assessment and are not addressed by this paper. Some screening values for window glass hazards are mentioned below, but the focus of the paper is structural failure hazards.

Establishing screening criteria has been accomplished in many ways. Historical references and industry guides often provide and update screening values for blast hazards. Subject matter experts with extensive experience with structures subjected to blasts have provided information, data, and methods for screening structural systems for blast response. Collection and comparison of damage to buildings affected by accidental explosion is also highly relied upon to set screening levels. Finally, research and blast testing are used to establish, refine, and supplement screening criteria.

Screening criteria have often been established based upon construction type (e.g. masonry buildings, pre-engineered metal buildings, light weight wood trailers, etc.). In an effort to simplify screening and evaluations, a single pressure value is often sought after that could be applied to many types of buildings in a “one size fits all” approach. It should also be pointed out that screening criteria does not typically directly address occupant vulnerability which is a primary intent of blast hazard assessment.

Diligent care must be used in order to apply screening criteria properly. A clear understanding of the background of the established screening criteria being used is critical. The industry that the criteria was intended for can dictate the type of blast loads that the information is applicable. For example, criteria established for Department of Defense use would likely assume highly energetic materials and explosives which tend to result in higher pressure shorter duration blast loads. While industrial facilities criteria such a refineries and chemical plants are more likely to criteria based on vapor cloud explosions (VCEs) with lower pressure and longer duration blast waves. It should be known whether the screen values are based on overpressure or free-field blast loading of applied loads to surfaces of a building. It is common to reference screening criteria based on pressure values alone. In such cases, criterion must be based on long duration blast loads such as those from VCEs (hundreds of milliseconds). However, guides and documents often do not always reference the type of explosion or assumed blast duration and present only a pressure value as it relates to a building damage.

3 Published Criteria

A sampling of published screening criteria in a variety of sources was reviewed and included documents and references from institutes and associations related to oil, gas, and chemical industries, government agencies, Department of Defense, and international standards.

3.1 API-752

API-752 and API-753[3] are two of the most recognized documents for recommended practices in the blast hazard evaluation in oil, gas, and chemical processing industries. Table 4 of the 1st [4] and 2nd [5] editions of the API-752 document includes of free-field overpressure values with consequences for various building types (a copy is shown below in Table 1). The document states "In a consequence analysis, it may be assumed that building occupants could incur injuries if the integrity of the building is exceeded.".

Table 1. Overpressure and Consequences on Various Building Types (1st and 2nd Edition of API-752)

Table 4—Overpressure on Various Building Types

Building Type	Peak Side-on Overpressure (psi)	Consequences
Wood-frame trailer or shack	1.0	Isolated buildings overturn. Roofs and walls collapse
	2.0	Complete collapse
	5.0	Total destruction
Steel-frame/metal siding pre-engineered building	1.5	Sheeting ripped off and internal walls damaged. Danger from falling objects
	2.5	Building frame stands, but cladding and internal walls are destroyed as frame distorts
	5.0	Total destruction
Unreinforced masonry bearing wall building	1.0	Partial collapse of walls that have no breakable windows
	1.25	Walls and roof partially collapse
	1.5	Complete collapse
	3.0	Total destruction
Steel or concrete frame w/unreinforced masonry infill or cladding	1.5	Walls blow in
	2.0	Roof slab collapses
	2.5	Complete frame collapse
	5.0	Total destruction
Reinforced concrete or masonry shear wall building	4.0	Roof and wall deflect under loading. Internal walls damaged
	6.0	Building has major damage and collapses
	12.0	Total destruction

Note: Source: *The Effects of Nuclear Weapons*, rev. ed., Samuel Glasstone, Editor
Prepared by the U.S. Department of Defense, published by U.S. Atomic Energy Commission

For the 5 building types included the minimum overpressure listed with a building damage consequence ranged from 1 psi to 1.5 psi. This may give the impression that buildings can be screened for blast damage hazards at about 1 psi. The values were given based on nuclear weapons testing prior to 1964 indicating very long duration blast loads.

Both the 1st and 2nd Editions of API-752 also included pressure effects on various building components (shown in Table 2) based on loads applied as reflected pressures. Assuming a reflection factor of about 2.0 for lower pressures the following values for selected common building components would result the following:

- 0.25-0.5 psi (20-35 mbar) Glass shattering with hazardous velocities
- 0.5-1.5 psi (35-100 mbar) Metal/Cemesto/Brick Cladding
- 0.5-1.5 psi (35-100 mbar) URM wall collapse, possible shattering

Table 2. Overpressure and Effects on Various Building Components (1st and 2nd Edition of API-752)

Table 3—Overpressure Effects on Various Building Components[a]

Building Component	Reflected Overpressure (PSIG)	Component Response
Glass	0.2	Breaking
Glass	0.5 – 1.0	Shattering with body penetrating velocities
Wooden frame	1.0 – 2.0	Structural failure and potential collapse
Steel cladding	1.0 – 2.0	Internal damage to walls, ceilings and furnishings
Concrete-asbestos cladding (Transite)	1.0 – 2.0	Shattering
Brick cladding	2.0 – 3.0	Blown-in
Unreinforced masonry	1.0 – 3.0	Wall collapse, possible shattering

Note: [a]Source: *The Effects of Nuclear Weapons* by Glasstone (1964).

As mentioned, Table 1 utilizes free-field overpressure and Table 2 utilizes reflected overpressure. It is important to know which is being used when relying on any source for pressure-based screening.

The most recent version of the API-752 document (3rd Edition) does not include any pressure to building or component damage related information. Rather, it promotes the use of updated technology for prediction of blast damage to buildings, determination of occupant vulnerabilities, and estimates of event frequencies. It also points the evaluators toward building damage level assessments using tools such as charts (or software that automate use of charts) that have been developed based on the assessment of representative buildings or detailed structural analysis. Tables listing the lowest overpressures from the charts that cause specific damage levels (pressure asymptotes) may also be used.

3.2 API 753

API-753 was written to specifically address process plant portable buildings. Table 2 of the document (included in Table 3 below) contains upper bound free-field pressure values two damage level descriptions for lightweight wood trailers. These are generally considered the weakest constructed portable building used in the processing industries. The establishment of the upper bound pressures was based on FEA modeling and compared with empirical damage observed at accident sites involving vapor cloud explosions. The lower limit value of 0.6 psi is regularly used to site temporary light wood trailers for low vulnerability to occupants. Some companies that are less risk-adverse use the 0.9 psi value.

Table 3. Upper Bound Pressure V Damage Level for Lightweight Wood Trailers

Table 2—Overpressure Effects on Light Wood Trailers

Building Damage Level (BDL)	BDL Description	Parameters Used for Light Wood Trailers	Upper Bound Pressure
2A	Trailer is damaged in localized areas. Individual components on walls facing the blast sustain up to major damage. Other walls and the roof sustain up to moderate damage. Window breakage and falling overhead items are expected.	Studs on the reflected wall (the wall facing the explosion) are expected to crack but remain in place.	0.6 psi
2B	Trailer damage is widespread, but structural collapse is not expected. Wall components facing the blast sustain major damage and may fail. Wall and roof components not facing the blast sustain up to major damage. Window breakage and falling overhead items are expected	Studs on the walls that do not face the explosion are expected to crack with more significant damage to the reflected wall.	0.9 psi
Data from *Pressure Levels for Siting Wood Trailers Using the API RP 752 Addendum Simplified Approach*, BakerRisk Paper No. 760-110-06, September 8, 2006.			

3.3 Chemical Industries Association UK

In the United Kingdom, the Chemical Industries Association's (CIA) presents a benchmark value for overpressure and damage threshold for buildings in the 3rd Edition of "Guidance for the location and design of occupied buildings on chemical manufacturing sites" [6]. Table 4.1 of the CIA guidance (shown in Table 4) cites a value of 0.4 psi (30 mbar) below which overpressure are insufficient to cause structural damage or significant glass hazards. The guide states "Where hazard criteria are not exceeded no specific building design features or upgrades are required." Therefore, the overpressure value is intended as encompassing screening value. Reviewing the source [7] for this value illustrates that it is a lower bound selected from a listing of a variety of construction components and qualitative damage descriptions over a range of overpressures. Although not explicitly noted, it is presumed that the 0.4 psi is based on free-field overpressure at the building location.

Table 4. Chemical Industry Association (UK) Benchmark

Table 4.1 Often applied Benchmarks for the hazard based approach.

Hazardous effect	Benchmark value below which no specific building safety measures are required	Basis
Explosion overpressure	30mbar	Overpressures below 30mbars are insufficient to cause structural damage or significant window glass hazards[28a]
Thermal radiation[19]	6.3 kW/m^2	Radiation levels below 6.3kW/m^2 are taken as "safe escape" (1% fatality 90 seconds exposure)
Flammable gas	LFL	Buildings outside LFL will not experience ingress of flammable gas above flammable concentrations
Toxic gas concentration	EPRG 3	Buildings outside EPRG 3 will not experience concentrations of concern from toxic gas ingress

28 a. *Derivation of Fatality Probability Functions for Occupants of Buildings Subject to Blast Loads, Phases 1, 2 & 3.* W S Atkins Science and Technology, Contract Research Report 147, ISBN 0 7176 1434 4.

3.4 TNO "Green Book"

Another international source, often referred to as the "TNO Green Book"[8], has been commonly used for building damage estimation based on tables of overpressures and damage descriptions. From a sampling of these tables, shown in Table 5, it is seen that in the pressure range of 1 to 2 psi damage is described as Minor to Moderate, partial roof collapse and 25% wall failure, and walls of concrete block have collapsed. Glass hazards are also noted at 0.4 psi (3kPa) with 50% of all window panes will be broken.

Table 5. TNO Green Book Damage Descriptions

70 kPa	:	More than 75% of all outer walls have collapsed.
35 kPa	:	The damage is not repairable; 50% to 75% of all outer walls are lightly to heavily damaged. The remaining walls are unreliable.
7-15 kPa	:	Not habitable without very major repair works. Partial roof failures, 25% of all walls have failed, serious damages to the remaining carrying elements. Damages to window-frames and doors.
3 kPa	:	Habitable after relatively easy repairs. Minor structural damage.
1-1.5 kPa	:	Damages to roofs, ceilings, minor crackformation in plastering, more than 1% damage to glass-panels.

Table 5. Damages to structures.

Description of Damage	P_s(kPa)
Connections between steel or aluminium ondulated plates have failed	7-14
Walls made of concrete blocks have collapsed	15-20
Brickstone walls, 20 - 30 cm, have collapsed	50
Minor damage to steel frames	8-10
Collapse of steel frames and displacement of foundation	20
Industrial steel self-framing structure collapsed	20-30

3.5 HUD and EPA-RMP

Two government agency documents include minimum pressure values for blast hazards on structures in which mitigation is not required. The U.S. Housing and Urban Development (HUD) and Environmental Protection Agency (EPA). The HUD guidebook[9], "Siting of HUD-assisted Projects near Hazardous Facilities (HUD-1060-CPD, Sept. 1996)" provides the technical guidelines to determine acceptable separation distances. It indicates a minimum pressure of 0.5 psi is acceptable based on the statement in the document. *"Research conducted by military services indicated that 0.5 psi is an acceptable level of blast overpressure for both people and buildings. At this level, people will probably not be injured (especially if located inside a building) and no major structural damage will result to buildings, with the exception of broken windows."*

The EPA requires facilities which store or produce hazardous materials at various minimum quantities to have a Risk Management Plan (RMP). EPA has prepared a separate document, *RMP Offsite Consequence Analysis Guidance*[10], which provides simple methods and reference tables for determining distance to an endpoint for worst-case and alternative release scenarios.

In the document, a 1.0 psi overpressure is given for acceptable exposure for offsite structures. It does not exclude the possibility of severe injuries or death. It does qualify its guidance with the following: *"this overpressure may cause property damage such as partial demolition of houses, which can result in injuries to people, and shattering of glass windows, which may cause skin laceration from flying glass".*

3.6 High Explosive Related Regulations

Department of Defense (DoD) Explosives Safety Manual 6055.9 [[11]] contains published maximum overpressure exposure limits for inhabited building and public property lines. This document requires that without detailed analysis inhabited buildings may not be exposed to more than1.2 psi and 0.9 psi for small explosion and large explosions, respectively. Above these thresholds mitigation measures are required or detailed analysis is needed to show structural damage is limited to acceptable levels.

NATO's AASTP-1[[12]] is a similar document to the DoD 6055.9. In the AASTP-1, 0.72 psi (50 mbar) is given as the limit for exposure for inhabited buildings. This is reduced to 0.3 psi (20 mbar) for high importance buildings (e.g. schools, hospitals, and glass clad buildings). The 0.72 psi limit is qualified with, *"The distances are intended to prevent serious structural damage by blast, flame or projections to ordinary types of inhabited buildings (23 cm brick or equivalent) or caravans and consequent death or serious injuries to their occupants."* It is further added that the limits are "not sufficiently large to prevent breakage of glass and other frangible panels or cladding used in … buildings of vulnerable construction.".

3.7 American Society of Civil Engineers

The American Society of Civil Engineers (ASCE) "Design of Blast Resistant Buildings in Petrochemical Facilities" [[13]] was written with a specific audience of design engineers supported the petrochemical industry. It includes recommendations and methodologies for development of blast loads, dynamic analysis of structures, responses criteria, and damage limits specifically related to hazards associated with petrochemical facilities. While focused on design, the document does address siting buildings, designed for conventional loads only, at an overpressure of 1 psi or less. It goes on to state that *"…unstrengthened buildings can sustain damage less than five percent of the replacement cost and personnel are provided a high degree of protection from death or serious injury."* The basis selection of this value is provisions of DoD 6055.9 limits for inhabited buildings (see Section 3.6 for discussion of DoD 6055.9). It should be noted that the ASCE committee is currently considering a reduction of this over pressure in future editions of the guide.

As can be seen from the sampling of literature regarding blast hazard assessments on building, there is a range of minimum values that are presented or may be interpreted as overpressure screening data. A summary of those examined here is shown in Table 6.

Table 6. Summary of Building "Screening" Values

Source	Building/Component Type	Screening Pressure (psi)
API 752 2nd Edition (2003)[1]	Glass shattering with hazardous velocities	0.25 - 0.5
	Metal/Cemesto/Brick Cladding	0.5 - 1.5
	URM wall collapse, possible shattering	0.5 - 1.5
API 753	Level 2A Damage	0.6
	Level 2B Damage	0.9
Chemical Industries Association	No structural damage or significant glass hazard	0.44
TNO Green Book	Minor to Moderate Damage Partial roof collapse and 25% wall failure	1 - 2
HUD	No major structural damage with the exception of broken windows. Low probability of injury.	0.5
EPA-RMP	Partial demolition of houses, shattering of glass windows Some injuries to people and possible skin laceration from flying glass	1.0
DoD 6055.9	Inhabited Buildings and Property Boundaries – small explosions	1.2
	Inhabited Buildings and Property Boundaries – small explosions	0.9

Source	Building/Component Type	Screening Pressure (psi)
NATO AASTP-1	Schools, hospitals, and glass clad buildings	0.3
	Ordinary inhabited buildings Prevent serious structural damage by blast, flame or projections to ordinary buildings and consequent death or serious injuries to their occupants.”	0.72
ASCE – Design of Blast-Resistant Buildings in Petrochemical Facilities	Based on DoD 6055.9 Unstrengthened buildings can sustain damage less than five percent of the replacement cost and personnel are provided a high degree of protection from death or serious injury	1.0[2]

[1]3rd Edition removed the values and no new minimums were established
[2]Committee currently considering a reduction in this value

4 Reasons for Caution

Selection of a single value for screening buildings of different construction is without a doubt challenging. Determination of a screening overpressure for a single type of construction can also be difficult. Two buildings with the same basic construction can have significantly different load carrying capacities due to differences in details and intended structural response.

Lack of ductility in a structural component dramatically reduces its blast resistance and allowable response levels. As an example, a common construction type in many facilities utilizes concrete masonry units (CMU) or block walls. In locations with very low or no seismic loading requirements, many CMU walls were constructed without steel reinforcement for out of plane loads. A comparison of applied pressure and impulse capacities of unreinforced CMU walls with a similar wall with minimal reinforcement included is illustrated in the Figure 1. Figure 1 is a traditional Pressure-impulse (P-i) diagram. These P-i diagrams are for applied loading as are all of the diagrams shown in the paper. As can be seen in the diagrams, the minimal amount of reinforcement more than doubles its pressure asymptote. For a building evaluator, the visual difference between these two walls can be negligible. It is stressed that these diagrams are applied loads to the wall surface; hence, if the wall is facing the blast a reflection factor would apply to the loading.

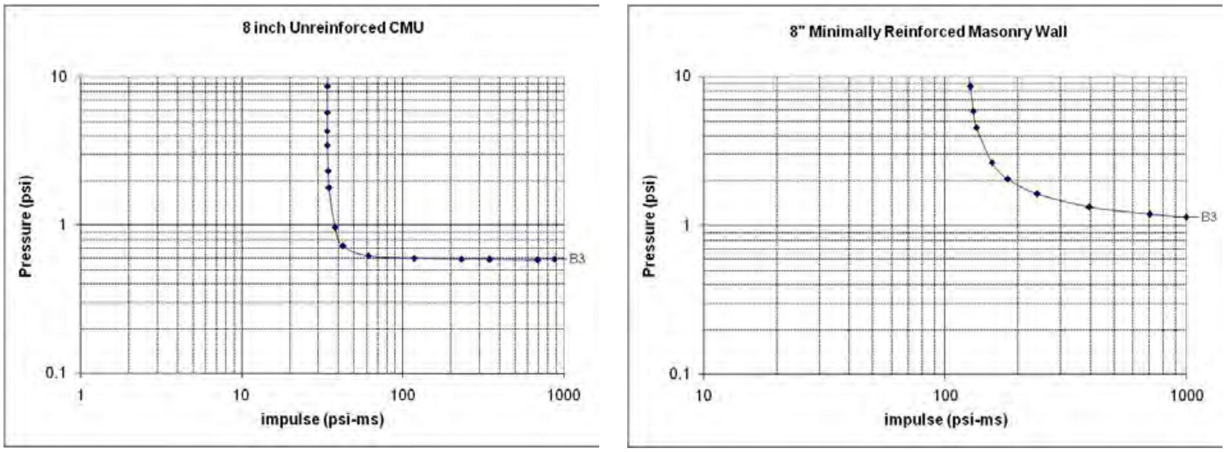


Figure 1. P-I Diagram for Unreinforced and Minimally Reinforced CMU Wall

Another common structural item which can have large differences in blast capacity with seemingly little differences in construction are open web steel joists (OWSJ). When designed for conventional loading, the OWSJ is a very efficient load transferring element. Depending on the design, the load carrying limits may be shear or flexure controlled. A shear-controlled joist will over load its web bracing axially when pushed beyond its full ultimate capacity. Buckling of the bracing ensues and the joist loses its geometric section and load carrying ability rapidly. A flexural-controlled joist will yield in its tension chord first allowing for some limited plastic deformation and energy absorption prior to failure. A comparison of P-i diagrams for shear-controlled and flexural-controlled OWSJ is shown in Figure 2. Again, the pressure capacity increases by a about a factor of 2.

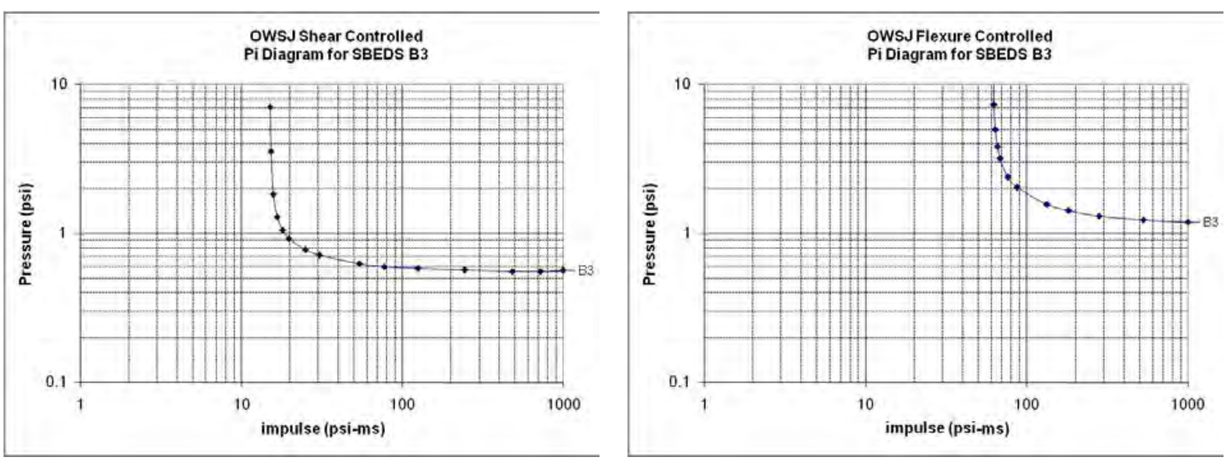


Figure 2. P-I Diagram for Shear and Flexural Controlled OWSJ

Connection detailing in a pre-engineered metal buildings can also make a considerable difference in blast capacity. For a cold-formed girt constructed with a bypass connection (continuous over the outside flange of a column) can exhibit an applied load pressure asymptote about twice the magnitude versus a simply connected member spanning between the columns as seen in Figure 3. Both members are ductile responding and it is the change in support condition for the bypass connection that increases the capacity.

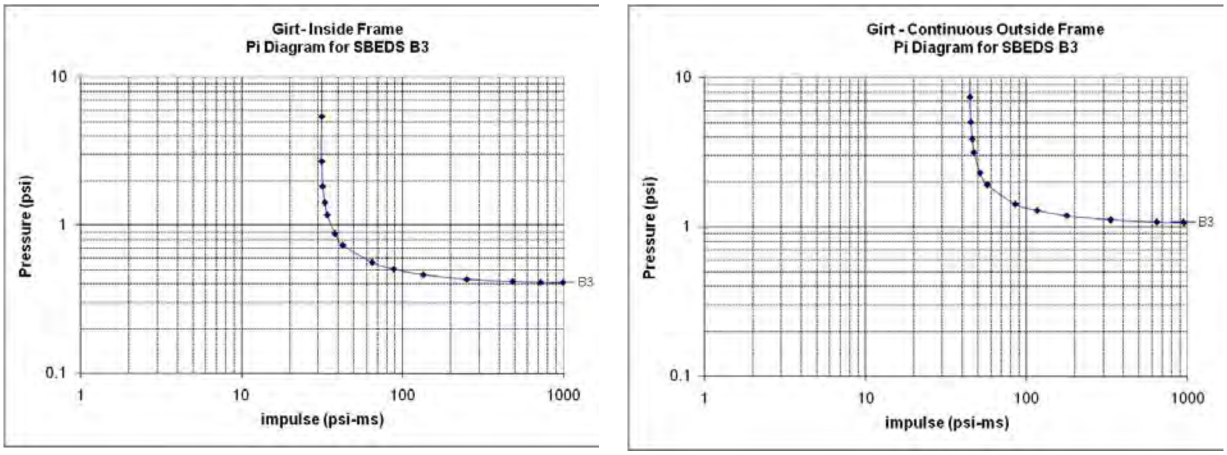


Figure 3. P-I Diagram for Shear and Flexural Controlled OWSJ

Even seemingly robust structural members may have lower blast capacities than intuitively thought. Precast reinforced concrete can have substantial blast resistance due to its strength and mass. However, connections for these members may not always be capable of resisting large reaction associated with a large blast rating. Some of these are intended to only hold members in place and the member itself either bears on another member or connection pocket with gravity being the primary uplift resistance.

Blast capacity rating differences should be identified and addressed before a screening process can be performed to evaluate the building for blast load hazards.

5 Summary and Recommendations

Building screening based on a single pressure value can be an attractive and efficient tool for rapid evaluation of blast hazards. The evaluator or screener should be careful to ensure that screening criteria is properly applied. A clear understanding of the background, industry, and even specific building construction are critical to using an established screening criterion.

A sampling of industry documents and guides demonstrates a broad range of minimal pressure values and damage relationships under which buildings can be considered “safe” or “screened” without further evaluation. This range, of as low as 0.3 psi to as high as 2.0 psi, complicates the ability to select a single value for screening. A rule of thumb of 1.0 psi for building screening has been used in some instances and would appear to be too high to cover the wide range of constructions.

Considerable conservatism is required to select a single value pressure for building screening. This being the case, it is likely that low value must be selected. A conservative value may be so low that only a few buildings will be screened out and further analysis will be required. Essentially, making the screening process ineffective.

The end goal of building evaluation in facility siting processes is typically to determine the risk to occupants. Many of the values presented do not address occupant vulnerability associated with them.

As the API committees move forward to the next editions of recommended practices, the following recommendations are presented for consideration:

- Clearly discuss if there is a need for a single screening value for all building construction types
- Provide understanding that both pressure and impulse should be considered in screening and distinguish between reflected loads and free-field loads in any tables or curves.
- Evaluate and address variability of screening values on similar construction and the need to fully understand considerations such as reinforcement ratios, shear controlled situations, and quality of connections.
- Consider the effectiveness of the screening process for proposed values
- Assess and include occupant vulnerability levels associated with any screening pressure or impulses proposed

6 References

[1] Baker, W.E., Cox, P.A., Westine, P.S., Kulesz, J.J., and Strehlow, R.A., "Explosion Hazards and Evaluation," Fundamental Studies in Engineering 5, Elsevier Scientific Publishing Company, 1983.

[2] API Recommended Practice 752, Management of Hazards Associated with Location of Process Plant Permanent Buildings, Third Edition, December 2009.

[3] Management of Hazards Associated with Location of Process Plant Portable Buildings, American Petroleum Institute Recommended Practice 753 (API RP 753), First Edition, June 2007.

[4] API Recommended Practice 752, Management of Hazards Associated with Location of Process Plant Permanent Buildings, 1st Edition, May 1995.

[5] API Recommended Practice 752, Management of Hazards Associated with Location of Process Plant Permanent Buildings, 1st Edition, November 2003.

[6] Chemical Industry Association, "Guidance for the location and design of occupied buildings on chemical manufacturing sites", 3rd Edition, October 2010.

[7] WS Atkins Science and Technology, "Derivation of fatality probability functions for occupants of buildings", Prepare for the Health and Safety Executive, Report 147, 1997.

[8] TNO, "Methods for the determination of possible damage to people and objects from releases of hazardous materials, CPR 16E, First Edition, 1992.

[9] United Stated Department of Housing and Urban Development, Siting of HUD-assisted Projects near Hazardous Facilities, *Acceptable Separation Distances from Explosive and Flammable Hazards*, HUD-1060-CP, Sept. 1996.

[10] United Stated Environmental Protection Agency, EPA 550-B-99-009, March 2009.

[11] Department of Defense Explosives Safety Board, "Department of Defense Ammunition and Explosives Safety Standards," DoD 6055.9-STD, February 2008.
[12] NATO International Staff – Defence Investment Division, "Manual of NATO Safety Principles for the Storage Of Military Ammunition and Explosives", Allied Ammunition Storage And Transport Publication, Edition 1, May 2006.
[13] American Society of Civil Engineers, "Design of Blast Resistant Buildings in Petrochemical Facilities 2nd Edition," ASCE
Task Committee on Blast Resistant Design, New York, NY, 2010

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Utilizing Turbulent Combustion Models to Better Quantify Far-Field VCE Blast Loads

Robert English*, Paul Hassig, John Mould, Vincent Nasri, and James Wesevich
Thornton Tomasetti, Applied Science, 2100 West Loop South, Suite 680, Houston, TX 77027
Thornton Tomasetti, MMI, The Brew House Wilderspool Park, Greenall's Avenue, Warrington Cheshire, WA4 6HL
* Presenter E-mail: renglish@thorntontomasetti.com, JWesevich@ThorntonTomasetti.com

Abstract

Properly quantifying the blast overpressures due to vapor cloud explosions (VCE) are an integral aspect of a facility siting Quantitative Risk Assessment (QRA). Currently the onshore petrochemical industry utilizes a line-of-sight methodology for developing blast overpressures from vapor cloud explosions (VCEs) at building locations, and usually assumes a shock loading waveform. This simplified methodology falls short in accurately capturing potential wave propagation effects such as shielding and channeling which can considerably alter the blast overpressures and blast waveform shape imposed on a structure. Ignoring these wave effects will lead to an incorrect determination of building damage level, which in turn can mislead owners/operators in understanding the level of risk occupants are subjected to, and improper allocation of valuable capital improvements funding.

By utilizing a turbulent combustion code, such as FLACS to calculate the near field blast source, as an input to drive a far-field fast running Computational Fluid Dynamics (CFD) code, such as FacilityBlast VCE, engineers can more accurately quantify the blast loads imposed on various occupied structures across an onshore facility. This paper aims to demonstrate the benefit of utilizing a turbulent combustion model to calculate the initial blast source term as opposed to simpler specified flame speed approximations to calibrate a far field CFD calculation. The improvement in accuracy will lead to better risk predications and in-turn better decision making by owner/operators.

Keywords: facility siting, vapor cloud explosion, building damage, occupant vulnerability, channeling and shielding effects, quantitative risk assessment

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Pressure Relief Valves Stability: Current Models Comparison and an Approach to Simplify Dynamic Modelling

A. Aldeeb*
Siemens Energy, Inc.
Houston, Texas
*Presenter E-mail: abdul.aldeeb@siemens.com

Abstract

The industry engineering guidance to size, select, and install pressure relief valves provides design criteria to prevent unstable operation or “chatter” of valves. Generally, the design is based on steady-state operating conditions and a typical blow-down pressure setting. However, the stability of the pressure relief valve is influenced by the dynamic response of the valve disk to the unsteady pressures and forces exerted by the fluid on the valve’s disk coupled with the protected system, i.e., vessel and pressure relief valve inlet and outlet piping, hydraulic performance.

Several models have been developed to predict the stability of the pressure relief valves performance. However, each model has own challenges that are contributed to either modelling requirements complexity, limitations of flow phase modelling, or limitations on handling complex system configurations.

In this presentation, a detailed comparison of available pressure relief valve stability models is discussed to develop a comprehensive view of modelling capabilities and limitations. In addition, a recently developed simplified pressure relief valve stability model is presented to address major existing models’ limitations.

The simplified model predictions have been benchmarked against available lab and full-scale experimental data to define validity windows.

Keywords: Pressure Relief Valve Stability, Chatter, Stability Modeling

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Comparison of safety indexes for chemical processes under uncertainty

Mahmoud M. El-Halwagi[2], Arturo Jiménez-Gutiérrez[1], Vasiliki Kazantzi[4], Nikolaos K. Kazantzis[3], and Andrea P. Ortiz-Espinoza[1]*

[1] Departamento de Ingeniería Química, Instituto Tecnológico de Celaya, Celaya, Gto., 38010, México

[2] Chemical Engineering Department, Texas A&M University, College Station, Texas 77843, U.S.

[3] Department of Chemical Engineering, Worcester Polytechnic Institute (WPI), Worcester, MA 01609-2280, USA

[4] Department of Business Administration, University of Applied Sciences (TEI) of Thessaly, Larissa, 41110, Greece

*Presenter E-mail: andrea.ortiz@iqcelaya.itc.mx

Abstract

The fatal consequences of industrial incidents have made evident the need for suitable tools to develop inherently safer process designs. Traditionally, in a process design project, the evaluation of safety aspects is left for analysis after the detailed design has been completed. This approach leads to the use of control loops, barriers and protection layers as the only ways to prevent incidents and to reduce the possible outcomes. An alternative to this approach is the application of the concept of inherent safety, which was introduced to set up several principles that aim to enhance process safety by eliminating, avoiding or minimizing sources of risk.

In this work, we present a comparison of different safety metrics in their role to evaluate the risk associated with a given process design. The indices selected for consideration are better applied at the conceptual stage of the process design, and they were the Dow's fire and explosion index (F&EI), the fire and explosion damage index (FEDI), the process route index (PRI) and the process stream index (PSI). All these indices use different input information and their outcomes have different rankings. The metrics were applied to an ethylene production process to identify risk levels, and the location of streams and pieces of equipment that pose the highest risk within the process. An evaluation of the indices in their capability to track design changes in operating conditions aiming to improve the safety level of the process was developed. To perform the assessment of the safety metrics in a more extensive manner, an uncertainty analysis based on a Monte Carlo simulation framework was implemented and compared to the traditional use of single-value design variables. Within this context, an insightful assessment of uncertainty's effect on process safety characteristics was achieved because of the identification of ranges of safety-relevant performance outcomes (zones of risks and opportunities) that can be probabilistically characterized. The approach was applied to a case study related to the production of ethylene from shale gas. The results showed how some indexes are better suited to capture the risk characteristics associated with the process when changes in the operating conditions of the section with highest risk were implemented. The methodology can be extended to other processes of interest, and may serve as a basis for the safety and process design community to propose adjustments in the structure of the safety indices based on a better understanding of their performance and reliability as part of the efforts towards the continued improvement of those safety metrics.

Keywords: Process design, ISD

1. Introduction

Traditionally, safety analysis in a process design project is performed after the detailed design is completed. Within this approach, little can be done to modify the design in order to enhance safety performance (Lee et al., 2019). Instead, control loops, barriers, and protection layers are used to reduce the possible outcomes in case of an incident (Khan et al., 2003). Despite the usefulness of these devices to contain or minimize the consequences of an incident, past events have shown that these devices may fail to cause fatal consequences (Abidin et al., 2016). Inherent safety aims to eliminate, reduce or avoid sources of risk, thus improving the safety properties of the process (Rahman et al., 2005; Kidam et al., 2016).

Inherent safety principles are better applied at early design stages, where the design can be easily modified to include safer features. To assess if the changes introduced to the design result in a safer process, it is necessary the use of proper metrics that evaluate safety levels of the process design. There are different tools to evaluate a process in terms of safety performance. Among the most popular ones are the hazard and operability (HAZOP) method and the quantitative risk assessment (QRA) (Roy et al., 2016). The HAZOP method is a qualitative tool that requires detailed information about the process. Typically, the type of information needed for a HAZOP analysis is not available in early design stages. The QRA is based on the probabilistic estimation of failures and consequences. Although this method may be suitable for the analysis of pieces of equipment (Medina-Herrera et al., 2014a; Medina-Herrera et al., 2014b) its use in a complete process may not be suitable at early design stages.

As an alternative to these tools, safety indices have been developed to consider process characteristics that may result in potential incidents (Roy et al., 2016). The first index reported in the literature was the Dow's fire and explosion index (F&EI). This index is based on material and process factors (AIChE, 1998) and although it considers detailed information of the process, it can be simplified to assess safety characteristics at the conceptual design stage (Suardin et al., 2007; Vázquez et al., 2018; Ruiz-Femenia et al., 2017). The Dow's F&EI relies heavily on the material factor, which only reflects the characteristics of the chemicals but not the operating conditions. The latter aspect motivated the development of other indices that combine both operating conditions and chemical characteristics to obtain a more reliable safety assessment. One such index is the Fire and Explosion Damage Index (FEDI) developed by Khan and Abbasi (1998). This index classifies the units of a process according to its purpose and assesses the potential to cause hazards. Both indices, Dow's F&EI and FEDI, consider the components in the process as individual components, not as mixtures. For the evaluation of both indices, only the characteristics of the most hazardous component are considered, overlooking the contribution of other hazardous components. To overcome this limitation, other indices have been introduced, such as the process route index (PRI) and the process stream index (PSI). These indices consider the hazardous characteristics of mixtures instead of those of single components. Additionally, these indices were developed to obtain information directly from process simulators, which eliminates the tedious procedure of information transfer and thus avoiding errors during the safety evaluation process (Leong & Shariff, 2009; Shariff et al., 2012). The combination of PRI and PSI may be used to identify hazardous areas in process designs, and examine the result of potential changes in the operating conditions of such areas on items such as risk and economic performance (Ortiz-Espinoza et al., 2017). The PSI uses the principle of relative ranking to identify the most hazardous streams in a process in terms of fire and explosions, while PRI considers stream parameters such as combustibility, energy, density and pressure to rank different processes. While Dow's F&EI and FEDI have an established ranking to interpret the results from the evaluation, the PRI index does not classify the results of the evaluation according to the level of hazard.

The evaluation of these indices typically relies on information that, although represented as average values, is commonly uncertain. The use of these types of input values may lead to the misinterpretation of the results, which may affect the decision-making process. The problem then is to formulate the evaluation model so that uncertainty in key design variables is included. One way to accomplish this task is the use of Monte Carlo (MC) simulation methods (Koc et al., 2012) which allows the consideration of multiple uncertain inputs. The uncertainty in the selected inputs is represented using probability distributions and then propagated through the model. Within this framework, distribution profiles are obtained for the evaluated metrics. Such profiles can be statistically characterized, and ranges of performance outcomes can be generated. This type of results provides more valuable insights that can be used by process decision-makers to make more informed decisions when selecting among different design options.

In this work, the Dow's F&EI, the FEDI, the PRI, and PSI indices are compared to identify which one may be more suitable to use at the conceptual stage of a process design. To complete the analysis, the evaluation of the indices is performed under a systematic uncertainty analysis framework. The metrics are applied to an ethylene production process, where the most hazardous areas or pieces of equipment in the process are identified. Modifications to the operating conditions are then implemented to find which index captures better such modifications. Within the proposed uncertainty analysis, framework distribution profiles are obtained and probabilistically characterized for each index. It should be pointed out that these safety indices profiles represent a potential advantage for decision-makers since possible underestimation of process risks in the presence of uncertainty could pose significant adverse effects.

2. Approach

The four indices analyzed in this work, the Dow's fire and explosion index (F&EI), the fire and explosion damage index (FEDI), the process route index (PRI), and the process stream index (PSI), take into account the characteristics of the chemicals and the process conditions that can result in a fire and/or explosion incident. Each index takes into account different types of information from the process design, and their structure is different. A brief description of those indices is given below.

2.1 The Dow's Fire and Explosion Index (F&EI)

The F&EI was developed in 1964 by the Dow Company (Roy et al., 2016). The index is calculated based on the material factor (MF) and the process unit hazards factor (F_{3Dow}). The MF is selected according to the flammability and reactive characteristics of the chemical molecule involved in the process units. When more than one flammable or reactive chemical is present, the material factor is selected based on the most hazardous one. The process unit hazards factor is the result of the product of two other factors named general process hazards factor (F_{1Dow}) and special process factor (F_{2Dow}). Both factors result from the addition of a base factor and the penalties that result from considering some process characteristics. Equations 1 and 2 show how these factors are calculated, while equations 3 and 4 show the way in which F_{3Dow} and the F&EI are computed.

$$F_{1Dow} = 1 + \sum_{i=1}^{6} penalty_{i_{F_1}} \tag{1}$$

$$F_{2Dow} = 1 + \sum_{i=1}^{12} penalty_{i_{F_2}} \tag{2}$$

$$F_{3Dow} = (F_{1Dow})(F_{2Dow}) \tag{3}$$

$$F\&EI = (MF)(F_{3Dow}) \tag{4}$$

The results obtained for the F&EI can be classified according to the degree of hazard proposed by the classification guide by AIChE (1994) (see Table 1).

Table 1. Classification of units according to the F&EI

F&EI range	**Degree of hazard**
1 – 60	Light
61 – 96	Moderate
97 – 127	Intermediate
128 – 158	Heavy
159 – up	Severe

2.2 The Fire and Explosion Damage Index (FEDI)

The FEDI was developed as part of a system named hazard identification and ranking (HIRA) (Khan and Abbasi, 1998). This index classifies the units of an industrial process according to its purpose, as shown in Table 2.

Table 2. Classification of units for FEDI estimation

Group	Type of unit	Examples
I	Storage	Storages tanks, intermediate process inventories
II	Involving physical operation	Pumps, compressors, units involving heat transfer, mass transfer or phase change
III	Involving chemical reactions	Reactors
IV	Transportation	Pipelines
V	Other	Boilers, direct-fired heat exchanger, flares, furnaces

Once the unit to be evaluated has been classified, different energy factors are considered. The first energy factor (F_{1FEDI}) accounts for chemical energy. F_{1FEDI} is given by the amount of chemical processed in the unit (M) and the heat of combustion (H_c). Energy factors F_{2FEDI} and F_{3FEDI} account for energy due to the internal pressure of the unit (physical energy). In the case of a unit of group III, a fourth factor (F_{4FEDI}) is used. Equations 5 to 8 are used to calculate each energy factor,

$$F_{1_{FEDI}} = (0.1)(M)\left(\frac{H_c}{K}\right) \tag{5}$$

$$F_{2_{FEDI}} = (1.304x10^{-3})(PP)(Vol) \tag{6}$$

$$F_{3_{FEDI}} = (1x10^{-3})\left(\frac{1}{T+273}\right)(PP-VP)^2(Vol) \tag{7}$$

$$F_{4_{FEDI}} = (M)\left(\frac{H_{rxn}}{K}\right) \tag{8}$$

where M is in kg/s, PP is the operating pressure in kPa, Vol is the volume of the vessel in m^3, T is the operating temperature in °C, VP is the vapor pressure in kPa and H_{rxn} is the heat released by chemical reactions in kJ/kg.

After the estimation of the energy factors, penalty values are assigned to account for the severity of some process parameters such as temperature, pressure, capacity, and the characteristics of the chemicals. Then, energy factors and penalties are added to estimate the hazard potential (hazpot) according to equations 9 to 13.

$$hazpot_{Group_I} = \left[\left(F_{1_{FEDI}}\right)(pn_1) + (F)(pn_2)\right]\left(\prod_{i=3}^{8} pn_i\right) \tag{9}$$

$$hazpot_{Group_{II}} = \left[\left(F_{1_{FEDI}}\right)(pn_1) + (F)(pn_2)\right]\left(\prod_{i=3}^{8} pn_i\right) \tag{10}$$

$$hazpot_{Group_{III}} = \left[\left(F_{1_{FEDI}}\right)(pn_1) + (F)(pn_2) + \left(F_{4_{FEDI}}\right)(pn_9)(pn_{10})\right]\left(\prod_{i=3}^{8} pn_i\right) \quad (11)$$

$$hazpot_{Group_{IV}} = \left[\left(F_{1_{FEDI}}\right)(pn_1) + (F)(pn_2)\right]\left(\prod_{i=3}^{9} pn_i\right) \quad (12)$$

$$hazpot_{Group_{V}} = \left(F_{1_{FEDI}}\right)\left(\prod_{i=1}^{8} pn_i\right) \quad (13)$$

Finally, the hazard potential is transformed into the FEDI with the use of Equation 14.

$$FEDI = 4.76\ (hazpot)^{\frac{1}{3}} \quad (14)$$

The results for the FEDI can be ranked according to values in Table 3.

Table 3. Hazard ranking according to FEDI values from the HIRA methodology*

FEDI	**Hazard characterization**
FEDI > 500	Extremely hazardous
500 > FEDI > 400	Highly hazardous
400 > FEDI > 200	Hazardous
200 > FEDI > 100	Moderately hazardous
100 > FEDI > 20	Less hazard
else	No hazard

*Source: Khan and Abbasi (1998)

2.3 Process Route Index (PRI) and Process Stream Index (PSI)

The PRI and the PSI were developed to include the contribution of individual components in mixtures to the process stream parameters associated to those indices (Leong & Shariff, 2009; Shariff et al., 2012). Both indices are based on parameters that impact the outcome of an explosion incident. Such parameters are density, pressure, energy, and combustibility. Although PRI and PSI are based on the same parameters, these indices are structured differently and have different purposes. The PRI is used to rank processes while the PSI is used to identify the most hazardous process streams within a process. An advantage of both indices is that the process stream parameters can be directly obtained from process simulators, easing off the computation process.

2.3.1 Calculation of the Process Route Index (PRI)

To estimate the PRI, values of density, pressure, and mass heating value (energy) for each stream are obtained from process simulations. In addition, to estimate the combustibility of the process streams, information such as stream composition and temperature is also extracted. Then, the information obtained from the process simulation is combined with data related to the lower and upper flammability limits (LFL and UFL) and the heat of combustion (ΔH_c) for each component in the streams.

Equations 15 and 16 show the effect of temperature in the flammability limits. Once the flammability limits of each component are adjusted due to the effect of temperature, flammability limits for the mixtures are computed as shown in equations 17 and 18,

$$LFL_T = LFL_{25}\left[1 - \frac{0.75(T-25)}{\Delta H_c}\right] \tag{15}$$

$$UFL_T = UFL_{25}\left[1 + \frac{0.75(T-25)}{\Delta H_c}\right] \tag{16}$$

$$LFL_{mix} = \frac{1}{\sum_{i=1}^{n}\left(\frac{y_i}{LFL_i}\right)} \tag{17}$$

$$UFL_{mix} = \frac{1}{\sum_{i=1}^{n}\left(\frac{y_i}{UFL_i}\right)} \tag{18}$$

where LFL_T and UFL_T stand for lower and upper flammability limits at a given temperature T, LFL_{25} and UFL_{25} are the lower and upper flammability limits at 25 °C, and ΔH_c is the heat of combustion; LFL_{mix} and UFL_{mix} are the lower and upper flammability limits of the mixture, y_i is the mole fraction of component i, and LFL_i and UFL_i are the lower and upper flammability limits of component i. Combustibility is then estimated with Equation 19.

$$combustibility = UFL_{mix} - LFL_{mix} \tag{19}$$

Once combustibility is obtained, the average values of the parameters can be used to calculate the PRI for the process using Equation 20.

$$PRI = \frac{\left[\begin{pmatrix} average\ mass \\ heating\ value \end{pmatrix}\begin{pmatrix} average\ fluid \\ density \end{pmatrix}\begin{pmatrix} average \\ pressure \end{pmatrix}\begin{pmatrix} average \\ combustibility \end{pmatrix}\right]}{10^8} \tag{20}$$

2.3.2 Calculation of the Process Stream Index (PSI)

PSI uses the principle of relative ranking to determine the more hazardous streams of a process. The index is composed of four sub-indices in which the four parameters (density, pressure, energy, and combustibility) are compared to the average parameter value for the process as in equations 21 to 24.

$$I_e = \frac{heating\ value\ of\ individual\ stream}{average\ heating\ value\ of\ all\ streams} \tag{21}$$

$$I_P = \frac{pressure\ of\ individual\ stream}{average\ pressure\ of\ all\ streams} \tag{22}$$

$$I_\rho = \frac{density\ of\ individual\ stream}{average\ density\ of\ all\ streams} \tag{23}$$

$$I_{FL} = \frac{combusibility\ of\ individual\ stream}{average\ combustibility\ of\ all\ streams} \tag{24}$$

To calculate the value of PSI, the values from equations 21 to 24 are combined as follows,

$$PSI = A_0(I_e I_p I_\rho I_{FL}) \tag{25}$$

where A_0 is a constant used to adjust the order of magnitude of the index (we used a value of 10 in this work).

2.4 Uncertainty evaluation

To account for the uncertainty in the inputs and propagate it through the model, an integrated framework using MC simulations was considered. The approach is based on the one proposed by Ortiz-Espinoza et al. (2019) and described in Figure 1.

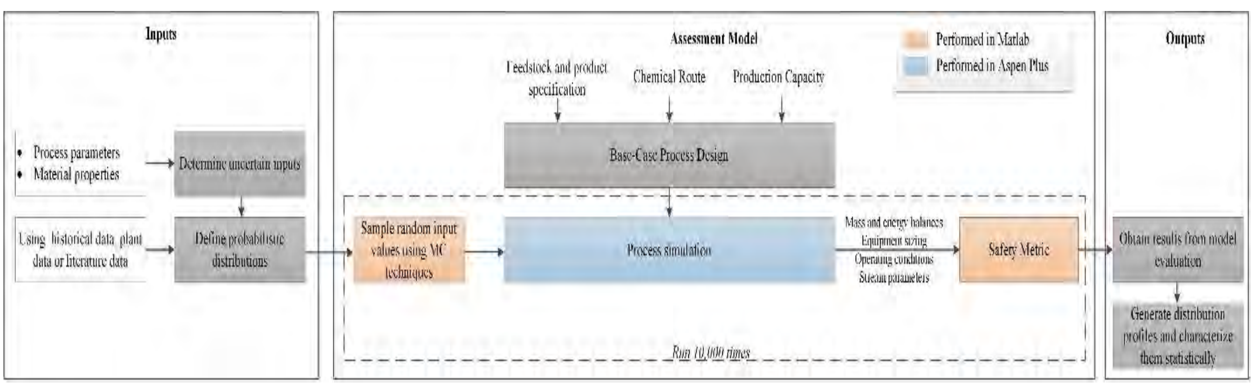


Figure 1. Integrated framework for the inclusion of uncertainty in the evaluation of safety performance of chemical processes

A base case for the process is first developed. Then, it is necessary to select the safety evaluation model and to identify the input information needed, and probabilistic distributions are derived from information obtained from historical, plant, or literature data.

After the probabilistic distributions are established, random values are sampled for each input using MC simulations. These values are then fed to the process simulator and the safety evaluation model. Data from process simulations and external information are used to evaluate the safety metrics. The results are gathered to generate the distribution profiles for the index. This step is repeated a sufficient number of times (10,000 in this case) to generate sufficient results so that a reliable characterization of the profiles can be done. The statistical characterization of the profiles includes minimum and maximum values, mean value, standard deviation, and values of risk and opportunity.

3. Case Study

To compare the selected safety metrics and its performance in the presence of uncertainty, an ethylene production process was evaluated. The process takes the production of ethylene from natural gas via the production of methanol. A great part of this process occurs in gas phase and with the presence of flammable gases (e.g. methane, hydrogen, carbon monoxide). The process consists of three stages, namely reforming, methanol synthesis, and olefins production. A detailed description of the process structure and its conditions may be consulted in Ortiz-Espinoza et al. (2017a).

The safety, economic and sustainable features of this process were previously analyzed by Ortiz-Espinoza et al. (2017b) in which the PSI was used to detect the most hazardous area of the process, and the PRI was used to assess changes in operating conditions. The Dow's F&EI and the FEDI are additionally considered in this work; these indices give a numerical value per piece of equipment, so this helps to identify the most hazardous units in the process. Then, the highest number of all the values obtained is selected as the representative number for the whole process, and changes in the design are evaluated to see if the indices are able to account for the effects of such changes. The first two steps are performed using nominal values, after which the inclusion of uncertainty is carried out using the proposed approach displayed in Figure 1.

3.1 Assumptions for safety evaluation

3.1.1 PSI

For the evaluation of the PSI, the four parameters considered by the index are put together by a multiplication rule. An important characteristic that is observed for this index is that since all factors are weighted equally, the results may be biased by the presence of different stream phases, due to high differences of density. Therefore, liquid and gas streams are considered separately, i.e. the gas phase streams are evaluated with the average value of the gas streams only, and the liquid streams are evaluated only with liquid streams data.

3.1.2 F&EI

For the estimation of the Dow's F&EI, the assumptions and recommendations in the classification guide (AIChE, 1998) are followed. For the estimation of the $penalty_{7_{F_2}}$ term, the amount of flammable material that can be released from the process unit within 10 minutes is considered.

Penalties for unit location ($penalty_{4_{F_1}}$), access ($penalty_{5_{F_1}}$), drainage and spill control ($penalty_{6_{F_1}}$), corrosion and erosion ($penalty_{8_{F_2}}$), and leakage ($penalty_{9_{F_2}}$) are not considered, since the information needed for their calculations is not available at the conceptual design stage of the process.

3.1.3 FEDI

The estimation of the FEDI is made using the methodology reported in Khan et al. (2001). For the assessment of distillation columns, the quantity of material is estimated as proposed in Castillo-Landero et al. (2019) using Equation 26. The conditions at the top of the column are used for safety calculations as suggested in Thiruvenkataswamy et al. (2016).

$$M = Feed + L + V' \tag{26}$$

Since the index considers the volume of the vessel as an important component to calculate energy factors, small equipment units such as mixers and splitters are not evaluated.

3.1.4 PRI

For the assessment of the PRI only streams in gas phase are considered, since most of the process streams are in the gas phase.

4. Results

4.1 Safety evaluation

4.1.1 PSI

The evaluation of safety indices was performed using the information obtained from Aspen Plus simulations and external data sources (e.g. NFPA, Dow's F&EI guide). The results for the PSI evaluation are summarized in Table 4, and the most hazardous streams are highlighted in Figure 2. As can be observed, the most hazardous gas streams are contained in the methanol synthesis loop. According to the values in Table 4, the main contribution to the PSI values of such streams is the sub-index I_P that accounts for the effect of pressure. The two most hazardous liquid streams are also highlighted in Figure 2.

Although the consideration of the phase stream may be relevant, e.g. a liquid stream leaking will release more material than a gaseous stream at the same conditions, to assess the hazard levels correctly would require the consideration of other factors such as flash point and vapor pressure, and not only the stream density.

Table 4. PSI results for the streams of the ethylene process

Stream	I_e	I_P	$I\rho$	I_{FL}	PSI	Stream	I_e	I_P	$I\rho$	I_{FL}	PSI
1	0.425	0.712	0.590	0.320	0.573	26	0.608	0.043	0.027	0.628	0.004
2	0.409	0.570	0.527	0.313	0.384	27	1.271	0.370	0.644	0.534	1.619
3	0.409	0.570	0.318	0.464	0.343	28	1.276	0.370	0.641	0.534	1.618
4	0.348	0.570	0.161	2.055	0.654	29	1.331	0.370	0.656	0.534	1.727
5	0.515	0.570	0.525	1.660	2.557	30	1.331	0.698	1.096	0.542	5.517
6	0.515	0.570	0.525	1.660	2.557	31	1.356	0.698	1.580	0.519	7.769
7	0.914	0.570	0.340	1.660	2.943	32	1.367	0.698	1.755	0.963	16.116
8	0.914	0.570	0.340	1.660	2.943	33	1.826	0.251	0.218	0.950	0.949
9	0.394	0.570	0.944	1.073	2.272	^34	1.144	0.380	0.994	1.723	7.437
10	0.914	0.570	0.340	1.660	2.943	^35	1.144	0.872	0.997	1.723	17.124
11	0.760	0.570	0.420	1.571	2.858	^36	1.110	1.057	0.853	0.580	5.812
12	0.758	0.570	0.410	1.577	2.793	37	1.293	0.575	2.212	0.243	3.996
13	0.758	2.364	0.990	1.743	30.956	38	1.293	0.624	2.396	0.243	4.702
14	0.786	2.364	1.081	1.567	31.472	39	1.104	0.817	0.868	0.445	3.716
15	0.751	2.364	1.531	1.186	32.247	C4's	1.276	0.216	0.885	0.231	0.566
16	0.753	2.307	1.928	1.108	37.108	^C5's	1.129	0.328	1.047	0.404	1.567
17	0.759	2.202	1.812	1.105	33.443	^Ethane	1.177	0.880	0.813	0.512	4.308
18	0.860	2.136	1.610	1.045	30.920	Ethylene	1.329	0.581	1.913	0.928	13.709
19	0.860	2.136	1.610	1.128	33.377	Hydrogen	2.814	0.570	0.103	1.967	3.245
20	0.860	2.136	1.610	1.128	33.377	Natural Gas	1.441	0.741	0.885	0.281	2.658
21	0.860	2.136	1.610	1.128	33.377	^Propane	1.117	0.945	0.846	0.458	4.094
22	0.860	2.364	1.706	1.136	39.412	Propylene	1.292	0.624	2.428	0.244	4.776
23	0.860	2.364	1.429	1.177	34.214	Purge	0.866	0.285	0.368	0.552	0.502
^24	0.539	3.236	1.260	1.585	34.799	Syngas Purge	0.860	2.136	1.610	1.128	33.377
^25	1.129	0.328	1.047	0.405	1.567	Tail gas	2.314	0.251	0.196	1.228	1.397

^Liquid streams

4.1.2 Dow's F&EI

The results for the estimation of the Dow's F&EI are reported in Table 5, and the hazzard classification for each piece of equipment is shown in Figure 3. Similarly to the results for PSI, the equipment unit identified as the most hazardous one is the methanol synthesis reactor. Additionally, most of the units in the methanol synthesis loop are classified as intermediate in terms of hazard. The rest of the equipment is classified as moderate or light hazard, except for the reactors in the reforming stage. This result may be due to the penalties considered for exothermic or endothermic reactions, a characteristic that is not addressed in the PSI estimation.

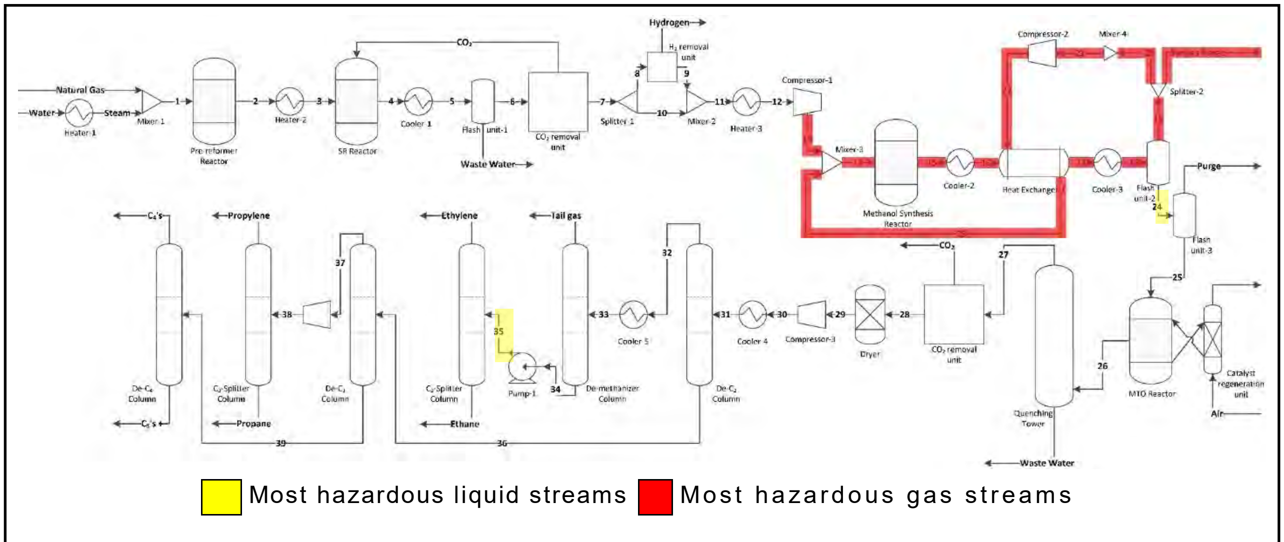


Figure 2. Identification of hazardous streams using process stream index (PSI)

Table 5. Dow's F&EI results for the equipment of the ethylene process

Piece of equipment	F&EI	Classification	Piece of equipment	F&EI	Classification
Heater-1	1.7	Light	Splitter-2	99.6	Intermediate
Mixer-1	85.2	Moderate	Mixer-4	90.9	Moderate
Pre reformer reactor	100.3	Intermediate	Compressor-2	116.0	Intermediate
Heater-2	83.6	Moderate	Flash unit-3	48.7	Light
SR Reactor	125.2	Intermediate	MTO Reactor	90.8	Moderate
Cooler-1	104.3	Intermediate	Catalyst regenerator	94.4	Moderate
Flash unit-1	93.8	Moderate	Quenching tower	82.0	Moderate
CO_2 removal unit	93.8	Moderate	CO_2 removal unit	82.2	Moderate
Splitter-1	93.8	Moderate	Dryer	82.2	Moderate
H_2 removal unit	81.7	Moderate	Compressor-3	99.0	Intermediate
Mixer-2	91.4	Moderate	Cooler-4	94.2	Moderate
Heater-3	91.4	Moderate	De-C_2 column	94.2	Moderate
Compressor-1	112.6	Intermediate	Cooler-5	84.4	Moderate
Mixer-3	105.3	Intermediate	De-methanizer	77.5	Moderate
Methanol synthesis reactor	136.8	Heavy	Pump-1	93.8	Moderate
			C_2-Splitter	81.9	Moderate
Cooler-2	104.7	Intermediate	De-C_3 column	62.9	Moderate
Heat exchanger-1	105.0	Intermediate	Compressor-4	59.0	Light
Cooler-3	103.9	Intermediate	C_3-Splitter	59.0	Light
Flash unit-2	103.9	Intermediate	De-C_4 column	42.8	Light

4.1.3 FEDI

Results for the ethylene process using the FEDI index are presented in Table 6 and Figure 4. Some discrepancies are observed with respect to the PSI and the F&EI results. According to the FEDI evaluation, the most hazardous piece of equipment is the C_3-Splitter column, followed by the de-propanizer unit and the methanol reactor, which are classified as hazardous. One important characteristic of this index is that it considers the volume of the vessel in the estimation of the physical energy factor (F_{2FEDI} and F_{3FEDI}). Therefore, for the biggest units such as distillation columns, the results may be influenced by their size. From the results of the PSI and F&EI, however, this may not necessarily represent an accurate hazard level for the process unit.

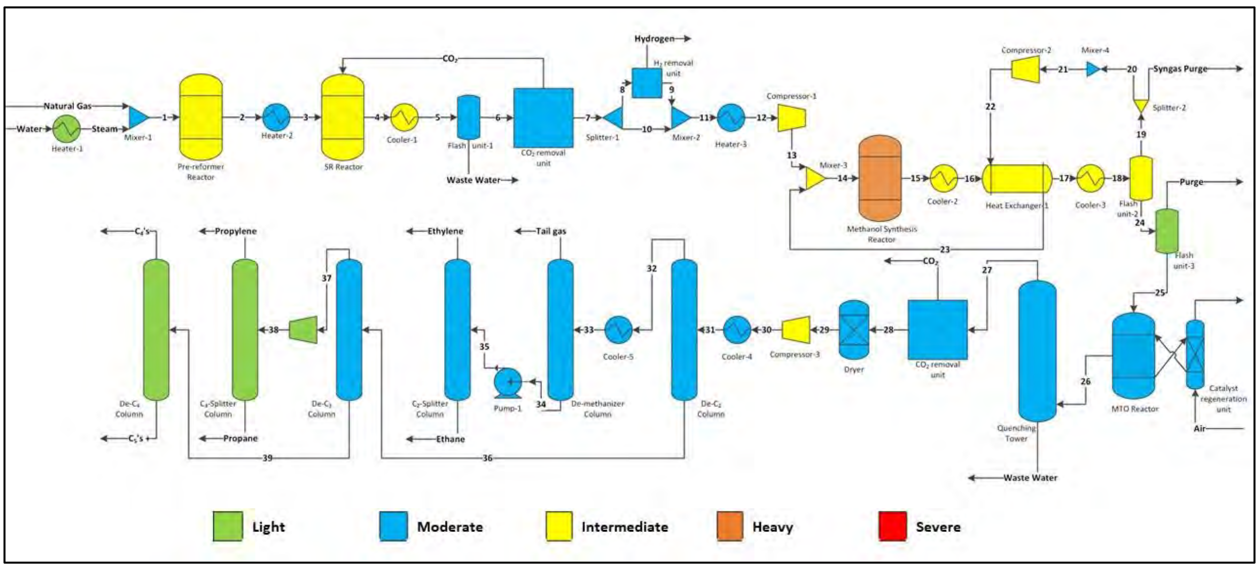


Figure 3. Classification of equipment according to degree of hazard using the Dow's F&EI

4.2 Assessment of design changes

Given that we are dealing with a conceptual design stage of the process and that we have identified the most hazardous pieces of equipment, changes to the design to enhance safety levels can be readily analyzed. To keep track of the effect of the changes in the process safety performance, the safety metrics are evaluated for each individual change implemented for the process conditions. To evaluate the response of the indices on the same basis, the modifications were made to the operating pressure of the methanol synthesis loops, since two out of the three indices identified this area of the process as the most hazardous. The results for the evaluation of the different indices at different operating pressures are reported in Table 7.

Table 6. FEDI results for the equipment of the ethylene process

Piece of equipment	FEDI	Classification	Piece of equipment	FEDI	Classification
Heater-1	18.0	No hazard	Flash unit-3	93.1	Less Hazardous
Pre reformer reactor	140.4	Moderately hazardous	MTO Reactor	123.8	Moderately hazardous
Heater-2	148.1	Moderately hazardous	Quenching tower	119.0	Moderately hazardous
SR Reactor	151.3	Moderately hazardous	CO_2 removal unit	91.3	Less Hazardous
Cooler-1	157.5	Moderately hazardous	Dryer	91.3	Less Hazardous
Flash unit-1	156.9	Moderately hazardous	Compressor-3	89.6	Less Hazardous
CO_2 removal unit	134.9	Moderately hazardous	Cooler-4	89.7	Less Hazardous
Heater-3	107.5	Moderately hazardous	De-C_2 column	199.8	Moderately hazardous
Compressor-1	107.6	Moderately hazardous	Cooler-5	87.4	Less Hazardous
Methanol synthesis reactor	306.6	Hazardous	De-methanizer	113.8	Moderately hazardous
			Pump-1	71.9	Less Hazardous
Cooler-2	119.7	Moderately hazardous	C_2-Splitter	164.8	Moderately hazardous
Heat exchanger-1	119.5	Moderately hazardous	De-C_3 column	300.3	Hazardous
Cooler-3	122.5	Moderately hazardous	Compressor-4	147.9	Moderately hazardous
Flash unit-2	122.4	Moderately hazardous	C_3-Splitter	526.0	Extremely hazardous
Compressor-2	76.9	Less Hazardous	De-C_4 column	187.7	Moderately hazardous

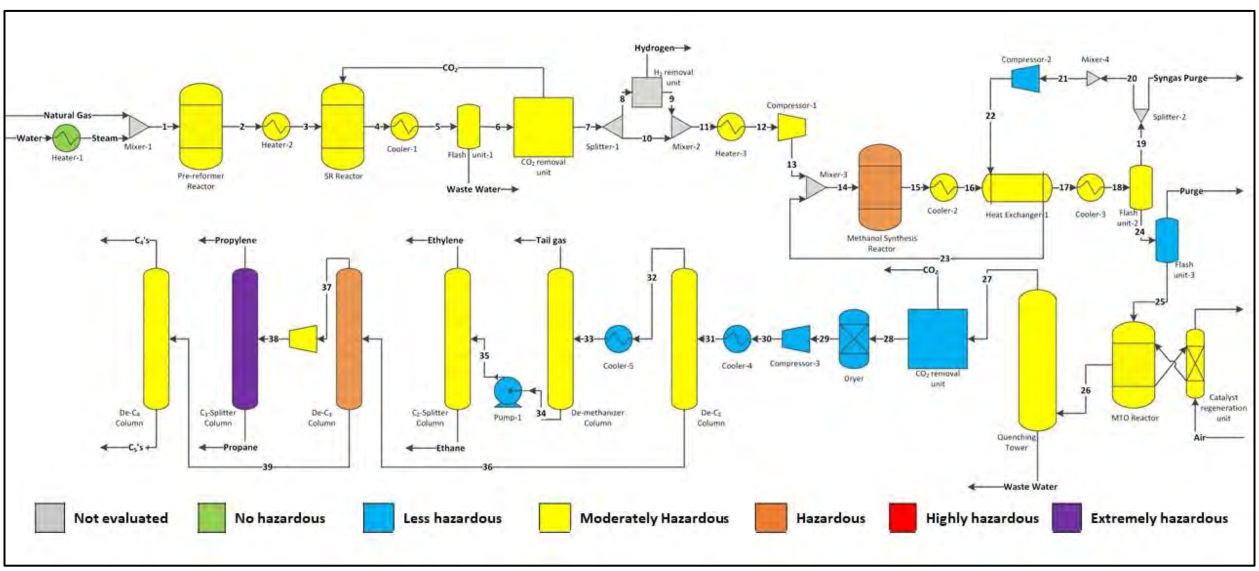


Figure 4. Classification of equipment according to hazard levels using the FEDI

Table 7. Safety indices evaluated for different pressures of the methanol synthesis reactor

Pressure, bar	PRI	F&EI	FEDI
83	9.47	136.8	306.6
70	8.00	135.8	306.5
60	6.84	135.4	306.4
50	5.81	135.3	306.3

The F&EI and the FEDI do not present a significant change. While changes in the PRI values are more notorious, the lack of a ranking for the PRI hinders the possibility to classify these changes in terms of hazard levels. One possible reason for the minor change in the F&EI and FEDI indices is the way in which they are structured, i.e. while there is a decrease of pressure, an increase in the quantity of chemical handled by the unit may compensate the overall effect on the value of the index.

4.3 Uncertainty analysis

The uncertainty analysis was made considering the probability distributions shown in Table 8. These distributions take into account the pressure ratio of the compressors in the methanol synthesis loop, where most of the hazardous equipment or streams are located.

By applying the approach depicted in Figure 1, we obtained the cumulative probability distributions shown in figures 5 to 7. The doted lines in those figures represent the expected (nominal) values.

Table 8. Uncertain inputs and probability distributions^{+}

Variable	Minimum	Most likely	Maximum
Compressor-1 pressure ratio (83 bar)	3.94	4.15	4.37
Compressor-2 pressure ratio (83 bar)	1.05	1.11	1.17

$^{+}$Note: Distribution types were triangular.

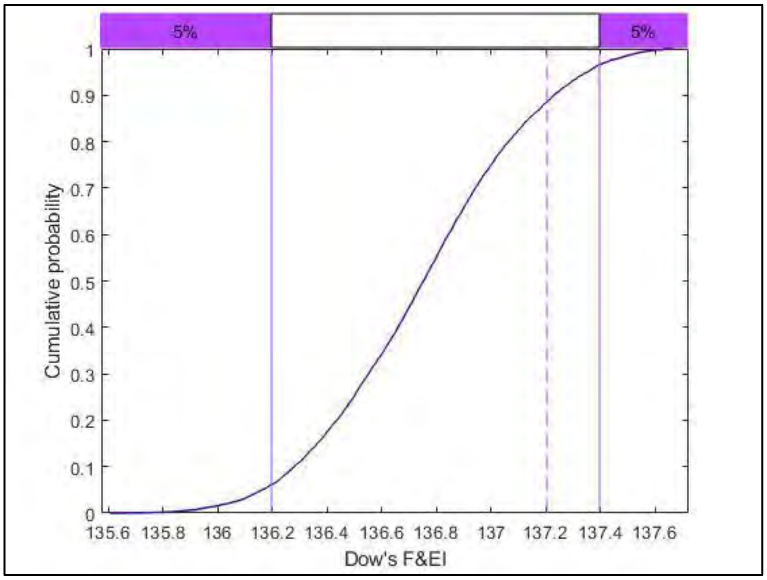


Figure 5. Probability distribution for the Dow's F&EI

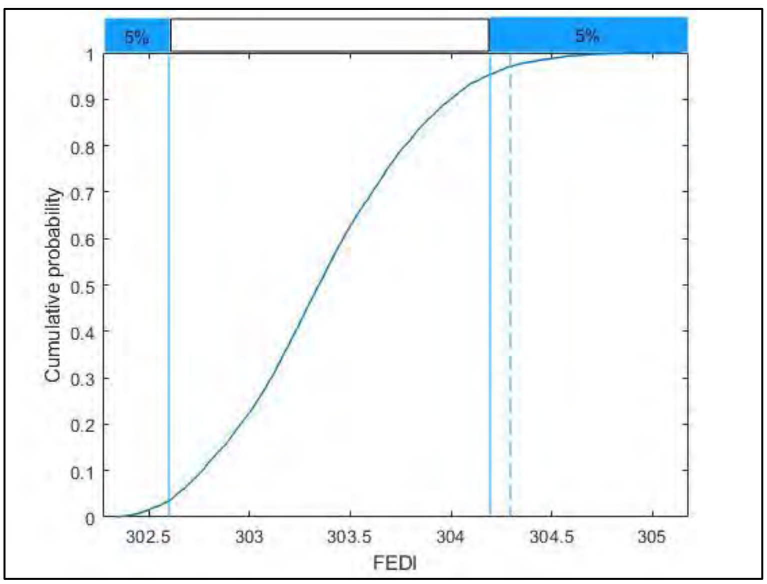


Figure 6. Probability distribution for the FEDI

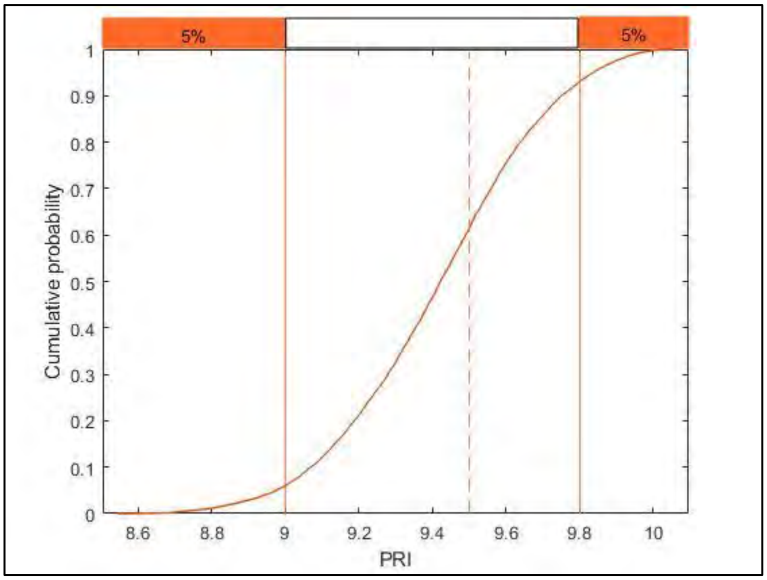


Figure 7. Probability distribution for the PRI

The results show that the expected values for the F&EI and the FEDI have a high probability of occurrence, 87% and 97.3% respectively, while the PRI expected value has only 57%. This observation indicates that the F&EI and the FEDI indices can produce good results with nominal values. It should be pointed out that it is always desirable that the calculated occurrence of an index value is as high as possible, because a low probability could represent an underrating of the indices when using nominal values. The results were complemented by the probabilistic characterization of the three indicators reported in Table 4. Standard deviation values for the three indices as fairly low, in accordance with the minimum and maximum values that were obtained for the calculation of the indices.

Table 4. Probabilistic characterization of results for the MTO process with methanol synthesis

Metric	Mean	Minimum	Maximum	Standard deviation	P5	P95
PRI	9.41	8.54	10.06	0.26	8.98	9.84
F&EI	136.75	135.61	137.67	0.36	136.16	137.35
FEDI	303.37	302.34	305.14	0.47	302.64	304.18

5. Conclusions

Four safety indices were analyzed, out of which three (PRI, F&EI and FEDI) are related to the performance of the overall process and one of them (PSI) to the risk characterization of streams within the process. assessment of safety The indices are conveniently applied during the conceptual design of a process. Regarding the indices related to the overall process performance, their comparison identified some disadvantages of those metrics when evaluating flowsheets that contain processing tasks carried out mostly in the gas phase. The comparison was completed with an uncertainty analysis that provides insightful information about the metrics. It was observed that the PSI and F&EI indices classified the streams and the units within the same process area as the most hazardous. The FEDI also identified the equipment pieces in the same area as hazardous, but with a lower risk level. This result may be influenced by the term of volume that is used in the calculation of the FEDI index. With regard to the usefulness of the indices to track changes in the process design, only the PRI was able to reflect a significant numerical change, but its lack of relationship with respect to a hazard level characterization of the process limits the usefulness of this finding. The results obtained for the indices call for the need to develop a new or modified index through a careful inclusion of the major characteristics of the three indices analyzed in this work, so that items that appear to be relevant for the evaluation of risk are taken into account. On the other hand, elimination of terms that bias the results towards a particular class of streams or equipment units that are not necessarily characterized as risky items within the process should be considered.

Acknowledgements

Financial support for the development of this project from the Mexican Council for Science and Technology, CONACYT, through the research grant CB-2015-01-255164 is gratefully acknowledged.

References

Abidin, M.A.; Rusli, R.; Buang, A.; Shariff, A.M.; Khan, F.I. Resolving inherent safety conflict using quantitative and qualitative technique. *J. Loss Prev. Process Ind.* **2016**, *44*¸ 95. DOI: 10.1016/j.jlp.2016.08.018

AIChE. *Dow's Fire and Explosion Index Hazard Classification Guide, 7th Ed.*; AIChE: New York, 1994.

Castillo-Landero, A.; Ortiz-Espinoza, A.P.; Jiménez-Gutiérrez, A. A process intensification methodology including economic, sustainability and safety considerations. *Ind. Eng. Chem. Res.* **2018**, *58*, 6080. DOI: 10.1021/acs.iecr.8b04146

Khan, F.I.; Abbasi, S.A. Multivariate hazard identification and ranking system. *Process Saf. Prog.* **1998**, *17*, 157. DOI: 10.1002/prs.680170303

Khan, F.I.; Husain, T.; Abbasi, S.A. Safety weighted hazard index (SWeHI) a new, user-friendly tool for swift yet comprehensive hazard identification and safety evaluation in chemical process industries. *Trans IChemE*. **2001**, *79*, 157.

Khan, F.I.; Sadiq, R.; Amyotte, P.R. Evaluation of available indices for inherently safer design options. *Process Saf. Prog.* **2003**, *22*, 83. DOI: 10.1002/prs.680220203

Kidam, K.; Sahak, H.A.; Hassim, M.H.; Shahlan, S.S.; Hurme, M. Inherently safer design review and their time during chemical process development and design. *J. Loss Prev. Process Ind.* **2016**, *42*, 47. DOI: 10.1016/j.jlp.2015.09.016

Koc, R.; Kazantzis, N.K.; Nuttall, W.J.; Ma, Y.H. Economic assessment of inherently safe membrane reactor technology options integrated into IGCC power plants. *Process Saf. Environ. Prot.* **2012**, *90*, 436.

Lee, Y.; Kim, J.; Ahmed, U.; Kim, C.; Lee, Y.-W. Multi-objective optimization of Organic Rankine Cycle (ORC) design considering exergy efficiency and inherent safety for LNG cold energy utilization. *J. Loss Prev. Process Ind.* **2019**, *58*, 90. DOI: 10.1016/j.jlp.2019.01.006

Leong, C.T.; Shariff, A.M. Process route index (PRI) to assess level of explosiveness for inherent safety quantification. *J. Loss Prev. Process Ind.* **2009**, *22*, 216. DOI: 10.1016/j.jlp.2008.12.008

Medina-Herrera, N.; Grossmann, I.E.; Mannan, M.S.; Jiménez-Gutiérrez, A. An approach for solvent selection in extractive distillation systems including safety considerations. *Ind. Eng. Chem. Res.* **2014a**, *53*, 12023. DOI: 10.1021/ie501205j

Medina-Herrera, N.; Jiménez-Gutiérrez, A.; Mannan, M.S. Development of inherently safer distillation systems. *J. Loss Prev. Process Ind.* **2014b**, *29*, 225. DOI: 10.1016/j.jlp.2014.03.004

Ortiz-Espinoza, A.P.; Noureldin, M.M.B.; El-Halwagi, M.M.; Jiménez-Gutiérrez, A. Design, Simulation and Techno-Economic Analysis of Two Process for the Conversion of Shale Gas to Ethylene. *Comp. Chem. Eng.* **2017a**, 107, 237-246.

Ortiz-Espinoza, A.P.; Jiménez-Gutiérrez, A; El-Halwagi, M.M. Including Inherent Safety in the Design of Chemical Processes. *Ind. Eng. Chem. Res*. **2017b**, 56, 49, 14507-14517.

Ortiz-Espinoza, A.P.; Kazantzi, V.; Eljack, F.T.; Jim nez-Guti rrez, A.; El-Halwagi, M. M.; Kazantzis, N. K. Framework for Design Under Uncertainty Including Inherent Safety, Environmental Assessment, and Economic Performance of Chemical Processes. *Ind. Eng. Chem. Res.* **2019**, *58*, 29, 13239.

Rahman, M.; Heikkilä, A.M.; Hurme, M. Comparison of inherent safety indices in process concept evaluation. *J. Loss Prev. Process Ind.* **2005**, *18*, 327. DOI: 10.1016/j.jlp.2005.06.015

Roy, N.; Eljack, F.; Jiménez-Gutiérrez, A.; Zhang, B.; Thiruvenkataswamy, P.; El-Halwagi, M.; Mannan, M. S. A review of safety indices for process design. *Curr. Opin. Chem. Eng.* **2016**, *14*, 42. DOI: 10.1016/j.coche.2016.07.001

Ruiz-Femenia, R.; Fernández-Torres, M.J.; Salcedo-Díaz, R.; Gómez-Rico, M. F.; Caballero, J. A. Systematic tools for the conceptual design of inherently safer chemical processes. *Ind. Eng. Chem. Res.* **2017**, *56*, 7301. DOI: 10.1021/acs.iecr.7b00901

Shariff, A.M.; Leong, C.T.; Zaini, D. Using process stream index (PSI) to assess inherent safety level during preliminary design stage. *Safety Sci.* **2012**, *50*, 1098. DOI: 10.1016/j.ssci.2011.11.015

Suardin, J.; Mannan, M.S.; El-Halwagi, M.M. The integration of Dow's fire and explosion index (F&EI) into process design and optimization to achieve inherently safer design. *J. Loss Prev. Process Ind.* **2007**, *20*, 79. DOI: 10.1016/j.jlp.2006.10.006

Thiruvenkataswamy, P.; Eljack, F.T.; Roy, N.; Mannan, M.S.; El-Halwagi, M.M. Safety and techno-economic analysis of ethylene technologies. *J. Loss Prev. Process Ind.* **2016**, *39*, 74. DOI: 10.1016/j.jlp.2015.11.019

Vázquez, D.; Ruiz-Femenia, R.; Jiménez, L.; Caballero, J.A. Multiobjective early design of complex distillation sequences considering economic and inherent safety criteria. *Ind. Eng. Chem. Res.* **2018**, *57*, 6992. DOI: 10.1021/acs.iecr.8b00577

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Consideration of Non-Structural Internal Debris in Siting of Blast Resistant Modules

Jodi L. Kostecki, Thomas J. Mander*, and James Kelly Thomas
Baker Engineering and Risk Consultants
3330 Oakwell Court, Suite 100
San Antonio, TX 78218-3024
*Presenter E-mail: TMander@BakerRisk.com

Abstract

Blast resistant modules (BRMs) have become prevalent at petroleum refining and chemical processing facilities over the last decade. A primary rationale for utilizing a BRM is to allow a building housing essential personnel (e.g., operators) to be sited near the process units for which they are responsible. BRMs are selected based on a pressure-rating and response level (typically Low, Medium, or High). A common misconception is that a BRM will be undamaged and reusable for a specified blast overpressure rating, and such buildings are often incorrectly referred to as "blast-proof". In order to absorb blast energy, the walls and roof of a BRM are designed to undergo transient accelerations and displacements. The allowable displacements are dictated by the selected response level, and that stated response level does not directly communicate the hazard associated with wall deflection and non-structural debris.

Displacement and acceleration of a BRM wall can lead to significant non-structural internal debris hazards, as has been observed in testing programs and incident investigations. These hazards become more severe as the BRM blast rating and response level increases. Such hazards are sometimes overlooked when siting a BRM. A structural analysis of a BRM may be required to predict wall accelerations in order to quantify these hazards and properly site the BRM, rather than relying solely on a blast overpressure rating. This paper provides insight into the hazards associated with interior finish-out and wall-mounted items commonly observed in BRMs, and the means necessary to mitigate these hazards.

Keywords: Debris hazards, BRM, blast damage, facility siting study

1 Introduction

Occupied buildings in refining and processing facilities are required to be assessed for potential explosion, fire, and toxic hazards as documented in the Occupational Safety and Health Administration (OSHA) standard 29 CFR Part 1910. These assessments are performed as part of a facility siting study (FSS). FSSs often show that buildings not deliberately designed to withstand blast loads, and buildings located close to process units, have insufficient blast resistance to withstand the postulated worst-case blast loads. As a result, owners must then decide whether to strengthen the existing building in place or construct a new building that is designed for the required level of blast-resistance.

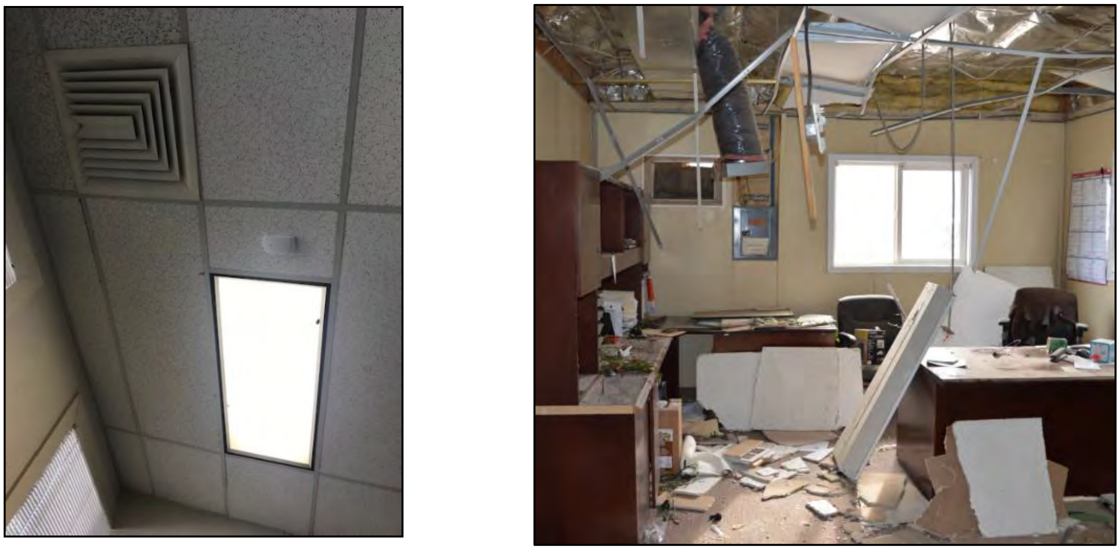
Safety requirements and inherent hazards at refining and processing facilities make on site construction more expensive than traditional commercial construction. Building upgrades can be intrusive to occupants and business interruption is therefore another owner consideration when deciding between building upgrades or complete building replacement. Modular buildings are viewed as an attractive option to owners to reduce the on-site construction time and disruptions to daily operations. These buildings are branded in the industry as blast resistant modules (BRMs).

BRMs are constructed similar to shipping containers, albeit with thicker corrugated wall panels and a heavier steel frame (beams and columns). While the construction is stronger than a shipping container, the structural members are still expected to sustain damage in a design-basis blast to absorb blast energy. This point is sometimes misunderstood, with owners and operators believing they are risk-free in a BRM, expecting little to no damage after a design-basis blast event. Depending on the allowable structural response, some BRMs may not be immediately habitable following a design-basis blast event.

While a properly-designed BRM will protect building occupants from structural failures during a blast, there are other secondary hazards that are often overlooked. Non-structural items that are necessary for the daily operating function of a BRM such as cabinets, shelves, desks, electrical equipment, ducting, lighting, etc. can become sources of hazardous debris to building occupants, even at blast loads below the BRM blast rating. This paper discusses current industry practice for addressing non-structural debris, the mechanisms that cause hazardous internal debris, and mitigation effectiveness in BRMs.

2 Examples of Non-structural Debris

Typical interior non-structural overhead debris consists of drop ceiling components, lights, mechanical ductwork and vents, as illustrated in Figure 1a. Drop ceiling lay-in panels generally create the largest volume of interior overhead debris, as observed in Figure 1b, because they “lay” between steel framing and are not physically anchored to supports. They are therefore prone to becoming dislodged with minor ceiling movement. Drop ceiling tiles weigh between 1 to 2 psf, equating to a weight of between 8 to 16 lbs for a standard 2 ft × 4 ft lay-in panel.



(a) Typical overhead items *(b) Post-blast event overhead debris*

Figure 1. Overhead Non-Structural Debris

Figure 1b also shows non-structural debris from overhead lights (troffers) and vents. These items can cause higher vulnerability to occupants upon impact than ceiling tiles due to their increased weight (10 to 20 lb troffers and 5 to 10 lb vents). Troffers and vents can either be built into a drop ceiling or stand-alone, typically connected to the structural roof members with vertical gauge wire. Failures of these elements include tension failure in the wire itself or unraveling of a poor tie connection of the wire. Mechanical ductwork tends to have the heavier connections consisting of steel straps or hangers, and failures in this components are less common, but have been observed in accidents.

Figure 2 shows common wall-mounted or near-wall architectural and electrical items such as cabinets, bookcases, TV/computer monitors, and electrical boxes that are potential sources of interior debris in a blast event. As shown in Figure 2a, occupants in single BRMs are inevitably located near exterior walls, which increases the vulnerability from non-structural debris compared to personnel located at the interior of a larger building. Electrical boxes (Figure 2b) are most typically anchored to the interior surface of exterior walls, and it is common for operator control panels (Figure 2c) to also be located at exterior walls to optimize the use of interior space.

(a) *Single module layout* (b) *Wall-mounted electrical boxes* (c) *Control monitors*

Figure 2. Example Wall-Mounted or Near-Wall Potential Debris Sources

Cabinets, bookcases and other items with an elevated center of gravity are generally placed directly adjacent to an exterior wall surface. These types of items are typically observed to topple over when placed near a blast-loaded exterior wall, as illustrated in Figure 3. Electrical boxes, picture frames, and wall mounted TVs and cabinets have been observed to fail and be thrown inward due to poor overall anchorage capacity to the structure, or failure of the element itself. In the first instance, the anchorage typically pulls out of the supporting wall component and creates a debris hazard. If the anchorage is sufficiently strong preventing this from occurring, failure can still occur in the non-structural component itself. This is observed in Figure 3, where the face of an electrical box has been dislodged but the box is still attached to the wall surface.

Figure 3. Wall mounted Non-Structural Building Debris

3 Industry State-of-the-Practice

Typical BRM exterior dimensions are between 10 and 14 ft wide, up to 50 ft long, and between 8 and 12 ft tall. Single module units became popular replacements to wood trailers after the catastrophic 2005 Texas City refinery explosion and have become more prevalent as permanent structures in the past decade. Where larger footprints are desired, individual BRMs are field connected to one another. These multi-module BRMs are often classified as permanent structures but can also be temporary structures used for turnaround. BRMs can therefore be classified as either temporary or permanent structures. Figure 4 provides exemplar photographs of single and multi-module BRMs located near process units.

Figure 4. Single-module BRM (Left) and Multi-module BRM (Right)

While OSHA standard 29 CFR Part 1910 states that a FSS must be performed to assess potential hazards to occupants, it does not state the specific procedures for the assessment, or impose mandatory building design requirements. The principal documents for performing a FSS on permanent and temporary (portable) buildings are, respectively, API RP 752 *Management of Hazards Associated with Location of Process Plant Buildings* [1,2,3] and API RP 753 *Management of Hazards Associated with Location of Process Plant Portable Buildings* [4]. These recommended practice (RP) documents are non-mandatory guidelines but are considered as the industry standard for FSS. While intended for different building types, the RPs universally state that a detailed structural analysis is required for new buildings designed to resist blast loads and that non-structural debris should be evaluated. The state-of-practice for structural and non-structural design and evaluation is discussed in the following subsections.

3.1 Structural Design Philosophy

It is important for the reader to understand the basic methodologies used for blast analysis of building structures. The structural elements such as columns, beams and wall panels that make up a BRM are typically analysed as individual components. Each component is analysed as an equivalent single-degree-of-freedom (SDOF) system, using the mid-span displacement as the point of interest. As shown in Figure 5, a SDOF component is loaded with a transient blast load, and the mid-span displacement is tracked. The magnitude of peak deflection is of primary interest, and this value is used to approximate the level of damage each component will undergo. Unless designed to remain elastic, which is rarely the case for any structural component, there will be a permanent deflection which may limit the reusability of a structure. Figure 6 further illustrates this with post-test photographs of an exemplar BRM panel that was blast tested using a shock tube.

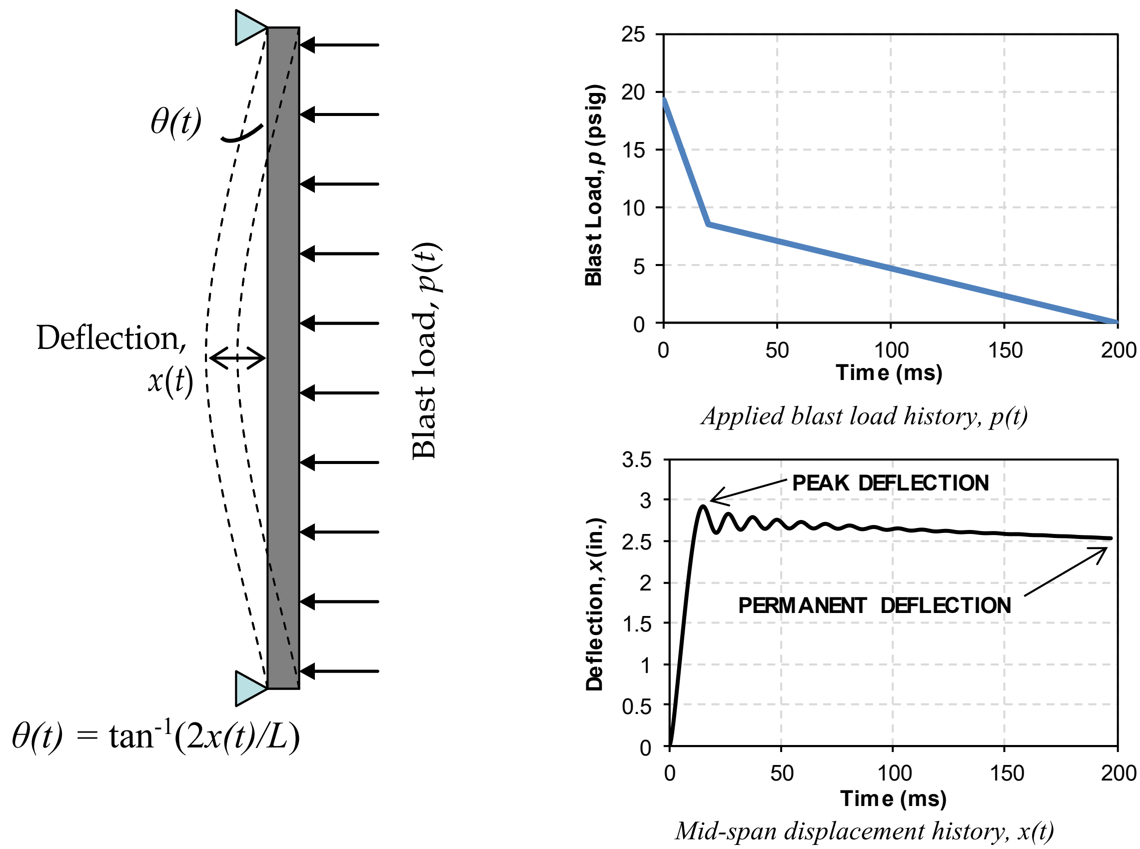


Figure 5. Example SDOF Blast Analysis Methodology

API 752 and API 753 both recommend the use of the ASCE Petrochemical Guideline for the design and assessment of blast-loaded buildings. API 752 [3] also cites the PIP STC01018 manual and the USACE PDC Technical Report 06-08 [9], but neither of these documents specifically address the design of BRMs. The ASCE guideline provides deflection limits for the design of wall and roof components, such as the corrugated plate walls, columns and beams. These are known as response limits, which are intended to correlate the maximum predicted displacement to qualitative levels of *structural* damage, without consideration of non-structural debris.

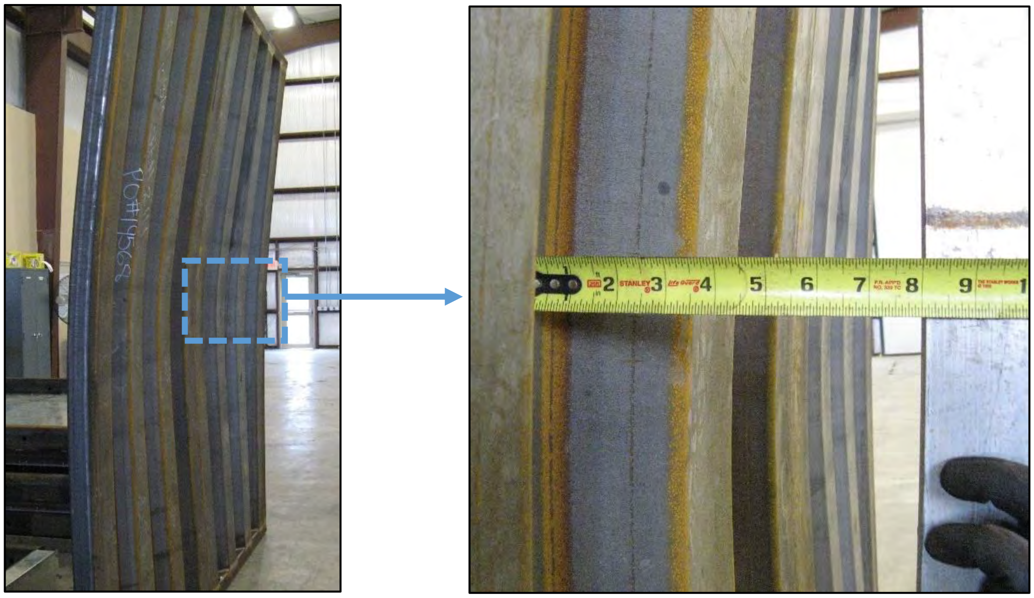


Figure 6. Example Permanent Deflection of a Tested BRM Wall Panel

There are three damage thresholds specified in the ASCE Petrochemical Guideline [5,6]; Low, Medium, and High. The qualitative damage descriptions for each of these states are listed in Table 1. Note that the damage descriptions are only indicative of structural damage and do not consider non-structural debris. Qualitative descriptions are correlated to quantitative response limits, which dictate allowable structural component deflections caused by blast loading. Quantitative limits have historically been developed using scaled- and full-scale high-explosive (HE) and shock tube test data and accident investigation observations.

Limited test and accident data are available for the crimped wall panels used on BRMs, and consequently there is not a prescribed response criterion for this type of structural component. The ASCE Petrochemical Guideline recommends that this type of crimped wall panel is designed for a response between a light-gauge corrugated panels (typical on metal warehouse-type buildings) and flat steel plate. Table 2 lists the quantitative limits for these component types. The table also includes the ductility factor, μ, which is the ratio of maximum displacement to yield displacement. Hence a value exceeding unity implies the component has yielded and there will be permanent deflection. The qualitative and quantitative limits in the PIP STC01018 [7,8] manual are replicates of the ASCE Petrochemical Guideline.

Based on the ASCE Guideline [6], it is customary practice for an average of the two limits to be used for the design of crimped plates for BRMs. Light-gauge panels have a propensity to buckle, which is why their limits are much less than that of flat steel plates. If buckling is explicitly accounted for in the analysis, the response limits of flat steel plates can be adopted, allowing larger displacements in the wall and/or roof panels. Note that the original ASCE Guideline [5] had no considerations for the design of BRMs, and guidance was first provided in the 2010 2nd Edition.

As previously mentioned, the overall dimensions of a BRM can vary significantly. The roof eave height is typically the most consistent across modules, ranging between 8 ft and 12 ft. Table 3 is provided as an example of the magnitude of allowable structural component deflections in a typical

BRM design. Most BRM structural components are designed to sustain Medium damage, which corresponds to an allowable peak mid-span deflection of 5 inches for a 12 ft span. Because typical BRM crimped wall panels are stiff, the permanent displacement would be expected to at least 80% of the peak deflection.

Table 1. Qualitative Damage States for Component Blast Design [6]

Damage Level	Component Response
Low	Component has none to slight visible permanent damage.
Medium	Component has some permanent deflection. It is generally repairable, if necessary, although replacement may be more economical and aesthetic.
High	Component has not failed, but it has significant permanent deflections causing it to be unrepairable.

Table 2. Quantitative Criteria for Steel Panels and Plates [6]

Element Type	Low		Medium		High	
	μ_a	θ_a	μ_a	θ_a	μ_a	θ_a
Secured cold-formed panels	1.75	1.25°	3	2°	6	4°
Flat steel plates	5	3°	10	6°	20	12°
Average (used for BRM crimped panels)	**3.4**	**2.1°**	**6.5**	**4°**	**13**	**8°**

Table 3. Allowable Panel Deflections for Different Wall/Roof Panel Spans

Damage Level	θ_a	Maximum Mid-span Deflection			
		Span = 8 ft	Span = 10 ft	Span = 12 ft	Span = 14 ft
Low	2°	1.7″	2.1″	2.5″	2.9″
Medium	4°	3.4″	4.2″	5.0″	5.9″
High	8°	6.7″	8.4″	10.1″	11.8″

3.2 Non-structural Design Guidance

The recommendations and methodologies in the blast guidelines and recommended practices are discussed herein. Non-structural design guidance is most commonly qualitative, and limited quantitative measures are provided. Table 4 provides a summary of these for the most common U.S. guidelines used for blast assessment of buildings in refineries and processing facilities.

Table 4. Non-Structural Debris Design Recommendations from Different Blast Documents

Title	Guidance	Recommendation
API RP 752 (3rd Ed.)	Qualitative	Assessment must address non-structural components (roofs, walls, ceilings and mechanical services) that may present debris hazards to occupants.
API RP753 (1st Ed.)	Qualitative	Design should limit dislodgement of internal features. Secure internal furniture, office equipment and fixtures
ASCE Petrochem (2nd Ed.)	Qualitative	Permanent fixtures and equipment should be designed to withstand local building motions. Seismic anchorage techniques are valid for blast. Functional or decorative objects should not be mounted on the interior surface of an exterior wall.
	Quantitative	Place file cabinets and other furnishings off the interior surface of an exterior wall greater than the maximum predicted displacement of the wall.
PIP STC01018 (2nd Ed.)	Quantitative	**Suspended items:** Anchorage for a statically applied force equal to the mass of the item times the maximum acceleration of the roof, or five times the weight of the item, whichever is less. Items weighing more than 10 pounds should be independently anchored. **Equipment and Internally Mounted Items:** Instrumentation or electrical equipment shall not be mounted on the interior face of walls subjected to blast loads without owner's approval. All fixed floor-supported items (e.g. lockers, electrical cabinets, racks) shall have a minimum clearance from exterior walls equal to the maximum calculated lateral blast load deflection. The maximum deflection shall be the sum of both the overall building sidesway and the deflection of and wall component(s), calculated based on the maximum blast loads. Supports and anchorage for equipment shall be designed to resist a lateral force equal to 20% of the equipment weight.

The API 752 and API 753 RPs recognize the need to assess non-structural debris hazards in different qualitative ways, depending on the edition. Appendix D in the 1st and 2nd editions of API 752 include an example building checklist for assessing risk-reduction measures in occupied buildings. The questions include looking at whether large office equipment, stacks of materials, lighting fixtures, ceilings, or wall-mounted equipment are "well-supported" or "adequately secured". Quantitative recommendations for determining what type of connection is adequate are not provided in the document. This checklist was removed from the 3rd Edition of API 752 and readers were instead made aware of non-structural debris as a cause of occupant vulnerability with the following statement:

> "*The primary hazards to personnel located indoors are building collapse and debris. Debris may include building materials thrown from exterior walls or dropped from ceilings/roof. Building contents located on, against, or near external walls may also become debris.*"

API 752 (3rd Edition) states that the evaluation of existing buildings (Section 6.6) and new buildings (Section 6.8) address non-structural components that may present debris hazards from roofs, walls, ceilings and mechanical services. However, like the 1st and 2nd editions of API 752, there is no recommendation on how to perform this assessment, or correctly design the anchorage. API 753 also acknowledges non-structural debris in portable buildings can cause injuries to occupants and requires blast assessments address internal non-structural features. Further recommended risk reduction practices include securing internal furniture, office equipment, and fixtures, but without specific examples or guidance on how to do so.

Non-structural debris is discussed in the ASCE Petrochemical and PIP STC01018 guidelines that are referenced by API 752. ASCE Petrochemical states that "*permanent fixtures and equipment should be designed to withstand the calculated local building motions as a results of blast loads.*" This guideline stops short of providing quantitative guidelines for designing restraints and direct the user to seismic guidelines that provide anchorage methods for non-structural items in earthquake prone buildings. As stated in ASCE, "*all non-structural upgrades recommended for buildings subject to earthquake loads are also applicable for blast resistant design.*"

The ASCE manual covers architectural items in more detail, albeit somewhat contradictory to the aforementioned statements. Architectural items fall under the discipline of the architect, who is not often knowledgeable of expected building damage. Quantitative guidance is given that file cabinets and furnishings should be placed off the interior surface of the wall at least the distance of the maximum predicted wall displacement. ASCE also states that functional or decorative architectural objects should not be placed on the interior surface of an exterior wall.

PIP STC01018 provides the most quantitative guidance minimum structural and non-structural design criteria requirements for permanent blast resistant buildings. Any item weighing more than 10 pounds (5 kg) and suspended from the roof, should be anchored to structural framing members. The anchorage should be designed to resist a static force that is the lesser of 5 times the weight of the object, or the mass of the object multiplied by the peak predicted acceleration. Hence if a roof member has a blast acceleration that exceeds 5***g*** (***g*** = acceleration of gravity), then the anchorage would only be designed for 5 times the weight of the object. Other clauses are similar to ASCE, where interior items should not be wall mounted, and fixed-floor items should be spaced a distance equal to the total wall deflection.

4 Reasons for Non-structural Debris

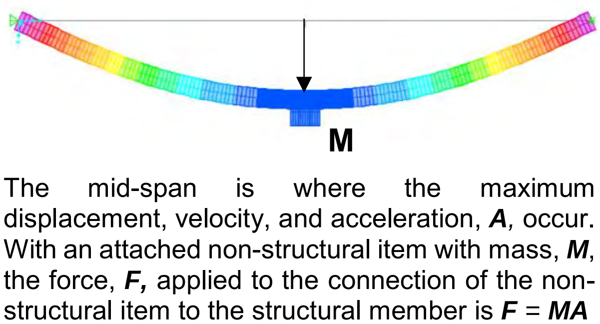
Non-structural debris generated during an explosion are primarily caused by wall or roof displacement. BRMs differ from permanent buildings, as they are not always integral with a foundation, and they can slide during a blast event. Both of these phenomena cause large decelerations to occur to objects within a BRM. This is analogous to rapid deceleration in an automobile, where occupants are thrust forward in their seat as a car is traveling forward and brakes suddenly. Accelerations can be significant from both local (wall or roof) and global (sliding) movement during a blast event in BRMs, and both of these are discussed in more detail herein.

4.1 Wall or Roof Deflection

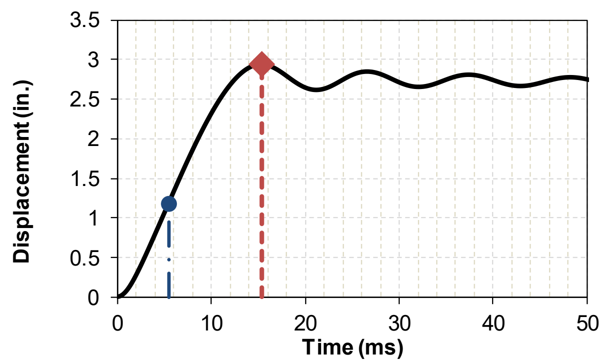
As previously discussed, wall and roof members of BRMs are allowed to undergo large displacements. Guidance for placing items off the walls is not always followed, particularly in single module BRMs to maximize the useable floor area. As previously shown in Table 3, an interior partition wall would need to be spaced between 4 to 6 inches off the interior surface of the exterior wall to not be directly impacted by the wall. This is not possible with interior ceiling items, which by necessity must be connected to a structural member to be suspended. Hence this section focuses on items rigidly attached to a wall or roof surface to demonstrate connection the magnitude of connection forces.

As plotted in Figure 7a, peak displacements, and therefore velocities and accelerations, will occur at the mid-span of a member responding in flexure. When a member reaches peak displacement, indicated with the dotted-line and diamond marker in Figure 7b, the velocity of the wall is nil (Figure 7c), and the wall deceleration is maximum (Figure 7d).

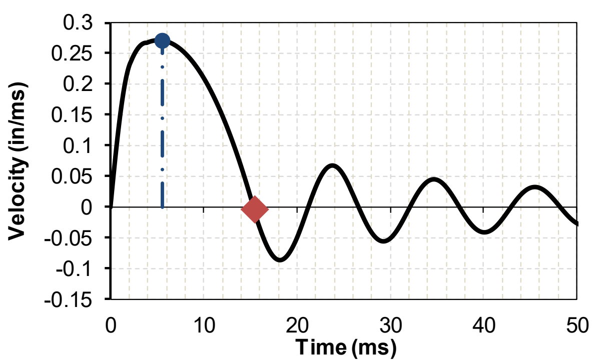
In the case of non-structural wall or roof debris rigidly attached to the structural wall, the peak deceleration coincides with the maximum force that will be experienced in the connection of the non-structural item to the structural member. The connection force, F, is equal to the product of the maximum deceleration, A, of the structural member and the mass, M, of the non-structural item. Hence for the example in Figure 7, the peak deceleration of the structural member is around 140g which means any non-structural item would need to be anchored for 140 times its own mass.



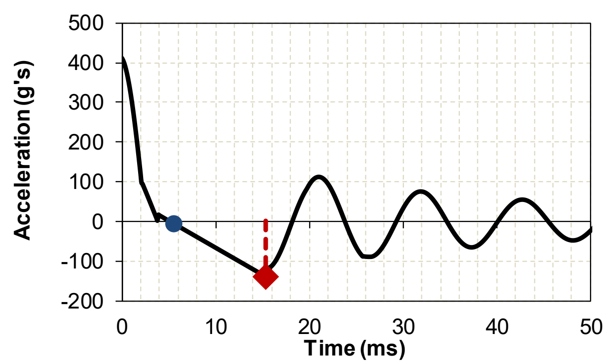
(a) Deflected shape at arbitrary time



(b) Mid-span displacement



(c) Mid-span velocity



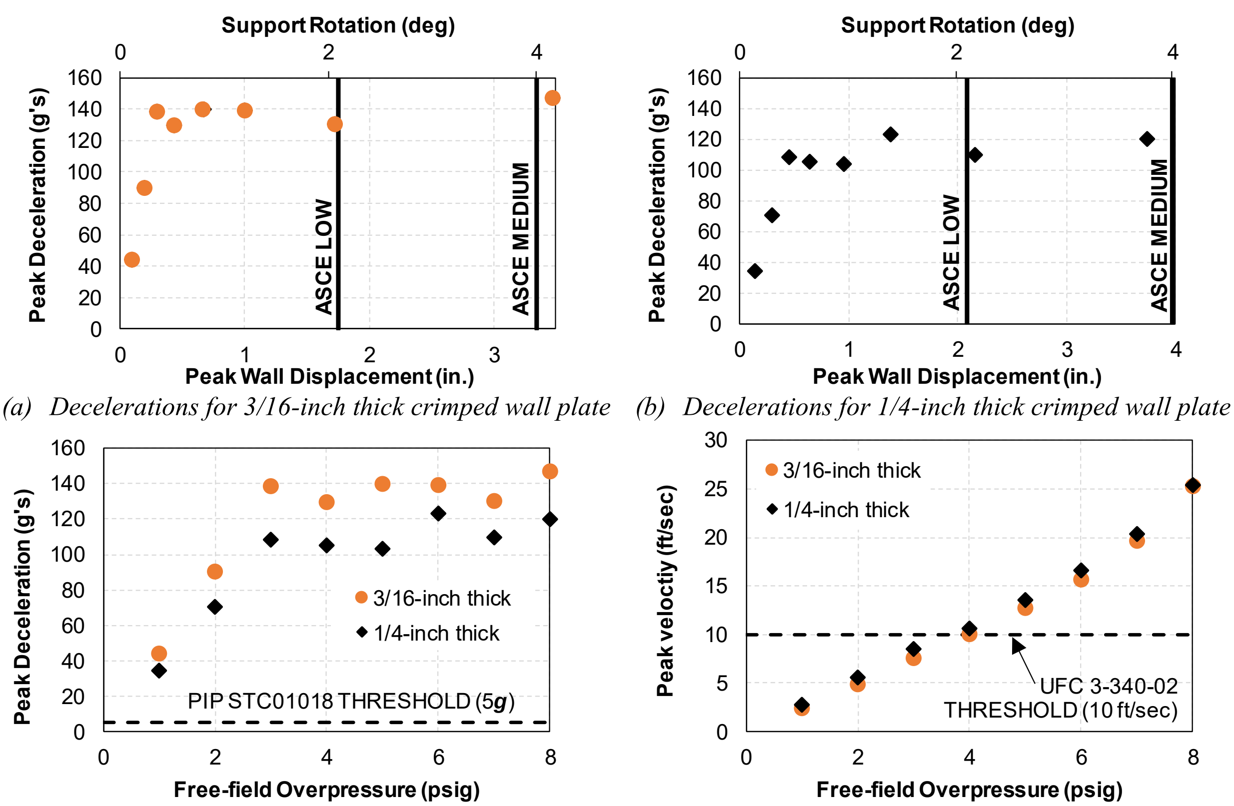
(d) Mid-span acceleration

Figure 7. Example SDOF Analysis to Predict Connection Forces and Debris Velocities

It is evident that for this arbitrary wall panel, the guidance by PIP STC01018 (5 times the member weight) would significantly under-predict the required anchorage force. Figure 7 plots a dash-dotted line with a circular marker to represent this case. It can be observed that the non-structural item would detach prior to the structural wall or roof element reaching peak displacement. A non-structural item would therefore detach and be launched with an initial velocity (Figure 7c) near the peak wall velocity. This phenomenon is what causes wall or roof mounted debris to be launched into occupied areas of BRMs.

Individual 3-inch deep crimped walls, one with 3/16-inch thick plate spanning 8 ft, and the other with ¼-inch thick plate spanning 9.5 ft are selected for demonstration purposes. The profiles selected are representative of BRM construction and satisfy an ASCE Medium response for an 8 psig free-field overpressure. SDOF analyses were completed from which the peak decelerations and velocities were computed to examine the predicted differences in rigid non-structural element connections.

Figure 8a and Figure 8b plots the peak decelerations for the 3/16-inch thick and ¼-inch thick plate, respectively. These graphs demonstrate that the wall accelerations are independent of the wall deflection, provided the wall deflection exceeds the yield point, which is usually on the order of ½-inch. Hence a BRM will still experience the same deceleration at a wall displacement that is less than the allowable displacement. Comparison of these two graphs also demonstrates the concept that heavier wall panels will have lower decelerations than lighter panels. Figure 8c further demonstrates these concepts with respect to free-field overpressure.



(a) Decelerations for 3/16-inch thick crimped wall plate *(b) Decelerations for 1/4-inch thick crimped wall plate*

(c) Deceleration for different wall panels *(d) Peak velocities for different wall panels*

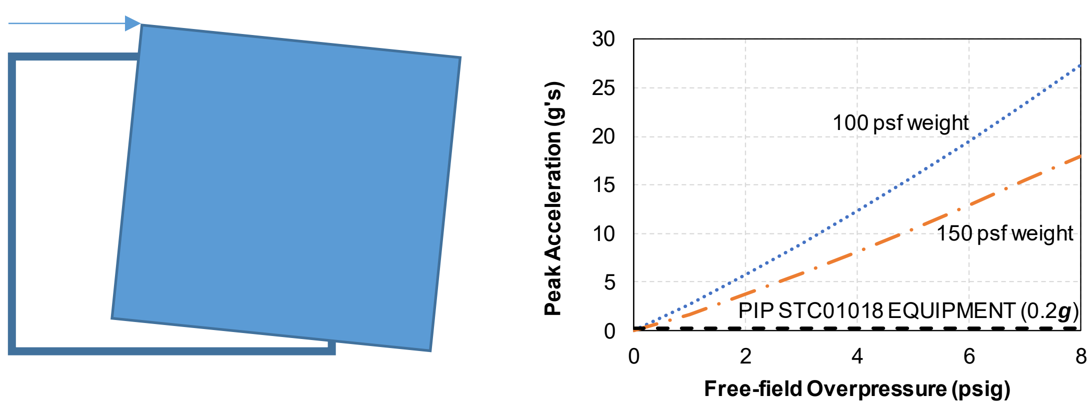
Figure 8. Peak Wall Decelerations and Velocities for Representative BRM Wall Panels

Figure 8d plots the peak velocity of the different wall panels with respect to free-field overpressure. Also included in this plot is the 10 ft/sec threshold specified by UFC 3-340-02 [10] as a critical velocity for serious injury to personnel due to fragment impact. Serious injury is expected if a fragment is traveling faster than 10 ft/sec and exceeds 2.5 lbs (impacting the thorax), 6 lbs (impacting the abdomen), or 8 lbs (hitting the head). For the representative BRM wall panels analyzed, this threshold would be exceeded at approximately 4 psig, or half the design-basis blast load of 8 psig.

4.2 Sliding Acceleration

BRMs that are not anchored to a foundation, or only anchored for conventional wind loads, are susceptible to sliding during a blast event, as illustrated in Figure 9a. This causes global accelerations to be imparted to non-structural items, even if they are anchored off a wall surface. The magnitude of the horizontal accelerations incurred depends on the BRM weight, dimensions, blast load and coefficient of friction between the BRM and foundation (or soil) beneath it.

An example case is created for a 12 ft tall, 12 ft wide BRM with an assumed coefficient of friction of 0.3, representative of steel on concrete. Representative weights per floor area, 100 psf and 150 psf, were selected. Figure 9b plots peak horizontal accelerations as a function of free-field overpressure. While increased weight reduces the horizontal acceleration, pressures less than a typical 8 psig design pressure exceed the PIP STC01018 recommended design acceleration of 0.2***g*** for equipment. Hence debris can credibly be produced even if interior items are spaced off the interior walls and anchored for a notional force equivalent to 20% the item weight.



(a) Schematic of rigid body sliding *(b) Global acceleration using friction coefficient of 0.3*

Figure 9. Sliding Acceleration in BRMs

5 Conclusions and Recommendations

Non-structural debris is recognized as a credible hazard in blast documents that are used to site and design temporary and permanent buildings at chemical processing and refining facilities. This paper summarized the limited quantitative guidance available intended to mitigate against these hazards. Simplified modeling of crimped wall panels representative of BRMs demonstrated that anchorage forces for wall-mounted non-structural items are significant and may be impractical to develop in some structural substrates. This conclusion also applies to architectural and mechanical equipment attached to the interior roof structure of a BRM.

While some guidance documents instruct designers to place non-structural items off the interior face of exterior walls, this is not possible to do with ceiling items which must be attached to the superstructure to remain suspended. Even if this guidance is followed for walls, global sliding accelerations are applied to all interior non-structural items in unanchored BRMs. This paper demonstrated that these sliding accelerations can be significantly higher than the recommended design forces in blast guidelines, therefore increasing the likelihood of debris generation. BRMs should be designed with these factors as a consideration. Design forces should be based on detailed computational models, where the non-structural elements are accounted for in the model. Alternatively, representative wall or roof assemblies can be blast tested to determine if non-structural connections are sufficiently strong to prevent non-structural items from becoming debris hazards.

6 References

1. American Petroleum Institute (API), *Management of Hazards Associated with Location of Process Plant Buildings, API Recommended Practice 752*, First Edition, Washington, D.C., May 1995, 34 pp.
2. API, *Management of Hazards Associated with Location of Process Plant Buildings, API Recommended Practice 752*, Second Edition, Washington, D.C., November 2003, 34 pp.
3. API, *Management of Hazards Associated with Location of Process Plant Buildings, API Recommended Practice 752*, Third Edition, Washington, D.C., December 2009, 27 pp.
4. API, *Management of Hazards Associated with Location of Process Plant Portable Buildings, API Recommended Practice 753*, First Edition, Washington, D.C., June 2007.
5. American Society of Civil Engineers (ASCE) Task Committee on Blast-Resistant Design, *Design of Blast-Resistant Buildings in Petrochemical Facilities*, First Edition, Reston, VA, 1997.
6. ASCE Task Committee on Blast-Resistant Design, *Design of Blast-Resistant Buildings in Petrochemical Facilities*, Second Edition, Reston, VA, 2010.
7. Process Industry Practices (PIP), Construction Industry Institute, (2006). *PIP STC01018: Blast Resistant Building Design Criteria*, The University of Texas at Austin, Complete Revision, Oct. 2006.
8. Process Industry Practices (PIP), Construction Industry Institute, (2014). *PIP STC01018: Blast Resistant Building Design Criteria*, The University of Texas at Austin, Complete Revision, Oct. 2014.
9. PDC TR-06-08, "Single Degree of Freedom Response Limits for Antiterrorism Design," USACE PDC *Technical Report 06-08*, Jan. 2008.
10. U.S. Department of Defense (DoD). "Structures to Resist the Effects of Accidental Explosions," *Unified Facilities Criteria (UFC) 3-340-02*, Dec. 2008.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

How Effective Are Safety Gaps at Mitigating Explosions: Large Scale Testing of Safety Gaps to Prevent DDTs

Scott Davis*
Gexcon US – 4833 Rugby Ave, Ste 100
Bethesda, MD 20184
*Presenter E-mail: sgdavis@gexcon.com

Abstract

A large vapor cloud explosion (VCE) followed by a fire is one of the most dangerous and high consequence events that can occur at petrochemical facilities. As the size and complexity of facilities increase, designs must consider the potential adverse effects associated with vapor cloud explosions in large congested areas. In fact, if the vapor cloud within the congested area is large enough, the resulting flame or deflagration can continually accelerate within these regions and ultimately reach the point where the deflagration can transition to a more devastating detonation or deflagration-to-detonation transition (DDT). As the consequences of DDTs can be orders of magnitude larger than deflagration, facilities that are at risk need to implement mitigation measures to prevent flames from continuously accelerating in these regions. One method is to provide "safety gaps" or open areas (gaps) within the congested region to interrupt the flame acceleration and provide regions where the flame will actually slow down prior to arriving at the next congested area. The key to this design is to provide a wide enough gap or region between the congested areas so that the flame exiting the first region will decelerate or slow down to adequate levels prior to arriving at the second region.

The problem is that almost all of the safety gap tests have been performed with narrow congested regions where the width is on the order of 3 meters. Unfortunately, most practical congested areas in petrochemical facilities are much wider than 3 meters and recent tests have shown that wider congested areas may be more susceptible to DDTs. Hence, the present paper will present results of large scale testing to access explosion development in both narrow (~3.5 m) and wide (~7 m) congested areas, and the effectiveness of safety gaps in mitigating DDTs. The results will be a valuable contribution to facilities owners and designers in helping to provide inherently safer designs at practical scales.

Keywords: deflagration to detonation transition, explosion modeling, DDTs

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Safety-centered process control design based on dynamic safe set

Joshiba Ariamuthu Venkidasalapathy*, Costas Kravaris, M. Sam Mannan
Artie McFerrin Department of Chemical Engineering,
Texas A&M University
College Station, Texas 77843-3122, USA
*Presenter E-mail: joshvenkat03@tamu.edu, kravaris@tamu.edu

Abstract

Despite significant efforts to make operation of chemical plants safer, the occurrence of incidents clearly indicates the need for better design approaches. Studies to identify the root causes of incidents in hydrocarbon industries reveal that poor design and inadequate control systems contribute to more than 20% of the offshore incidents[1] and 30% of the thermal runaway incidents [2] analyzed. Characterizing and quantifying process safety performance is a complex problem. Traditional control engineers used the concept of phase margin and gain margin to measure the stability of single feedback loops. Although it can be viewed as a measure of safety, the method does not account for multiloop interactions and the presence of constraints in the system. More recently, researchers have used model predictive control (MPC) theory to address safety concerns. The objective of the MPC optimization problem is maximization of cost and other performance metrics, where safety is modelled as a set of additional constraints that must be enforced. The approach is not adequate as there is not a clear method to quantify the safety performance for application in design. Process safety engineering concepts emerge from cause-effect based analysis like HAZOP analysis, fault trees and event trees. These methods do not account for multivariable and non-linear interactions. The objective of this research is to develop an approach for the process control problem with safety as the primary target.

In this paper, the concept of dynamic safe set (DSS) is formulated. The DSS is a set of states of the process that guarantee enforcement of safety critical constraints, in the presence of bounded safety threatening disturbances. Already existing mathematical concepts from the systems literature, namely maximal output admissible sets [3, 4] and the reference governor theory[5, 6] are used for evaluating the DSS. The DSS is calculated around a steady-state operating point. It is safe in the sense that if the initial state belongs to the DSS, then for all modeled disturbances the closed-loop system is guaranteed to not violate the constraints at any time in the future. The safety threatening disturbances that can increase the possibility of safety constraint violation by pushing the system to a risky operation zone are also modeled while calculating the DSS.

A method to quantify the size of the DSS is also proposed by defining the concept dynamic safety margin (DSM). It is defined as the minimum distance of the steady-state operating point from the boundary of DSS. The DSM margin is relevant and important because it is not possible to model

all possible disturbances. That is, a DSS with larger DSM will be able to handle unmodeled random disturbances that push the states away from the steady-state. This will be used as a safety performance metric for control system design. This will lead to designing processes with safety as the primary objective and all other performance metrics are treated as secondary considerations.

The DSS approach is also extended to applications in abnormal event management. Under upset scenarios, there is often a need for sudden and large set-point changes. To safely respond to those changes, control strategies need to be designed to stay away from the safety critical constraints. For this purpose, the concept of reference governor is used. The reference governor is a supervisory nonlinear control scheme that works along with an existing closed-loop system.

The DSS approach is tested on an exothermic process in a CSTR. The approach helped in selecting the operating condition of the process by identifying steady-states that are relatively safer. The closed loop process design was studied under proportional (P) and proportional-integral (PI) control strategies. It showed that the controller parameters played a significant role on the DSM of the process. The trade-off between control and safety performance can be analyzed using the DSM concept. The effect of maximum available control input on the system's safety performance was also investigated. The reference governor was also implemented to the CSTR. The dynamic responses of the process under large disturbances, demonstrate significantly superior control performance when compared to the process without reference governor.

1 Introduction

Ensuring safe operation is critical in chemical industries considering the potential consequences of incidents to life, environment and equipment. Traditional safety engineering concepts emerge from cause-effect based analysis like HAZOP analysis, fault trees and event trees [1-4]. The causation models used as the basis for developing process safety engineering tools have their limitations. These methods fail to account for multivariable and non-linear interactions, oversimplifying the incident process by using only direct cause-effect relations. Studies on incidents in process industries reveal that poor design and inadequate control systems contribute to more than 20% of the offshore incidents [5] and 30% of the thermal runaway incidents [6] analyzed. The objective of this paper is to change the way the process control design problem is approached by bringing process safety upfront.

Process safety can be encompassed within the systems engineering framework by representing it as a set of constraints that have to be met, failing of which may lead to undesirable consequences. These safety critical constraints are the pivotal elements of process safety and they must be chosen to prevent the loss of containment of flammable chemicals. They are conditions that ensure safe operation of the plant without compromising the integrity of the process. Examples of such constraints include limits on liquid level in vessels and bounds on pressure and temperature of columns. Constraints such as limits on available control input should be included as they determine the system's ability to be resilient. In addition to considering constraints that are restricted to individual units, it is important to incorporate constraints that account for the system as a whole, such as the overall energy and mass balance of the plant. A comprehensive set of safety critical constraints, when carefully chosen, can capture the safe region of operation for the process and hence will be used in the design and control problem.

A few researchers have adopted a system-theoretic perspective of addressing process safety as a set of constraints. In the context of safety, Model Predictive Control (MPC) theory is often used as a tool to incorporate the constraints in real-time implementation [7]. MPC computes control actions for the manipulated inputs by solving dynamic optimization problems in real-time and takes advantage of the process model while accounting for constraints. Ensuring closed-loop stability, feasibility and performance under MPC along with safe operation is challenging and has only been explored recently [8-10]. It is important to note that MPC allows for operating the process while riding by the safety critical constraints as it focusses mainly on maximizing the objective function. This may push the process operation closer to unsafe region, increasing the risks. As a result, the need to bring safety as the primary objective of the process control design problem is critical.

The use of MPC for integrating safety constraints and proposed conditions that are required to be satisfied for effective control of safety constraints was proposed in [7]. Lyapunov-based MPC (LMPC) schemes that could drive the closed-loop state to a safe operating region (defined via Lyapunov level sets), where safety is ensured at a prescribed rate in the presence of small process uncertainties was developed in [11]. However, for large disturbances the Safety-LMPC does not guarantee operation in safe region. The safe region represented by Lyapunov level sets can also be restrictive. A safeness index was developed in [12] to represent safe region of operation and used it as a hard constraint while implementing MPC. They demonstrated guaranteed closed-loop stability for sufficiently small disturbances. However, the approach does not guarantee closed-loop stability and feasibility of the optimization problem for large disturbances. In [13], a model-based proactive safety system that incorporates safety constraints in the framework was developed. They used the safety constraints to perform real-time receding-horizon operability analysis to detect operation hazards. Unlike MPC, they are computationally less expensive. However, they can only detect the inadequacy in the control system's manipulated variable and was not capable of taking necessary corrective action. The above works aim to model safety constraints in the design of process control systems, but their limitations clearly indicate the need for a holistic approach.

In this paper, the concept of dynamic safe set (DSS) is proposed to capture the essence of safety critical constraints. The DSS is defined as a set of process states that guarantee the enforcement of safety critical constraints, in the presence of unknown safety threatening disturbances. It is a closed set that is calculated around a steady state operating condition. Already existing mathematical concepts from the systems literature, namely maximal output admissible sets and the reference governor theory are used for evaluating the DSS. A meaningful method to quantify the size of the DSS is proposed via the concept called dynamic safety margin (DSM). It is defined as the minimum distance of the steady state operating condition from the boundary of the DSS. This will be used as a measure of safeness of processes for designing safer systems. The potential applications of the DSS and DSM concepts in process control design are proposed in this paper. This will lead to designing processes with safety as the primary design objective with all other performance metrics treated as secondary considerations.

The paper is organized as follows: in section 2 the dynamic safe set approach is discussed; the brief and necessary overview of the mathematical concepts required to calculate the dynamic safety sets (DSS) is provided in section 3 along with the proposed definition and calculation procedure for the dynamic safety margin (DSM); the proposed DSS and DSM applications in designing the safer process control system is outlined in section 4; the proposed approach is implemented on the T2 Laboratories exothermic reaction handled in a continuous stirred tank reactor (CSTR) in section 5; lastly, in section 6, conclusions and future directions are discussed.

2 The Dynamic Safe Set (DSS) Concept

The primary objective of the proposed approach is to reformulate the process design and control problem bringing safety upfront. In this paper, safety is represented as a set of safety critical constraints that must be met. Integrating the safety constraints during the design phase has the advantage of minimizing hazards by choosing safer operating conditions, controller strategies and adequate equipment design. The first challenge is to identify a meaningful way to characterize and evaluate the process safeness, that is, a measure of how safe the design is. In this paper, process safety is viewed as a measure of the resilience of the process against disturbances. It is viewed as the ability of the process to return to its normal operating condition in the presence of disturbances and upsets while also respecting the physical constraints that must be satisfied.

A concept called dynamic safety sets (DSS) is formulated to characterize the process safeness. As its name suggests the DSS is a collection of states of the process that guarantees the enforcement of safety critical constraints at any point of time in the future. The safety critical constraints are such that they must be satisfied at all times, failing of which may result in serious consequences. The DSS will be determined around a steady state operating condition. If the process state is found to be away from the steady state operating point but within the DSS, then it is guaranteed that the system can be brought to the necessary steady state safely. The transient states that return the process from the disturbed condition to the steady state operating point, will also lie within the DSS; hence the set will be called the *dynamic* safe set. In the proposed work, the DSS will be evaluated for multi-dimensional systems with safety critical constraints while also accounting of possible disturbance inputs.

Maximal output admissible sets and reference governor are the key theoretical concepts used to calculate the DSS. The maximal output admissible set is defined as the set of all initial states that guarantee the satisfaction of the input/output constraints at any time in the future, even in the presence of unknown disturbance inputs with predefined disturbance bounds[14, 15]. If the initial state belongs to the maximal output admissible set, then for any anticipated disturbance sequence (that is within the predefined bounds), the closed-loop system always satisfies the constraints. Some disturbances can increase the possibility of safety constraint violation by pushing the system to a risky operation zone and they will be referred to as safety threatening disturbances in this paper. These disturbances may manifest through faults and failures originating within the system of interest as well as through abnormal situations occurring in upstream and downstream units. Hence, when the safety critical constraints and the safety threatening disturbances are included in the process model, the maximal admissible set becomes the DSS of the process. Since it is not possible to account for all possible disturbances in a real system, the size of the DSS could be used as a safety metric to measure the ability of the process to eliminate effects of other random disturbances.

Figure 1 below is a schematic explaining the DSS, where the dynamic response from point $\mathbf{P_1}$ in state space that lies within and point $\mathbf{P_2}$ in state space that lies outside the DSS, under a perturbed scenario.

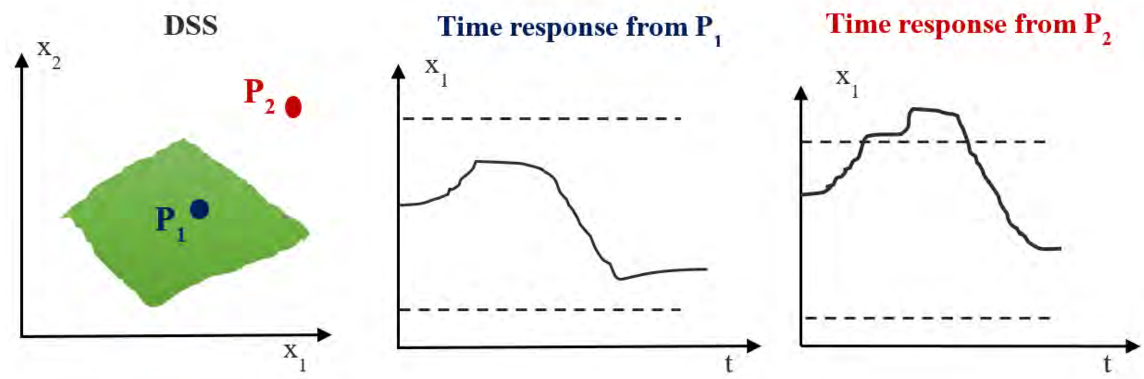


Figure 1: Illustration of the dynamic safe sets (DSS) concept

Set point changes in processes are not uncommon in industry, especially during abnormal scenarios when there may be a need for large and sudden set point changes. Control strategies must be designed to accommodate such requirements while accounting for the safety critical constraints in order to achieve maximum safety. For this purpose, the concept of reference governor [16] is used. Reference governor is a supervisory nonlinear control scheme that is added to an existing closed-loop system that attenuates the reference signal that is to be tracked, only when necessary, to avoid constraint violations and stay within the safe region. The traditional control-loop and reference governor scheme are shown in figure 2. The reference governor requires information to help predict the possibility of future constraint violation. The maximal output admissible sets will be used as the predictive tool that enables the implementation of reference governor in this work.

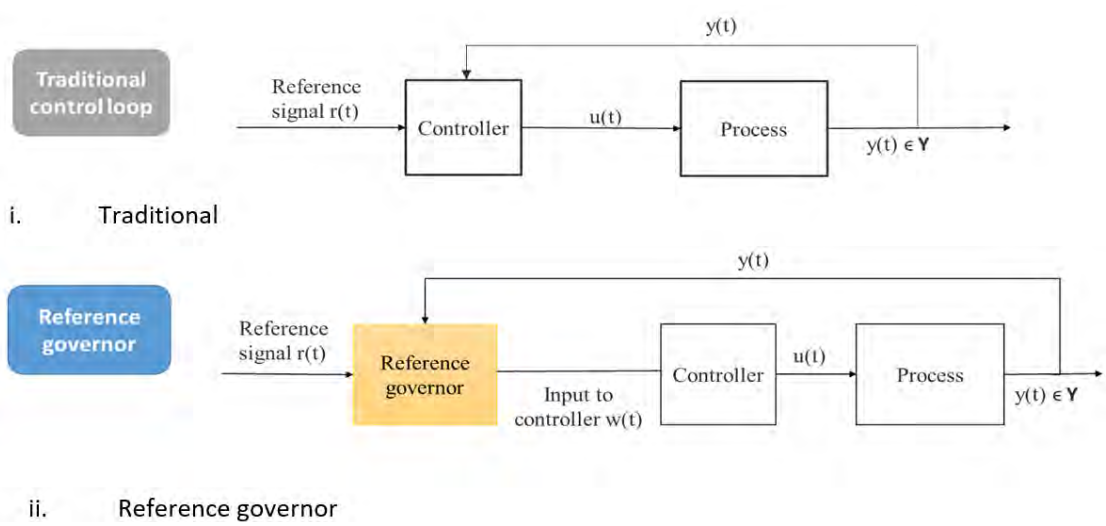


Figure 2: i. Traditional and ii. Reference governor control schemes

3 Mathematical formulation of the concept of dynamic safe set (DSS)- Dynamic safety margin (DSM)

An overview of the maximal output admissible sets for disturbance-free case and with disturbance inputs accounted for is briefly reviewed first. The concepts are based on the theory developed in [14] and [15]. It is followed by an introduction to the reference governor theory [16]. The overview of theoretical concepts will be followed by the proposed mathematical definition of dynamic safe sets (DSS). Lastly, a quantitative methodology to evaluate the size of n-dimensional DSS is proposed via defining the dynamic safety margin (DSM).

3.1 Brief overview of pertinent systems theory concepts

3.1.1 Determination of maximal output admissible sets without disturbance inputs (based on [14]):

Consider a discrete-time linear system:

$$x(t+1) = A_P x(t) + B_P u(t) \tag{1}$$

$$y(t) = C_P x(t) + D_P u(t) \tag{2}$$

where $x \in \mathbf{R^n}$, $y \in \mathbf{R^p}$ and $u \in \mathbf{R^m}$ are the states, outputs and control inputs for the process. A_P, B_P, C_P, D_P are real matrices of appropriate dimensions.

If the control input is assumed to take the form of a linear state feedback law with $u(t) = K\,x(t)$ with K being the controller gain, then the closed-loop system can be described as below:

$$x(t+1) = A\,x(t), \text{where } A = A_P + B_P\,K \tag{3}$$

$$y(t) = C\,x(t), \text{where } C = C_P + D_P\,K \tag{4}$$

The set of output constraints that the system outputs should meet at all times is **Y,** that is,

$$y(t) = \{\,Cx(t) \in \mathbf{Y} \quad \forall \quad t \in \mathbf{N}^+\} \tag{5}$$

where $\mathbf{N}^+$ is the set of positive integers. Note that the state and process input constraints can be expressed through the set **Y** as a set of inequalities in y.

The maximal output admissible set ($\mathbf{O}_\infty$) is defined as the set of all initial conditions **Z**, s.t, $x(0) \in \mathbf{Z}$ implies, $Cx(t) \in \mathbf{Y}$ is satisfied for all $t \in \mathbf{N}^+$.

That is,

$$\mathbf{O}_{\infty}\,(A, C, Y) = \{x \in \mathbf{R^n} \colon\; CA^t\,x \in \mathbf{Y} \quad \forall \quad t \in \mathbf{N}^+\} \tag{6}$$

The $\mathbf{O}_\infty$ is represented by a finite set of linear inequalities if and only if $\mathbf{O}_t = \mathbf{O}_{t+1}$ for some finite t where,

$$\mathbf{O_t} = \{x(0) \in \mathbf{R^n} \colon \quad y(k) \in \mathbf{Y} \quad \forall \quad k = 0, \dots, t\} \tag{7}$$

The finite determination of $\mathbf{O}_\infty$ is feasible under some reasonable assumptions (see [14])

More often **Y** is defined by inequalities,

$$\mathbf{Y} = \{\,y \in \mathbf{R^p} \;:\; f_i(y) \le 0,\; i = 1, .., s\}. \tag{8}$$

For such systems, under the assumptions,

- **i.** A is Lyapunov stable,
- **ii.** the functions $f_i \colon \mathbf{R^n} \to \mathbf{R}$, for $i = 1, .., s$ are continuous and
- **iii.** $f_i(0) \le 0$

and by defining $g_i \colon \mathbf{R^n} \to \mathbf{R}$, with

$$g_i(x) = \sup\{ f_i(CA^t x): \quad t \in \mathbf{N}^+\}, \tag{9}$$

the maximal output admissible set can be defined by,

$$\mathbf{O}_{\infty} = \{x \in \mathbf{R}^{\mathbf{n}} : \ g_i(x) \le 0, \ i = 1,..,s\} \tag{10}$$

See [14] for proof.

For $\mathbf{O}_{\infty}$ represented by eq. (10), there exists a nonempty set of integers $S^* \subset \{1, \ldots ,s\}$ and indexes t_i^*, $i \in S^*$, such that $t^* = \max\{ t_i^*, i \in S^*\}$. That is,

$$\mathbf{O}_{\infty} = \{x \in \mathbf{R}^{\mathbf{n}} : \ f_i(CA^t x) \le 0, \ i \in S^*, t \in \{0, \ldots, t_i^*\}\} \tag{11}$$

Eq. (11) can also be represented by the following recursion that will be the basis for algorithms used in mathematical programming software to determine $\mathbf{O}_{\infty}$.

$$\mathbf{O}_{\mathbf{t+1}} = \mathbf{O}_{\mathbf{t}} \cap \{x \in \mathbf{R}^{\mathbf{n}}: \ CA^{t+1} x \ \in \ \mathbf{Y} = \ f_i(CA^t x) \le 0\}, \quad \mathbf{O}_{\mathbf{0}} = \{x : \ Cx \in \mathbf{Y}\} \tag{12}$$

The reader can refer to [14] for conditions necessary for finite determination O_∞ and the recursive optimization algorithm for calculating O_∞.

3.1.2 Determination of maximal output admissible sets with disturbance inputs (based on [15])

The system described in the previous subsection may be subject to bounded disturbance inputs $w(t) \in \mathbf{W} \subset \mathbf{R}^{\mathbf{m}}$, $t \in \mathbf{N}^+$ in addition to $y(t) \in \mathbf{Y}$, $t \in \mathbf{N}^+$. It is then represented by,

$$x(t+1) = Ax(t) + Bw(t) \tag{13}$$

$$y(t) = Cx(t) + Dw(t) \tag{14}$$

where $w(t) \in \mathbf{R}^{\mathbf{m}}$ is the disturbance vector and x(t) and y(t) are same as in the previous disturbance free case. A, B, C and D are real matrices in appropriate dimension.

Then the maximal output admissible set is defined as the set of all initial conditions x(0) such that,

$$y(t) \in \mathbf{Y}, \quad \forall\, w(t) \in \mathbf{W}, \quad \forall \quad t \in \mathbf{N}^+. \tag{15}$$

That is,

$$\mathbf{O}_{\infty} = \{x(0) \in \mathbf{R}^{\mathbf{n}} : \ y(t) \in \mathbf{Y}, \ \forall\, w(t) \in \mathbf{W}, \forall\, t \in \mathbf{N}^+\} \tag{16}$$

The output y(t) is represented by,

$$y(t) = \begin{cases} Cx(0) + Dw(0), & t = 0 \\ CA^t x(0) + \sum_{k=0}^{t-1} CA^{(t-k-1)} Bw(k) + Dw(t), & t \ge 1 \end{cases} \tag{17}$$

In order to establish the recursion necessary for the algorithmic determination of O_∞, define

$$\mathbf{O}_{\mathbf{t}} = \{x(0) \in \mathbf{R}^{\mathbf{n}}: y(k) \in \mathbf{Y} \ \forall\, k = 0, \ldots, t \text{ and } \forall\, \mathbf{w} \in \mathbf{W}\} \tag{18}$$

Then,

$$\mathbf{O}_{\mathbf{0}} = \{\phi \in \mathbf{R}^{\mathbf{n}}: C\phi + D\psi \in \mathbf{Y} \ \forall\, \psi \in \mathbf{W}\} = \Gamma \tag{19}$$

$$\mathbf{O}_{\mathbf{t+1}} = \{\phi \in \mathbf{R}^{\mathbf{n}}: \quad C\phi + D\psi \in \mathbf{Y}, \quad A\phi + B\psi \in \mathbf{O}_{\mathbf{t}} \quad \forall\, \psi \in \mathbf{W}\}$$

$$= \{\phi \in \Gamma: \quad A\phi + B\psi \in \mathbf{O_t} \quad \forall\, \psi \in \mathbf{W}\}, t \in \mathbf{N}^+ \tag{20}$$

The Pontryagin difference (P-subtraction) is used to represent eq. (19) and eq. (20) suitable for algorithmic procedures. P-subtraction is a set operation that can be defined for sets $\mathbf{U}, \mathbf{V} \subset \mathbf{R}^n$ as below:

$$\mathbf{U} \sim \mathbf{V} = \{z \in \mathbf{R}^n: z + v \in \mathbf{U}\ \forall\, v \in \mathbf{V}\} \tag{21}$$

The P-subtraction is used to represent $\mathbf{O}_{t+1}$ in a compact form and thus help in the development of algorithmic procedures for determining the maximal output admissible sets.

Applying the P-difference to eq. (17),

$$\mathbf{Y_0} = \mathbf{Y} \sim D\mathbf{W}, \tag{22}$$

$$\mathbf{Y_t} = \mathbf{Y} \sim D\mathbf{W} \sim \ldots\ldots \sim CA^{(t-1)}B\mathbf{W}, t \geq 1 \tag{23}$$

Then,

$$\mathbf{O_t} = \{x(0) \in \mathbf{R}^n: \quad CA^k x(0) \in \mathbf{Y_k}\ \forall\, k = 0, \ldots, t\} \tag{24}$$

Combining eq. (22), eq. (23) and eq. (24), the recursions are established as follows:

$$\mathbf{Y_{t+1}} = \mathbf{Y_t} \sim CA^t B\mathbf{W}, \qquad \mathbf{Y_0} = \mathbf{Y} \sim D\mathbf{W} \tag{25}$$

$$\mathbf{O_{t+1}} = \mathbf{O_t} \cap \{\phi \in \mathbf{R}^n: CA^{t+1}\phi \in \mathbf{Y_{t+1}}\}, \quad \mathbf{O_0} = \{\phi : C\phi \in \mathbf{Y_0}\} \tag{26}$$

The conditions for finite determination of $\mathbf{O}_\infty$ and the optimization algorithm for calculating O_∞ in eq. (26) are given in [15].

3.1.3 Reference governor:

Reference governor is a nonlinear add-on device to an already existing closed-loop system, which attenuates the input command, when necessary. The theory on discrete-time reference governors developed in [16, 17] is adopted for implementation in this work. An overview of this concept for systems without disturbance inputs is given below.

Consider the system,

$x(t+1) = Ax(t) + Bv(t)$

$y(t) = Cx(t) + Dv(t)$

where $x(t) \in \mathbf{R}^n$ is the state vector, $v(t) \in \mathbf{R}^m$ is the reference signal vector that is to be tracked and $y(t) \in \mathbf{R}^p$ is the output vector of the closed-loop system for $t \in \mathbf{N}^+$. See figure 3 below for a schematic of the reference governor.

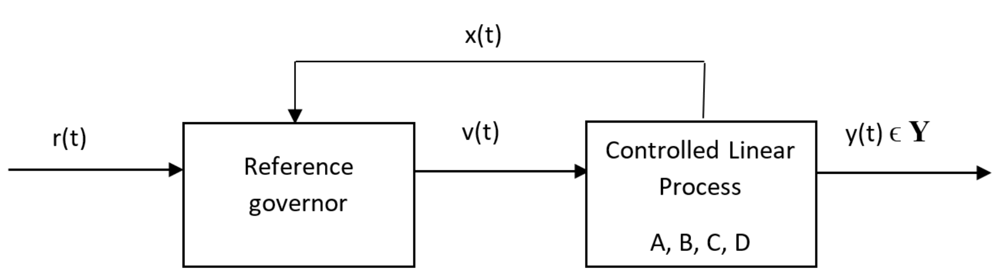


Figure 3: Schematic for reference governor

The reference governor modifies the input signal as follows,

$$v(t+1) = v(t) + K(r,x)\,(r(t) - v(t)) \text{ where } K \in [0,1],$$

$$K = \max\left\{k \in [0,1]: \begin{bmatrix} v & k(r-v) \\ Ax + B_v v & 0 \end{bmatrix} \in \mathbf{O}_\infty \right\} \tag{27}$$

This will result in the following closed-loop system:

$$x_G(t+1) = A_G x_G(t) + B_G k(r(t) - [I\ 0]x_G(t))$$

$$y_G = C_G x_G(t) \in \mathbf{Y}$$

where,

$$x_G = \begin{bmatrix} v \\ x \end{bmatrix}, A_G = \begin{bmatrix} I & 0 \\ B & A \end{bmatrix}, B_G = \begin{bmatrix} I \\ 0 \end{bmatrix}, C_G = [\,D \quad C\,]$$

$$K = \max\{k \in [0,1]: x(t+1) \in \mathbf{O}_\infty\,(A_G, B_G, \mathbf{Y})\} \tag{28}$$

The maximal output admissible set will be calculated for the system in eq. (29) by setting K as 0 initially. The algorithm for implementing reference governor for systems with disturbance inputs are provided in [18]. The optimization algorithm required for real time implementation is also provided in [18].

Although these concepts have existed in literature for more than 2 decades, its application has been mostly limited to aerospace and electrical engineering [19-23]. In chemical engineering literature, the use of maximal output admissible sets is limited to stability proofs in MPC schemes [10, 24, 25]. In this paper, we aim to exploit its capability in designing safer control systems for chemical processes.

3.2 Definition of the Dynamic Safe Set (DSS)

The concepts introduced above are used to mathematically define the dynamic safe sets. The definition of maximal output admissible set in eq. (16) shows that the output y(t) is forced to lie within the constraint set **Y** at all times. Typically, the safety critical constraints are derived from imposing bounds on linear combinations of state and output variables like the onset temperature of a runaway reaction, the maximum allowable working pressure of a vessel and the limits on controller actuator. These inequalities can be incorporated through the set **Y** such that the maximal output admissible set guarantees the satisfaction of safety critical constraints. The trajectory of output y(t) defined in eq. (17) considers also the possibility of disturbances w(t) in the process. This allows for designing systems that respect the constraints, accounting for system dynamics even in the presence of unknown disturbances.

Furthermore, there can be several possible disturbances and random noises that can push the system away from the steady-state, which the control system is generally capable of handling. In addition to these, there could be unusually large and sudden persistent disturbances occurring during abnormal situations of plant operation. Such disturbances can have severe impact on the dynamics of the process. These adverse disturbances that threaten the integrity of the process are referred to as the safety threatening disturbances in this paper. It is important that for safe operation of the process, the effects of these disturbances on the process dynamics must be included in the control system design. The set **W** in eq. (16) can include the ranges of safety threatening disturbances that are defined through linear inequalities, with only little information known about the anticipated disturbances. Thus, from the definition of maximal output admissible sets, the set **W** inherently accounts for any possible disturbance sequence w(t), including sudden or erratic ones, by forcing y(t) to satisfy the output constraints **Y** for any w(t) in **W**.

Hence, when the system in eq. (16) has the safety critical constraints (**Y**) and the potential safety threatening disturbance ranges (set **W**) accounted for, the maximal output admissible sets become the dynamic safe sets. The dynamic safe set is the collection of all initial states that guarantee the enforcement of the safety critical constraints while respecting the process dynamics even in the presence of adverse safety threatening disturbance sequences. When the DSS is large, the process has the capability to eliminate the effect of disturbances even when the process state is initially perturbed due to unknown reasons. Some causes of these perturbations can be model uncertainties, inaccuracies in measurement sensors and equipment failures and faults. Hence, it is possible to enhance safety by increasing the size of the DSS by choosing the design parameters accordingly. The challenge however is to identify a meaningful DSS quantification methodology that can be useful for interpreting the DSS of higher order systems.

3.3 Definition of the dynamic safety margin (DSM)

It is necessary to develop a method to extract physically meaningful information from the n-dimensional DSS that is relevant and aids in safer design. For this purpose, a concept of dynamic safety margin (DSM) is proposed in this paper. It is defined as the minimum distance of the steady state operating point from the boundary of the DSS that is represented by a set of linear inequality constraints. The dynamic safety margin can be viewed as the maximum radius of a ball in the n-dimensional state space centered at the steady state that lies within the DSS.

Of course, to be able to define a norm in the presence of different units of the state variables, appropriate normalization will be necessary. Normalization of the state variables with respect to the potential consequences associated with their deviation from the steady state value seems reasonable since the ultimate design objective is to maximize safety. The potential to cause harm, in other words, the hazard associated with the magnitude of deviation is different for different state variables. The difference in increased threat is leveraged to define the scale factor (σ) for each state variable. It is the ratio of change in a state variable (x_i) to change in a reference state variable (x_r) that produces the same effect on the hazard evaluated.

That is,

$$\sigma_i = \frac{\Delta x_i}{\Delta x_r} \tag{29}$$

The scale factors for the states are used to transform the DSS from the original state coordinates to the transformed coordinates $\bar{x} = \Sigma x$, where the transformation matrix Σ is given by,

$$\Sigma = \begin{bmatrix} \sigma_i & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_n \end{bmatrix},$$

Assume the DSS in the original state space calculated around the steady state x_S is defined by the set of inequalities,

$$\boldsymbol{\Phi} = \{ \phi_j(x) = a_j^T x - c_j \le 0, j = 1, \dots . q\}$$

Then, the set of inequalities defining the DSS in the transformed state space is,

$\phi_j(\bar{x}) = \bar{a}_j^T \bar{x} - c_j \le 0,\ j = 1, \dots . q$, where $\bar{a}_j^T = (a_j^T \Sigma^{-1})$

Using the projection theorem from linear algebra, the minimum distance of the steady-state $\bar{x}_S$ from each of the boundary equation $\left(\phi_j(\bar{x}) = 0\right)$ can be given by,

$$d_j = \text{abs}\left(\frac{\left(c_j - \bar{a}_j^T . \bar{x}_S\right)}{\| \bar{a}_j \|_2}\right), \quad j = \{1, 2, \dots . q\} .$$

The dynamic safety margin (DSM) is then defined as,

$$\text{DSM} = \min_j d_j , \quad j = \{1, 2, \dots . q\}. \tag{30}$$

The safety margin of states can be represented in units of the reference variable or the individual state variable by dividing the DSM by the respective σ_i. This is a measure of the minimum tolerable deviation of the state variable from its steady state value. The DSM depends on the ranges of safety threatening disturbances along with the other design parameters. It could be a conservative measure of the process safety performance, especially when adverse scenarios representing abnormal situations are included in the disturbance set **W**. An example application of the individual state margins is to design the process such that the margins of each state are at least as large as the accuracy of their measurement sensors.

An approach to address the process control design problem based on the proposed DSS and DSM concepts are outlined in the next section.

4 Proposed DSS based approach for process control design

The key ideas identified in the control system design with maximal safety, that form the basis of the proposed approach, are now outlined. Firstly, the controller set point that sets the steady state of operation of the process can play a role in system safeness. Secondly, the actuator characteristics and the control strategy and their parameters can significantly affect the system dynamics in presence of disturbances and set point changes. Thirdly, in the event of abnormal situations that may be accompanied by large and sudden changes in operating conditions, it is of utmost importance that the control system is capable of handling them while satisfying the safety critical constraints.

The proposed approach is devised based on the understanding that DSS reasonably characterizes the safeness of the process, by accounting for safety constraints and dynamic effects of safety threatening disturbances. It then leads to the conceptual idea that the DSS along with the DSM can be used as a guide in addressing the ideas stated above. It is assumed that a process model to capture the dynamics is available and that the safety critical constraints are identified based on a thorough understanding of the process. It is also reasonable to account for disturbance inputs that represent possible abnormal situations in the DSS calculation.

Typically, the control system is designed with objective to eliminate the effects of disturbances quickly and safely around a set point. Of course, it is assumed that potential set points considered maintain certain essential performance metrics with respect to other design criteria. The favorable set points can then be chosen based on the DSS and DSM they offer under some nominal controller and actuator design. Once the relatively safer steady states are identified, the control system can be designed, that includes the actuator system and the selection of strategy and parameters. A grid of design parameters that consist of possible control laws, actuator design parameters and controller tuning parameters can be used to generate a set of closed-loop systems, operating at each of the identified safe set points. The DSS and DSM calculations can be performed for these closed-loop systems.

The approach will provide designs that represent maximal safeness. When there are multiple designs that offer reasonable safeness, the controller performance requirements can be used as additional performance metrics. Financial considerations involved in the actuator system design can also be used as metrics to identify the final design.

In the event of an abnormal situation, there may be a need for a large and sudden set point change. Because controllers that are normally used for disturbance rejection are tuned to be aggressive (with large controller gains), when there is a sudden need for a set point change, special care should be taken for safe transition. The use of reference governor scheme is proposed as an addon scheme to guide the system and help prevent potential actuator saturation.

It will be seen from the case study that follows that the proposed approach captures multiple facets of safety considerations. The final design configuration will provide maximal safeness and reasonable performance with respect to other criteria. The time responses of the closed-loop system for the final design configuration along with the reference governor scheme will indicate the effectiveness of the design approach.

5 Case Study

5.1 Case study description

The DSS approach for safety-centered design and control was tested on a continuous-stirred-tank-reactor (CSTR) handling an exothermic reaction. T2 Laboratories manufactured methylcyclopentadienyl manganese tricarbonyl in a 2500-gallon batch reactor. In 2007, an explosion occurred at the plant during the production process resulting in 4 fatalities and several injuries. The incident took place when there was insufficient cooling provided to the reactor and the temperature increased uncontrollably causing reactor rupture. Hydrogen and other flammable chemicals were ignited resulting in a massive explosion. In this paper, the reactions of T2 Laboratories that led to the explosion are modeled in a CSTR reactor (as shown in Figure 4), instead of the batch reactor originally used at T2.

The feed streams reactant methylcyclopentadiene (A) in solvent diglyme (S) and liquid sodium (B), are both heated in a preheater before being fed to the reactor. The reactor temperature control loop maintains the reactor temperature at the required set-point. The temperature of the reactor (T) is the controlled variable, the cooling system heat transfer coefficient (U) is the manipulated variable (control input) and the fluctuations in reactor inlet feed temperature (T_0) is accounted for as potential disturbance source in the model. The heat transfer coefficient is manipulated by adjusting the flowrate of the cooling water based on correlations available from literature. For the sake of simplicity, U will be treated as the manipulated input for this case study.

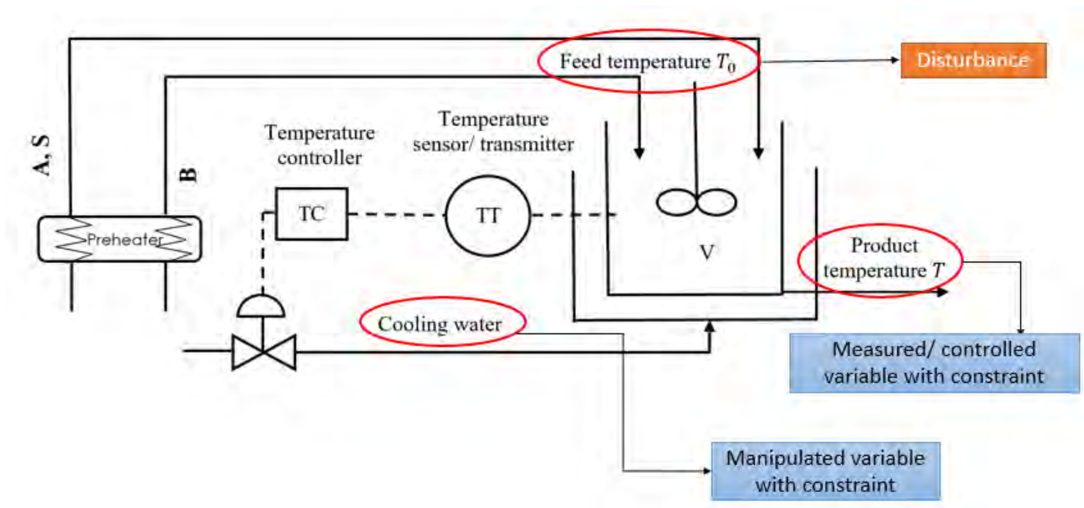


Figure 4: Process flow diagram of the modified T2 Laboratories process in a CSTR

The reactions considered for study can be modelled as follows:

Reaction 1: $A + B \xrightarrow{k_1} C + \frac{1}{2} D$

Reaction 2: $S \xrightarrow{k_2} 3D + \text{byproducts}$

In particular,

Methylcyclopentadiene (**A**) + Sodium (**B**) $\xrightarrow{\text{Diglyme (S)}}$ Sodium Methylcyclopentadiene (**C**) + Hydrogen (**D**)

Diglyme (**S**) $\xrightarrow{\text{Sodium}}$ Hydrogen (**D**) + byproducts

The mass and energy balances for the reactor are presented below:

$$\frac{dC_A}{dt} = r_{1A} + v_0 * \frac{(C_{A0} - C_A)}{V}$$

$$\frac{dT}{dt} = \frac{V * (r_{1A}\,\Delta H_{r1A} + r_{2S}\,\Delta H_{r2S}) - (U_S + U) * A_x * (T - 373)}{\Sigma NC_p}) + v_0 * \frac{(T_0 - T)}{V}$$

where C_A is the concentration of the reactant methylcyclopentadiene, T is the temperature of the reactor, v_0 is the volumetric flowrate of the feed and V is the reactor volume, U_S is the steady state heat transfer coefficient, ΣNC_p is the heat capacity of the system, A_x is the heat transfer area of the exchanger, r_{1A} and r_{2S} are the reaction rates for reactions 1 and 2 respectively, ΔH_{r1A} and ΔH_{r2S} are the heat of reactions for reactions 1 and 2 respectively.

The closed-loop processes under proportinal (P) and proportional-integral (PI) contol strategies can be respresented by, P-Controller: $U = k_{c*}(T_S - T)$ and

PI-Controller: $U = k_c * (T_S - T) + \frac{I}{\tau_i}$ along with the ode $\frac{dI}{dt} = T_S - T$ to account for the integral of error calculation,

where k_c and τ_i are the controller parameters, gain and integral time respectively.

Reaction 2 is a side reaction that has a negligible rate when operated at temperatures less than 460 K. However, upon reaching 480 K the rate of side reaction becomes significant as it has an activation energy of more than 6 times that of the desired main reaction. This will cause an uncontrolled increase in reaction rate at higher temperatures. As both reactions produce hydrogen gas, there is a possibility of steep increase in the pressure that can cause a reactor wall rupture. Based on these observations, the following temperature constraint will be imposed.

$T < 480$ K

The maximum available manipulated input (U_{max}), which is a design parameter, will be included as a safety critical constraint. The reason here is that a sustained violation of this constraint may lead to divergence of the deviation in reactor temperature, which may result in a runaway scenario.

$U < U_{max}$

It is anticipated that upstream units and preheater malfunction may bring in fluctuations in the reactor feed temperature. The range of the reactor feed temperature (T_0) is expected to be between 405 K and 430 K. The upper limit was intentionally chosen to be an unusually large value to account for rare events which can more than likely push the system to hazardous operation zone. Hence, T_0 is included as a safety threatening disturbance.

$405 < T_0 < 430$ K

Based on the system description provided, the design parameters that are to be chosen are (i). the maximum heat transfer coefficient (U_{max}) and (ii). the controller parameters (k_c for P-Controller, k_c and τ_i for PI-controller). This system can be viewed as a representative example for exothermic reactors with cooling and temperature control system.

The above nonlinear dynamic model is linearized and discretized around different operating conditions that are to be investigated, as shown in eq. (13) and eq. (14) of section 3:

$$x_d(k+1) = A_d x_d(k) + B_d w(k),$$

$$y_d(k) = C_d x_d(k) + D_d w(k),$$

where the states $x_d = [C_A;\ T]$, output $y_d = [T; U]$,

$w \in \mathbf{W} = \{ 405 \leq w = T_0 \leq 430\}$ and

$y_d \in \mathbf{Y} = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} y_d \leq \begin{matrix} 480 \\ U_{max} \end{matrix} \}$

<u>Selection of scale factor for normalizing the states required for determining the DSM</u>

For this case study, the increase in reaction rate is chosen as the common hazard used to define the scaling factor (SF) for normalizing the states (discussed in section 3). If temperature is chosen as the reference state variable, the scale factor of concentration becomes the ratio of change in concentration to change in temperature that brings similar effect on change in reaction rate. The SF for temperature is 1 based on the definition. The SF for the state variables will depend on the steady state operating conditions. For the operating conditions between 440 and 465 K, a value of 80 is chosen as the SF for concentration.

$$\sigma = \begin{bmatrix} 80 \ \frac{\mathrm{K}}{\mathrm{mol}/l} \\ 1 \end{bmatrix} \tag{31}$$

This is used to calculate the DSM around the steady state in the normalized DSS. The DSM is expressed in temperature units in the discussions that follow.

5.2 Application of the DSS approach

The approached proposed in section 4 for control system design are tested on this CSTR. This case study can be viewed as a representative example for exothermic reactors with cooling system and control system design. The results from the investigation are organized as follows:

1.1. Steady-state selection and significance of accounting for possible disturbance inputs

2.DSS calculations for process operating at the different steady-states with nominal cooling and control system, with and without including disturbance inputs

↓

2. Effect of cooling system and control system design on DSM

DSS and DSM calculations for the process operating at relatively safer steady-states with different cooling system and control system design parameters

↓

3. Reference governor implementation using DSS

DSS application in managing sudden and large set-point changes in the controlled variable

5.2.1 <u>Steady state selection and significance of accounting for possible disturbance inputs</u>

The steady state ranges that are investigated are chosen to guarantee a minimum reactant conversion of 85% as the design basis. This led to selecting set point temperatures (T_S) greater than 440 K. The upper limit of the temperature range was fixed as 465 K to provide a minimum of 15 K margin with respect to the temperature constraint ($T < 480$ K). At these operating temperatures, the steady state heat transfer coefficient required varies between 5 and 48 kJ/K/m^2/hr. For the steady states identified for analysis, the DSS is calculated for the closed-loop system operating with nominal cooling system and control system design.

The maximum heat transfer coefficient (U_{max}) is the cooling system design parameter that is manipulated by adjusting the cooling water flowrate typically. In this case study, U_{max} is treated as an independent design parameter for illustrating the DSS and DSM concepts. Nominal values of cooling system (U_{max}) chosen are 55 and 70 kJ/m^2/K/hr so that they provide a minimum of 10

% and 38 % control input margin respectively, for all the steady states evaluated. The nominal control system chosen is a P-only controller, which is commonly used for temperature control in industry. The controller gain (k_c) of -25 is selected.

The DSS is determined for both disturbance-free case and with disturbance case to compare and understand the safety relevant information that is lost by not accounting for disturbance effects in steady state selection. The DSS for closed-loop system with nominal cooling and control system, without accounting for the disturbance inputs are shown in Figure 5 and Figure 7 respectively. For the same process, disturbance inputs were included and the results are shown in Figure 6 and Figure 8.

The results for U_{max} of 55 show that at steady states 450 and 455 K, the DSS is reduced to null sets once disturbance input was included. Accounting for disturbance input with U_{max} of 70 resulted in relatively smaller DSS (Figure 8) when compared to Figure 7 for all steady states. The results show a strong effect of choice of steady state and heat exchanger design on the size of dynamic safety. However, there are some steady states, namely, 460 and 465 K, that seem more favorable relative to the others, irrespective of the heat exchanger design. These will be taken in to account in the discussions to follow.

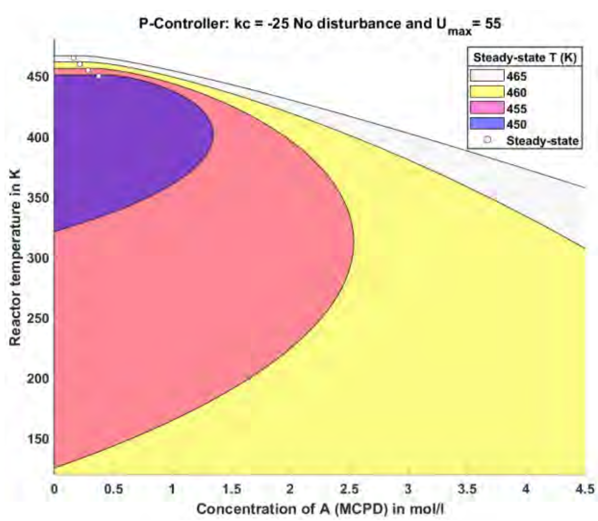


Figure 5: The DSS for P-Controller with k_c -25 and U_{max} 55. Disturbance not included.

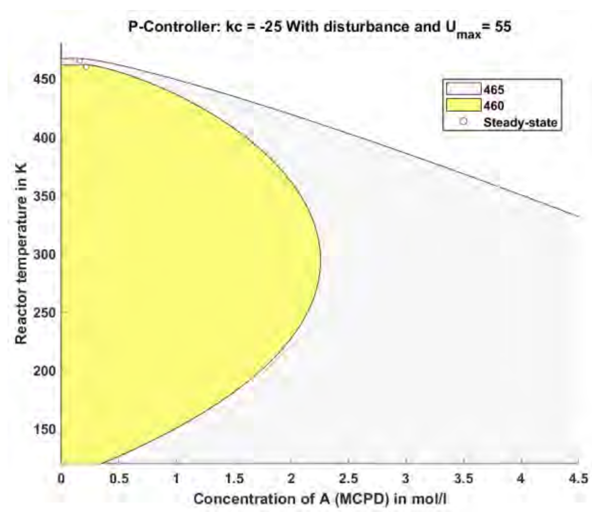


Figure 6: The DSS for P-Controller with k_c -25 and U_{max} 55. Disturbance included.

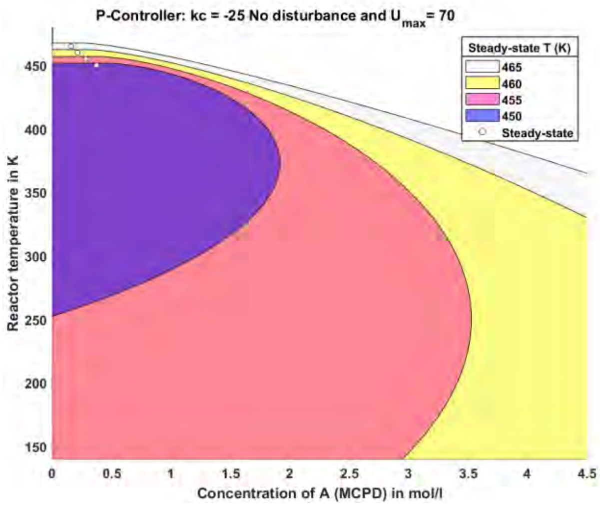


Figure 7: The DSS for P-Controller with k_c -25 and U_{max} 70. Disturbance not included.

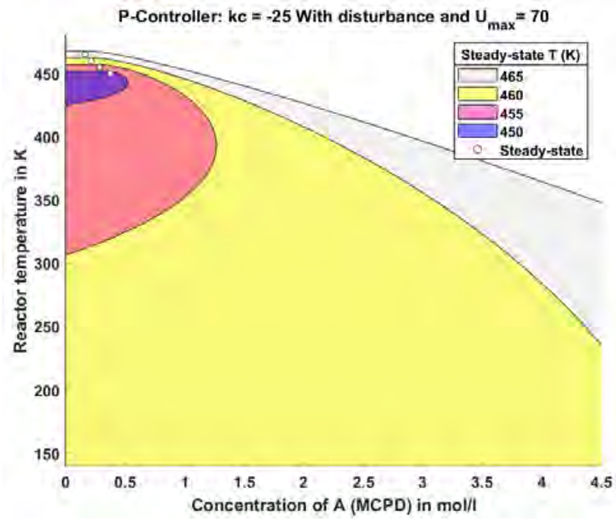
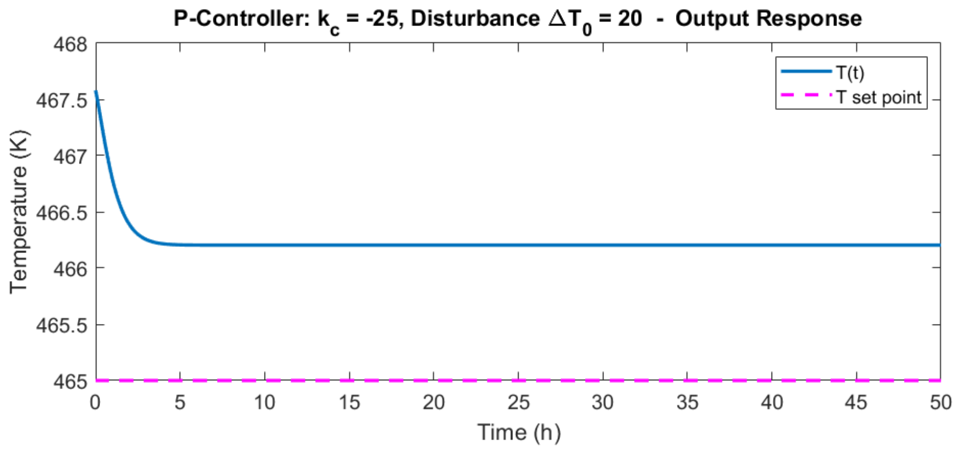
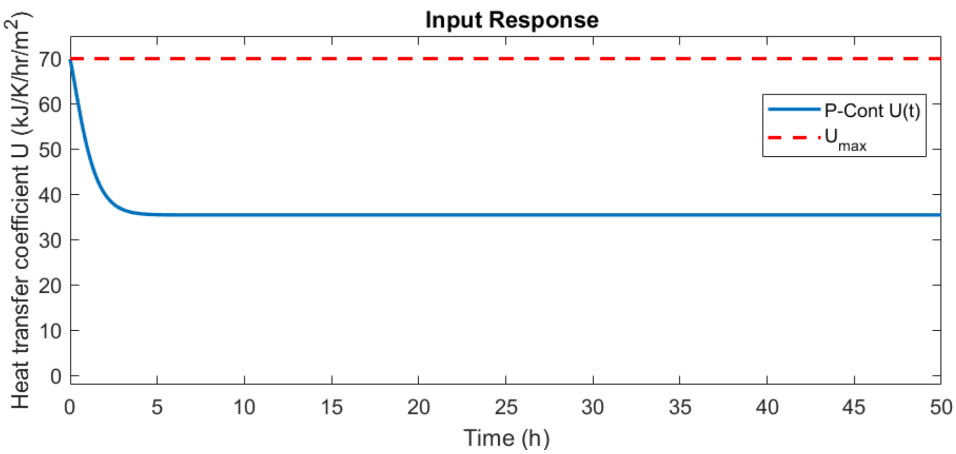


Figure 8: The DSS for P-Controller with k_c -25 and U_{max} 70. Disturbance included.

To understand the implications of the DSS better, the time responses for a system operating at 465 K with a U_{max} of 70 kJ/m^2/K/hr and an initial impulsive disturbance that results in a 2.58 K shift in reactor temperature are shown below. In addition to this, a persistent step disturbance of 20 K in T_0 is induced to the system to illustrate the most adverse conditions the system can tolerate. Figure 9 shows the output and input responses simulated for the nonlinear closed-loop system based on a P only controller with k_c -25 that was simulated in MATLAB.



(i). Output response



(ii). Input response

Figure 9: (i). Output response and (ii). Input response of the system operating at 465 K, U_{max} 70 kJ/m^2/K/hr based on a P Controller with k_c -25, under initial impulsive disturbance that shifts T by 2.58 K and step disturbance of 20 K in T_0

Although the DSS are calculated for linearized and discretized systems, these simulations show that they are adequate for designing the nonlinear process. From the results shown in figures 5 - 8, it is seen that the size of DSS tends to increase with increasing steady state temperature for a particular heat exchanger design (U_{max}). The reason for this is that with decreasing steady state temperature (T_s), the steady state cooling requirement (U_s) increases. This results in a decrease in the difference between U_{max} and U_s as T_s decreases. As a result, the excess manipulated input available for eliminating the effect of disturbances decreases. Another important observation is that, accounting for disturbances provides insights that are normally ignored while approaching the design and control problem. For this case study, the proposed DSS approach led to identifying operating steady-states 460 and 465 K as more favorable choices as they can sustain the effect of the large persistent disturbances and provide a reasonable DSS area. Analysis to further investigate the effect of other design parameters will be carried out in the next subsection.

5.2.2 Effect of cooling and control system design on DSM

P-only Controller

A grid of different heat exchanger and control system design parameters are selected for analysis in this subsection. The effect of heat exchanger design parameter was partly seen in subsection 5.2.1. The controller tuning parameters are critical design parameters as they have a direct effect on the process performance and safeness of the plant. More aggressive controllers may provide good responses but may significantly reduce the size of DSS. Firstly, the DSS was evaluated for P- controller based closed-loop system with different gains (k_c) with a fixed U_{max}. The DSM was calculated for these systems based on eq. (30) for the scale factor identified in eq. (31). It is the measure of margin of safety (or the safety buffer) around that steady state that lies within the DSS. The DSM is reported in units of the reactor temperature (K). i.e, the minimum tolerable initial deviations in the reference state variable T and the scaled state variable C_A, from their steady state values. Table 1 and Figure 10, shows the DSM with U_{max} of 70 kJ/m^2/K/hr for P-controller based closed-loop system with gains of -25, -55 and -75, while accounting for the disturbance input.

The DSM is 0.5 K for the process operating at 450 K with controller gain k_c of -75. This means, there are high chances of violation of safety critical constraints, if the reactor temperature is off by as little as 0.5 K from the steady state temperature. The results in Table 1 show that the range of DSM lies between 0.5 to 2.6 K. Although the safety margin seems to be low, it is important to note that DSM is a conservative measure of safety especially when it accounts for deliberately large disturbances. It is understood that if the ranges of disturbances accounted for are narrower, the size of the safety margin could increase and possibly allow more feasible operating steady states without null sets.

Table 1: DSM for P-only Controller with [k_c]= {-25, -55, -75} and U_{max} of 70 kJ/m^2/K/hr, after accounting for disturbance input

	DSM for process with U_{max} of 70 (scale factor 80) in K		
Steady state reactor temperature T (K)	**P-Controller k_c**		
	-25	**-55**	**-75**
465	2.6	1.2	0.9
460	2.3	1.0	0.8
455	2.0	0.9	0.7
450	1.5	0.7	0.5

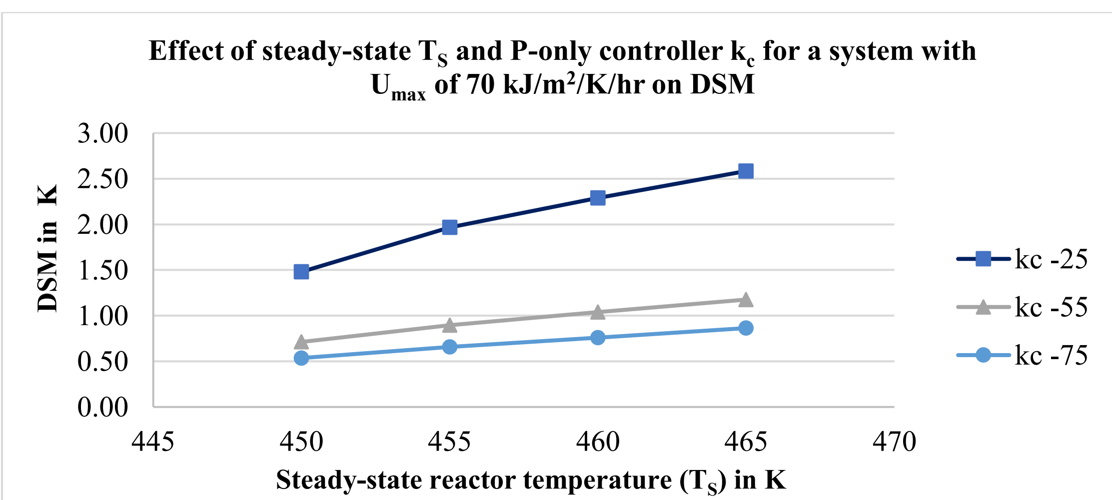
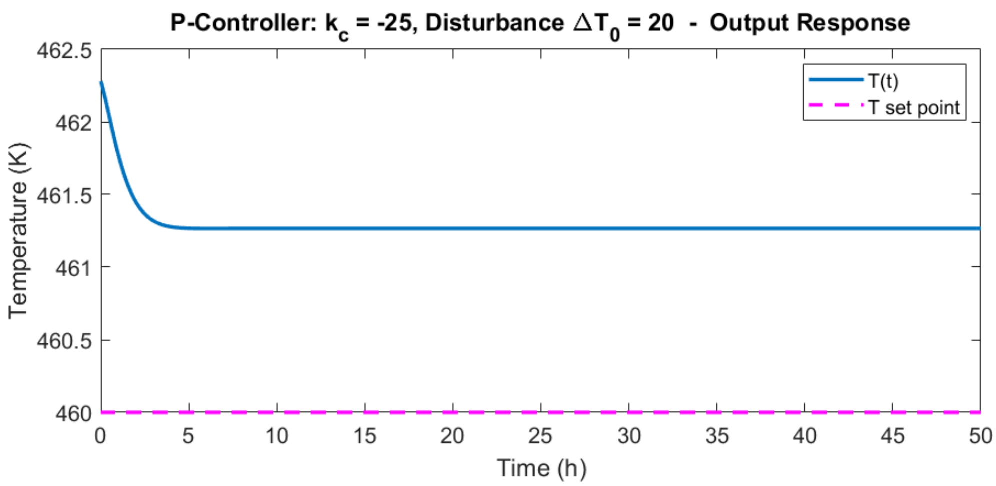
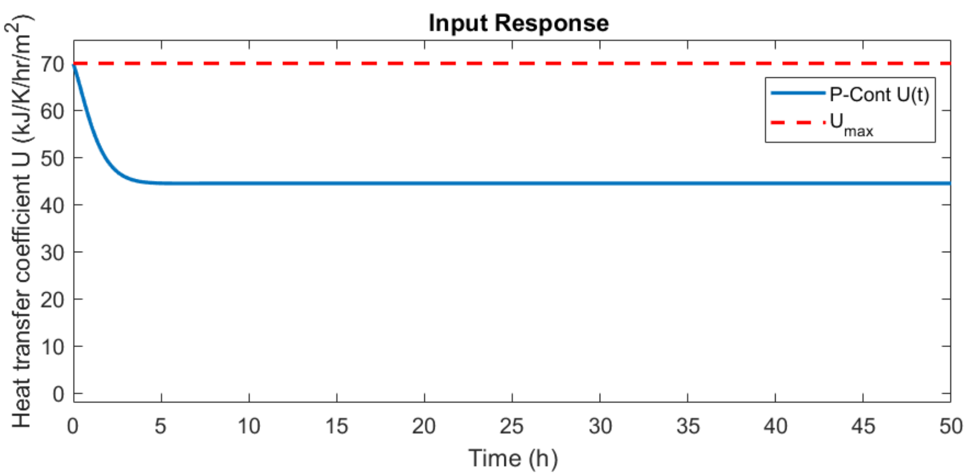


Figure 10: DSM (K) for closed-loop system with U_{max} 70 kJ/m^2/K/hr, effect of steady state temperature T_S = {450, 455, 460, 465} and P-Cont. gain k_c={-25, -55 and -75} on DSM

The time responses of the P-control based closed-loop system operating at 460 K with a gain k_c of -25 and U_{max} of 70 are shown below. From Figure 10, it is seen that the DSM is 2.28 K, that is the control system and process design can eliminate the effect of a step disturbance of 20 K in T_0, even if the reactor temperature (T) is initially perturbed by 2.28 K by an impulsive disturbance. See Figure 11 for output response and input response for the non-linear process model. The control input and the reactor temperature constraints are not violated and the effect of the disturbances in T_0 and T are both contained. There is an offset in the output variable since a P-only controller is used and the reactor reaches a new steady-steady of ~461.3 K. Increasing the absolute value of the controller gain can help reduce this offset. However, the DSM will decrease as seen in Table 1. Figure 12 show the dynamic responses of the process operating at similar conditions but with a gain k_c of -75 under an impulsive disturbance in reactor temperature that shifts it by 0.76 K and a persistent step disturbance of 20 K in T_0. The offset in the reactor temperature is decreased to 0.4 K. However, the system may violate the safety constraints for initial disturbances greater than 0.76 K.

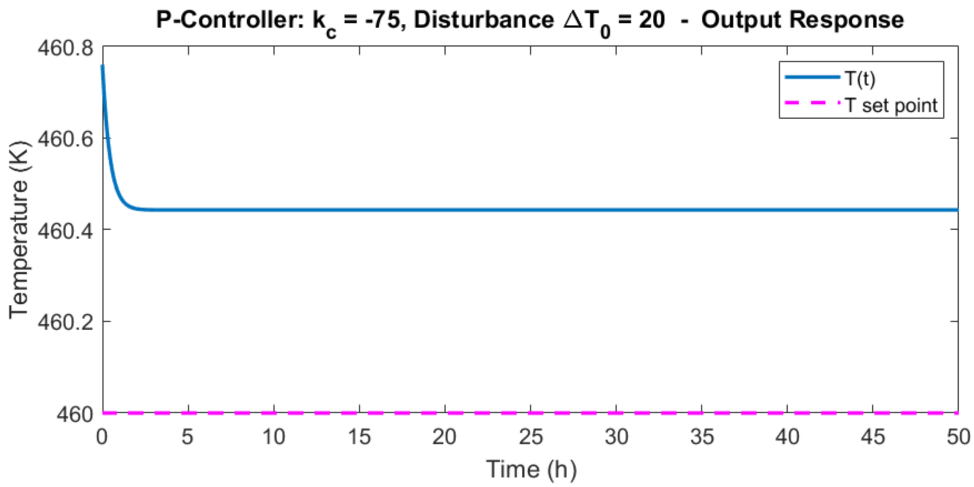


(i). Output response

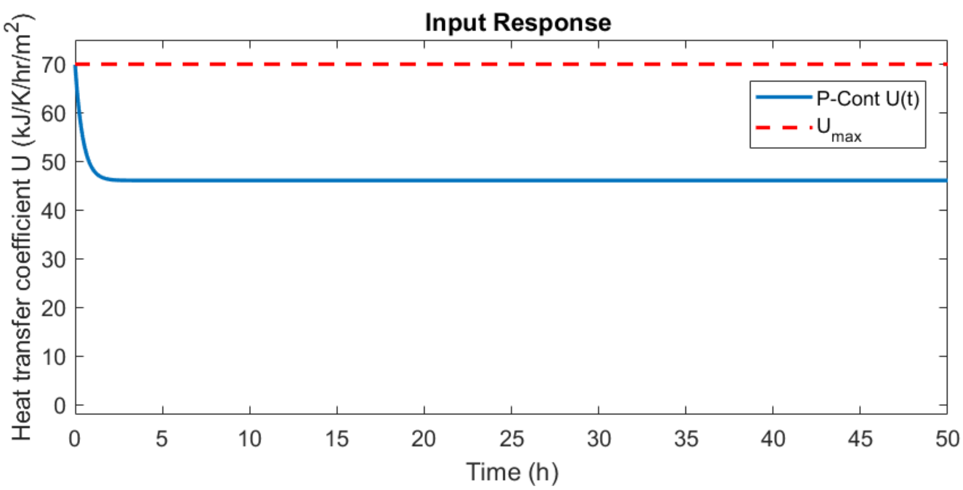


(ii). Input response

Figure 11: (i). Output response T(t) and (ii). Input U(t) response to a +20 K step disturbance in T_0 and an initial impulsive disturbance that shifts T by 2.28 K for a P-controller based closed-loop system with k_c of -25, operating at 460 K.



(i). Output response



(ii). Input response

Figure 12: (i). Output response T(t) and Input response U(t) to a +20 K step disturbance in T_0 and an initial impulsive disturbance that shifts T by 0.76 K for a P-controller based closed-loop system with k_c of -75, operating at 460 K.

<u>*P and PI Controller*</u>

The effect of U_{max} on the DSM will be investigated for the favorable steady states of 460 and 465K. Subsequently, the effect of control strategy and controller parameters will also be simultaneously studied. See figures 13-18 for the DSS calculated for different heat exchanger design parameter (U_{max}) and closed-loop system based on P and PI control strategies with gain of -25. These results demonstrate the significant role played by the integral time in determining the size of the DSS irrespective of the U_{max}. For example, the DSS is reduced to null set for a system operating at 460 K with U_{max} of 55 under the PI controller with integral time of 2 in Figure 14. In all cases, it is seen that the PI controller with an integral time of 2 significantly reduces the range of temperature (T) and concentration (C_A) that lies within the DSS when compared to the respective P-only controller based closed-loop systems.

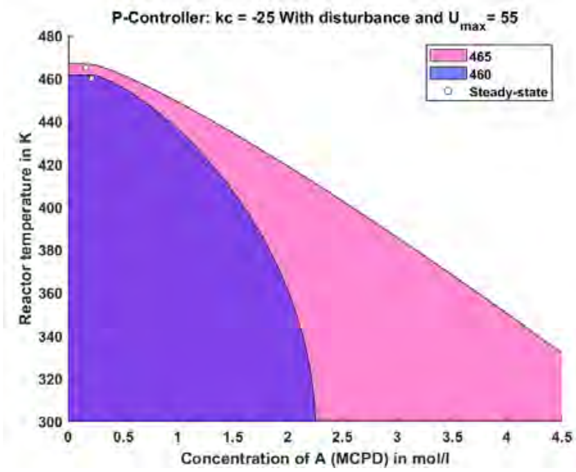


Figure 13: The DSS for P-Controller with k_c -25 and U_{max} 55 with disturbance input included

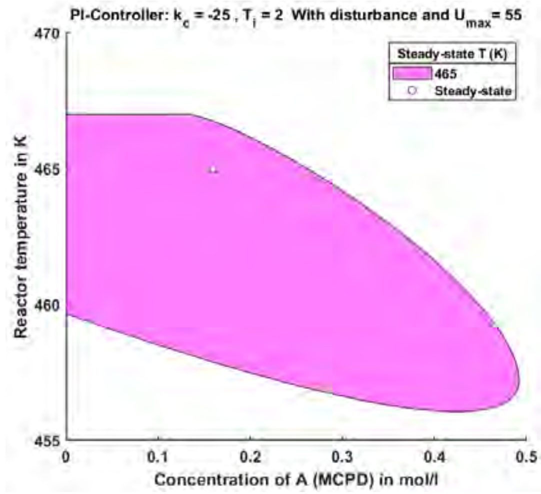


Figure 14: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 55 with disturbance input included

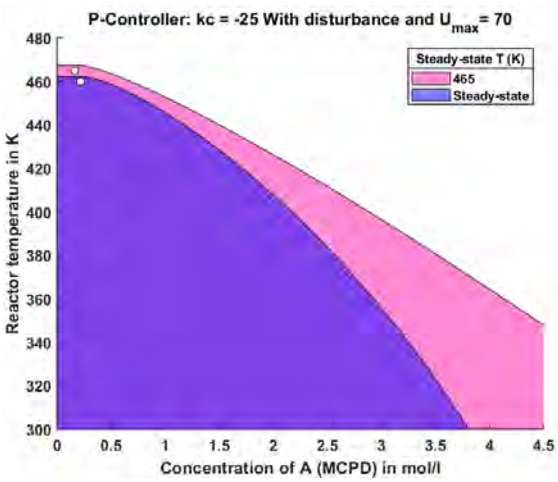


Figure 15: The DSS for P-Controller with k_c -25 and U_{max} 70 with disturbance input included

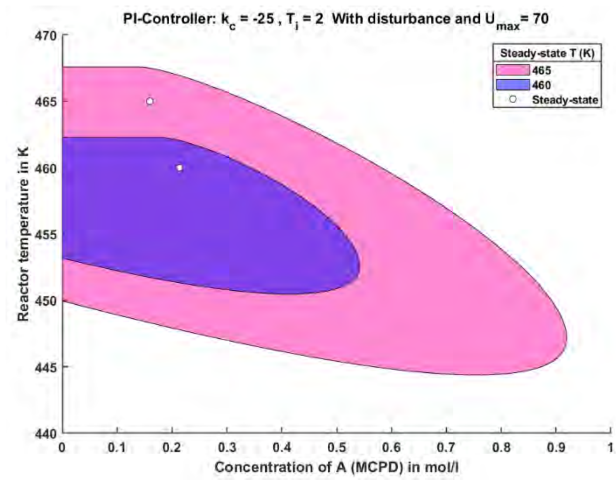


Figure 16: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 70 with disturbance input included

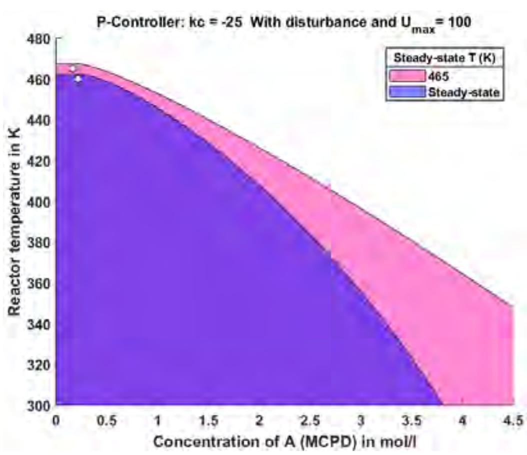


Figure 17: The DSS for P-Controller with k_c -25 and U_{max} 100 with disturbance input included

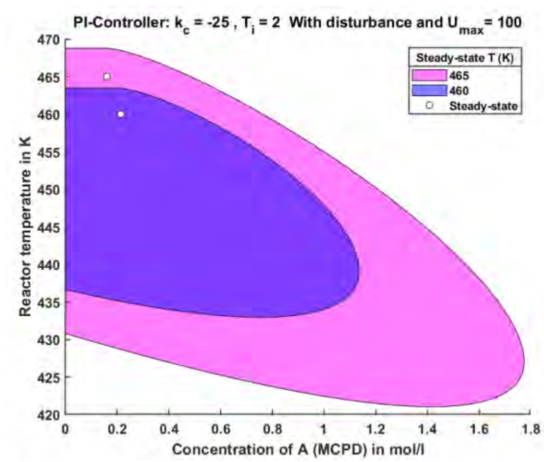


Figure 18: The DSS for PI-Controller with k_c -25 and τ_i 2 and U_{max} 100 with disturbance input included

Figure 19 shows the DSM in units of reactor temperature for different heat exchanger design parameter U_{max} (55, 70 and 100 kJ/m^2/K/hr). The results for both P and PI controller strategies with k_c of –25 and τ_i of 0.75 and 2 are shown to compare the effect of integral time and U_{max} on DSM for the system operated at set points 460 and 465 K. The key observations are as follows:

- As expected, the DSM increases with increasing U_{max} and τ_i.
- U_{max} of 100 kJ/m^2/K/hr provides a maximum DSM of 3.8 K when a PI controller with integral time of 2 is used for the closed-loop design when operating at steady state 465 K.
- U_{max} of 55 kJ/m^2/K/hr provides a DSM of up to 1.7 K for a P only controller and reduces the DSS to null set for PI control with integral times of 2 and 0.75 when operating at 460 K.

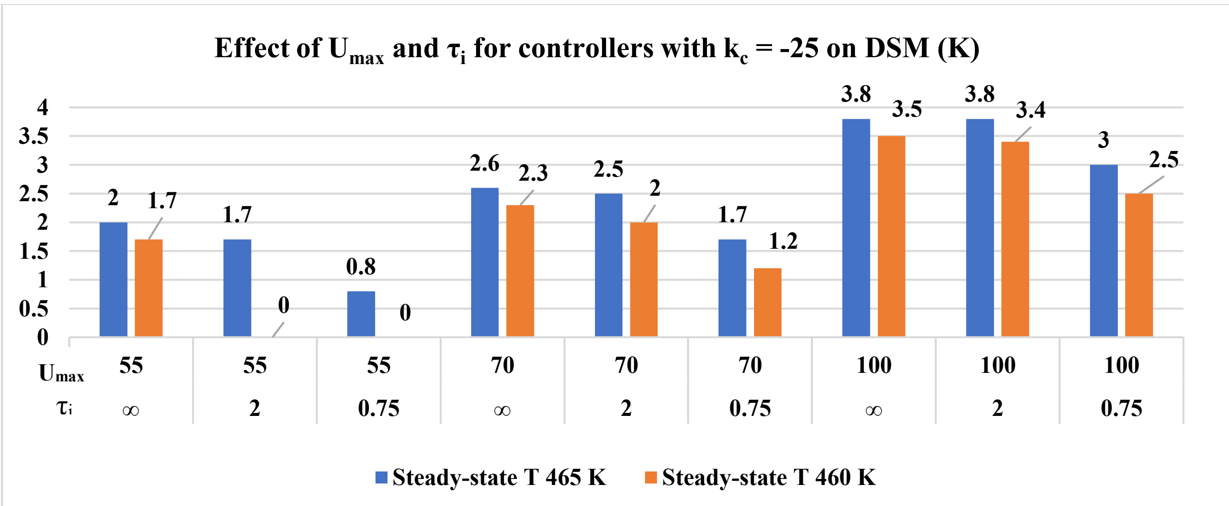


Figure 19: The DSM in units of reactor temperature (K) for [U_{max}] ={55, 70, 100}, with disturbance input included for P and PI Controllers with k_c = -25 and [τ_i]= {∞,2, 0.75}

Figure 20 shows the DSM for different controller gains and integral times for a fixed U_{max} when operated at 460 and 465 K steady states. Although, lower negative k_c and higher τ_i favors larger DSM, it is accompanied by a compromise in controller performance. That is, high negative gains can decrease the offset when using a P controller and provide faster response with zero offset when using a PI controller. The lower the integral time, the faster will be the elimination of the disturbance effects. However, very low integral times will result in unfavorable oscillatory behavior. The times responses for system with 0.75 integral time, shows such oscillatory behavior for the system operating at 460 K under a persistent disturbance of 20 K in T_0 as well as an initial impulsive disturbance of 2.5 K in T in Figure 21. Figure 22 shows the effect of using a PI controller with a higher integral time τ_i of 5 for the same disturbances, with no oscillatory behavior.

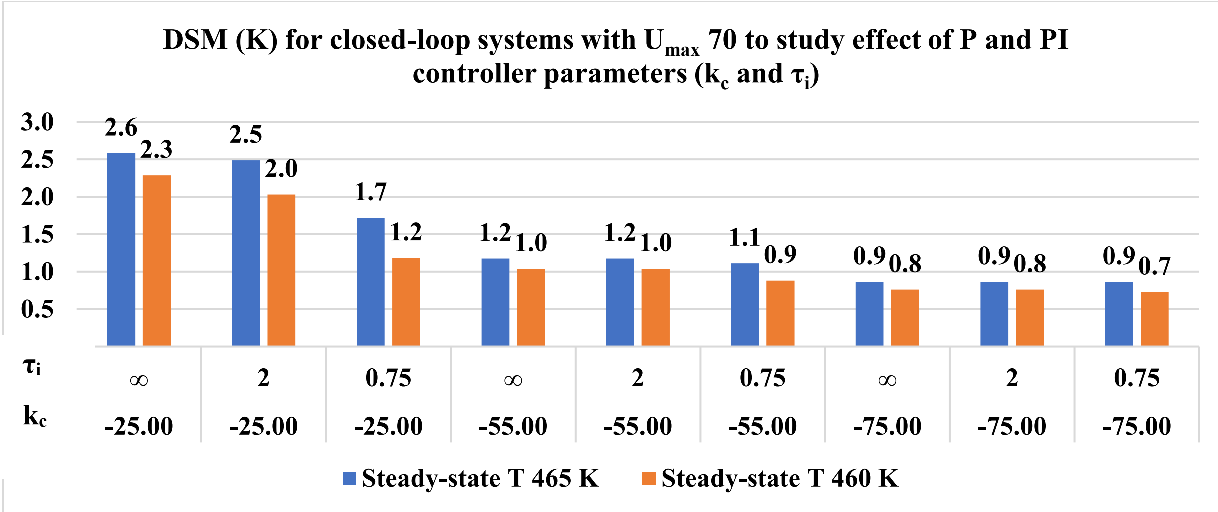
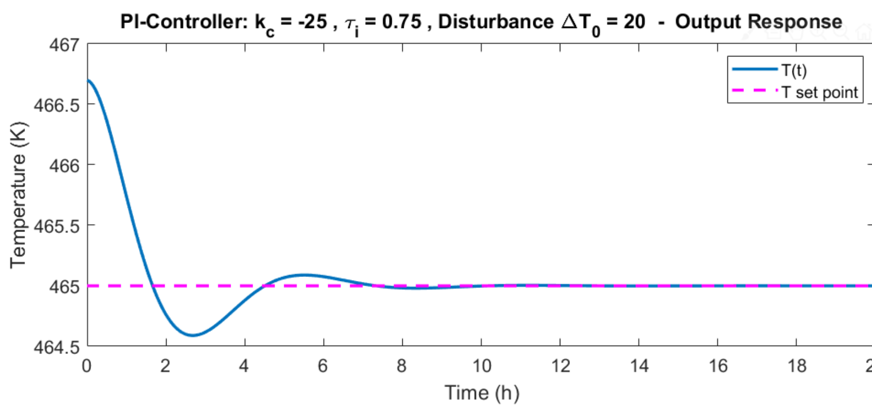
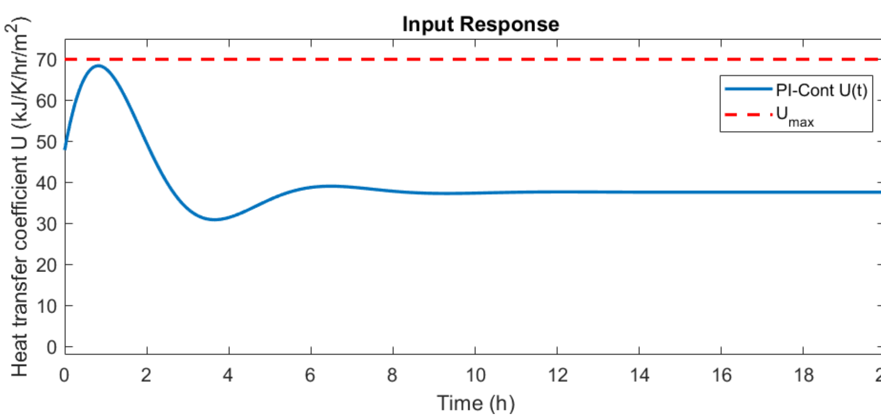


Figure 20: The DSM in units of reactor temperature (K) for U_{max} 70, with disturbance input included for P and PI Controllers with $[k_c]=\{-25, -55, -75\}$ and $[\tau_i]= \{2, 0.75\}$

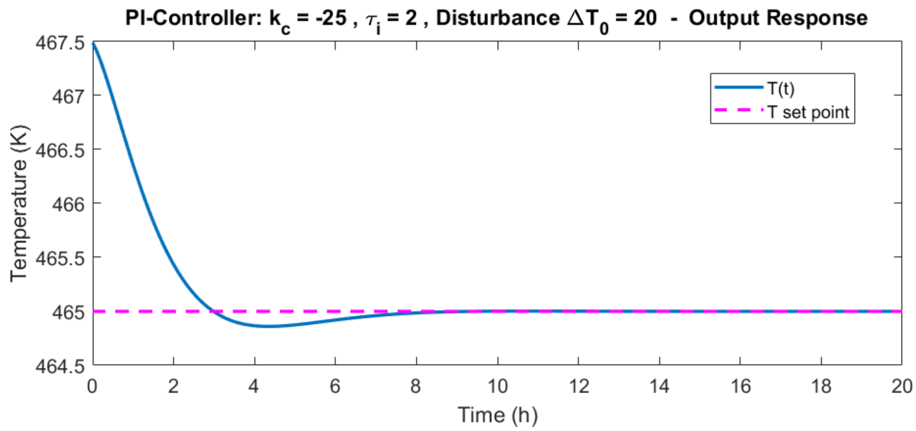


(i). Output response

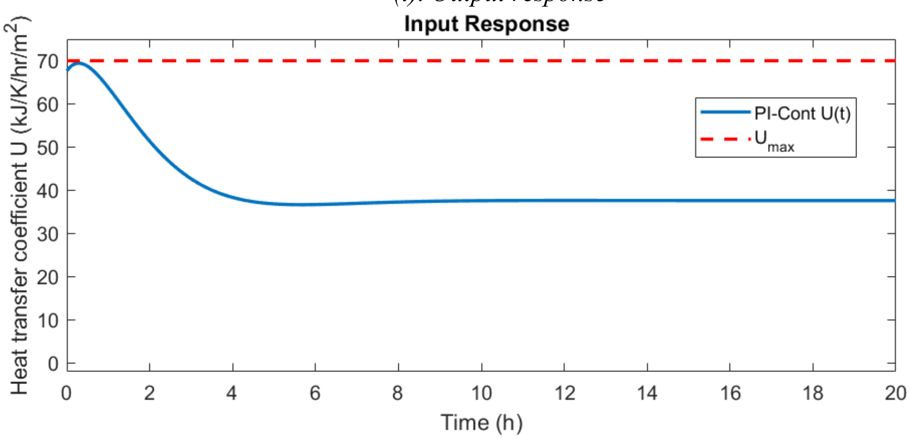


(ii). Input response

Figure 21: (i). Output response T(t) and (ii). Input response U(t) to a +20 K step disturbance in T_0 and initial impulsive disturbance that shifts T by 1.7 K. The PI-controller based closed-loop system with k_c of -25 and τ_i of 0.75 operating at 465 K.



(i). Output response



(ii). Input response

Figure 22: (i). Output response T(t) and (ii). Input response U(t) to a +20 K step disturbance in T_0 and 2.6 K initial impulsive disturbance in T. The PI-controller based closed-loop system with k_c of -25 and τ_i of 2 operating at 465 K.

The Table 2 below summarizes the results obtained for various U_{max}, k_c and τ_i for both P and PI control strategies. The results are shown for operating points 460 and 465 K operating points with disturbance input included. The DSM lies between 0 and 3.8 for the grid of design parameters investigated. As mentioned before, the margins of this range are low, but reasonable as it accounts for process dynamics under the possibility of sudden and adverse disturbances that were deliberately chosen as a representative of severe abnormal scenarios. In this paper, it is assumed that process should handle deviations in temperature up to +/- 2 K, that is, a minimum DSM of 2 K. As there are offsets present with P-only controllers, they will not be recommended for this process. Finally, under the assumption that U_{max} is too expensive of a choice for heat exchanger design, some design recommendations are highlighted in Table 2 that makes sense in the context of process safeness criterion.

Table 2: DSM in units of reactor temperature (K) for various design configurations

Type	k_c	τ_i	U_{max}	Steady state T: 465 K	Steady state T: 460 K
				DSM (K)	
P-Only	-25.00	∞	55	2.0	1.7
P-Only	-55.00	∞	55	0.9	0.8
P-Only	-75.00	∞	55	0.7	0.6
P-Only	-25.00	∞	70	2.6	2.3
P-Only	-55.00	∞	70	1.2	1.0
P-Only	-75.00	∞	70	0.9	0.8
P-Only	-25.00	∞	100	3.8	3.5
P-Only	-55.00	∞	100	1.7	1.6
P-Only	-75.00	∞	100	1.3	1.2
PI	-25.00	5	55	2.0	1.5
PI	-55.00	5	55	0.9	0.8
PI	-75.00	5	55	0.7	0.6
PI	-25.00	5	70	2.6	2.3
PI	-55.00	5	70	1.2	1.0
PI	-75.00	5	70	0.9	0.8
PI	-25.00	5	100	3.8	3.5
PI	-55.00	5	100	1.7	1.6
PI	-75.00	5	100	1.3	1.2
PI	-25.00	2	55	1.7	0.0
PI	-55.00	2	55	0.9	0.7
PI	-75.00	2	55	0.7	0.5
PI	-25.00	2	70	2.5	2.0
PI	-55.00	2	70	1.2	1.0
PI	-75.00	2	70	0.9	0.8
PI	-25.00	2	100	3.8	3.4
PI	-55.00	2	100	1.7	1.6
PI	-75.00	2	100	1.3	1.2
PI	-25.00	0.75	55	0.8	0.0
PI	-55.00	0.75	55	0.7	0.0
PI	-75.00	0.75	55	0.6	0.0
PI	-25.00	0.75	70	1.7	1.2
PI	-55.00	0.75	70	1.1	0.9
PI	-75.00	0.75	70	0.9	0.7
PI	-25.00	0.75	100	3.0	2.5
PI	-55.00	0.75	100	1.7	1.6
PI	-75.00	0.75	100	1.3	1.2

These recommendations require further refining and optimization before choosing the final design. There is a need for another yard stick to evaluate the other performance criterion. Prescreening of steady states done in the previous subsection, guarantees a minimum reactant conversion of 85%. Since the system is exothermic in nature, the reactant conversion percentage increases as the operating temperature increases. This will lead to choosing 465 K as the most favorable steady-state. The PI controller based designs ensures there are not any offsets. The simulations show that there are not any oscillations observed in time responses for the integral times of 5 and 2 unlike for the integral value of 0.75. It is also assumed that the heat exchanger design with U_{max} of 100 kJ/K/hr/m^2 is too expensive of a choice. Based on the observations for the parameter grid analyzed, a final design that could be recommended for this case study is as follows:

Steady state temperature: 465 K
Heat exchanger design parameter (U_{max}): 70 kJ/K/hr/m^2
PI controller gain (k_c): -25
PI controller integral time (τ_i): 2

The above design parameters will be used in the next subsection for illustrating the reference governor concept.

5.2.3 Reference governor implementation using DSS for managing large set point changes during an upset scenario

The reference governor concept is implemented on this system to demonstrate its use in managing any sudden and large set point change that arise during abnormal events. It is illustrated for the system that is based on the final design recommended in the previous subsection. Figure 23 shows the DSS evaluated for the system operating at 465 K with a U_{max} of 70 kJ/K/hr/m^2 and a PI-Controller based closed-loop system with k_c of -25 and τ_i of 2. The 3 dimensional DSS shows the effect of the temperature set point on the DSS. From the figure, it can be inferred that the feasible and safe set points that can be handled by this system lie between 455 and 475 K.

During the event of a downstream upset scenario associated with a reactor effluent heat exchanger malfunction, it is required that the reactor operating temperature is decreased from 465 K to 457 K. In order to test the performance of the reference governor scheme in adverse conditions, the system is assumed to be under a persistent disturbance of 20 K in T_0, in addition to the downstream upset situation. The time responses of the output and input variables while using only a PI controller is shown in Figure 24. The time responses of the output, input and the reference governor parameter (K in eq. (28)) for the system with PI controller and the reference governor scheme is shown in Figure 25.

Figure 24 shows that the process runs with control input saturation for over 15 h before reaching the new steady-state. This is avoided in the case with the reference governor that eliminates the effect of disturbance while also taking the system to the new steady state in 10 h, without sustained input constraint violation. The control input responses from the two cases clearly demonstrate the benefits of using the reference governor to handle sudden and large set point changes.

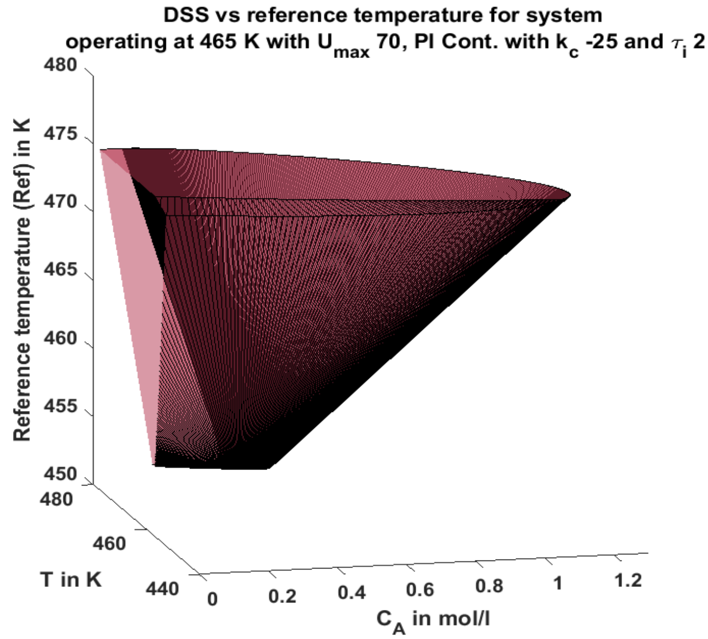
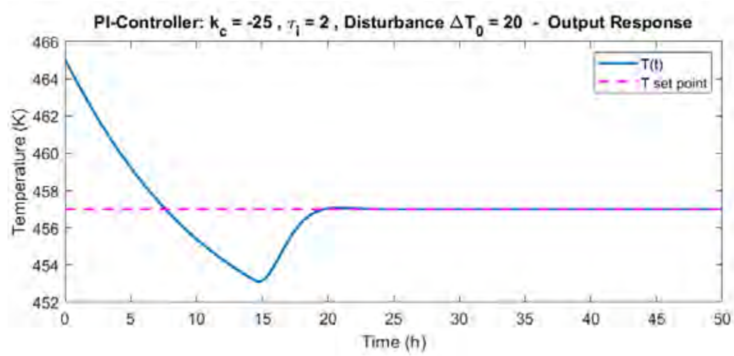
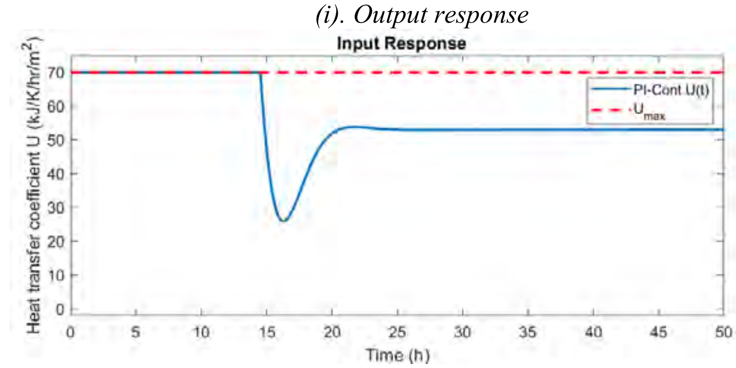


Figure 23: DSS for reference governor implementation. Process operating at steady state temperature of 460 K based on a PI controller with k_c -25, τ_i 2 and U_{max} 70.

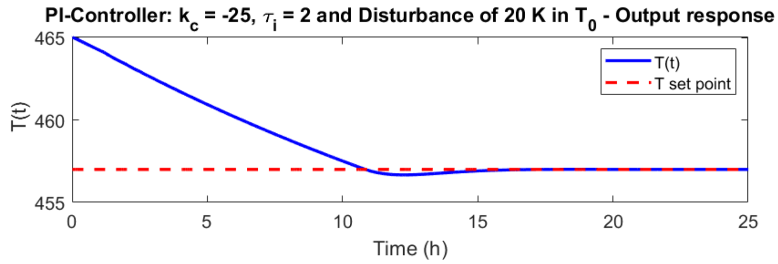


(i). Output response

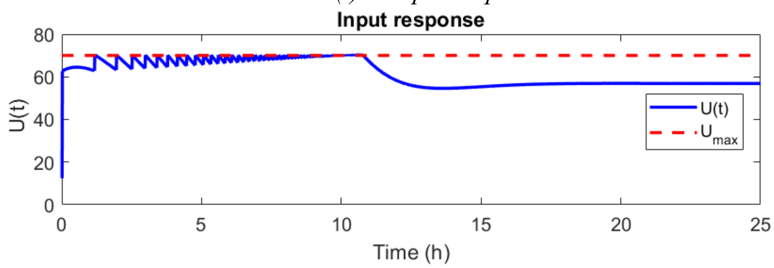


(ii). Input response

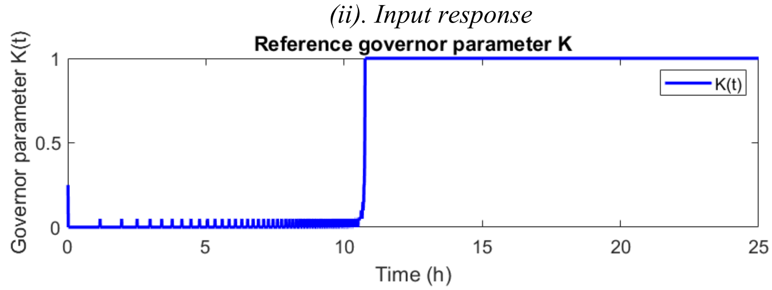
Figure 24: Set point change without reference governor. (i). Output response T(t) and (ii). Input response U(t) under a +20 K step disturbance in T_0 for the PI-controller based closed-loop system with k_c of -25 and τ_i of 2 operating at 465 K.



(i). Output response



(ii). Input response



(iii). Reference governor parameter K(t)

Figure 25: Set point change with reference governor. (i). Output response T(t), (ii). Input response U(t) and (iii). Governor parameter K(t) (in eq. (28)) under a +20 K step disturbance in T_0 for the PI-controller based closed-loop process with k_c of -25 and τ_i of 2 operating at 465 K.

6 Conclusions and future directions

An approach to design the process control system with safety as the primary target is proposed in this paper. The proposed approach explores an alternative perspective of safety-centered design as opposed safety as secondary considerations. The conceptualization of dynamic safe sets (DSS) and dynamic safety margins (DSM) and its application in control system are the key contributions of this paper.

The DSS is a collection of safe initial states that guarantee the satisfaction of safety constraints at present and future time instants, while also accounting for effects of unknown bounded disturbances. Existing theoretical concepts from systems literature were used to determine and evaluate the DSS that is an n-dimensional closed set. The DSM was conceptualized to quantify the size of the DSS that can be used to compare different designs. It is defined as the maximum radius of the n-dimensional ball centered at the steady state that completely lies within the DSS. The dynamic safety margin provides a measure of how resilient the closed-loop system is towards handling disturbances that are not accounted for, system faults and failures, measurement sensor noises and model uncertainties. An approach to design a maximally safe process control system based on the DSS and DSM concepts was proposed.

The proposed approach was tested on an exothermic CSTR as a representative example for systems with exothermic reactions with cooling system and control system. It was possible to select safe set point that provided a relatively larger dynamic safety margin. The steady state reactor temperature of 465 K was identified as the favorable set point for this case study. The dynamic responses of the process under disturbances validated the concepts as they could safely eliminate effects of both initial impulsive disturbances in reactor state variables and persistent disturbances in feed temperature. The DSM evaluated for the normalized states, provided insights on the resilience of the process towards other disturbances and failures that were not accounted for in the DSS calculations. The control system design affected the DSM significantly. It was seen that for P controllers, larger absolute values of gains that provided smaller offsets but reduced the DSM significantly. In one case, using a gain of -75 for a P-controller provided a DSM of 0.5 K, that is even a 0.5 K initial perturbation in reactor temperature could push the process to unsafe operation zone. For PI controllers, the DSM decreased with increasing integral action as expected. The final design recommendations were made such that the DSM (2 K in units of temperature) was acceptable, a reasonable controller performance (no oscillatory behavior) was attained and cooling system U_{max} was realistic and affordable. The reference governor scheme also helped in enhancing process safety for dealing with abnormal situations that demand sudden large set point changes in the process. The time responses under downstream upset scenario showed superior performance when compared to the process without reference governor. The use of reference governor avoided sustained constraint violations and provided relatively quicker response.

In the future, DSS applications in other areas of plant design and operation will be explored. A potential application of the DSS envisioned is in process monitoring once the control system design and reference governor scheme have been implemented. The DSS can be integrated with the alarm system to alert the operator when the process lies outside of the safe set. This will allow for the operator to troubleshoot and take proactive measures to prevent the process from violating constraints. The system faults not accounted for while designing, such as sensor faults, actuator faults and equipment unavailability, can be included in the form of additional constraints. The dynamic safe sets evaluated for the different faulty scenarios can be coupled with a fault diagnosis system to automatically update the DSS.

The concept of safety margin is used in several engineering disciplines and sometimes mandated by law to adhere to safety margin standards. For example, a scale factor of 11 is used for elevators and a factor of safety of 2 is used for each structural member in building construction. It would be useful if there could be some design specifications on safety margins that is developed for chemical processes. The DSM is a quantitative and dynamic measure of characterizing safety performance that has the potential to be viewed as *the margin* for chemical processes. In future, the proposed approach will be applied to several chemical engineering systems that are safety critical to develop specific design specifications for DSM. Potential systems for investigations include, polymerization reactors and large-scale plants often used as test beds by the control academic community [26-28]. The results from these investigations will be used to develop fundamental engineering guidelines for safety-centered process and control system design.

7 References

1. Mannan, M.S., S. Sachdeva, H. Chen, O. Reyes-Valdes, Y. Liu, and D.M. Laboureur, *Trends and Challenges in Process Safety*. 2015. p. 3558-3569.
2. Willey, R.J., *Layer of Protection Analysis.* Procedia Engineering, 2014. **84**: p. 12-22.
3. Pasman, H.J., S. Jung, K. Prem, W.J. Rogers, and X. Yang, *Is risk analysis a useful tool for improving process safety?* Journal of Loss Prevention in the Process Industries, 2009. **22**(6): p. 769-777.

4. Mannan, S., *Lees' Process Safety Essentials : Hazard Identification, Assessment and Control*. 2013, Oxford, UNITED STATES: Elsevier Science & Technology.
5. Halim, S.Z., S. Janardanan, T. Flechas, and M.S. Mannan, *In search of causes behind offshore incidents: Fire in offshore oil and gas facilities.* Journal of Loss Prevention in the Process Industries, 2018. **54**: p. 254-265.
6. Saada, R., D. Patel, and B. Saha, *Causes and consequences of thermal runaway incidents—Will they ever be avoided?* Process Safety Environmental Protection, 2015. **97**: p. 109-115.
7. Leveson, N.G. and G. Stephanopoulos, *A system-theoretic, control-inspired view and approach to process safety.* AIChE Journal, 2014. **60**(1): p. 2-14.
8. Qin, S.J. and T.A. Badgwell, *A survey of industrial model predictive control technology.* Control Engineering Practice, 2003. **11**(7): p. 733-764.
9. Darby, M.L. and M. Nikolaou, *MPC: Current practice and challenges.* Control Engineering Practice, 2012. **20**(4): p. 328-342.
10. Morari, M. and J.H. Lee, *Model predictive control: past, present and future.* Computers & Chemical Engineering, 1999. **23**(4-5): p. 667-682.
11. Albalawi, F., A. Alanqar, H. Durand, and P.D. Christofides, *A feedback control framework for safe and economically-optimal operation of nonlinear processes.* AIChE Journal, 2016. **62**(7): p. 2391-2409.
12. Albalawi, F., H. Durand, and P.D. Christofides, *Process operational safety using model predictive control based on a process Safeness Index.* Computers & Chemical Engineering, 2017. **104**: p. 76-88.
13. Ahooyi, T.M., M. Soroush, J.E. Arbogast, W.D. Seider, and U.G. Oktem, *Model-predictive safety system for proactive detection of operation hazards.* AIChE Journal, 2016. **62**(6): p. 2024-2042.
14. Gilbert, E.G. and K.T. Tan, *Linear systems with state and control constraints: The theory and application of maximal output admissible sets.* IEEE Transactions on Automatic control, 1991. **36**(9): p. 1008-1020.
15. Kolmanovsky, I. and E.G. Gilbert. *Maximal output admissible sets for discrete-time systems with disturbance inputs*. in *Proceedings of 1995 American Control Conference-ACC'95*. 1995. IEEE.
16. Gilbert, E.G., I. Kolmanovsky, and K.T. Tan, *Discrete-time reference governors and the nonlinear control of systems with state and control constraints.* International Journal of robust nonlinear control, 1995. **5**(5): p. 487-504.
17. Gilbert, E.G., I. Kolmanovsky, and K.T. Tan. *Nonlinear control of discrete-time linear systems with state and control constraints: A reference governor with global convergence properties*. in *Proceedings of 1994 33rd IEEE Conference on Decision and Control*. 1994. IEEE.
18. Gilbert, E.G. and I. Kolmanovsky, *Fast reference governors for systems with state and control constraints and disturbance inputs.* International Journal of Robust Nonlinear Control: IFAC-Affiliated Journal, 1999. **9**(15): p. 1117-1141.
19. Gutman, P.-O. and M. Cwikel, *Admissible sets and feedback control for discrete-time linear dynamical systems with bounded controls and states.* IEEE transactions on Automatic Control, 1986. **31**(4): p. 373-376.
20. Kolmanovsky, I. and E.G. Gilbert, *Theory and computation of disturbance invariant sets for discrete-time linear systems.* Mathematical problems in engineering, 1998. **4**(4): p. 317-367.

21. Hirata, K. and Y. Ohta. *The maximal output admissible set for a class of uncertain systems*. in *2004 43rd IEEE Conference on Decision and Control (CDC)(IEEE Cat. No. 04CH37601)*. 2004. IEEE.
22. Lombardi, W., A. Luca, S. Olaru, and S.-I. Niculescu. *State admissible sets for discrete systems under delay constraints*. in *Proceedings of the 2010 American Control Conference*. 2010. IEEE.
23. Wang, C. and C.J. Ong, *Constraint-admissible sets for systems with soft constraints and their application in model predictive control.* International Journal of robust nonlinear control, 2012. **22**(11): p. 1229-1243.
24. Manthanwar, A., V. Sakizlis, V. Dua, and E. Pistikopoulos, *Robust model-based predictive controller for hybrid system via parametric programming*, in *Computer Aided Chemical Engineering*. 2005, Elsevier. p. 1249-1254.
25. Choi, J., H.S. Ko, and K.S. Lee, *Constrained H∞ optimal control of chemical processes.* IFAC Proceedings Volumes, 2001. **34**(25): p. 591-595.
26. Ricker, N.L., *Decentralized control of the Tennessee Eastman challenge process.* Journal of Process Control, 1996. **6**(4): p. 205-221.
27. Ricker, N., *Optimal steady-state operation of the Tennessee Eastman challenge process.* Computers & Chemical Engineering, 1995. **19**(9): p. 949-959.
28. Venkidasalapathy, J.A., M.S. Mannan, and C. Kravaris, *A quantitative approach for optimal alarm identification.* Journal of Loss Prevention in the Process Industries, 2018. **55**: p. 213-222.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Finding Health & Safety Buried Treasure with AI

Thomas Garvin*, Scott Kimbleton
IBM
Houston, TX
*Presenters E-mails: twgarvin@us.ibm.com, kimbleton@us.ibm.com

Abstract

The challenge to glean understanding and insight from an array of historical safety-related reports and observations has existed since the dawn of the HSE discipline. While most organizations today use traditional methods to analyze past events and activities along structured elements (time, place, risk rating and so on), a vast amount of wisdom around hazard identification, root causes and risk control measures remains buried in textual descriptions and reports, and teachable moments become lessons lost.

The hands and minds that developed these textual artifacts may be among the most seasoned in the organization, bringing years of experience to bear on the issues and opportunities involved. Such artifacts are then clearly buried treasure. Exploring and surfacing the insights contained in artifact repositories calls for new tools. Using these, a new type of H&S performance indicator could emerge: latent indicators, lying concealed within the written record, offering as much or more value as the leading and lagging indicators used today.

This paper describes leveraging the power of artificial intelligence (AI) to absorb large amounts of safety-related textual information, find common themes and identify similar events, which are then analyzed for patterns in causes and controls. This solution, used in concert with traditional analytics, offers unprecedented power to comprehend and visualize collective safety knowledge from historical record. Transforming words to wisdom in this manner not only illuminates the past but also provides a basis for actioning improvements in operational excellence.

Keywords: Safety, Hazards, Risk Assessment, Investigation, Lessons Learned, Observations, Bowtie, Integration with Operations

1 What is AI?

Artificial Intelligence (AI) is both a powerful and a misunderstood technology. An AI system can be characterized by four key behaviors:

- Understanding: Making sense of images, language and unstructured data through human tutoring
- Reasoning: Grasping underlying concepts, forming hypotheses, inferring ideas
- Learning: New data, interactions and outcomes are automatically added to its knowledge foundation so that further interactions are improved
- Interacting: Listening to, interpreting and conversing with humans in a natural way

Rather than defining any particular software platform, or programming language, AI has evolved rapidly in a very short number of years to comprise a suite of services that represent a number of distinct behaviors, which when integrated are intended to perform a very specific function. Figure 1 display a diagram with several of these services depicted.

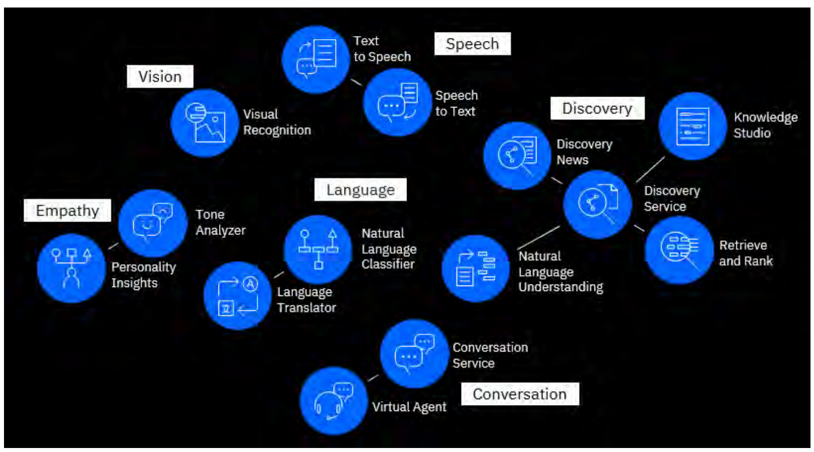


Figure 1 - AI-related services

Without going into the technical details of these services, one could easily surmise by the above selection that they are targeting particular human artifacts – spoken language, written word, penned drawing. This is indeed the case, with the intention being to uncover meaning, relevance or sentiment, not only within one instance of such an artifact, but within large collections of such artifacts. That this is not only feasible but blindingly effective was demonstrated in 2011 when IBM’s Watson defeated the reigning Jeopardy champions, by analyzing the equivalent of about one million books and responding to Jeopardy questions in under three seconds [1].

AI itself can be considered a component of a larger landscape of modern technologies aimed at value-adding interactions with humans (see Figure 2 below). With today’s data deluge from more and more sources - internet-connected devices, social media, the digitizing of new organizations and even nations - such tools are invaluable for automating workflows, detecting anomalies, and analyzing the numerous forms of evidence of modern human existence. Make no mistake – such tools are not nearly capable of replacing humans at this stage, but clearly they are "force multipliers" for assimilating data and exploring for treasure (insights).

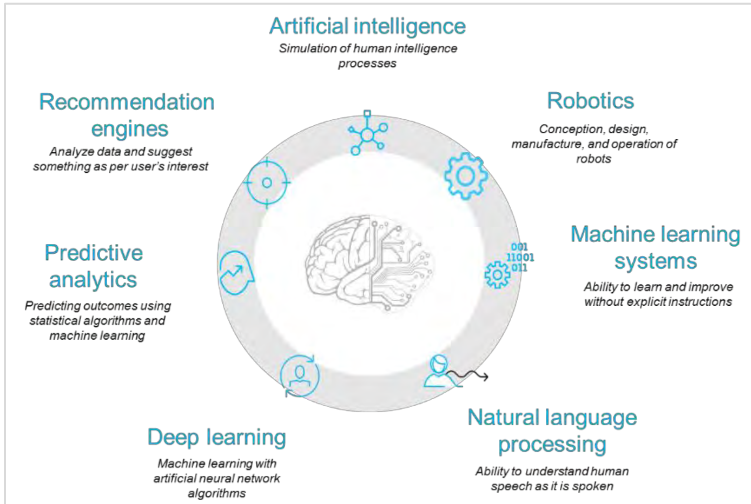


Figure 2 - AI universe of emerging technologies

2 What are the Benefits of AI in HSE?

Most of the valuable information in the world today exists in an unstructured form; by some estimates, 80 to 90 percent [2]. In addition, the growth rate of the information universe has been said to be exponential, doubling every 12 months [3]. Without a fast and effective means to explore this expanding universe, one can get a sense of falling behind the pace and failing to leverage the wisdom and insights buried within, expressed in unstructured forms. Some have used the appropriate term "dark data" to describe this buried treasure, which remains hidden due to the limitations of traditional analytical tools and techniques.

The Health and Safety domain is awash in unstructured data sources. Internal documents such as incident investigations, safety observations, risk assessments, hazard studies and the like exist everywhere, and go back years in time; even our treasured incident reporting databases, primary sources of HSE performance indicators, contain important textual observations and lessons learned which are all but invisible to traditional analytical methods.

Extracting the buried treasure from these resources calls for new technologies and approaches, in order to surface the hidden insights and discover undiscerned patterns that may be "hiding in plain sight". While text analytics has been around for some years as a tool for probing unstructured data, AI has evolved into a much more powerful approach for understanding meaning and context, both within unstructured data and from the querying human analyst, expressed in natural language. Gartner has used the term "augmented analytics" to describe this new approach, defining it as "a next-generation data and analytics paradigm that uses machine learning to automate data preparation, insight discovery and insight sharing" [4]. In a subsequent paper, Gartner predicted "By 2020, augmented analytics will be the dominant driver of data and analytic systems" [5].

Numerous advantages can be seen in leveraging AI in the HSE domain. Among them:

- Time and effort savings: HSE analysts and others spend a large amount of time on investigations, audits and studies, poring over past incident reports and other artifacts to find specific bits of information from textual entries. This type of exercise is repeated for each new study or research request. An AI solution trained to recognize key elements within unstructured text such as hazard conditions, activities, equipment, materials and so on, can illuminate such elements within hundreds or thousands of documents in seconds. In addition, an AI solution can gather the set of key concepts within one document (such as an incident report), and search an entire document repository to find reports similar in thematic content, returning those documents in order of relevance. The value of near-instant identification of incidents similar to one being investigated is difficult to overestimate for the analyst/auditor.

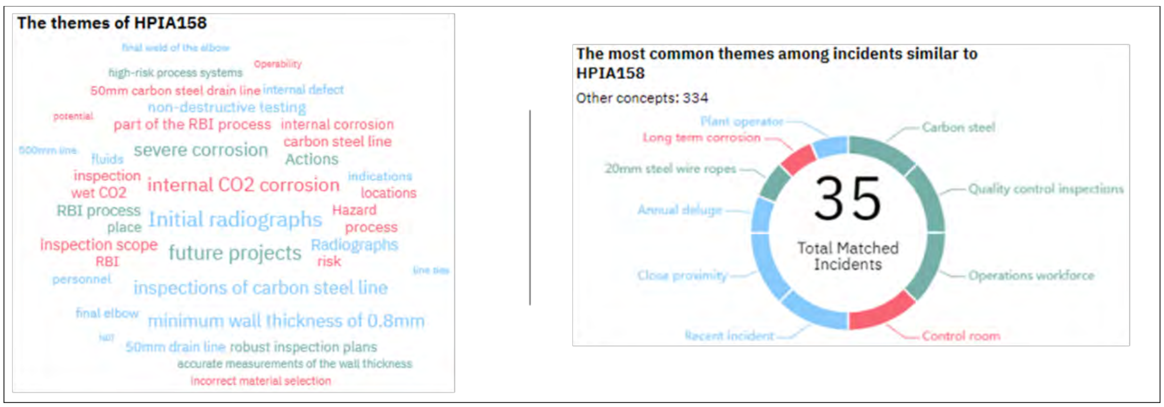


Figure 3 - Example search results from an AI query for similar incidents, illuminating key concepts and common themes. Incident Report source: APPEA [13]

- Scaling expertise: An AI solution targeted for use in a specific domain such as HSE must be trained in the key concepts, terms and important elements pertinent to that domain, so that they can be recognized within reports and other documents. Training is done by subject matter experts (SMEs), and the AI solution grows in competency and accuracy with continued training and analysis of more and more documents. Whereas traditional software tools encapsulate knowledge of "how" to perform certain tasks, with myriad subroutines and calculations, an AI solution encapsulates the "what" – the key elements imparted by SMEs, which enable the solution to find those elements, interpret meanings and even identify new concepts. AI both preserves and scales knowledge of a handful of SMEs across an entire organization, especially when distributed via an enterprise-wide medium such as the cloud.
- Finding Lessons Lost: Operating companies often internally broadcast specific incident reports and outcomes with the hope that the lessons contained within will be absorbed and retained by all. With today's information overload and dynamic properties, many such missives do not make it to the top of the stack; staff and contractor turnover can also contribute to the lessons being lost over time. Safety alerts and broadcasts may also be confined to business unit or even site battery limits. Corporate centralized databases for

lessons learned are clearly a step in the right direction for establishing a knowledge repository, but these may be subject to the same constraints as traditional relational databases, with limited search capability. Moreover, such internal resources do not tap into the wealth of lessons and insights available in publicly-available repositories such as those supported by BSEE, IOGP, APPEA and many others. An AI solution is able to explore both internal and external information sources and illuminate the key elements within, automating and accelerating insight discovery

- Accelerated time-to-value: Numerous points along the value creation chain for analyzing HSE information are accelerated with an AI solution. The typical process includes data location and gathering, cleansing and loading, followed by analysis and presentation. Once pointed at an information resource, an AI solution can reduce data exploration and discovery of buried insights to near-real-time, which in turn enables faster time to actioning the discovered insights. An indicative example of AI's instant transformation of unstructured data to insights is shown in Figure 4 below, with the bowtie report illustrating a set of entities recognized by the AI model (Causes, Controls, Hazards, Activities etc.).

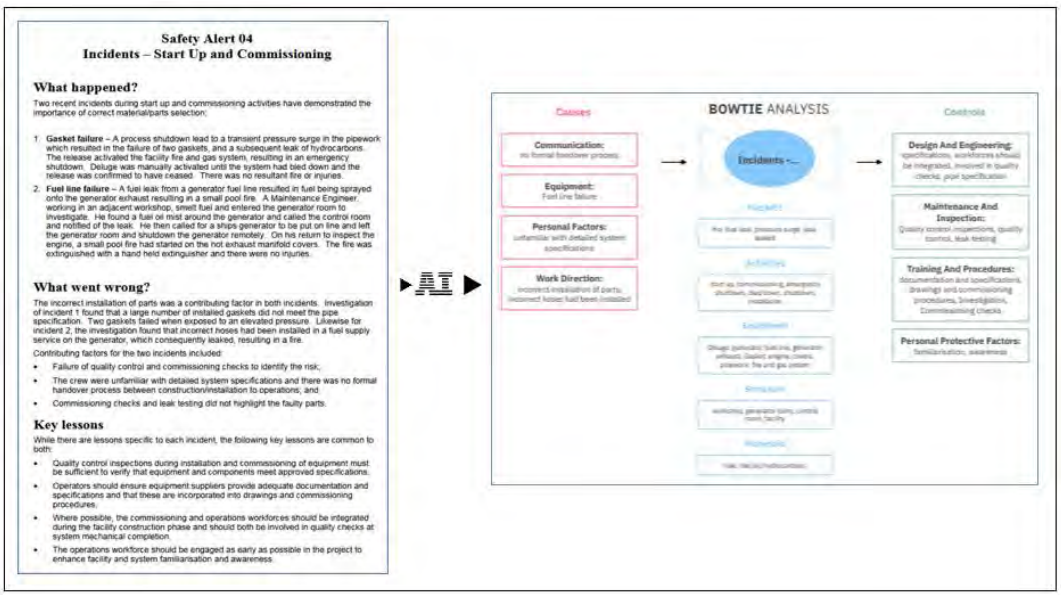


Figure 4 - Example of insight extraction from an incident report by an AI model for HSE. Incident Report source: NOPSA [14]

3 Future Value

Surfacing new insights: An AI tool able to understand natural language structure and concepts can leverage this ability with domain-specific information sources to identify safety themes and patterns which may go unnoticed by HSE analysts. For example, in a recent trial, a model trained to recognize "inspection" and "testing" as two risk controls, automatically identified the phrase "Incomplete inspection and testing regime" as a causal factor within an incident report. In another example, a model trained on hazardous conditions in the natural resources industry but no specific training on medical risks or symptoms of deep vein thrombosis, correctly identified both "blood clot" and blood pooling as hazard conditions in long-haul flights, as a result of context understanding. Similarly, this model is being extended to recognize a "malware infection" as a hazard in the cybersecurity space, "food poisoning" from the galley of an offshore platform, and a "rockfall" in mining.

Asking new questions: The value of an AI solution originates from its ability to understand unstructured data, and interpret unstructured queries. The "naturalness" of this approach is the opposite of traditional software solutions, which depend heavily on pre-defining and storing discrete data elements. The latter approach constrains the types of queries against that data, as they are limited to the pre-defined parameters, and therefore the types of analyses are also bounded. The AI approach allows much more flexibility in analysis, and responds easily to questions that are difficult if not impossible to ask of traditional systems – for instance, "Find incidents dealing with poor risk assessments in lifting operations", or "which sites have the most number of incidents where training is mentioned as a risk control". An AI solution empowered with the ability to recognize activities, risk controls, equipment and other items greatly expands analytical capabilities and the ability to ask more questions.

Discovering latent indicators: The majority of today's incident reporting solutions are geared to be backward-looking, focusing on the details of what happened, and the causes. They are most appropriate for use with lagging indicators, which are reactive in nature. For leading indicators, the focus is typically on planned versus actual activities and other targets or expectations, which, when not met, may increase risk or the probability of incident occurrence. Leading indicators are typically used as preventive measures. To be truly forward-looking and more predictive in our assessments of future risk, we need a more holistic understanding of our past safety incidents combined with the past wisdom of the experts involved who left advice for future incident prevention. This is the realm of *latent indicators*: the underlying and evidential patterns of behavior, situations, or conditions occurring over time that present clear and present risk for an enterprise. Such indicators can be site-specific, regional or enterprise-wide; at any level, the discovery and addressing of these hidden characteristics could enable more proactive incident prevention and lead to improved safety statistics. Given their predictive nature, latent indicators could better equip operations and maintenance functions with improved risk assessment capability in future work.

4 Finding YOUR Treasure

There are many approaches a company may take on its journey to becoming a "cognitive enterprise", one which infuses concepts such as AI and machine learning throughout its internal functions, and exploits to competitive advantage its vast data "natural resource" in all its myriad forms. In such an enterprise, technology is often the easy part – the cognitive enterprise incorporates organizational components such as a top leadership vision of scaled intelligence, to re-engineered internal workflows, to “citizen data scientist” knowledge workers driving innovation. In order to execute a successful cognitive journey, a carefully thought out journey management plan is mandatory, which considers key elements such as starting position, competencies, risks and resolve to reach the destination. From an AI project perspective, one possible path is outlined below in three key steps, with a set of five attributes to consider in each.

1. **Proof of Value** – set the example for AI value with a strong use case
   a. Business value: be able to demonstrate clear business value and ROI
   b. Tight use case: define clear scope boundaries and expectations
   c. Success criteria: make it clear what success looks like
   d. Proven technology: Don’t go for the bleeding edge, which could introduce project or sustainability risks
   e. Good data: Assure the quality, availability and richness of your data source

2. **Pilot Program** – establish a scalable foundation
   a. Capability assessment: Perform an honest assessment of internal AI competencies
   b. Data sources: Identify additional data sources supporting the value case
   c. Infrastructure: Establish a scalable technical foundation
   d. Resourcing: Onboard project team and dedicate subject matter experts
   e. Advertise: Promote the project across functions and business lines

3. **Enterprise Launch** – execute a formal implementation campaign
   a. Leadership resolve: assure top line support and advocacy
   b. Education plan: promote training in AI value exploration and publish lessons learned
   c. Deployment trajectory: set realistic rollout goals, considering business readiness, data quality, resource availability and program sustainability
   d. Change management: be mindful that organizational impacts of AI and human factors must be considered; new ways of working and modified functional integrations can result
   e. Ground support: establish both a technical support team and a business-facing center of excellence

5 AI Successes

Business interest in AI has grown tremendously over the past few years, in concurrence with the maturity, accessibility and advances in the technology. It also coincides with the rise of “big data”, and the perception that AI is a necessary tool for gleaning insights from the staggering amount of data now being generated across the globe. According to some estimates, by next year we will see the equivalent of 1.7MB of data generated every second for every person on earth [6]. The rise in interest is not limited to business – a Google search for “AI arms race” produces over 100,000 hits, finding recent articles from notable publications such as Foreign Policy, Wall Street Journal, and

Financial Times describing billions of dollars being spent by China, Russia and the US toward national AI strategies.

In the HSE domain, there have been several success stories over the years. Most recently, Woodside Energy was awarded in 2018 by both the Australian Petroleum Production & Exploration Association (APPEA) and Institute of Chemical Engineers (IChemE) for its innovative implementation of IBM's Watson AI platform in HSEQ. The safety solution is used across the company for scanning hundreds of thousands of documents for past insights, aiming for improved hazard identification and risk assessments in operations and capital projects [7, 8].

The rail transportation industry has been keenly interested in detailed analysis of safety information. In the UK, the Rail Safety and Standards Board (RSSB) has taken particular interest in machine learning and its value propositions for automated classification and analysis of safety-related records, automating inspection and predictive maintenance, and improved operational performance [9]. RSSB and the Institute of Railway Research have worked jointly on a program termed Big Data Risk Analysis (BDRA). One of the primary data sources utilized in this program is RSSB's Close Call System, a centralized repository of text-based close call (near miss) incident reports. The "Learning from Close Calls" project under BDRA developed a natural language software program for automatically analyzing free text entries [10].

In the aviation field, NASA's Aviation Safety Program and the System-wide Safety and Assurance Technologies (SSAT) project have developed text analytics for scanning hundreds of thousands of safety reports and logs looking for hidden patterns which could lead to better understanding of incident precursors. Their efforts have been recognized and incorporated by several major carriers, as well as the Federal Aviation Administration [11].

6 Summary

Like any expedition setting out to uncover buried treasure, the deployment of an AI solution for HSE must be methodically and purposefully planned. The treasure is certainly out there – we would not go to such great lengths to develop detailed incident investigations, record HAZIDs and HAZOPs and compile lessons learned if capturing critical safety information and insights was not the goal. In a slower-moving world where workers retained the lessons, businesses retained the workers, and technology was relegated to numbers, advanced mining of unstructured data was not considered a necessity. But business velocity has changed significantly, and data of all kinds is considered by some to be the world's most valuable business resource [12]. Exploring data for insights buried within unstructured data is not only possibly today, but is all but impossible without AI, in order to assimilate the vast space and maintain pace. "AI-power" must now be considered along with manpower to find the buried treasure efficiently, and scale corporate knowledge effectively.

7 References

1 IBM, "A Computer Called Watson", https://www.ibm.com/ibm/history/ibm100/us/en/icons/watson/

2 Griffith, Eric. 90 Percent of the Big Data We Generate Is an Unstructured Mess. PC Magazine, 15 November 2018. https://www.pcmag.com/news/364954/90-percent-of-the-big-data-we-generate-is-an-unstructured-me

3 Kambies, Tracie; Roma, Paul; Mittal, Nitin; Sharma, Sandeep Kumar. Dark analytics: Illuminating opportunities hidden within unstructured data. Deloitte, Tech Trends 2017, 7 February 2017. https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/dark-data-analyzing-unstructured-data.html

4 Salam, Rita L.; Howson, Cindi; Idoine, Carlie J. Augmented Analytics Is the Future of Data and Analytics. *Gartner, Inc.*, 27 July 2017.

5 Cearley, David; Burke, Brian. Top 10 Strategic Technology Trends for 2019. *Gartner, Inc.,* 15 October 2018.

6 Ahmad, Irfan. How Much Data Is Generated Every Minute? Social Media Today, 15 June 2018. https://www.socialmediatoday.com/news/how-much-data-is-generated-every-minute-infographic-1/525692/

7 APPEA, "Smart safety systems earn Woodside an APPEA Award". 17 May 2018. https://www.appea.com.au/media_release/smart-safety-systems-earn-woodside-an-appea-award/

8 Woodside Energy, "Hats off to Watson". 1 November 2018. https://www.woodside.com.au/news-and-media/stories/story/wins-for-watson-for-hseq

9 RSSB, "Machine Learning and its value proposition for the rail industry". 8 November 2018. https://www.rssb.co.uk/Insights-and-News/Blogs/Machine-Learning-and-its-value-proposition-for-the-rail-industry

10 Rail Technology Magazine, "Big data risk analysis for rail". 1 March 2015. http://www.railtechnologymagazine.com/Comment/big-data-risk-analysis-for-rail

11 Marshall, Patrick. NASA applies deep-diving text analytics to airline safety. Government Computer News, 26 October 2012. https://gcn.com/articles/2012/10/26/nasa-applies-text-analytics-to-airline-safety.aspx

12 The Economist, "The world's most valuable resource is no longer oil, but data". 6 May 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

13 Australian Petroleum Production & Exploration Association. https://www.appea.com.au/wp-content/uploads/2014/06/High-Potential-Incident-Alert-158-Wall-thickness-loss-gas-compression-shutdown.pdf

14 National Offshore Petroleum Safety Authority. https://www.nopsema.gov.au/assets/Safety-alerts/Alert04.pdf

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Smart machine learning analytic tools for alarm rationalization

Tongwen Chen, Wenkai Hu, and Sirish L. Shah*
University of Alberta, Edmonton, Alberta, Canada
Presenter E-mail: sirish.shah@ualberta.ca

Abstract

This talk will present a new set of machine learning analytic tools that cohesively analyze alarm data, sensor (process) data and process connectivity information to provide a holistic view of the process. These data-based tools allow engineers to systematically carry out process and performance monitoring plus alarm design, monitoring and rationalization.

Recently updated industry standards (EEMUA 191 and ANSI/ISA 18.2) suggest that an operator should not receive more than six alarms per hour during the normal operation of the plant. This is, however, rarely the case in practice. Various studies show that the number of alarms each operator receives is far more than the standard (tens and even hundreds of alarms per hour, depending on the industry and their alarm generation policy); a majority of these are false or nuisance alarms. Too many false/nuisance alarms (alarm flooding) distract the operator from operating the plant and can bury important alarms. Industries reportedly lose millions of dollars every year due to alarm problems. As a result, there has recently been an increasing interest in industry to address this issue and seek systematic remedies to reduce the number of false and nuisance alarms.

This talk will present industrial case studies on the application of a new analytics toolbox that includes data-based alarm rationalization tools to reduce the number of false and missed alarms, identify and detect sources of alarm floods and thereby help processes become compliant to new industrial standards. Industrial case studies will be presented to show the efficacy and utilitarian value of the newly developed machine learning algorithms embedded in the analytics toolbox.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Opportunities and challenges of high-level visualization technology in process operations and safety

Shawn Bayouth *[a], Matthew E. Harvey [b, c], and Nir Keren *[b, c]
[a] Department of Disaster Preparedness and Emergency Management, Arkansas State University
[b] Department of Agricultural and Biosystems Engineering, Iowa State University
[c] Virtual Reality Application Center, Iowa State University
*Presenter E-mails: sbayouth@astate.edu, nir@iastate.edu

Abstract

The rapid development in high-level visualization technology in recent years has created tremendous opportunities for enhancing all facets of industry. Augmented reality (AR), mixed reality (MR), and virtual reality (VR) can be harnessed to support efforts in various stages of a life cycle of a facility. For example, AR technology can be utilized in the fabrication stage as well as in the validation and operation stages of the life cycle. MR can support efforts during fabrication, operation, and decommissioning stages. VR can be used in various dimensions of all stages of the life cycle.

This paper will review the forefront of technology of high-level visualization and will discuss the opportunities and challenges associated with this technology with respect to its implementation in the process operations and safety arena.

Keywords: Augmented reality, Mixed Reality, Virtual Reality, Process operations, Process safety

Introduction

Exponential increase in computational powers in recent years opened doors for evolvement of high-level visualization and its utilization in workforces. The term Extended Reality (XR) refers to a continuum presented in Figure 1. The continuum is composed of three segments of visualization technologies titled Augmented Reality, Mixed Reality, and Virtual Reality.

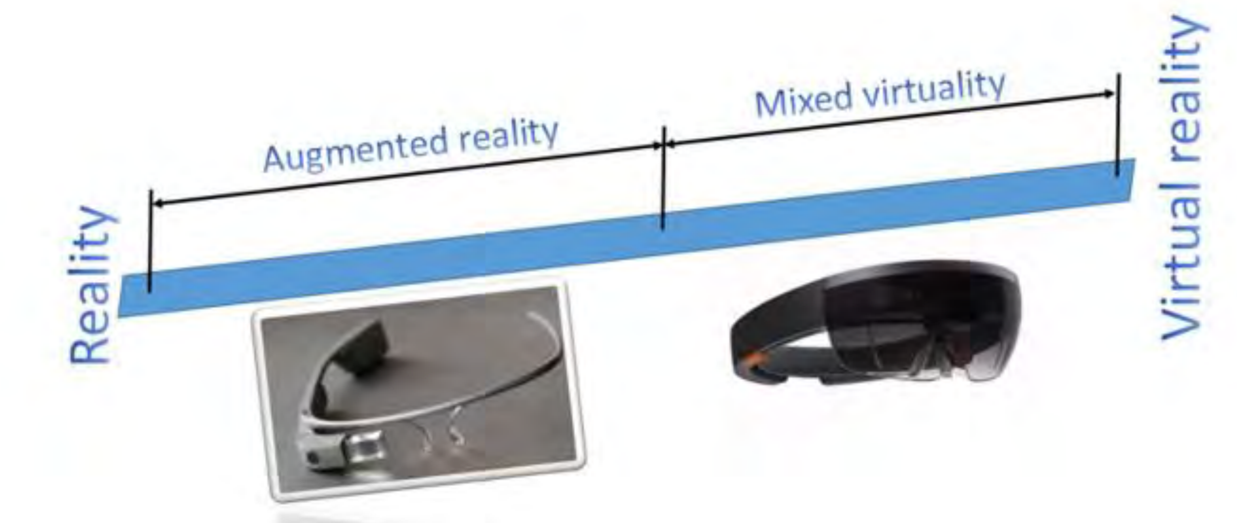


Figure 1. Reality-Virtuality continuum.

Augmented Reality (AR) is a platform that augments the real environment with digital data, allowing the user to seamlessly interact with these data and images. Cars, where GPS information is projected to the vehicle's windshield are facilitating AR technology.AR can be facilitated on mobile devices such as smartphones and tablets and on other computing platforms.

Mixed Realty (MR) are platforms that are anchoring 3D passive or dynamic holograms in the perceptual real environment. Once anchored, we forget that they are holograms and related to them as they are part of the environment. As with AR, MR can be facilitated on mobile devices such as smartphones and tablets. However, MR Head Mounted Devices (HMDs) provide enhanced control in locating holograms in the user's field of view and generate stronger sense of immersion. New generation of MR HMDs—such as Microsoft Hololense (Hololense 2, 2019) and Magic Leap (Magic Leap, 2019)— can operate as portable, standalone units. This facilitates functions that are more complicated when the HMD systems are connected to an external computing platforms such as laptops and desktops. Virtual objects may be anchored to real-world objects, allowing the user to interact with combined virtual/real objects.

Virtual Reality (VR) is a complete synthetically generated environment, where the user is isolated from reality and is immersed in a computer-generated realm. VR is the most used synthetic reality platform. The following sections further describe the technologies above and their use in the industrial arena.

Augmented Reality

Exhaustive review of literature, with respect to the utility of AR, identifys tremendous merit for AR technology, manufacturing, and maintenance (Palmarini et al., 2018)). Fiorentino et al. (2014) found the adding real-time information to operators' view has significant positive impact on the operators' perception of their environment. Scope AR (2018) points out that when operators used

AR, efforts for identifying proper maintenance steps dropped by more than 50% and the error rate dropped by more then 80%.

Schlueter (2018) explored the merit of using simplified visual-based AR content. This system would enable a remote specialist to create detailed AR content in real-time, and immediately deliver customized instructions to an on-site technician. His work also demonstrated that expert-assisted field maintenance can significantly reduce maintenance costs and errors.

Current challenges with AR are rooted in (1) the state of computational perception; (2) AR systems have limited computational power; (3) model-based recognition capabilities are very limited; and, (4) limited capacity of integration of artificial intelligence/machine learning to reduce cognitive load and dependency in third entity (remote expert).

Mixed Reality

In this section we refer to MR systems that are standalone HMDs systems, which allow interaction based on gaze, gestures, and vocal commands. MR utilizes two functions in order to implement the visualized MR:

(1) **Mapping the environment**: Once the MR platform mapped the environment it 'anchors' holograms in this environment and maintains its location fixed in the environment, independently of user's movement. MR platforms are preprogrammed to scan the environment and map them.

(2) **Recognizing shapes in the environment**: Recognizing objects and either representing them as holograms or implementing additional virtual holograms, that can be manipulated with respect to the physical objects, open the MR space for facilitating virtual, or remotely assisted operations.

Figure 2 presents a user operating a Microsoft Hololense MR system. Figure 3 presents the 'Recognition' feature of MR utilized to facilitated virtual guidance for assembly process.

Figure 2. Participant interacts with a Hololense system.

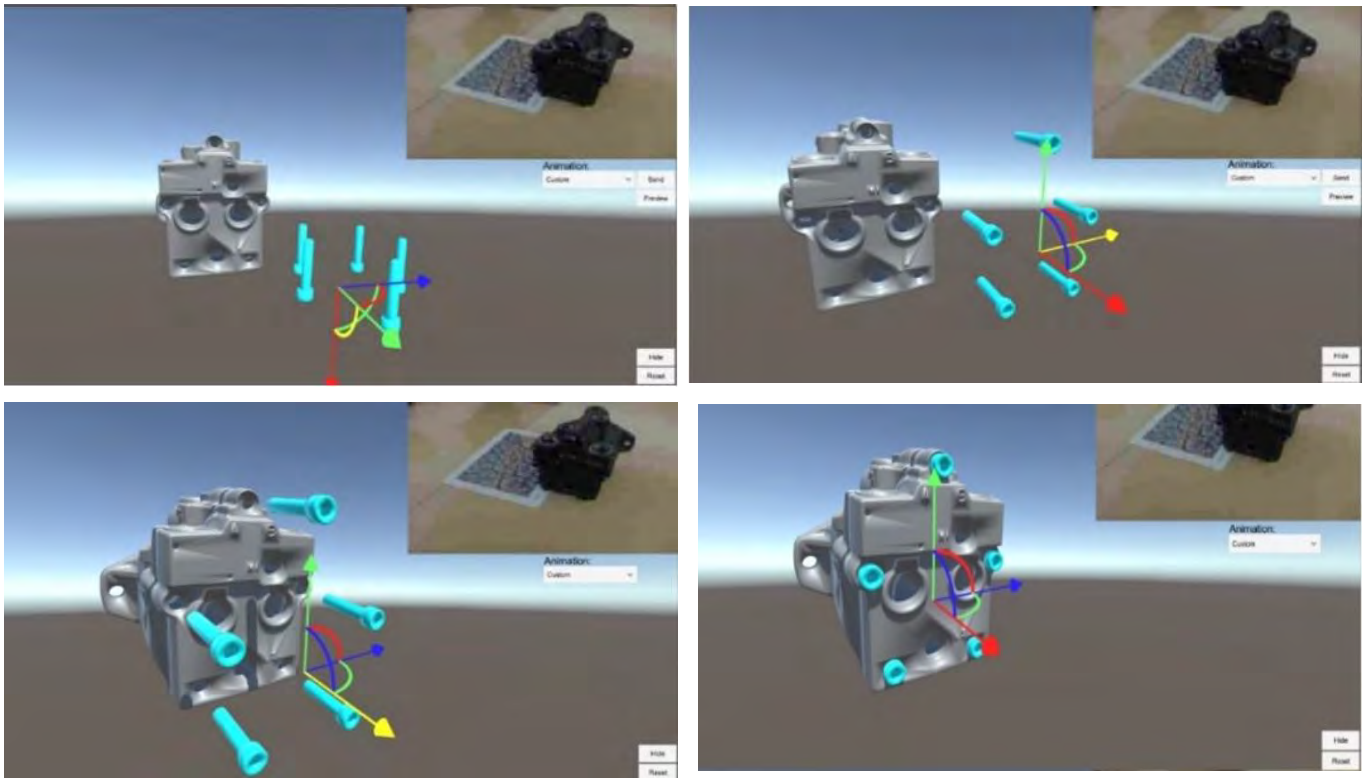


Figure 3[1]. Utilizing an MR platform for guided assembly.

While MR systems seem to have tremendous potential in industrial applications, their adoption is not as common.

Virtual Reality

VR is the most common synthetically generated environment in use. VR offers a multitude of facets that can be harnessed for various industrial applications. Due to its nature, VR disengages the user from his/her real environment and thus, by definition, excludes reality-connected applications from its scope.

VR systems span from room size VR facilities to HMD-based systems. Room size VR systems (Figure 4) allows multiple users to attend the environment simultaneously. HMD-based VR require developing specific applications that connect multiple users in the VR environment (VRE). The authors and their team developed a 3D, full-scale, highly interactive VR application titled Collaborative-VR (CVR) to allow multiple users to work in the virtual reality environment and build systems in the VRE (Figure 5a and 5b) (Slezak, Keren, et. al, 2018). A simplified overview of the CVR application is provided in figure 6. The system consists of a server in the cloud that receives an updated object state from one CVR client application and sends it to the rest of the

[1] Courtesy Jonathan Schlueter, Iowa State University.

clients to synchronize the virtual environment. The data flow is represented by bi-directional arrows, showing that the server cloud and client applications send and receive data. By continuously sending and receiving data from the server cloud, the system establishes real-time communication between users, bypassing the single-user limitation of VR and achieving a synchronized virtual environment. The only limitation for affective use is the quality of internet connection among the users.

Figure 4. Room-size VR system – The C6 at the Virtual Reality Application Center at ISU.

Figure 5. Multiple users with HMDs interact in the same VRE through the CVR system.

VR systems can be used for experiencing system designs in concept exploration stage and pre-fabrication phases. For example, Figure 6 presents a snapshot of a user exploring a bridge currently under construction between the states of Iowa and Illinois. The bridge was adopted into the author's VR systems, and the applications allowed for review of the design in full scale mode.

Multiple interactive features implemented afforded those constructing the bridge opportunities for enhancing exploration in VR, leading to many subsequent changes and initiated cost-saving methods.

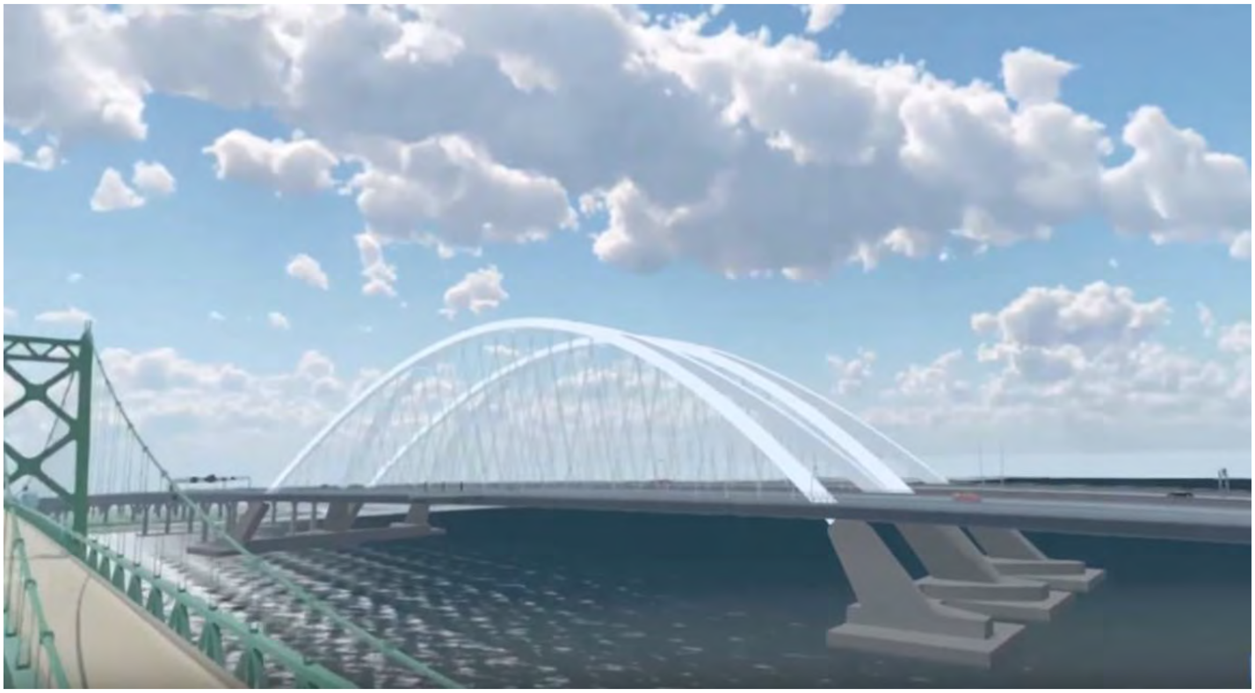


Figure 6. Review of bridge design in VR.

VR systems can be used for simple learning and training needs, and with proper development of a VR application can be harnessed for introducing users/trainees to more complex systems. Figure 7a shows a user with an HMD-based VR platform observing a full-scale internal combustion engine. Figure 7b demonstrates the user separating and interacting with the engine parts. The nefits of this application is that it helps the user create a proper mental model of the system. Furthermore, engine parts can be accompanied by audio files and animation to further enhance the introduction of the content.

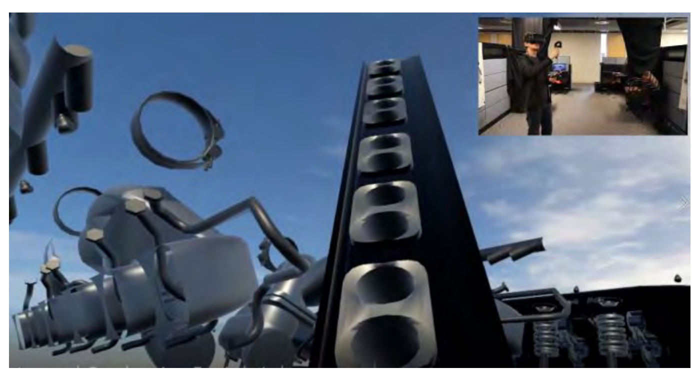


Figure 7a. User observes full-scale virtual internal combustion engine.

Figure 7b. User interacts with parts of virtual internal combustion engine.

One further remarkable aspects of simulated virtual reality environments is that participants tend to respond realistically to virtual situations even when the visual fidelity is low, and the representation of the physical reality is significantly reduced. . Three concepts have been reported as strong generators of immersive simulations:

- **Place illusion**: the strong sensation of being present in the space generated by the virtual reality environment, even though participants know they are not there (Held & Durlach, 1992; Sheridan, 1992; Barfield & Weghorst, 1993; Slater & Wilbur, 1997)
- **Plausibility**: the component of presence that is the illusion that the perceived events in the virtual environment are really happening (Bergstorm e al, 2017). In comparison to Place Illusion, which is a static characteristic, Plausibility is more concerned with the dynamics of events and the situation portrayed. de la Pena and colleagues (2010) provided an animated example to convey the sensation of Plausibility:

  > *"…suppose that you are (in physical reality) parking your car illegally. Just as you pull up to the curb, you notice a police officer standing by the street corner. Your heart misses a beat and you are just about to pull away rapidly when you notice that there is no police officer at all but a dummy stationed there. The police dummy is a failure in plausibility—for a moment the dummy was for you what it appeared to be, a real police officer. Then the plausibility, the sensation that something is real, that it is actually what it is represented to be…*" (p. 294)

- **Virtual body ownership**: utilization of multisensory correlations to provide people the illusion that alien objects are part of their body (Botvinick & Cohen, 1998).

The features above are effective in any of the applications described earlier. However, these features become an extreme asset when training users to respond to emergency situations. For example, the authors are using full scale VR system to research firefighters' situational awareness and decision making (Bayouth & Keren, 2019; Keren, Franke, Bayouth, 2013; Keren, Bayouth, Franke et. al, 2013; Bayouth, Keren, Franke, 2013), and for inoculating space workforce to stress associated with emergencies in space (Finseth, Keren, et al, 2016; Finseth, Keren, et al, 2018).

Summary

While enhanced visualization is yet in development stages, manufacturing and process industries can utilize AR/MR/VR application for enhancing operations and workforce development in a multitude of facets. Current challenges are as follows:

(1) developing models and applications for AR/MR/VR (the VR arena) require extensive efforts and expertise. As the virtual reality arena evolves, applications with user-friendly authoring systems will attract common users to develop and work with VR systems.

(2) VR systems demand strong computational resources. As the VR arena evolves and computation power continues to grow, mobile AR and MR systems must be capable to support operators in real-time.
(3) Systems designed with the VR arena in mind will allow operators to further delve into the manufacturing and industrial running processes. Implementation of visualization sensors (not pursued yet) will further enhance operators' mental models of the state of systems and support of mental models in emergencies.

The VR arena is in its infant stages but show great potential in supporting various aspects of process industry operation in the various life cycle stages.

References

Bayouth S. T., & Keren, N. (In Print). Fireground cue recognition: Effects on firefighter situational awareness when facing high-risk situations in virtual reality, *International Fire Service Journal of Leadership and Management*.

Bayouth, S. T., Keren, N., Franke, W. D., & Godby, K. (2013). Examining firefighter decision making: How experience influences speed in process and choice, *International Fire Service Journal of Leadership and Management*, 7.

Barfield, W., & Weghorst, S. (1993). The sense of presence within virtual environments: A conceptual framework. In G. Salvendy and M. Smith, Human-computer interaction. Software and hardware interfaces, 699 –704.

Bergstorm I., Azevedo S., Papiotis P., Saldanha N., & Slater M. (2017). The plausibility of a string quartet performance in virtual reality, IEEE Transactions on Visualization and computer graphics, 23(4), 1332-1339.

Botvinick, M., and Cohen, J. (1998). Rubber hands "feel" touch that eyes see. Nature, 391(6669): 756 –756.

de la Pena, N., Weil, P., Pomes, J. L. E. G. A., Spanlang B., Friedman, D., Sanchez-Vives, M V., Slater, M. (2010). *Presence*, Immersive journalism: Immersive virtual reality for the first-person experience of news, 19(4), 291-301.

Finseth, T. T., Keren, N., Franke, W. D., Dorneich, M., Anderson, C. C., Shelley M. C. (2018). Evaluating the effectiveness of graduated Stress exposure in virtual spaceflight hazards training, *Journal of Cognitive Engineering and Decision Making*, 12(4), 248-268.

Finseth, T. T., Keren, N. Shircliff, E., & Dorenich, M. (October, 2018). Demonstration 6: Standardized Stress Tests in Virtual Reality Environments (VR; Assessment and Research). In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, October 1-5, Philadelphia, PA.

Finseth, T. T., Keren, N., Franke, W. D., Dorneich, M. & Anderson, C. A. (2016). Graduated Stress Exposure of Spaceflight Hazards in a Virtual Environment, *Proceedings of the American Institute for Aeronautics and Astronautics annual meeting*, Long Beach: CA, September 13-16.

Fiorentino M., Uva A. E., Gattullo M., Debernardis S., and Monno G. (2014) Augmented reality on large screen for interactive maintenance instructions, *Comput. Ind*., 65(2), 270–278.

Held, R. M., & Durlach, N. I. (1992). Telepresence. Presence: Teleoperators and Virtual Environments, 1(1), 109 –112.

Hololense 2 (2019). Available online https://www.microsoft.com/en-us/hololens, last reviewed: August 29, 2019.

Keren, N., Franke, W. D., Bayouth, S. T., Godby, K. M., & Harvey, M. E. (December 2013). VirtuTrace: Training for Making Decisions under Stress in virtual environments. In Proceedings of the 2013 I/ITSEC - Concepts and Technologies, Empowering an Agile Force, Orlando, FL, December 2-5, 2013.

Keren, N., Bayouth, S. T., Godby, K. M., & Franke, W. D. (October, 2013) Examining the effect of stress and firefighters' experience level on time-to-decision in virtual reality, In *Proceedings of the 2013 International meeting of the Human Factors and Ergonomics Society,* San Diego, CA, September 30 - October 4, 2013.

Magic Leap (2019). Available online https://www.magicleap.com/, last reviewed: August 29, 2019.

Palmarini, R., J., Erkoyuncu A., Roy R., and Torabmostaedi H (2018). A systematic review of augmented reality applications in maintenance, *Robot. Comput. Integr. Manuf*., vol. 49, pp. 215–228, Feb. 2018.

Scope AR, "WorkLink - Scope AR," 2016. [Online]. Available: http://www.scopear.com/products/worklink/. [Accessed: 02-Apr-2018].

Schlueter J. A. (2018). *Remote maintenance assistance using real-time* augmented reality authoring, Thesis, Iowa State University.

Sheridan, T. B. (1992). Musings on telepresence and virtual presence. Presence: Teleoperators and Virtual Environments, 1(1), 120 –126.

Slater, M., & Wilbur, S. (1997). A framework for immersive virtual environments (FIVE): Speculations on the role of presence in virtual environments. Presence: Teleoperators and Virtual Environments, 6(6), 603– 616.

Slezak, R., Keren, N., Finseth, T. T. (November, 2018) Collaborative Risk Assessment in Virtual Reality Environments Proceedings of the *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, to be presented Nov 26- Nov 30, Orlando, FL.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Unified Hazard Assessment – Bringing Together HAZOP, LOPA, Hazard Registers, and Bowtie in a Unified Structure

Edward M. Marszal*
President, Kenexis Consulting Corporation
3366 Riverside Drive
Columbus, Ohio 43221
*Presenter E-mail: edward.marszal@kenexis.com

Abstract

Process hazards analysis studies, especially HAZOP and LOPA are ubiquitous in the process industries, but the information generated during these studies is not being used to its fullest extent. Management desires to have multiple scenarios rolled up into easier to use hazard registers, and to be able to visualize them with graphical approaches like bow-tie diagrams. Unfortunately, the data that is currently contained in most HAZOP and LOPA studies is not structured to allow easy hazard register generation and bow-tie visualization. The use of the "cause local – consequence global" approach to HAZOP has made the facilitator's life easier at the expense of others who need PHA data but can't find what they need because the resulting documentation is not logical. This paper discusses the use of a standardized data structures that are already revolutionizing PHA documentation, and the extension of these standardized data structures will allow the development of tools that can display a single set of data as a HAZOP worksheet, LOPA worksheet, or bow-tie diagram. Furthermore, the hazard analysis can be modified using any of these visualization techniques and have the results carried back across all diagram and worksheet types. Adoption of a unified hazard assessment data structure will benefit all users of PHA data and facilitate use of PHA data by other critical stakeholders, automatically.

Keywords: HAZOP, LOPA, Bow-Tie, Big Data

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Impact of water on toxic hydrogen fluoride generation from the decomposition of $LiPF_6$ in lithium-ion battery electrolytes

Ji Yun Han,[1]* Jeongwook Seo,[2+] Seungho Jung,[3]*
*Ajou University
+Samsung Electronics Co., Ltd.
[1] Department of Environmental and Safety Engineering, Ajou University, Suwon, 16499, Korea
[2] Samsung Electronics Co., Ltd., Suwon, Korea
*Presenter E-mail: jy0324han@ajou.ac.kr

Abstract

Toxic hydrogen fluoride (HF) gas can be generated when $LiPF_6$, a salt used in lithium-ion battery electrolytes, thermally decomposes and/or reacts with trace water. Simultaneous thermal analysis and mass spectrometry (STA-MS) was conducted on five different organic solvents containing $LiPF_6$ to determine the temperatures at which HF is generated and the activation energies of the decomposition reaction. STA-MS allows the simultaneous direct observation of electrolyte thermal stability and hydrogen fluoride generation, something that is not possible with gas chromatography–mass spectrometry alone, thus it represents a more efficient and simple experimental approach.

The five solvents tested in this study were anhydrous tetrahydrofurfuryl alcohol (THFA), 1,3-dioxolane (1,3-DL), diethyl carbonate (DEC), 1,2-dimethoxyethane (DME), and ethyl carbonate (EC). STA-MS analysis of the $LiPF_6$ in these solvents revealed that HF generation occurred at different temperatures for each electrolyte. In the case of 1M $LiPF_6$ in THFA, the addition of 1000 ppm of water reduced the thermal decomposition temperature compared to solid neat $LiPF_6$. Except for EC, all of the other electrolyte systems exhibited a lower HF generation temperature and a lower reaction activation energy (Ea) when water was present. Additionally, from a risk assessment perspective, the results indicate that the HF generation starts from the SEI layer decomposition stage which occurs early in the thermal runaway mechanism of the lithium-ion battery.

This research can be used to develop more thermally stable and safer electrolytes in the future, especially with respect to HF generation. In addition, this study highlights the need for research into measures to combat large-capacity lithium-ion battery fires, which may occur in electric vehicles and grid-scale energy storage systems.

Keywords: lithium-ion battery, electrolytes, fire, toxic gases, STA-MS experiment, thermal characteristics of Li-ion battery electrolytes, risk of HF gas.

Introduction

Lithium-ion batteries represent a type of rechargeable electrochemical energy storage system in which energy is charged and discharged by the transfer of lithium ions. During the discharge process, intercalated lithium ions are released from the anode and transferred to the cathode via an electrolyte. The reverse occurs during charging—the lithium ions are re-intercalated into the anode via an externally applied potential. During each charge and discharge cycle, a portion of the lithium ions are immobilized and can no longer participate in the charge–discharge process which leads to a loss of battery capacity over time.

The three most important characteristics of industrial and commercial lithium-ion batteries are their energy density, cycle life, and capacity retention. Energy density is the normalized amount of energy that is available from a battery and is calculated as either the available energy per unit of battery mass or as the available energy per unit of battery volume. The lithium-ion battery cycle life represents how many charge and discharge cycles the battery can perform before the remaining capacity is no longer sufficient for a given application. Capacity retention is how much of the initial or specified capacity (i.e., the amount of energy that can be stored in the battery) is left after a certain number of charge and discharge cycles. Currently, a lithium-ion battery cycle life is over 1500 cycles, with a capacity retention of over 85% of the initial discharge capacity (Ramanujapuram et al., 2016).

The advances in cycle lifetime and energy density over the past decade have attracted societal and industrial attention and have made it possible for these batteries to be employed in various applications, ranging from mobile phones to electric vehicles. In addition, rapidly growing renewable energy industries, such as wind, solar, and smart grid systems, require large-scale energy storage systems (ESSs) in the range of 3–20 MWh, for which lithium-ion batteries are considered the optimal technology (Park et al., 2018).

However, the high-energy storage capability of lithium-ion batteries also comes with some notable risks. For example, higher energy density and greater performance requirements have also increased the possibility of thermal runaway scenarios. Seven ESS fires have occurred in South Korea since 2017, leading to property losses of approximately 17 million US dollars. The South Korean government recently conducted an investigation into the cause of these ESS fires and published a report on their findings (Park et al., 2018).

Lithium-ion battery fires are not limited to large-scale ESS and have become a more frequent event globally. A U.S. Depart of Transportation investigation report stated that there were 265 air/airport incidences involving lithium/lithium-ion batteries being carried onboard as cargo or baggage. In fact, 42% of all incidents (112 incidents) occurred in the 3 most recent years spanning from 2017 to July 2019 (FAA Office of Security and Hazardous Materials Safety, 2019). These incidences were not limited to a certain battery product or the specific industries that utilize them. As a result, the issue of lithium-ion battery safety has become a serious topic of interest, especially as large battery fires, such as those from EV or ESS battery packs, cannot be easily extinguished and result in unstoppable fires in most cases.

Table 1. Examples of recent lithium-ion battery-related incidents (from Feng et al., 2018; Park et al., 2018; FAA Office of Security and Hazardous Materials Safety, 2019).

Date	Industry	Device (if application)	Location	Incident summary and probable cause
July 2019	Airline	Laptop / Tablet	US	A Unit Load Device (ULD) at JFK Airport produced smoke and caught on fire after external impact, internal short circuit
Jun. 2019	Airline	Cell Phone	US	A passenger's phone produced smoke and caught on fire, internal short circuit
May 2019	Airline	E-cigarette and spare battery	US	While loading baggage on DL flight 880 to Minneapolis, MN (MSP), a bag on the belt loader produced smoke and caught on fire, internal short circuit
Jun. 2018	Solar	19 MWh ESS	Gunsan, S. Korea	30 min after a full charge of the ESS, fire started on Rack No. 13 of the ESS, cause unknown
Aug. 2017	Wind	17 MWh ESS	Gochang, S. Korea	Fire started at ESS pack during summer time due to failure of the HVAC thermal management system, thermal abuse conditions created by HVAC failure
July 2016	EV	EV bus	Nanjing, China	The battery pack of an EV bus caught fire after heavy rain. Water immersion caused short circuit.
Apr. 2015	EV	EV bus	Shenzhen, China	Wuzhou Dragon EV bus caught fire during charging in a garage, overcharging of battery pack

The hazards of lithium-ion batteries, including thermal runaway scenarios, are closely related to the materials that compose the batteries. For example, when the $LiPF_6$ salt, the most commonly used salt in the lithium-ion battery electrolytes, decomposes to form LiF and PF_5, the PF_5 acts as a catalyst in the decomposition reaction of the electrolyte solvent (Lisbona et al., 2011; Abraham et al., 2006).

Thermal runaway in lithium-ion battery has been the focus of many recent studies. In these studies, the mechanisms responsible for lithium-ion battery fires have been investigated using accelerating rate calorimetry (ARC), differential scanning calorimetry (DSC), and isothermal microcalorimetry IMC (Inoue and Mukai, 2017). Liu et al. reported that there are various side reactions during the charge and discharge cycle of a lithium-ion battery in the solid electrolyte interface (SEI) layer on the surface of the anode and cathode that contribute to thermal runaway scenarios (Liu et al., 2014). Under thermal runaway situations, the heat generated will lead to decomposition of the lithium-ion battery electrolyte.

Most commercial lithium-ion batteries contain electrolytes consisting of $LiPF_6$ salt in an organic solvent mixture. This type of electrolyte is characterized by high conductivity, good electrochemical stability, and the ability to work at low temperatures. However, the thermal stability is poor. It is well known that $LiPF_6$ salt in the organic solvent of lithium-ion battery electrolytes can produce toxic hydrogen fluoride (HF) gas as a thermal decomposition reaction product (Gaulupeau., 2017). Larsson et al. have also reported gas generation due to electrolyte decomposition reactions and assessed the toxicity of the HF gas produced by $LiPF_6$ decomposition in the presence of water (Michalak, 2015; Wang, 2018; Larsson et al., 2017). $LiPF_6$ decomposition reactions are shown in Equations 1 to 3 where: Equation 1 is the anhydrous thermal decomposition of $LiPF_6$ salt, Equation 2 is the HF generation reaction of PF_5 (the product of Equation 1) with water (H_2O), and Equation 3 is the HF generation reaction of $LiPF_6$ salt in the presence of water (Larsson et al., 2017).

$$LiPF_6 \rightarrow LiF + PF_5 \tag{1}$$

$$PF_5 + H_2O \rightarrow POF_3 + 2HF \tag{2}$$

$$LiPF_6 + H_2O \rightarrow LiF + POF_3 + 2HF \tag{3}$$

Larsson et al. reported that the immediately dangerous to life or health (IDLH) level for HF is 0.025 mg/m^3 (30 ppm) and the 10-minute lethal concentration is 0.0139 g/m^3 (170 ppm) (Larsson et al., 2017). As a result, HF gas emitted from a fire involving a lithium-ion battery that operates in the range of kWh to MWh (the class used in electric vehicles) can be very dangerous and poses serious health risks (Larsson et al., 2017).

In this study, a new method to measure and analyze electrolyte stability using simultaneous thermal analysis–mass spectrometry (STA-MS) is presented, with a focus on HF gas generation. The association between the five different electrolyte stabilities and their activation energy, the generation of HF gas, and the effect of the addition of trace water is also reported.

Experiment

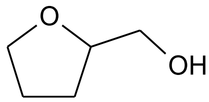
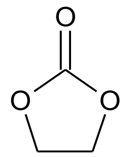
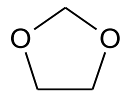
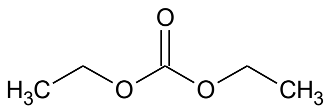
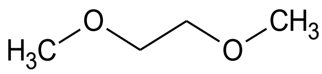
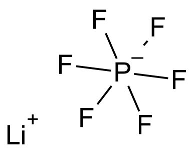
Five organic solvents were used to create 1 M electrolytes containing $LiPF_6$ salt. The electrolyte decomposition conditions were assessed using STA-MS in order to determine the thermal characteristics of the electrolyte solutions. The five solvents used were tetrahydrofurfuryl alcohol (THFA), 1,3-dioxolane (1,3-DL), diethyl carbonate (DEC), 1,2-dimethoxyethane (DME), and ethyl carbonate (EC), all purchased from Tokyo Chemical Industry (TCI). $LiPF_6$ salt, also purchased from TCI, was dissolved in each solvent to a concentration of 1 M. Two groups of samples were prepared: one containing anhydrous solvents and one containing trace amounts of water (1000 ppm).

The samples were sealed in a hermetic Al_2O_3 crucible pan in a nitrogen-filled box with flowing nitrogen gas to maintain a constant and stable atmosphere. Each of the crucibles was placed in the STA-MS instrument (409 PC and QMS 403C from NETZSCH) and the electrolyte analyzed at temperatures from 35 to 300℃ under a constant heating rate of 2℃/min. Thermogravimetry/differential thermal analysis (TG/DTA) results and the MS intensity for the fluorine ion current were recorded by the STA-MS instrument.

Results

The boiling point (bp), flash point (fp), and $LiPF_6$ decomposition temperatures are presented in Table 2 (Hara et al., 2012; Hess et al., 2015; PubChem, accessed July 22, 2019; Ken et al., 2016; NFPA, 2002). The decomposition temperature of $LiPF_6$ salt is 181°C, as reported by Xu et al. (2010). As can be seen in Table 2, the electrolyte solvent with the lowest bp is 1,3-DL (75°C) and that with the highest is EC (243°C).

Table 2. Chemical and physical characteristics of the electrolyte materials

Entry	Chemical name	Chemical structure	CAS No.	Molecular weight, g/mol	Boiling point, °C	Flash Point °C	Decomposition, °C
1	Tetrahydrofurfuryl alcohol (THFA)		97-99-4	102.13	178	75	-
5	Ethylene carbonate (EC)		96-49-1	88.06	243	145.5	-
2	1,3-Dioxolane (1,3-DL)		646-06-0	74.08	75	2	-
3	Diethyl carbonate (DEC)		105-58-8	118.13	126 ~ 128	33	-
4	1,2-Dimethoxy ethane (DME)		110-71-4	90.12	85	- 2	-
6	Lithium hexafluorophosphate ($LiPF_6$)		21324-40-3	151.91	-		181 neat (no solvent, solid phase)

The materials characteristic data suggest that, if an internal short or an external heat source were to increase the temperature of a lithium-ion battery to over 75°C, a battery using 1,3-DL as a solvent has an inherent risk of suffering internal damage due to the increase in pressure arising from solvent vaporization. The fp is also an indication of the temperature at which a fire can start if a battery's electrolyte is exposed to oxygen in the ambient air, such as when the protective outer case or pouch is breached by external damage or by the build-up of internal pressure.

Lithium-ion battery safety is strongly associated with environmental factors such as ambient temperature and humidity. When the protective housing of a battery is compromised, ambient humid air can infiltrate the internal components, while moisture can also be introduced into the battery components during production if strict quality control measures are not enforced. When compromised batteries are exposed to an internal short circuit or an external heat source, such as an open flame, any moisture present in the battery poses serious safety risks. In these cases, it is reasonable to expect that HF will be generated due to the thermal decomposition reaction described in the previous section. The presence of moisture can exacerbate this situation because it can affect the thermal decomposition temperature of the salt in the electrolyte.

The DTA spectra and the F^+ fragments characteristic of the mass spectrum for HF (m/z = 19) from the five 1M $LiPF_6$ electrolyte samples are presented in Figures 1–5. Gaulupeau et al. (2017) reported two characteristic fragments of gaseous HF ($^-F^+$ and HF^+) that can be used as evidence for the presence of HF. In the present study, F+ (m/z = 19) was used as an indicator for HF. Equation 3, in which HF is produced as an electrolyte decomposition product, is not significantly affected by the bp of the solvent in each electrolyte. The bp temperatures of THFA and EC were 178°C and 243°C, respectively, which was higher than the other solvents. However, HF generation started at 138°C and 134°C for THFA and EC, respectively, as can be seen in the DTA and HF (m/z = 19) mass spectra. In contrast, the same reaction was seen at 150°C, 164°C, and 128°C (and 180°C) for the solvents with a lower bp, 1,3-DL (75°C), DME (85°C), and DEC (126–128°C), respectively, as can be seen in Figures 1–5. This is consistent with a previous study in which it was reported that the solvated form of the Li^+ cation and the PF_6^- anion alters the bp and decomposition reaction temperature (Logan et al., 2018). This phenomenon can also be explained by the activation energy (Ea) of the thermal decomposition reactions, which applies to Equation 3 (Yamaki et al., 2015).

Calculation of the Activation Energy

The Kissinger method, which is used to determine the Arrhenius dependence of the rate constant on temperature, is a well-known and relatively reliable method for determining the activation energy (Ahn and Yoon., 2007). According to this approach, in the *n*th reaction system for the *n*th reaction, the rate constant is K $\left(\mathbf{k} = \boldsymbol{Ae}^{-\frac{Ea}{RT}}\right)$, and the reaction equation in relation to time is as follows:

$$\frac{dx}{dt} = k(1-x)^n = Ae^{\frac{-E_a}{RT}}(1-x)^n, \quad \textbf{(4)}$$

where x represents the conversion rate, *A* is the frequency factor, *Ea* is the activation energy, *R* is the gas constant, and *n* is the order of the reaction.

In most reactions, if *n* is constant, the differential speed of the reaction is 0 at the maximum reaction temperature (Tp). This leads to the derivation of the Kissinger equation to calculate the activation energy, as shown in the equation below:

$$\ln\left(\frac{q}{T^2}\right) = -\frac{E_a}{R}\left(\frac{1}{T_p}\right) + ln\left(\frac{R}{E_a} - A\right), \quad \textbf{(5)}$$

where $\mathbf{q} = \mathbf{dT/dt}$ is the heating rate.

The activation energies for the five electrolytes analyzed in the present study were calculated based on the derived Kissinger equation above. Data from STA-MS were obtained using a constant heating rate of 2°C/min (i.e. q = 2 °C/min), a gas constant of $\mathbf{R = 8.315}\ \boldsymbol{J/Kmol}$, and a frequency factor (A) of 1. The experimentally obtained values from STA-MS were used to calculate the activation energy for each electrolyte. The activation energies were calculated for both the anhydrous form of the electrolytes and the same electrolytes containing trace amounts of water.

Discussion of the STA-MS results

The Equation 3 HF generation temperature and activation energies were calculated and are presented in Table 2. Anhydrous THFA produced a strong HF (m/z = 19) ionic current peak at 138°C, as shown in Figure 1c. However, when water was present at 1000 ppm, the HF peak appeared at ~100°C, reaching a maximum at 168°C, and continuing up until 300°C. It is believed that the HF generation temperature is lower due to the lower activation energy in the presence of water, falling from 25.4 kcal/mol to 22.8 kcal/mol.

For EC, the presence of 1000 ppm water did not appear to have a significant impact. As shown in Figure 2b, a single strong endothermic reaction peak was observed regardless of the presence of water. The summit peaks of the HF mass trace (m/z = 19) resulting from $LiPF_6$ decomposition appeared at 128°C and 134°C. The only difference was the faster reaction rate, as illustrated by the difference in the width of the MS peaks for HF. The calculated activation energies were also consistent with these results, as can be seen in Table 3.

Table 3. Comparison of the HF reactions for 1 M $LiPF_6$ electrolytes with the addition of water (1000 ppm)

Electrolyte solvent (Salt: $LiPF_6$)	Trace water content (ppm)	HF generation reaction temperature (°C)	Activation energy of HF generation reaction (Ea, kcal/mol)
THFA	None	138	25.4
	1000 ppm	100, 168 (continuous generation from approx. 100 to 300)	22.8, 27.5
EC	None	134	25.1
	1000 ppm	128	24.7
1,3-DL	None	150 (continuous generation from	26.2

		approx. 100 to 300)	
	1000 ppm	120	24.2
DEC	None	128, 180	24.7, 28.3
	1000 ppm	106, 131	23, 24.9
DME	None	164	27.2
	1000 ppm	125 (slowly subsides from 100 to 300)	24.5

For anhydrous 1,3-DL, HF generation reached its maximum at approximately 150℃, and continued to 300℃, as shown in Figure 3c. In the presence of water, however, the HF generation temperature (via Equation 3) was about 30℃ lower and the HF peak became narrower and stronger, which suggests that the reaction rate was very rapid. The lowering of the HF generation temperature can be attributed to the lower activation energy (from 26.2 kcal/mol to 24.2 kcal/mol).

With anhydrous DEC, there were two HF generation peaks (m/z = 19), which matched the endothermic peaks in Figure 4b: one at 128℃ and the other at 180℃. The HF generation at 128℃ was minimal compared to that at 180℃. In the presence of 1000 ppm water, there were also two HF (m/z = 19) peaks that matched the endothermic peaks. However, these peaks appeared at temperatures that were 22℃ and 49℃ lower than the peaks observed for the anhydrous DEC. The activation energies were 24.7 and 28.3 kcal/mol without water present and 23.0 and 24.9 kcal/mol with the addition of water (1000 ppm).

For anhydrous DME, HF generation began at approximately 90℃ with a small peak, followed by a large peak at 164℃ that continued to 300℃, after which the HF (m/z = 19) peak slowly subsided (as shown in Figure 5c). In the presence of water, however, the HF generation temperature was lowered to 125 ℃, which can be attributed to the lower activation energy (27.2 kcal/mol to 24.5 kcal/mol).

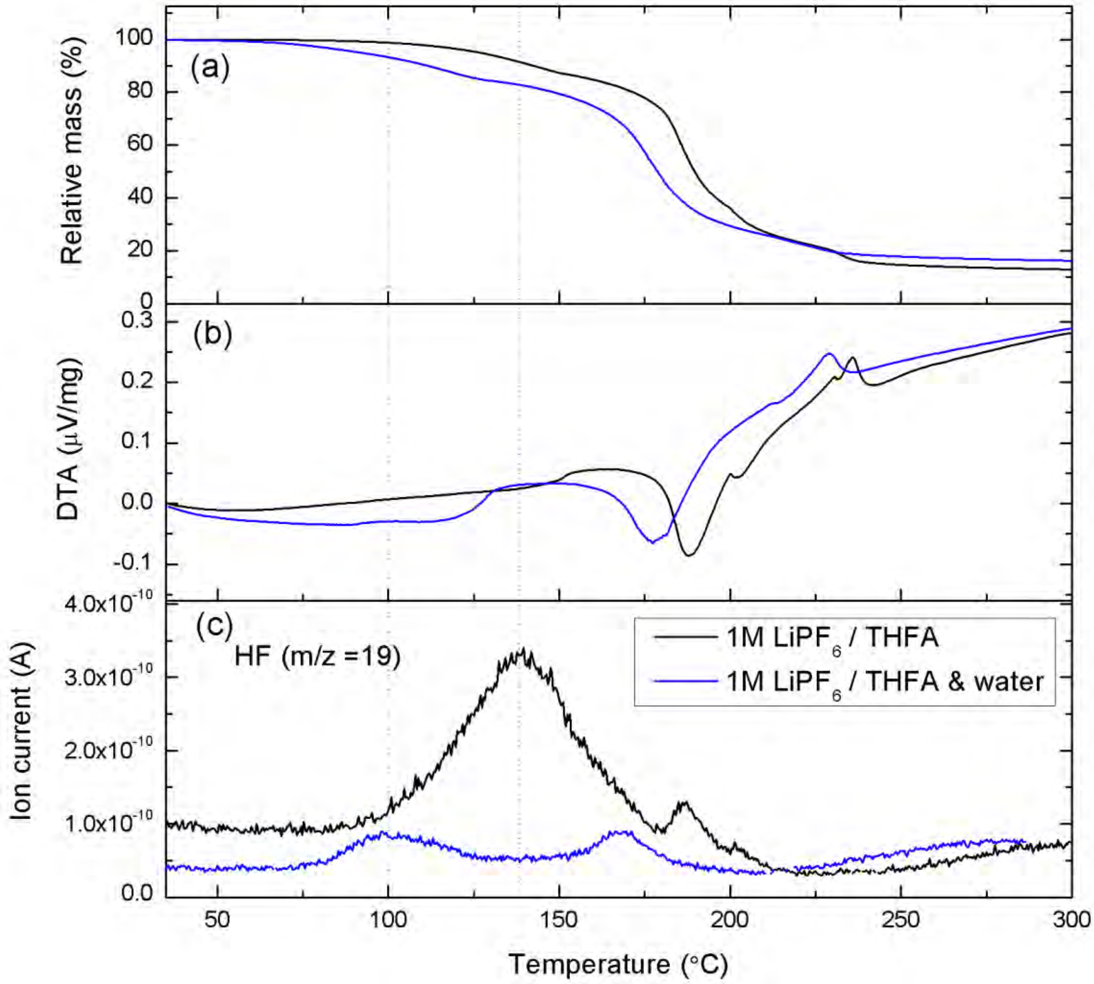


Figure 1. TG/DTA-MS results for the thermal decomposition of the anhydrous 1M $LiPF_6$/THFA electrolyte (black) and the 1M $LiPF_6$/THFA electrolyte with 1000 ppm of water added (blue): (a) TGA, (b) DTA, (c) MS.

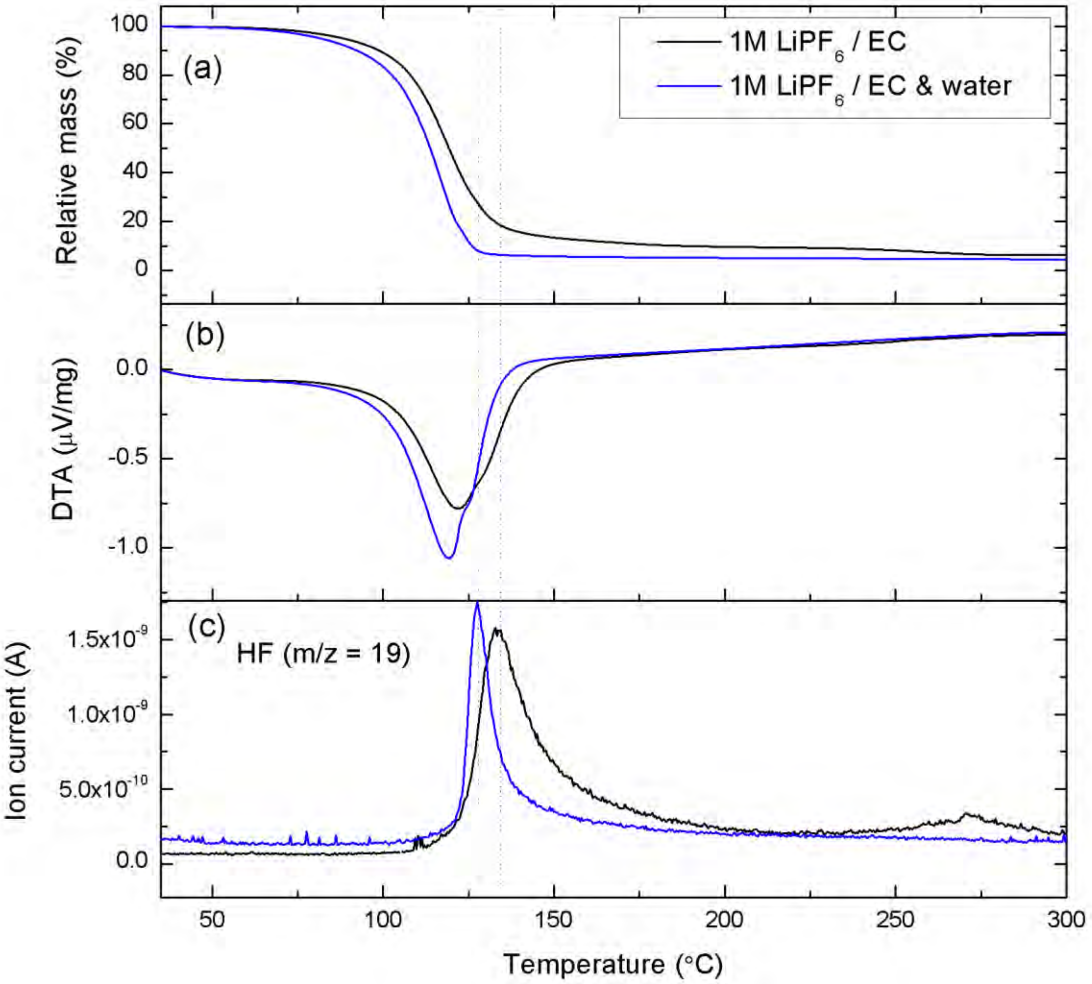


Figure 2. TG/DTA-MS results for the thermal decomposition of the anhydrous 1M $LiPF_6$/EC electrolyte (black) and the 1M $LiPF_6$/EC electrolyte with 1000 ppm of water added (blue): (a) TGA, (b) DTA, (c) MS.

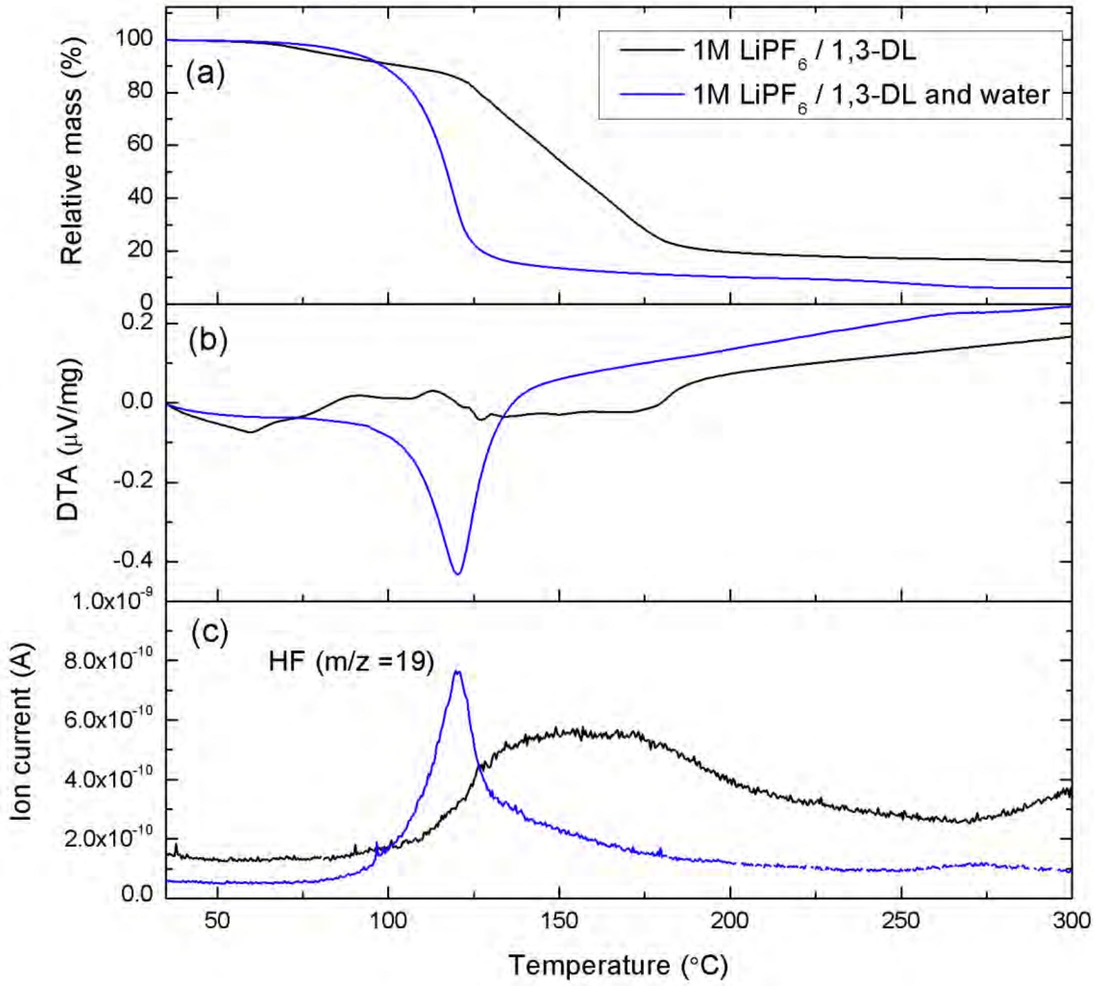


Figure 3. TG/DTA-MS results for the thermal decomposition of the anhydrous 1M $LiPF_6$/1,3-DL electrolyte (black) and the 1M $LiPF_6$/1,3-DL electrolyte with 1000 ppm of water added (blue): (a) TGA, (b) DTA, (c) MS.

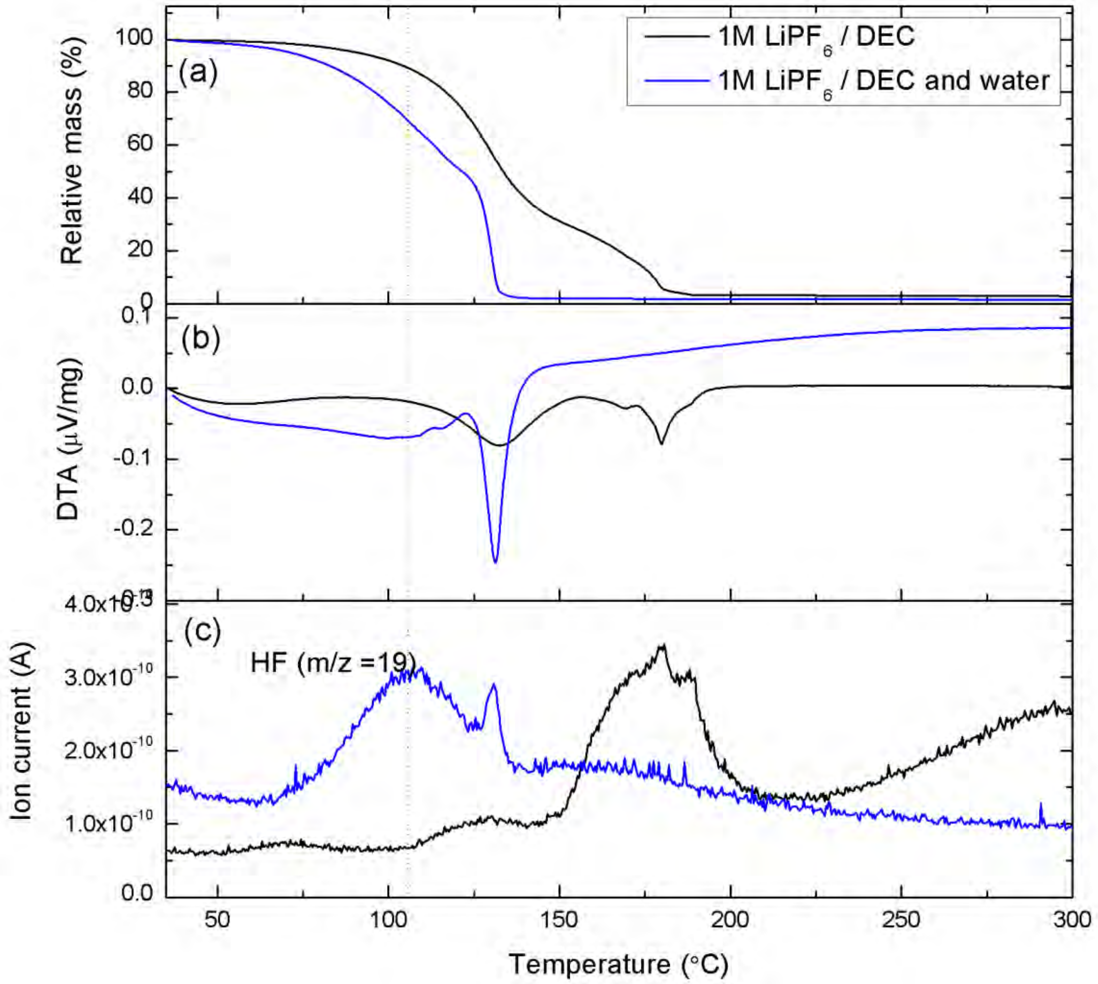


Figure 4. TG/DTA-MS results for the thermal decomposition of the anhydrous 1M $LiPF_6$/DEC electrolyte (black) and the 1M $LiPF_6$/DEC electrolyte with 1000 ppm of water added (blue): (a) TGA, (b) DTA, (c) MS.

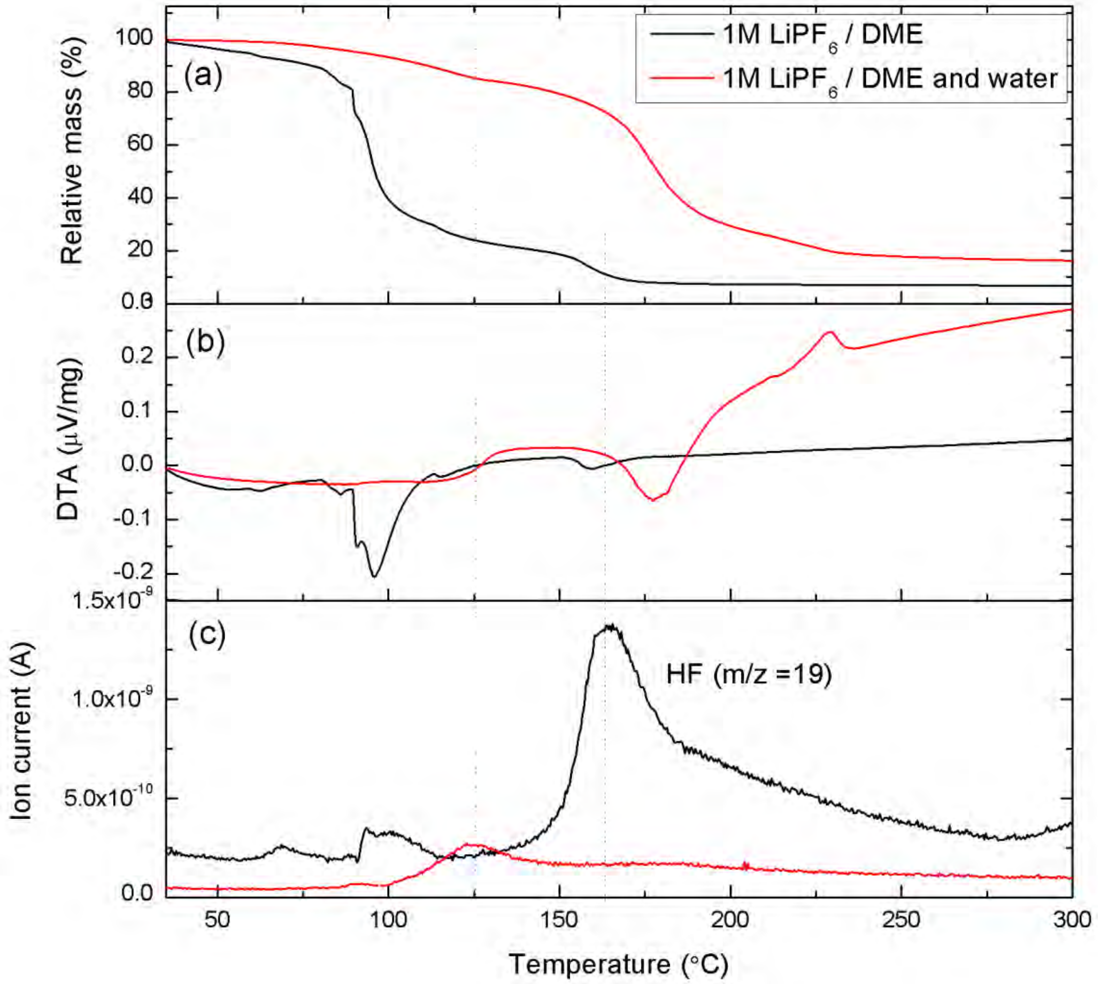


Figure 5. TG/DTA-MS results for the thermal decomposition of the anhydrous 1M $LiPF_6$/DME electrolyte (black) and the 1M $LiPF_6$/DME electrolyte with 1000 ppm of water added (red): (a) TGA, (b) DTA, (c) MS.

Risk assessment

Risk assessment for lithium-ion batteries can be broadly categorized into two categories: 1. The assessment of fire or thermal hazards associated with battery thermal runaway scenarios. 2. The assessment of exposure hazards for human inhalation toxicity scenarios due to the toxic gases generated during thermal runaway situations. Both thermal hazard and exposure assessments have been reported by several research teams in recent years (Larsson et al., 2017; Park et al., 2018; Feng et al., 2018). In a recent study, Peng et al. demonstrated that hydrogen fluoride (HF), sulfur dioxide (SO_2), nitric oxide (NO), nitrogen dioxide (NO_2), and hydrogen chloride (HCl) gases are generated during thermal runaway reactions of large-capacity lithium-ion batteries (68 Ah, Pouch type) by studying thermal runaway propagation behaviors. Peng et al. also reported that HF gas exhibited a large range of fractional effective concentrations (FECs) depending on the state of charge (SOC) of the battery cell: FECs of approximately 40%, 20%, 10%, and 5% for 100%, 75%, 50%, and 0% SOC, respectively. Moreover, Peng et al. highlighted the exposure hazards of HF gas in the toxicity evaluation by exhibiting a maximum concentration of HF at 165 ± 10 mg/m^3 which is approximately 5.7 times greater than the IDLH value of 24.6 mg/m^3.

From a thermal hazard perspective, this work has demonstrated that, in the presence of 1000 ppm of water, the temperature of toxic HF gas generation from the decomposition of $LiPF_6$ is lower than previously considered. In addition, in the presence of 1000 ppm of water, this work has also demonstrated at which stage of the thermal runaway mechanism the toxic HF gas is generated, as shown in Figure 7.

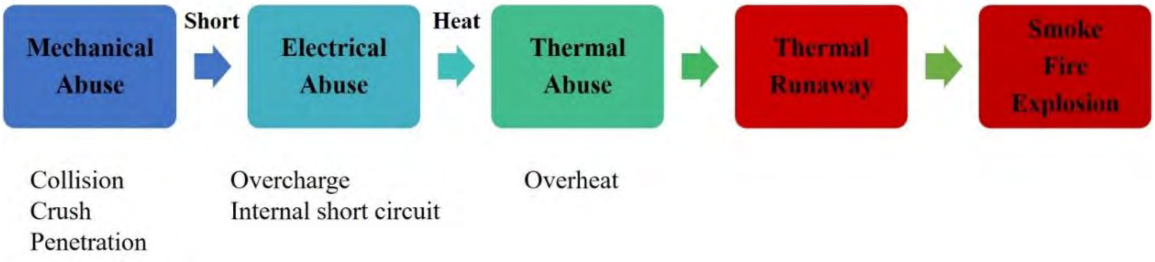


Figure 6. Causes of thermal runaway and lithium-ion battery failure (Feng et al., 2018).

In most thermal runaway mechanism studies, thermal runaway is largely divided into three or four stages with each stage having its own chain exothermic reactions that lead to rapid energy release. (Feng et al., 2018) As reported, the resulting thermal runaway may reach temperatures of up to 500°C very quickly. According to the mechanism described in a study published by Li et al., the SEI layer decomposition is the first to occur before an internal short circuit and the onset temperature is reported to be approximately 90°C at 100% SOC. From there, exothermic reactions between the anode and the electrolyte are initiated up to approximately 200°C. This is followed by separator melting, cathode decomposition, electrolyte decomposition, and, finally, a complete thermal runaway via internal short circuit (Feng et al., 2018; Li et al., 2019).

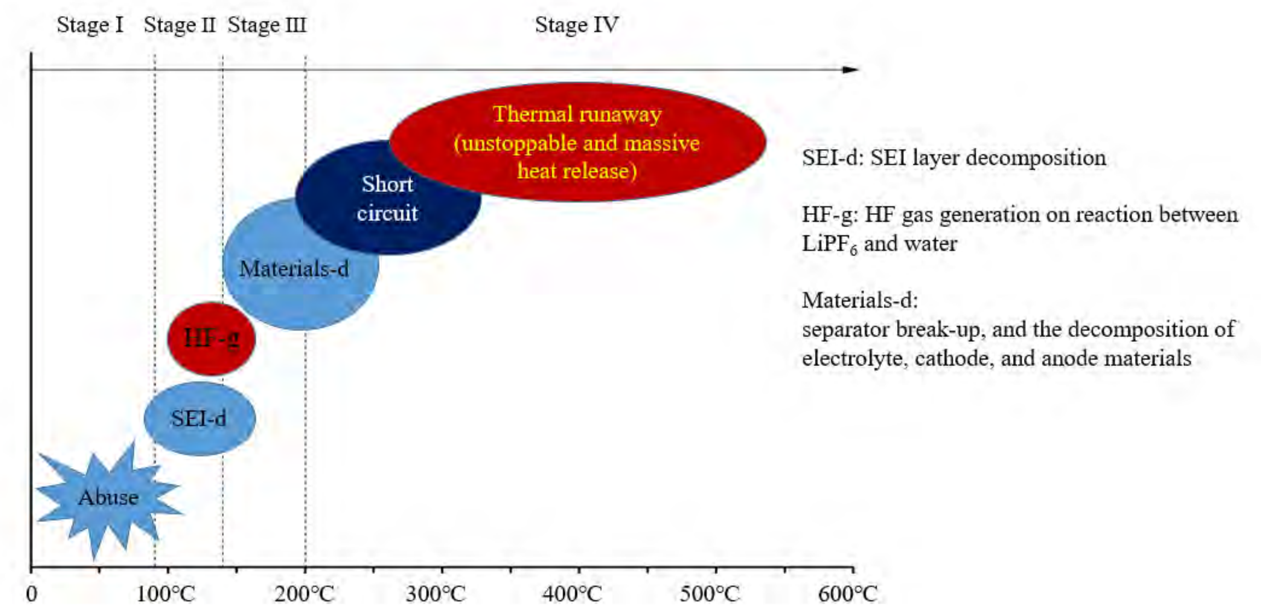


Figure 7. Schematic of thermal runaway mechanism

As previously shown in the TG/DTA-MS results, the presence of water can reduce the temperature at which HF is generated from $LiPF_6$ decomposition by tens of degrees Celsius depending on the electrolyte solvent. In conjunction with previous studies on the thermal runaway mechanism, it can be inferred that, in the presence of water, toxic HF gas is generated during the early stages of thermal runaway mechanism, namely the SEI layer decomposition, which starts at approximately 90°C, especially for the solvents THFA and DEC. In other solvents tested (EC, 1,3-DL, and DME), the temperature where HF is generated is slightly higher at approximately 120°C.

Conclusions

The presence of water in organic solvent-based electrolytes containing $LiPF_6$ lowers the temperature at which HF is generated due to the decomposition reaction between $LiPF_6$ and water. This was observed from the STA-MS analysis of five different electrolyte samples with and without trace amounts of water (1000 ppm). In some cases, the presence of water also accelerated the rate at which HF was generated, as evidenced by the narrower peaks observed in the MS spectra tuned to HF (m/z = 19). Of the five electrolytes tested, EC exhibited the smallest change in HF generation temperature in the presence of water. However, large changes in HF generation temperatures and Ea were observed in 1,3-DL, THFA, sDME, and DEC when water was present. The reduction in the HF generation temperature was also observed for the thermal decomposition of $LiPF_6$ salt in the presence of water. The calculated activation energies were consistent with these observations, with consistently lower activation energies when trace water was present.

In addition, from a risk assessment perspective, the lower HF generation temperature poses a higher risk of exposure as HF can be generated earlier than previously reported. The results indicate that HF gas is generated during the SEI layer decomposition stages at approximately 90°C with THFA showing the lowest generation temperature of 100°C. All other solvents have also been shown to generate HF gas before reaching 150°C.

Additional research is needed to investigate the exact chemical mechanisms responsible for the lowering of the HF generation temperature.

References

Ramanujapuram, Anirudh., Gordon, Daniel., Magasinski, Alexandre., Ward, Brian., Nitta, Naoki., Huanga., Cindy, Yushin, Gleb., 2016. Degradation and stabilization of lithium cobalt oxide in aqueous electrolytes. Energy Environ. Sci, 9, 1841-1848.

Park, Kwang-Muk., Kim, Jae-Hyun., Park, Jin-Yeong., Bang, Sun-Bae., 2018. A study on the fire risk of ESS through fire status and field investigation. Fire Sci. Eng, 32(6), 91-99.

Inoue, Takao, Mukai, Kazuhiko., 2017. Roles of positive or negative electrodes in the thermal runaway of lithium-ion batteries: Accelerating rate calorimetry analyses with an all-inclusive microcell. Electrochemistry Communications, 77, 28-31.

Liu, Lin, Park, Jonghyun., Lin, Xianke., Sastry, A. M., Lu, Wei., 2014. A thermal-electrochemical model that gives spatial-dependent growth of solid electrolyte interphase in a Li-ion battery, J. Power Sources, 268, 482-490.

Lisbona, D., Snee, T., 2011, A review of hazards associated with primary lithium and lithium-ion batteries. Process Saf Environ Prot, 89(6), 434-442.

Abraham, D.P., Roth, E.P., Kostecki, R., McCarthy, K., MacLaren, S., Doughty, D.H., 2006, Diagnostic examination of thermally abused high-power lithium-ion cells. J. Power Sources, 161(1), 648-657.

Wang, Aiping., Kadam, Sanket., Li, Hong., Shi, Siqi., Qi, Yue., 2018. Review on modeling of the anode solid electrolyte interphase (SEI) for lithium-ion batteries. Computational Material, 4, 15.

Larsson, Fredrik., Andersson, Petra., Blomqvist, Per., Mellander, Bengt-Erik., 2017. Toxic fluoride gas emissions from lithium-ion battery fires. Scientific Reports, 7, 10018.

Hess, Steffen., Wohlfahrt-Mehrens, Margret., Wachtler, Mario., 2015. Flammability of li-Ion battery electrolytes: flash point and self-extinguishing time measurements. J. Electrochem. Soc, 162 (2) A3084-A3097.

https://pubchem.ncbi.nlm.nih.gov/compound/7360#section=Melting-Point.

Ken, Tamamoto., Shigeyuki, Yamada., Masao, Higashi., Tsutomu, Konno., Takashi, Ishihara. 2016. Novel V- and Y-Shaped light-emitting liquid crystals with pentafluorinated bistolane-based luminophores. Journal of Fluorine Chemistry, 190, 23-30.

Xu, Mengqing., Xiao, Ang., Li, Weishan., Lucht, Brett L., 2010. Investigation of Lithium tetrafluorooxalatophosphate [$LiPF_4(C2O)_4$]as a lithium-Ion battery electrolyte for elevated temperature Performance. J. Electrochem. Soc, 157(1), A115-A120.

Logan, E. R., Erin M. Tonita, Gering, K. L., Lin Ma, Michael, K. G., Bauer,1 Jing Li, L. Y. Beaulieu, and Dahn, J. R., 2018. A study of the transport properties of ethylene carbonate-free Li electrolytes. J. Electrochem. Soc, 165(3), A705-A716.

Yamaki, Jun-ichi., Shinjo, Yohei., Doi, Takayuki., Okada, Shigeto., Ogumi, Zempachi., 2015. The rate equation of decomposition for electrolytes with $LiPF_6$ in Li-ion cells at elevated temperatures. J. Electrochem. Soc, 162(4), A520-A530.

Ahn, WonSool., Yoon, SooKong., 2007. A study on formation and thermal decomposition kinetics of PU elastomers by dynamic DSC and TGA analysis. Elastomer, 42, 47-54.

Gaulupeau, B., Delobel, B., Cahen, S., Fontana, S,. Herold, C., 2017, Real time mass spectroscopy analysis of Li-ion battery electrolyte degradation under abusive thermal conditions. J. Power Sources.,
, 342 (2017) 808-815.

FAA Office of Security and Hazardous Materials Safety, 2019. Lithium batteries & lithium battery-powered devices. Electronic reference available at https://www.faa.gov/hazmat/resources/lithium_batteries/media/Battery_incident_chart.pdf (accessed 17.08.19).

Feng, Xuning., Ouyang, Minggao., Liu, Xiang., Lu, Languang., Xia, Yong., He, Xiangming., 2018. Thermal runaway mechanism of lithium ion battery for electric vehicles. Energy Storage Mater, 10, 246-267.

Peng, Yang., Yang, Lizhong., Ju, Xiaoyu., Liao, Baisheng., Ye, Kai., Li, Lun., Cao Bei., Ni, Yong., 2020. A comprehensive investigation on the thermal and toxic hazards of large format lithium-ion batteries with $LiFePO_4$ cathode. J Hazard Mater, 381, 120916-120916., Advance online publication.

Li, Huang., Duan, Qiangling., Zhao, Chunpeng., Huang, Zonghou., Wang, Qingsong., 2019. Experimental investigation on the thermal runaway and its propagation in the large format battery module with $Li(Ni_{1/3}Co_{1/3}Mn_{1/3})O_2$ as cathode, J Hazard Mater, 375, 241-254.

MARY KAY O'CONNOR
PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Quantitative Structure-Property Relationships Methods to expedite Reactive Chemicals Hazards Assessment Processes

Harold U. Escobar-Hernandez[*, a], M. Sam Mannan[†, a], Maria I. Papadaki[b],
Qingsheng Wang[a], and Hong-Cai Zhou[c]
[a] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122, USA.
[b] Department of Environmental and Natural Resources Management, School of Engineering, University of Patras, Seferi 2, Agrinio, 30100, Greece.
[c] Department of Chemistry, Texas A&M University, College Station, TX 77842-3012, USA.
*Presenter Email: hu.escobar2208@tamu.edu

Abstract

Reactivity tests for identification and understanding of reactive chemical hazards are conducted using different experimental tools of calorimetry. These attempt to predict chemical properties and unsafe process conditions. Moreover, there is often an under prediction of reactivity-related properties (e.g. over pressure), and experimental techniques face significant challenges for its extensive duration and high costs. Quantitative Structure Property Relationships (QSPR) on the other hand are defined as mathematical correlations to predict chemical properties from a series of descriptors inherent from the substances.

A systemic approach is proposed to develop prediction tools based on QSPR. This, using laboratory test data and molecular modeling techniques. This methodology will be applied to the case study of metal-organic frameworks (MOFs), as emerging type of complex porous metals with potential applications in catalysis, carbon capture, energy among many other material science applications. Thus, by calculating molecular descriptors for a variety of MOFs using molecular modeling tools, decomposition properties obtained from thermogravimetric analysis are selected as target properties for this QSPR model. This will be followed by defining the limits of applicability and the development of a tool/software for the application of the model.

Keywords: Quantitative Structure-Property Relationships, Metal-Organic Frameworks, Descriptors, Reactive Chemicals.

[†]The authors dedicate this article to the memory of Doctor M. Sam Mannan (1954-2018). May his legacy be always with us.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Mitigation of a Reactive Relief Case by Instrumentation in Lieu of a Relief Device: A Case Study

Aristides Morillo*
Shell Global Solutions, Houston, TX 77082, USA
*Presenter Email: aristides.morillo@shell.com

Abstract

Styrene (A.K.A. styrene monomer or SM) is an important organic compound that is mostly used to produce polystyrene, styrene copolymers, latex, rubber, etc. Styrene can be industrially obtained via dehydrogenation of ethylbenzene, oxidation of propylene with ethylbenzene hydroperoxide, and from the reaction between toluene and methanol or benzene and ethane. Upsets in the SM manufacturing process can lead to the uncatalyzed SM polymerization reaction, which generates heat from the exothermic reaction and pressure from the consequent vaporization of the liquids present in the system, resulting in catastrophic failure of the process equipment, loss of containment, and fire/explosion with potential for multiple injuries/fatalities. Proper safeguarding of the SM units against the runaway polymerization reaction is a challenge. In addition, environmental regulations as well as the potential for community impact and/or reputational damage have motivated the industry to avoid the relief of hydrocarbons to the atmosphere during process upsets. This presentation gives an example of how to safeguard SM units by using safety instrumented systems in place of a safety relief valves.

Keywords: styrene, polymerization, runaway reaction, relief valve, safety instrumented system

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Comparison of Explosion Methods for Large-Scale Unconfined Elongated Explosions with Propane and Methane mixtures

Cassio Ahumada*, Pratik Krishnan, Frank-Ioannis Papadakis-Wood, Noor Quddus, Qingsheng Wang, and Shuai Yuan
Mary Kay O'Connor Process Safety Center
College Station
*Presenter E-mail: cassioahumada@tamu.edu

Abstract

Existing methods for flame propagation and deflagration to detonation transition (DDT) prediction can be divided into three main categories: empirical models, phenomenological and Computational Fluid Dynamics (CFD) based. The former relies on correlations derived from experimental tests and are usually very simple and fast to apply. Phenomenological methods are simplified models which represent the major physical processes in the explosion. CFD-based models, on the other hand, are more sophisticated and require a high degree of expertise for its usage and data analysis. Although all three types of methods are extremely useful for overpressure and flame speed prediction in scenarios involving accidental industrial explosions, they usually fail to predict the occurrence of deflagration-to-detonation transition (DDT) and flame acceleration for low and medium reactivity fuels, such as propane and methane, in elongated clouds. This can be related to the fact that detonation onset or highly turbulent flames are often ignored for such types of fuel. Having that in mind, this paper aims to conduct a review of current explosion models and compare them to recent large-scale tests with premixed propane-air and methane-air mixtures. The ultimate goal is to identify main flame parameters to be included in explosion analysis and propose modifications to improve overpressure and flame speed prediction for elongated vapor clouds.

Keywords: VCE, deflagration-to-detonation transition, explosion safety

1 Introduction

Flame propagation and explosion behavior of hydrogen and hydrocarbon-based mixtures remain critical issues for explosion safety in chemical plants, refineries, and nuclear power plants. In the last decades, a considerable number of incidents related to accidental releases of large quantities of flammable mixtures followed by ignition has been observed [1]. One of the most notorious cases include the explosions inside an oil terminal in Jaipur, India (October 2009) [1]. A gasoline leak that lasted around 75 minutes before ignition, resulted in a vapor cloud explosion that led to eleven deaths and several tank fires. Damage reached a distance of 2 kilometers. Evidence led to the conclusion that transition to detonation was the only possible explosion mechanism. In another instance, the explosion in Buncefield fuel storage depot in December 2005 measured 2.2 on the Richter scale and caused immense destruction to the area around, the damage reaching a radius of 1.5 kilometers, whereas the explosion was confined in a small area [2].The severity of the explosion could not have been predicted by any major hazard assessment method of the time [2].

Such incidents highlight the importance of proper design and robustness of explosion mitigation methods. From the practical point of view, safety professionals work towards estimating flame speeds and maximum overpressure build-up for a wide range of industrial releases scenario. This information is used to support safety design decisions and protective measure specifications. Defining the entire spectrum of plausible scenarios is not a straightforward task, it must address all affecting parameters including release locations, mixture concentration, the volume of flammable cloud, equipment density and disposition, and ignition position. This problem can be simplified by identifying and ranking conditions that are likely to lead to more severe explosion cases. Therefore, researchers have proposed empirical correlations [3]and numerical codes [4][to account for obstruction characteristics (equipment density and spacing) that might lead to deflagration to detonation transition (DDT) during explosion modeling analysis.

Existing methods for flame propagation and DDT prediction can be broadly divided into three categories: empirical models, phenomenological methods, and computational fluid dynamics (CFD) codes [1]. Empirical models are based on correlations derived from experimental results and are usually very simple and fast to apply. The Baker-Strehlow-Tang (BST) curves are an example of such a model that has been used extensively by oil and gas industry. They were updated in 2005 to include the likelihood of DDT and estimate overpressure based on flame speed [2]. This flame speed depends on three parameters: reactivity, confinement and congestion. There have been several efforts to improve the model by redefining the parameters and incorporating ground effects [3]. Another example is the TNO multi-energy method which predicts the overpressure based on strength curves [4].

CFD codes, on the other hand, tend to be more time consuming and require a certain degree of expertise to interpret the results. Models of this type calculate the overpressure by solving the Navier-Stokes equations and include additional sub-models to incorporate the effect of turbulence and combustion [5]. FLACS™ is one of the commercially available CFD package and has a specific methodology to predict the potential of DDT. This method has been validated against several small-scale experiments involving different types of fuel [6].
The primary goal of this study is to conduct a review of current explosion models and understand their limitations. The objective is to compare predicted results against recent large-scale tests with premixed propane-air and methane-air mixtures for elongated clouds [refer gexcon report].

2 Current explosion models used for comparison

An initial screening of the current methods utilized for large scale explosion modelling was made. A summary of the most common methods used can be seen in **Error! Reference source not**

found. grouped by their model type. Some methods were later discarded from this analysis due to the lack of guidance available in the open literature.

Table 1. List of common explosion methods for overpressure and flame speed prediction

Type of Model	List of Models Considered Initially	Source
Phenomenological	CLICHE*	[5]
	SCOPE*	[6]
Empirical Correlations	TNT Equivalent Method	[7, 8]
	TNO Multi-energy Method (MEM)	[9-11]
	BST	[3]
	Primary Explosion Site (PES)	[12-14]
	CAM Method Version 2	[15, 16]
	Melton and Marx correlation for flame speed	[17]
	Li *et al* (2014) Correlation	[18]
	Elongated VCE Blast Waves (Baker Risk)*	[19]
Numerical Models	REAGAS *	[20]
	EXSIM*	[21]
	FLACS*	[4]
*Methods highlighted were discarded from the analysis due to the lack of information available in the open literature		

The main objective of this study is to compare models that are easy and quick to apply and available. For that reason, only empirical correlations were investigated. Table 2 summarizes all empirical correlations used in this work, highlighting the main variable used, the weaknesses and strengthens.

Table 2. List of Empirical Correlations used in the current study

Model	Main Variables	Main Assumptions and Drawbacks
TNT Equivalent	Mass of fuel (M_{fuel}) Fuel Heat of Combustion (ΔH_{fuel}) Explosion yield factor (α_c) Distance from explosion center (r)	**Positive Aspects** Easy to use **Drawback/challenges** It compares a vapor cloud explosion (initially as deflagration) to a detonation type of regime, as a result of TNT explosion. Does not calculate flame speed and neglects effects from confinement and congestion regions
TNO Multi-energy	Volume Blockage Ratio (VBR) Obstacle Diameter (D) Flammable Cloud Length ($\mathrm{L_p}$) Laminar Flame Speed (S_{L}) Cloud Confinement (2D or 3D)	**Positive aspects** Relatively easy to apply Maximum overpressure is based on the flame speed which is a function of the listed variables. Only confined and/or congested regions are included in the calculation **Drawback/challenges** It assumes uniform congested levels and there are no limiting values for Pmax.
PES	Obstacle Diameter (D) Distance between obstacle (x) Flammable Cloud Radius (R) Laminar Flame Speed (S_{L}) Laminar flame thickness (δ)	**Positive aspects** Maximum overpressure is based on the flame speed which is a function of the listed variables. There is a limiting value for Pmax **Drawback/challenges** It assumes uniform congested levels. It assumes central ignition (spherical shape explosions) It requires fitting models to estimate empirical factors a and b
CAM 2	Area blockage ratio (ABR) Distance between obstacles (x) Number of obstacle rows (N)	**Positive aspects** Relatively easy to use

	Laminar Flame Speed (S_L) Laminar flame thickness (δ)	Maximum overpressure is based on the flame speed which is a function of the listed variables. **Drawback/challenges** It assumes uniform congested levels. It does not estimate flame speed
BST	Laminar Flame Speed (S_L) Volume Blockage Ratio (VBR) Confinement (2D, 2.5D, and 3D)	**Positive Aspects** Easy to use Quick Takes into account some geometrical details Handle multi-ignition point **Drawbacks/challenges** Can be over conservative Does not account for the real cloud size
Melton and Marx	Laminar Flame Speed ((S_L) Volume Blockage Ratio (VBR)	**Positive Aspects** Easy to use Quick Takes into account some geometrical details Handle multi-ignition point **Drawbacks/challenges** Assume uniform congested levels
Li et al (2014) Correlation[18]	Area blockage ratio (ABR) Volume blockage ratio (VBR) Laminar Flame Speed (S_L) Average obstacle size (D)	**Positive aspects** Relatively easy to apply Maximum overpressure is based on the listed variables. Only confined and/or congested regions are included in the calculation **Drawback/challenges** It assumes uniform congested levels and there are no limiting values for Pmax.

3 Experimental data used as basis in this work

The experimental data used in this paper is from the tests conducted by a joint SRI/Gexcon [22, 23] which is summarized in Table *3* . Tests were performed using an experimental test facility with geometries similar to a full-scale petrochemical facility, where flame acceleration can occur.

Obstacles inside the facility were designed to represent typical congestion that can cause acceleration of the flame front through homogeneous mixtures of flammable gas (*i.e.*, methane or propane with air).The Modular Flame Acceleration Test facility was made up of a set of 30 congestion modules. The modular form gave flexibility in arranging the orientation of the obstacles to the facility geometry. This flexibility enhanced control in achieving the desired environment, including overpressure range, areal variation of the overpressure within the facility, and flame speed. Each module measured approximately 3.7 m by 3.7 m by 3.7 m. The modules were designed so that the congestion level could be adjusted by populating the module with pipes. Four different test configurations were used in this study: a) the 24-module "low congestion", b) the 30-module "low congestion", c) the 30-module "high congestion", and d) the 14-module "high congestion" configurations.

Table 3. Summary of all experimental conditions tested in the facility with propane and methane-air mixtures

No.	Fuel	Equivalent Ratio	Congestion	Modules	Pmax (barg)	Maximum Flame Speed (m/s)	Combustion Regime
5[a]	Propane	1.1	Low	24	39.4	1790	DDT
6[a]	Propane	1.1	Low	24	20.2	1760	DDT
7[b]	Propane	1.05	Low	24	44.5	1680	DDT
8[b]	Propane	1.05	Low	24	12.8	1680	DDT
9	Methane	0.95	Low	30	0.1	85	Slow Deflagration
10	Propane	0.8	Low	30	0.05	70	Slow Deflagration
11	Propane	1.35	Low	30	0.14	135	Fast Deflagration
12[a]	Propane	1.1	Low	24	21.0	1750	DDT
13	Methane	1.05	High	30	0.5	250	Fast Deflagration
14	Propane	0.9	High	30	21.6	1790	DDT
15	Propane	1.35	High	30	52.6	1720	DDT
16	Methane	1.05	High	30	15.6	830	Choked

17[c]	Methane	1.05	High	14	0.05	80	Slow Deflagration
Notes:							
[a,b] Tests marked with letters presented similar experimental conditions							
[c] Test 17 was excluded from the analysis because analysed the impact of suppression systems in the early stage of flame propagation.							

Flame speed was determined via three different measurement techniques:

1. direct flame measurement using ion probes (partly unreliable)
2. direct flame tracking using the high-speed video
3. flame tracking using image gradient post processing.

4 Results and Discussion

This section is organized in three different estimated parameters: DDT predictability, source overpressure, and flame speed estimation. At the moment of this study, the data for overpressure at relative distance is not publicly available and, therefore, it is excluded from this analysis.

Table 4. List of parameters calculated by each model

Model	Calculated Parameters			
	Overpressure at relative distance	Flame Speed	Source Overpressure	DDT Potential
TNT Equivalent	X			
TNO MEM	X		X	X[a]
CAM 2	X		X	X[a]
BST	X	X	X	X
PES	X	X	X	X[b]
Melton and Marx Method	X	X	X	X
Li et al			X	X[a]

Notes:

a. Potential for DDT is assessed based on estimated overpressure. If overpressure exceeds 5 barg, then detonation is expected.
b. Potential for DDT is assessed based on estimated flame speed. If estimated flame speed exceeds the sonic velocity in the unburned mixture, then detonation is expected.

4.1 DDT Predictability

An initial analysis of the DDT predictability of each model was conducted using their original guidelines (see *Table 5*). Experiments with similar conditions are grouped in the same column. For methods that calculate source overpressure, DDT is assumed possible for case for which source pressure exceeds 5 barg. On the other hand, for methods that calculate flame speeds, DDT is considered probable when flame speed exceeds the sonic speed in the unreacted mixture.

It is interesting to observe that CAM 2 was the only method able to predict DDT for all cases that experienced this phenomenon. On the other hand, this model also highlights a potential for DDT in experiments with methane and high congestion (test 13,16, and 17). This is mainly due to the high dependency of the model on the obstruction parameters. It is important to have in mind that DDT for methane-air mixtures is extremely improbable, but this can be used as an indicator for flame acceleration.

The PES model only predicts DDT for tests with high congestion. Similar to CAM 2, PES has an exponential dependency with congestion parameters. The TNO MEM predicted DDT correctly for one test with propane-air mixture in high congestion.

Contrary to the other methods, BST and Melton and Marx model fail to predict DDT for all cases. This is because they exclude the possibility of DDT for fuels with medium reactivity such as propane [3].

Table 5. Results for DDT predictability based on original guidelines for each method. Cells marked by "x" indicates that DDT is possible. Green shade represents correct prediction and orange shade incorrect prediction.

	Tests with Propane						Tests with Methane			
	DDT				No DDT		No DDT			
	5,6,12	7,8	14*	15*	10	11	9	13*	16*	17*
TNO MEM			x					x	x	x
PES Model			x	x				x	x	x
CAM 2	x	x	x	x		x		x	x	x
BST 3										
Melton and Marx										
Li et al			x							
* Tests with high VBR (high congestion)										

Modifications to the listed methods, except CAM 2, were suggested based on this analysis and the comparison with flame speed results (see section 4.2). Results originated from the final guidelines are presented in from the final guidelines are presented in Section 4.3.

4.2 Flame Speed Comparison (deflagrative part)

Flames speeds results from PES model, BST, and Melton and Marx method were compared experimental results. For tests in which DDT occurred, only the deflagrative part was considered.

PES Model

Figure 1 shows the predicted values obtained from PES model versus experimental data. A big discrepancy was observed between the results for high congestion values. In those cases, congestion parameters were used based on current guidelines: 0.3m for obstacle spacing (x) and 0.5 for obstacle size over obstacle spacing (y/x). This discrepancy was greatly reduced when both parameters were modified with the actual values of 0.6 m and 0.3 m, respectively.

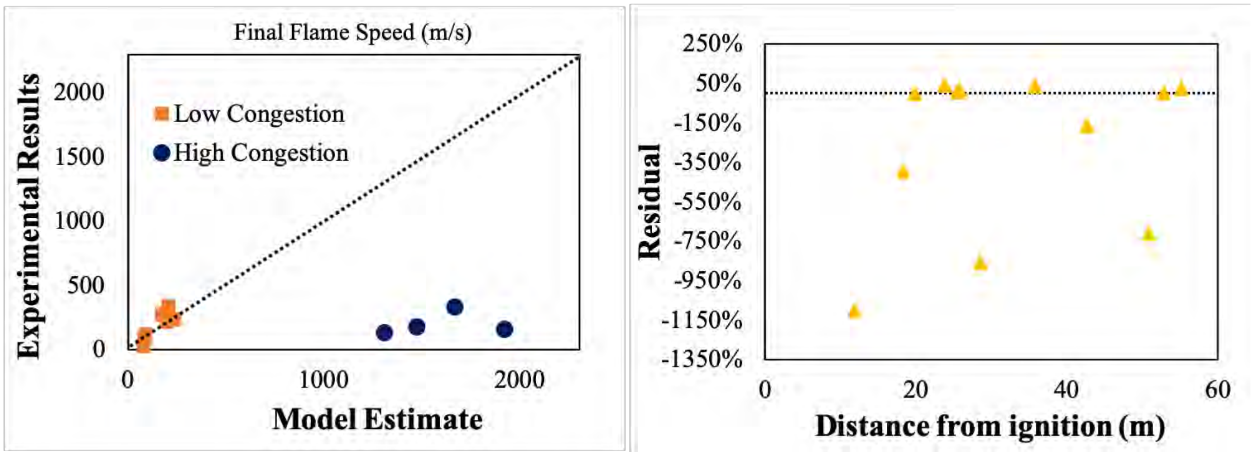


Figure 1. Comparison between predicted flame speed from PES model and experimental results, considering the deflagrative part (left -hand side), and the residual analysis (right-hand side). Congestion parameters are based on the method recommendations

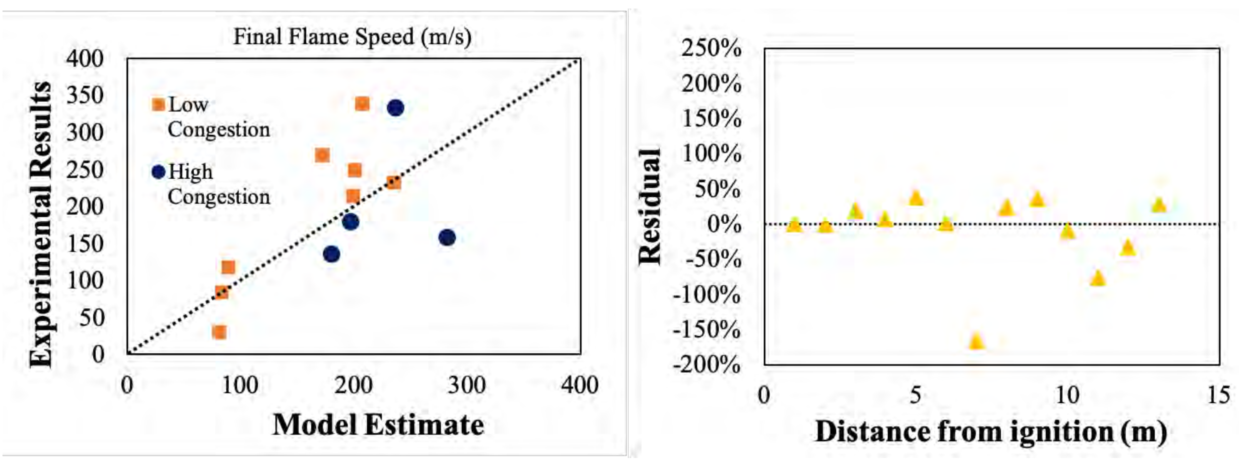


Figure 2. Comparison between predicted flame speed from PES model and experimental results, considering the deflagrative part (left -hand side), and the residual analysis (right-hand side). Congestion parameters were calculated using real parameters.

Melton and Marx Model

The Melton and Marx model combines the equation originated from MERGE experiments with the BST method to calculate flame speeds within a congested region. Although the results from this model were satisfactory using the normal guidelines (see Figure *3*), predictions were improved using a modified version (see Figure *4*). This modification simply consists of using the original values of Mach number (M_f) defined by Tang (ref needed). This new value are listed Table *6* and its applicability also improve the prediction of DDT as shown in section 4.3.

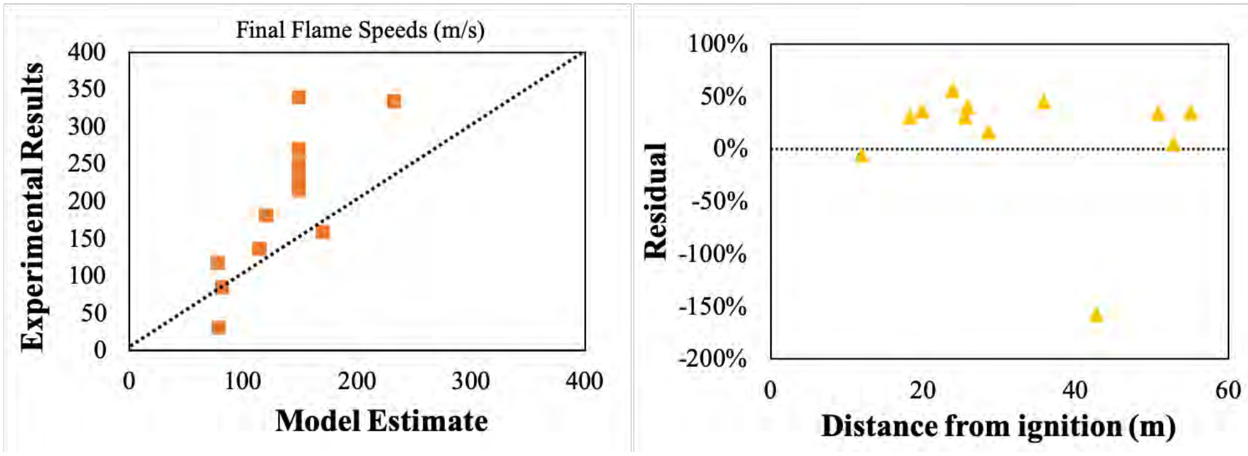


Figure 3. Comparison between predicted flame speed from Melton and Marx model and experimental results, considering the deflagrative part (left -hand side), and the residual analysis (right-hand side). Limiting Mach number (Mf) is calculated based on the method recommendations.

Table 6. Modified maximum Mach number (Mf) for flame speed calculation using Melton and Marx model

	Fuel Reactivity	Obstacle Density		
		H	M	L
2D Flame	H	5.3	5.3	0.81
	M	2	0.89	0.66
	L	0.89	0.66	0.13
2.5D Flame	H	5.3	5.3	0.66
	M	1.4	0.76	0.41
	L	0.7	0.49	0.09
3D Flame	H	5.3	5.3	0.5
	M	0.7	0.62	0.17
	L	0.48	0.32	0.06

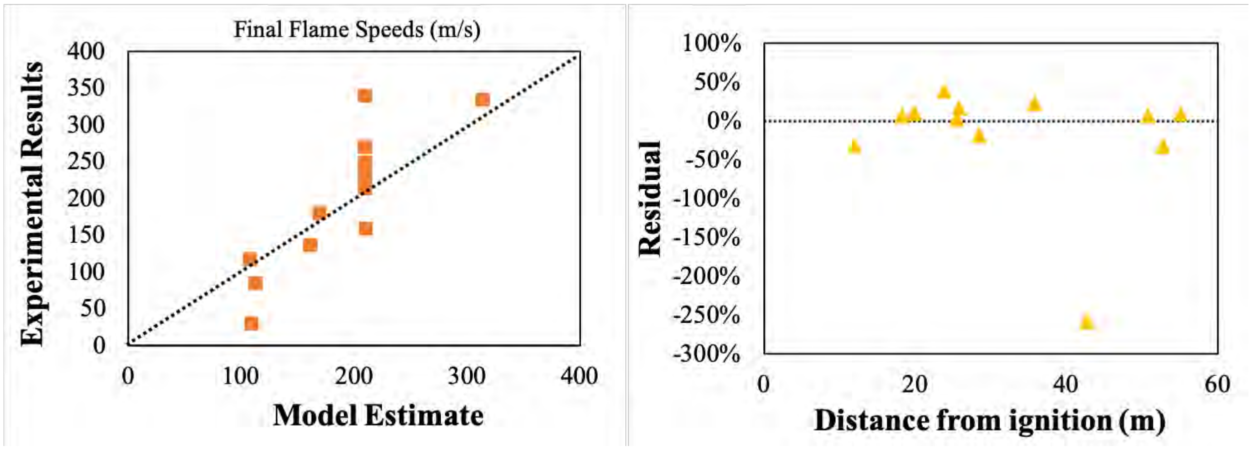


Figure 4. Comparison between predicted flame speed from Melton and Marx model and experimental results, considering the deflagrative part (left -hand side), and the residual analysis (right-hand side). Limiting Mach number (Mf) was modified based on the conversion between Mw and Mf published by Tang

4.3 DDT Predictability with Modified Guidelines

The prediction of DDT was improved for almost all the models used in this study, except for the one presented by Li et al because the number of data was scarce to proposed a significant change (see Table *7*).

Table 7. Results indicating the predictability of DDT using the modified version of each model guideline. Cells marked by "x" indicates that DDT is possible. Green shade represents correct prediction and orange shade incorrect prediction. Cells with* indicate suggested an improved result.

	Tests with Propane						Tests with Methane		
	DDT				No DDT		No DDT		
	5,6,12	7,8	14	15	10	11	9	13	16
TNO MEM	x*	x*	x					x	x
PES Model	x*	x*	x*	Def and DDT*				Def and DDT*	Def and DDT*
CAM 2	x	x	x	x		x		x	x
BST 3	Def and DDT*	Def and DDT*	Def and DDT*	Def and DDT*				Def and DDT*	
Melton and Marx	Def and DDT*	Def and DDT*	Def and DDT*	Def and DDT*				Def and DDT*	
Li et al			x						

For TNO MEM, the current guide for overpressure prediction in elongated clouds consist first in estimating ΔP for the smallest side. If this value exceeds $30kPa$, then it is suggested to calculate for the longest flame path. The initial value of $30kPa$ was selected randomly, without experiment validation. For that reason, and based on the current data, the authors of this paper recommend reducing the threshold to 25kPa. This slight reduction enables a better prediction of DDT potential and flame acceleration.

For BST, PES and Melton and Marx, a new guide for DDT prediction was applied following the Mach number ranges proposed by Geng *et al.* [19]:

- $M_f < 0.6$, only deflagration is expected
- $0.6 \leq M_f < 0.9$, both deflagration and DDT are possible
- $M_f \geq 0.9$, DDT is expected

Using this new guidance improved considerably the prediction for all those three methods.

4.4 Source Overpressure (deflagrative part)

Lastly, Table 8 shows the comparison between the overpressure estimated from each model and the median value from the experimental results, deflagrative wave only. As expected, the TNT model originated the most conservative results. This model assumes that a percentage of the flammable cloud detonates. This is not very good given that detonation and deflagration as completely different phenomena. Both TNO MEM and CAM 2 originated over conservative results (more than 1,000%) for similar cases.

Table 8. Comparison (in percentage) between overpressure estimated from each model and experimental values (median value)

Methods	Tests with DDT (deflagrative section)							Tests without DDT				
	5	6	7	8	12	14	15	9	10	11	13	16
TNT	8E3%	1E4%	2E3%	1E4%	4E4%	9E3%	3E4%	2E5%	6E5%	2E5%	1E5%	5E5%
TNO MEM	239%	649%	978%	666%	3E3%	55%	2E3%	1E4%	5E4%	1E4%	2E4%	1E3%
BST	-42%	-10%	58%	12%	185%	-33%	25%	358%	1E4%	359%	496%	508%
PES Model	-21%	22%	111%	50%	285%	-15%	122%	835%	3E3%	990%	1E4%	327%
CAM 2	188%	357%	685%	458%	2E3%	318%	1E3%	4E4%	2E4%	7E3%	5E3%	2E3%
Melton and Marx	-42%	-10%	58%	12%	185%	-33%	25%	358%	1E3%	359%	496%	508%
Li et al	-77%	-36%	-16%	-40%	168%	-98%	47%	2E3%	9E3%	2E3%	2E3%	-65%

5 Conclusion

This paper reviews the most common and new methods available for DDT prediction and overpressure estimation in large unconfined vapor cloud. Initially, using their respective original guidance, only CAM 2 was able to accurately predict DDT for the cases analyzed. For that reason, the authors proposed slight modification when utilizing each model, improving their performance. It interesting to observe that simple methodologies, such those one reviewed, can be applied to predict DDT for large structures.

6 References

[1] G. Atkinson, J. Hall, and A. McGilivray, "Review of Vapour Cloud Explosion Incidents ", The UK HSE, 2017.

[2] D. Bradley, G. Chamberlain, and D. Drysdale, "Large vapour cloud explosions, with particular reference to that at Buncefield," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* vol. 370, no. 1960, pp. 544-566, 2012.

[3] A. J. Pierorazio, J. K. Thomas, Q. A. Baker, and D. E. Ketchum, "An update to the Baker–Strehlow–Tang vapor cloud explosion prediction methodology flame speed table," *Process Safety Progress,* vol. 24, no. 1, pp. 59-65, 2005.

[4] C. Rosas, S. Davis, D. Engel, P. Middha, K. van Wingerden, and M. Mannan, "Deflagration to detonation transitions (DDTs): Predicting DDTs in hydrocarbon explosions," *Journal of Loss Prevention in the Process Industries,* vol. 30, pp. 263-274, 2014.

[5] R. Cleaver, C. Humphreys, J. Morgan, and C. Robinson, "Development of a model to predict the effects of explosions in compact congested regions," *Journal of hazardous materials,* vol. 53, no. 1-3, pp. 35-55, 1997.

[6] J. Puttock, M. Yardley, and T. Cresswell, "Prediction of vapour cloud explosions using the SCOPE model," *Journal of Loss prevention in the Process Industries,* vol. 13, no. 3-5, pp. 419-431, 2000.

[7] W. A. CCPS, Hoboken, NJ, 456 pages, $125.00, ISBN-13: 978-0-470-25147-8 Reviewed by Stanley S. Grossel, Process Safety and C. Design Consultant, NJ, "Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE, and Flash Fire Hazards, (August 2010)," *Process Safety Progress,* vol. 30, no. 2, pp. 187-187, 2011.

[8] W. Brasie and D. Simpson, "Guidelines for estimating damage from chemical explosions. Symp. Loss prevention in the Process Ind," in *63rd National Meeting AIChE, St. Louis, MO*, 1968.

[9] W. Mercx, A. Van den Berg, and D. Van Leeuwen, "Application of correlations to quantify the source strength of vapour cloud explosions in realistic situations. Final report for the project:'GAMES'," *TNO Report, PML1998-C53, Rijswijk, The Netherlands,* 1998.

[10] A. Van den Berg, "The multi-energy method: a framework for vapour cloud explosion blast prediction," *Journal of Hazardous Materials,* vol. 12, no. 1, pp. 1-10, 1985.

[11] A. Van den Berg and A. Mos, *Research to improve guidance on separation distance for the multi-energy method (RIGOS)*. HSE, 2005.

[12] S. Dorofeev, "Evaluation of safety distances related to unconfined hydrogen explosions," *International Journal of Hydrogen Energy,* vol. 32, no. 13, pp. 2118-2124, 2007.

[13] C. R. Bauwens and S. B. Dorofeev, "Effects of the primary explosion site and bulk cloud in VCE prediction: A comparison with historical accidents," *Process Safety Progress,* vol. 34, no. 2, pp. 147-153, 2015.
[14] S. B. Dorofeev, "A flame speed correlationfor unconfined gaseous explosions," *Process safety progress,* vol. 26, no. 2, pp. 140-149, 2007.
[15] J. Puttock, "Developments in the congestion assessment method for the prediction of vapour-cloud explosions," in *Loss Prevention and Safety Promotion in the Process Industries*: Elsevier, 2001, pp. 1107-1133.
[16] J. Puttock, "Fuel gas explosion guidelines—the congestion assessment method," in *Second European Conference on major Hazards Onshore and Offshore, IchemE*, 1995, p. 267.
[17] T. A. Melton and J. D. Marx, "Estimating flame speeds for use with the BST blast curves," *Process Safety Progress,* vol. 28, no. 1, pp. 5-10, 2009.
[18] J. Li, M. Abdel-jawad, and G. Ma, "New correlation for vapor cloud explosion overpressure calculation at congested configurations," *Journal of Loss Prevention in the Process Industries,* vol. 31, pp. 16-25, 2014.
[19] J. Geng, K. Thomas, and Q. Baker, "A study of the blast wave shape from elongated VCEs," *Journal of Loss Prevention in the Process Industries,* vol. 44, pp. 614-625, 2016/11/01/ 2016, doi: https://doi.org/10.1016/j.jlp.2016.05.026.
[20] A. Van den Berg, "REAGAS—a code for numerical simulation of 2-D reactive gas dynamics," *Report PML-1989-in,* vol. 48, 1989.
[21] B. Hjertager, "Numerical models of gas explosions (eg EXSIM)," *Proceedings of the explosion prediction and mitigation: congested volumes and complex geometries, University of Leeds, Leeds, UK,* 1997.
[22] S. Davis, M. Groethe, D. Engel, and K. van Wingerden, "Large Scale Testing-Development of Advanced CFD Tools for the Enhanced Prediction of Explosion Pressure Development and Deflagration Risk on Drilling and Production Facilities," in *Offshore Technology Conference*, 2016: Offshore Technology Conference.
[23] S. Davis, E. Merilo, D. Engel, A. Ziemba, M. Pinto, and K. van Wingerden, "Large scale detonation testing: New findings in the prediction of DDTs at large scales," *Journal of Loss Prevention in the Process Industries,* vol. 48, pp. 345-357, 2017.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Modelling of Explosion Venting Fireballs

Francesco Colella, Alfonso Ibarreta*, Timothy J. Myers, Sean C. O'Hern, Malima Wolf, and May Yen
Exponent, Natick, MA, U.S.A
*Presenter E-mail: aibarreta@exponent.com

Abstract

The purpose of this study is to compare calculated sizes of explosion venting fireballs to correlations for a range of gas explosions in enclosures fitted with an explosion vent. Explosion vents are commonly used to protect process equipment containing flammable gases. When properly designed, an explosion vent can reduce the peak overpressure inside the enclosure so that the enclosure does not permanently deform or fail catastrophically. The fuel and combustion products that exit the vent, however, create an external fireball hazard. Deflectors can be used to reduce the extent of that external fireball, but their effectiveness has not been rigorously tested for vessels larger than 20 m^3. Recently, there have been questions about the accuracy of correlations to predict fireball dimensions from explosion vents and the effects of deflectors on those dimensions.

The fireball size during venting is crucial in determining the thermal hazard area around the protected enclosure. The National Fire Protection Association standard NFPA 68 and International Standard EN14994 provide correlations for calculating the extent of the expected fireball during explosion venting scenarios. The formulas for gas-explosion fireball-sizes are empirical and based on data from a limited number of experiments.

In this study, explosion-venting scenarios are modelled numerically using FLACS v10. FLACS is a Computational Fluid Dynamics (CFD) software widely used in the oil and gas industry to perform explosion consequence modelling (Gexcon 2015). The CFD model was used to evaluate the fireball extent and temperature. The model results provide the fireball shape and size for different scenarios including scenarios with deflectors. A number of parameters are varied, including:

- Enclosure size
- Type of fuel
- Presence of a deflagration deflector plate

The study elucidates the relative importance of each of these parameters on the explosion fireball size. This can assist in designing future testing programs to examine fireball size and identifying parameters for use in improved fireball size correlations.

Keywords: venting, fireball, mitigation, industrial explosions, modelling

1 Introduction

Explosion protection by deflagration venting is a cost-effective and common method to protect equipment and enclosures that contain a flammable gas mixed with an oxidizer (normally air). Without an explosion vent, ignition of hydrocarbon fuel and air mixtures can result in pressures of several atmospheres, potentially causing permanent damage or bursting of the enclosure. Explosion vents are designed to open (or activate) in the case of a deflagration at relatively low pressures. The vent activation pressure, P_{stat}, is designed to be above the operating pressure, but well below the maximum allowable pressure of the vessel or enclosure. If designed properly, the explosion vent area allows sufficient venting of the gases to limit the maximum vented overpressure, P_{red}, below some maximum vessel pressure criteria. The maximum allowable P_{red} will depend on the strength of the enclosure and whether permanent deformation of the enclosure is allowed.

Even when the explosion vent is sized properly, the deflagration still needs to be vented to a safe location to avoid injuries. The maximum temperature of the combusted gases during a hydrocarbon-air deflagration under adiabatic conditions can reach temperatures on the order of 2,500 ˚C (4,500 ˚F). In addition to elevated temperatures, the vented explosion fireballs pose a thermal radiation hazard, due to radiation emitted by high temperature gases and soot.

A deflector plate can be used to reduce the extent of a venting fireball, as outlined in NFPA 68: Standard on Explosion Protection by Deflagration Venting. The use of a deflector reduces the hazard distance calculated under the standard. A deflector is designed as a plate, similar in geometric shape to the explosion vent but larger in scale, placed in front of the vent, at an inclined angle.

In this study, explosion venting scenarios including scenarios utilizing a deflector are modelled numerically using FLACS. A threshold temperature of 1,000 K (727 °C or 1,340 °F) is used to mark the fireball extent. This temperature value is chosen because it is well within the area where soot particles would glow and be visible, signifying the extent of the visible fireball. Other threshold criteria can be used with these simulations to predict the extent of a hazard area. Using a lower threshold temperature extends the calculated fireball length in the simulations. The hazard area may also be larger than the temperature contour boundary identified due to the additional radiative heat transfer from the fireball.

In this paper, the fireball sizes for different gas explosion configurations, including the use of deflector plates, were evaluated using the CFD model and compared to US (NFPA 68) and European (EN 14994) empirical relations. This work is a continuation of the fireball modelling work described in Ibarreta et al. (2018), where combustible dust and flammable gas deflagration fireballs were modelled using FLACS.

2 Empirical Formulas for Fireball Size

The National Fire Protection Association standard NFPA 68 *Standard on Explosion Protection by Deflagration Venting* provides procedures to calculate explosion vent sizing as well as the extent of the expected fireball resulting from the vent activation. The formulas for gas explosion fireball sizes are empirical and based on data from a limited number of experiments (Mesa & Rockwell 2018).

For gas deflagration venting, NFPA 68 provides the maximum axial fireball distance from the vent (*D*) as

$$D = 3.1\left(\frac{V}{n}\right)^{0.402} \tag{1}$$

where *V* is the volume of the enclosure and *n* is the number of evenly distributed vents. NFPA 68 - 6.6.2.3 provides that the use of a deflector as specified in the standard reduces the calculated maximum axial fireball distance by 50% of the value calculated in Equation 2.

A similar formulation can be found in EN 14994 (2007). According to that standard, the fireball length for gas deflagration venting *(D)* can be estimated as

$$D = 5V^{1/3} \tag{2}$$

where *V* is the volume of the enclosure.

The empirical correlations for fireball sizes outlined above only depend on the protected enclosure volume and number of vents. The equations, therefore, do not take into account the vent geometry, mixture reactivity, peak overpressure or vent performance (*i.e.* activation pressure).

3 The Use of Deflectors for Fireball Reduction

Deflectors are obstructions specifically designed to deflect the explosion fireball generated during venting. They are used to protect occupied areas located in front of an explosion vent by reducing the fireball extent in case of deflagration. NFPA 68 - 6.6.2.4 specifies the design of a deflector for use with a given vent geometry as follows:

> *6.6.2.4 A deflector design shall meet all of the following criteria:*
>
> *(1) The deflector for a rectangular vent shall be geometrically similar to the vent and sized with a linear scale factor of at least 1.75. For a round vent, the deflector shall be square shaped and at least 1.75 times the vent diameter.*
>
> *(2) The deflector shall be inclined 45 degrees to 60 degrees from the vent axis, as shown in Figure 6.6.2.4.*
>
> *(3) The centerline of the deflector shall be coincident with the vent axis.*

(4) The distance from the vent opening to the deflector on the vent axis shall be 1.5D, where D is the equivalent diameter of the vent.

(5) The deflector plate shall be mounted so as to withstand the force exerted by the vented explosion, calculated as Pred times the deflector area.

(6) The deflector location shall not interfere with the operation of hinged vent closures.

EN 14994 has identical requirements for the dimensions of deflector plates. In accordance with these guidelines, deflectors were modelled in FLACS as square plates, , with the side length of the plate equal to twice the vent side length (1.75 times the vent equivalent diameter, defined as $2\sqrt{A/\pi}$). The plates were placed at a 45 degree angle, with the upper edge of the deflector angled away from the vent opening, and the center point of the plate placed at a distance of 1.5 times the equivalent diameter of the vent (1.7 times the vent side length).

NFPA 68 allows the use of a deflector plate to limit the hazard distance to 50% of the original length for enclosure volumes ≤ 20 m^3. According to NFPA 68 Section A.6.6.2.5, "[t]he ability of this deflector to limit flame length for [larger] vessels is uncertain." EN 14994 also indicates that the use of a deflector plate limits the hazard distance to 50% of the original value. Likewise, EN 14994 also has a similar limitation, stating "[t]he influence of deflectors has only been investigated for enclosure volumes up to 20 m^3 and shall therefore not be installed when the enclosure volume is greater."

4 Computational Fluid Dynamics (CFD) Model

The FLACS CFD software was used in this paper to model the vented deflagration phenomena and evaluate the maximum extent of the vented fireballs. FLACS is a commercial CFD software that is used in the oil and gas industry to model the behavior of explosions and deflagrations of vapors and gases. The software uses a three-dimensional finite element algorithm to simultaneously solve the combustion, radiation, and fluid equations governing dispersed fuel and air combustion. FLACS models take into account complex geometries that influence combustion behavior, as well as the effects of explosion vents. The FLACS model provides the time-dependent pressure field during an explosion event. The CFD model provides a time-dependent solution to the Navier-Stokes equations. In the model, conservation equations for mass, momentum, energy and gas concentrations are solved on a Cartesian grid using a finite volume method.

4.1 Model Geometries

The model geometries (see example in Figure 1) involve cubic enclosures of varying sizes located above a ground plane. A single rectangular vent is located at one side of the enclosure wall at the center of the wall. All the vents are square in shape and centered on the enclosure surface opposite the ignition location. The vents are set to be solid until the activation pressure, P_{stat}, is reached. At that time, the vents instantaneously open fully.

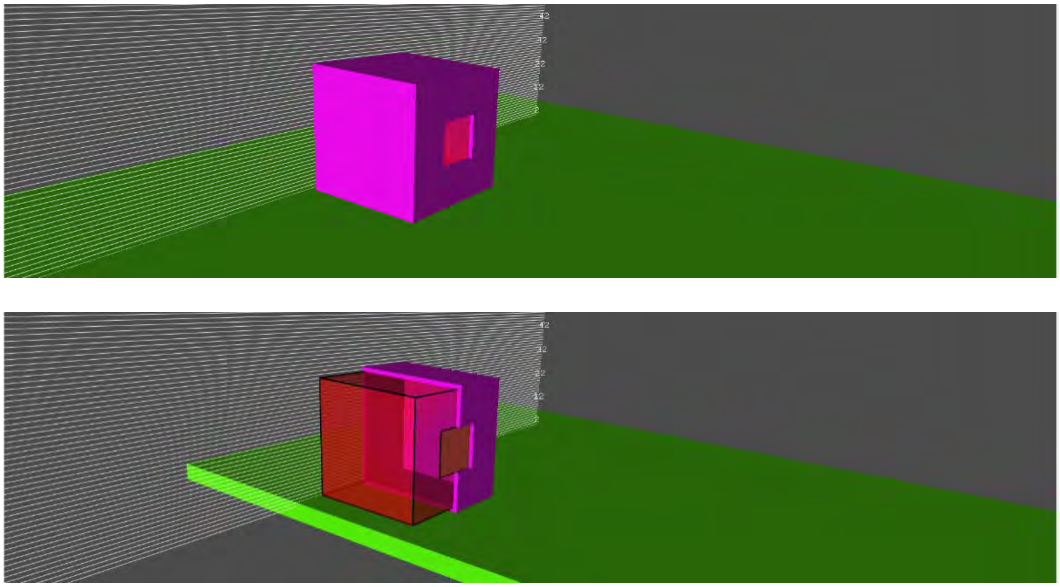


Figure 1. Sample CFD Model geometry without a deflector plate. The top image shows the entire geometry, while the bottom image shows a cut view highlighting the flammable cloud and explosion vent area.

The flammable gas mixture initially uniformly fills the entire volume enclosure, as shown in Figure 1. The ignition of the cloud occurs at time = 0 on the wall opposite to the location of the explosion vent, at the center point on the wall. The flammable gas combustion starts with stagnant conditions (zero velocity and turbulence) inside the enclosure.

In some scenarios, a deflector plate (see Figure 2) was placed in accordance with the description in Section 3.

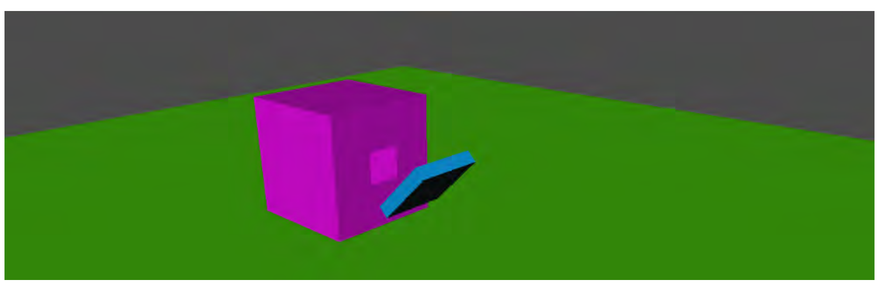


Figure 2. Sample CFD Model geometry with a deflector plate.

4.2 Scenario Conditions

Calculations were performed using methane, propane and ethylene fuels to determine the effect of fuel burning velocity and expansion ratio on fireball extent. The range of scenarios modelled is shown in Table 1. For FLACS calculations, combustion properties are the default values in the software libraries. The NFPA 68 and EN 14994 fireball length correlations do not use fuel specific parameters.

Two basic grid geometries were used, depending on the size of the enclosure and domain: (1) a fine grid with 10 cm minimum grid spacing inside the enclosure and downstream of the vent; and (2) a coarser grid, with 20 cm minimum grid spacing inside the enclosure and downstream of the vent. The calculations have 14 to 50 grid cells across the width of the enclosure, meeting the requirements of the FLACS manual to have at least "5-6 grid cells in smallest direction [of] flame acceleration" for a confined vessel (Gexcon 2015). A coarser grid was necessary for the > 30 m^3 enclosure volumes to keep the total grid size manageable. Similarly-sized volumes were run in both the 10 cm and 20 cm grids. The reduced pressure inside of the vented enclosure (P_{red}) was found to be grid size dependent, but the fireball dimensions were found to be relatively independent of the grid size used in calculations.

Table 1. Scenario matrix

Fuel	Methane	Propane	Ethylene
Concentration	Phi = 1.0	Phi = 1.0	Phi = 1.0
Fuel[1] S_u	38 cm/s	45 cm/s	74 cm/s
Enclosure Volume	4 – 1,000 m^3	4 – 1,000 m^3	4 – 1,000 m^3
Vent Size	0.2 – 16 m^2	0.2 – 16 m^2	0.2 – 16 m^2
Vent Activation Pressure	0.1 barg	0.1 – 0.2 barg	0.1 barg
# of scenarios	7	24	7

5 Flammable Gas Explosion Venting Results

FLACS calculated fireball lengths of propane, methane, and ethylene gas mixtures were compared with empirical formulas provided in NFPA 68 and EN 14994 as discussed in Section 2. Figure 3 shows the evolution of a typical gas explosion venting simulation, in this case, for a 3m x 3m x 3m cubic enclosure containing a stoichiometric mixture of propane and air with a 1-m^2 vent that activates at 0.1 barg. At 0.5 seconds after ignition, the jetting fireball has already reached a distance of 17 meters from the vent opening. At 1 second, the fireball has reached 23 meters from the vent opening. At 4.5 seconds, the fireball is nearing its maximum extent of 31.8 meters. Gas explosion fireballs for other sizes of enclosure and other fuel mixtures follow a similar development pattern. The results show how the fireball length is much greater than the height or width of the fireball, in contrast to the correlation in NFPA 68 that assumes all three dimensions are the same.

Figure 4 shows the same case as Figure 3 but with a deflector plate placed directly in front of the vent opening as described as Section 3. At 0.5 seconds after ignition, the jetting fireball has reached a distance of 10 meters from the vent opening, 40% shorter than the case without a deflector. At 1 second, the fireball has reached a distance of 11.5 meters from the vent opening, 50% shorter than the case without a deflector. At 2.25 seconds, the fireball has reached its maximum extent of 12.9 meters, 60% shorter than the case without the deflector.

[1] Default values in FLACS library

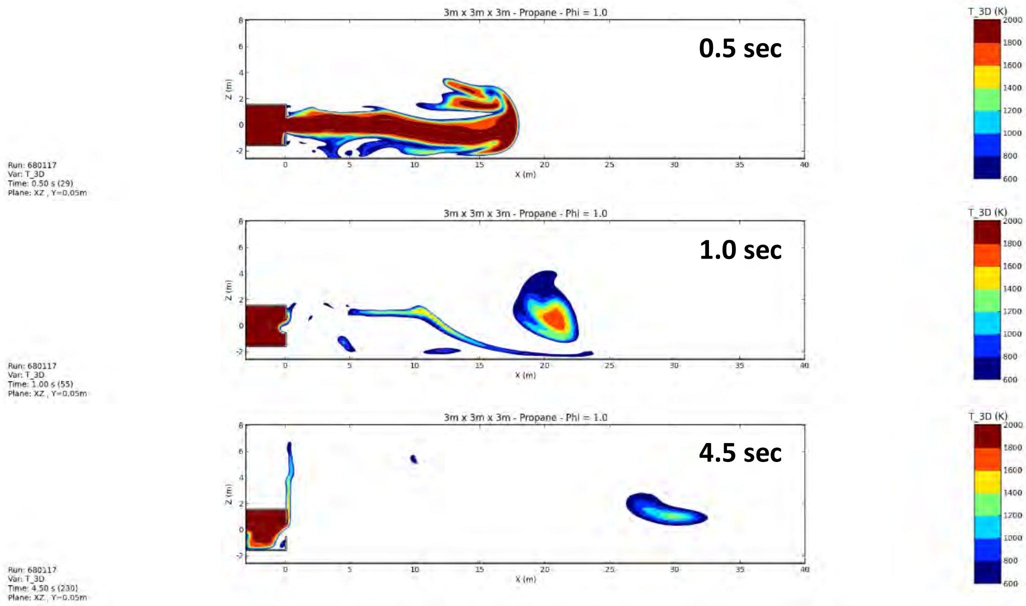


Figure 3. Time sequence of fireball temperature contours showing FLACS simulation of a propane/air (Phi = 1) vented explosion for a 3m x 3m x 3m enclosure with a 1 m^2 vent that activates at 0.1 barg. The maximum overpressure (P_{red}) for this scenario is 0.33 barg; and the maximum fireball extent is calculated to be 31.8 meters, based on the 1,000 K contour.

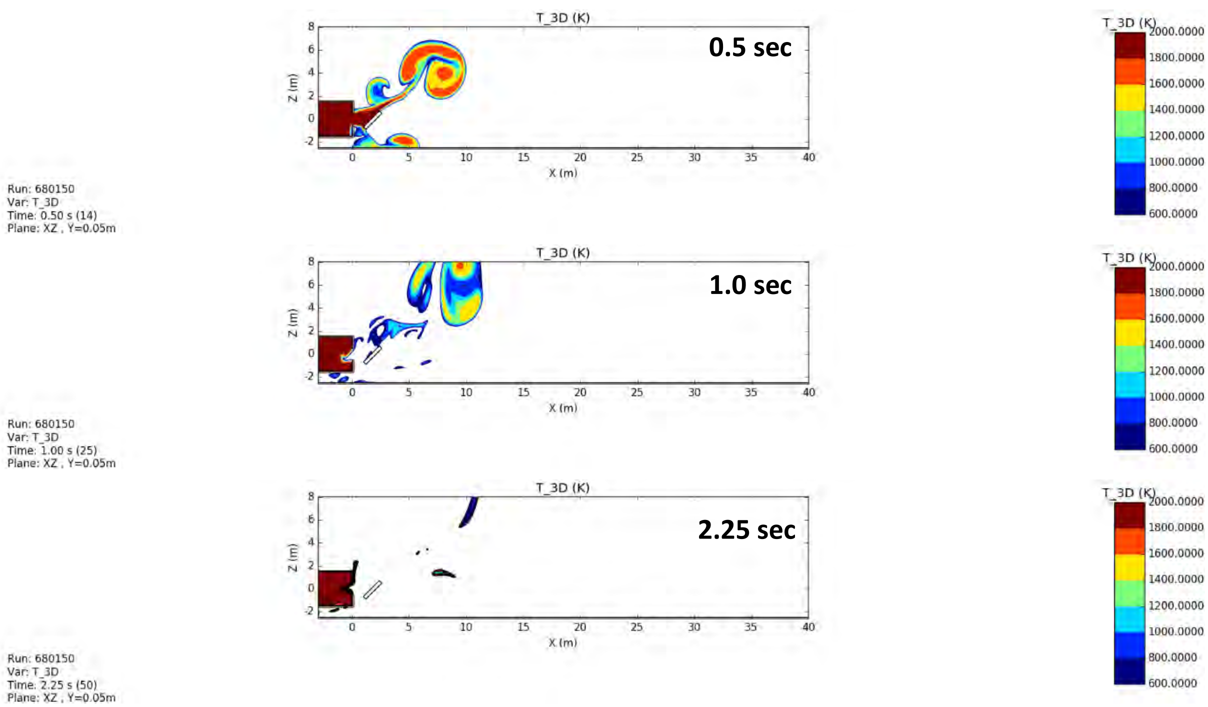


Figure 4. Time sequence of fireball temperature contours showing FLACS simulation of a propane/air (Phi = 1) vented explosion for a 3m x 3m x 3m enclosure with a 1 m^2 vent that activates at 0.1 barg with a 45degree deflector that has the center surface located 1.7 m away from the vent opening

To calculate the fireball extent, output data from FLACS simulations were analyzed to determine the furthest distance from the vent opening that reached the threshold temperature, taken as 1,000 K (727 °C or 1,340 °F).Figure 5 shows the calculated fireball lengths for stoichiometric mixtures of propane, methane, and ethylene in air as a function of enclosure volume. The calculated fireball lengths are compared to the fireball extent correlations from NFPA 68 and EN 14994, as discussed in Section 2. The fireball lengths calculated from the FLACS simulations are significantly larger than both correlations. The fireball length for methane deflagrations is smaller than that of propane for a given enclosure volume, while the fireball length for ethylene is similar to that of propane for lower enclosure volumes but longer at some larger enclosure volumes.

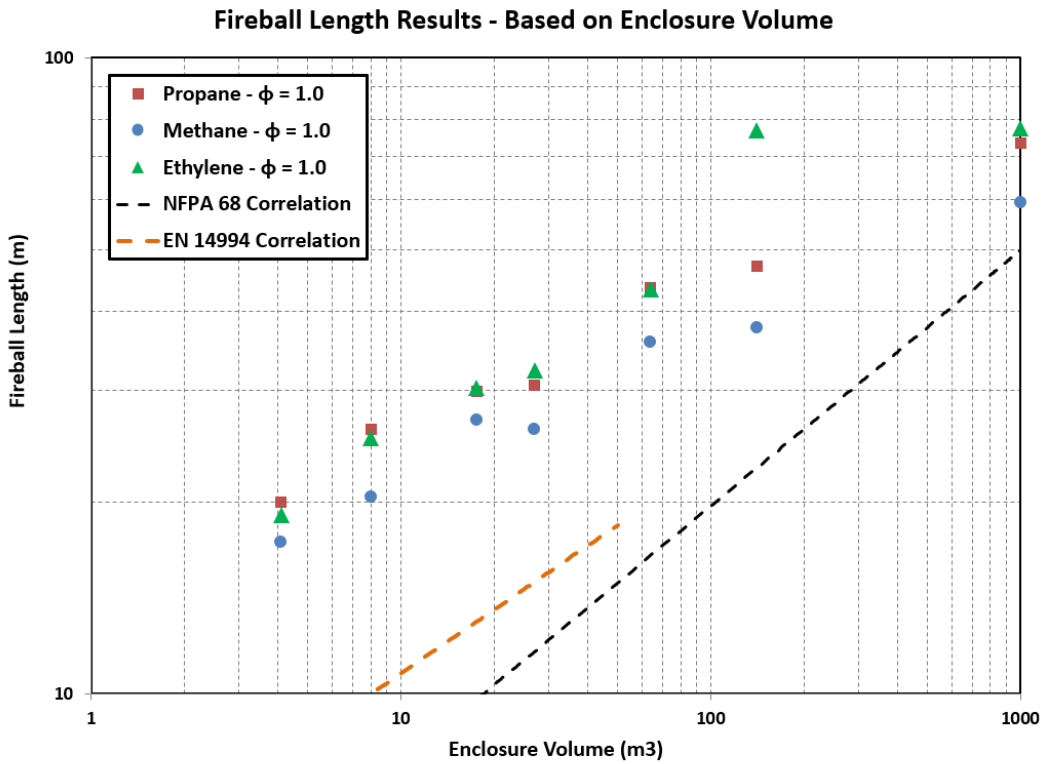


Figure 5: FLACS calculated fireball length for propane/air, methane/air, and ethylene/air mixtures at an equivalence ratio of 1 compared to the NFPA 68 and EN 14994 predicted values.

Both the maximum overpressure or expansion ratio and flame speed of the fuels increases from methane to propane to ethylene. It is likely that the differences in fireball dimensions are due to differences in the expansion ratios of the fuel, however, further analysis is required to separate the effect of expansion ratio and flame speed.

The effect of a deflector plate as a function of enclosure is shown in Figure 6. The fireball length of the FLACS simulations with and without the deflector plate are plotted against the given enclosure volume. The data show how the presence of a deflector plate has a very large impact on the fireball length, especially for smaller enclosures. The reduction in flame length is diminished for larger enclosures but is still sizeable. Correlations of fireball length with enclosure volume by EN 14993 and NFPA 68 with and without deflectors are also shown. What is not clear in Figure 6 is that the deflector plate not only reduces the downstream extent of the fireball, but also angles it upward, so that the longest flame extent occurs at an elevated location, further protecting potentially occupied areas near ground level. The fact that the FLACS calculations with a deflector plate agree with the NFPA 68 correlation for fireballs without a deflector plate is merely coincidental. The deflector plate shortened the fireball extent by at least 50% in all cases except for the case with a 1000 m^3 enclosure volume which had a fireball extent that was shortened by 30%. Cases where the enclosure volume was less than 20 m^3, the flame extent was shortened by at least 60%. The presence of an inclined deflector plate is therefore shown to decrease the length of the fireball by a factor of 1.5 to 3.6, with larger decreases for smaller enclosures.

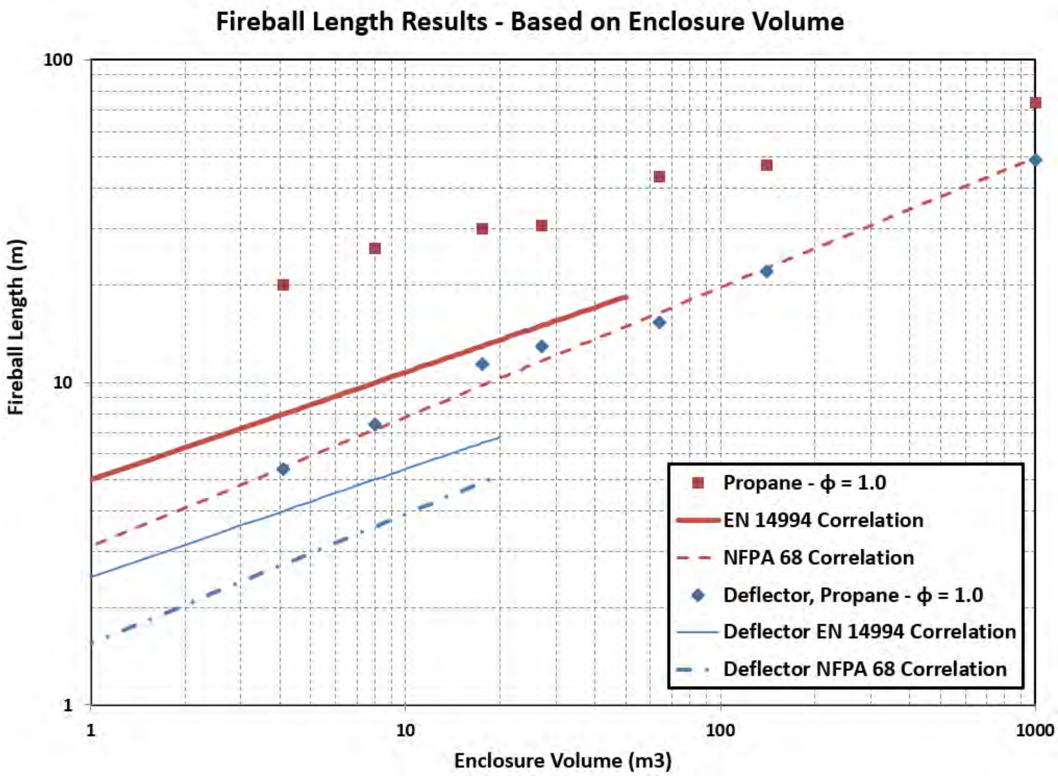


Figure 6. FLACS calculated fireball length for propane/air mixtures with and without a deflector plate as a function of enclosure volume compared to the NFPA 68 and EN 14994 predicted values.

6 Conclusions

This paper describes the results of CFD simulations of gas deflagration events in vented enclosures. The models were used to estimate the fireball extent, as well as the reduced enclosure overpressure resulting from the deflagration events. The paper presents a comparison between the numerical results and the empirical correlations in internationally recognized standards on deflagration venting, such as NFPA 68 and BS EN 14994.

Relatively-poor agreement was obtained between gas deflagration venting simulation fireball length data and the empirical correlations presented in the standards. In particular, the fireball size calculated using the FLACS CFD model is up to 2 to 3 times larger than the estimates obtained using the standard correlations. The simulations also show that the length of the fireball is much longer than the width or height of the fireball, whereas NFPA 68 assumes that all three dimensions are identical. Furthermore, a dependency of the fireball size on flammable gas species has been identified with propane and ethylene leading to larger fireballs.

The presence of an inclined deflector plate is shown to decrease the length of the fireball by a factor of 1.5 to 3.6, with larger decreases for smaller enclosures. The presence of a deflector plate not only reduces the downstream extent, but can also deflect the flame upward, further protecting locations near ground level.

Further analysis is required to determine the relative role of the expansion ratio and flame speed on the fireball dimensions. Intermediate and large-scale testing is recommended to better understand and characterize fireball sizes involving gas deflagration venting.

7 References

British Standard BS EN 14994 (2007) *Gas explosion venting protective system.*

Gexcon AS (2015), "FLACS v10.4 User's Manual" December 1, 2015.

Ibarreta, A., Colella, F., Wolf, M., O'Hern, S. & Myers, T. (2018) Modelling of Explosion Venting Fireballs. 12th International Symposium on Hazards, Prevention and Mitigation of Industrial Explosions (ISHPMIE) Kansas City, USA - August 12-17, 2018.

Mesa, G. & Rockwell, S (2018). Estimation of Fireball Dimensions from NFPA 68. Fire Protection Research Foundation Report, April 2018.

NFPA 68 (2018) *Standard on explosion protection by deflagration venting.*

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Heavy gas concentration prediction on complex terrain using CFD with Monin-Obukhov similarity theory

Charles Glover[a], Delphine Laboureur[a,b], and Jiayong Zhu[a]*
a Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, Texas, 77843-3122, USA
b Von Karman Institute for fluid Dynamics, 72, chaussée de Waterloo, Sint-Genesius-Rhode, Belgiumon
*Presenter E-mail: jychriszhu@tamu.edu

Abstract

Under stable atmospheric conditions (***i.e.,*** low wind speed and low heat radiation), once heavy gases (***e.g.,*** CO_2, H_2S, LNG) release to the atmosphere, the gas clouds tend to stay near the ground for long period of time, thereby causing high concentration zone and increasing the threats to the local population and the environment. Despite of the advanced development of computational fluid dynamic (CFD) modelling, or the Reynolds-Averaged Navier-Stokes (RANS) models with standard turbulence closures (***e.g.,*** standard $\kappa-\varepsilon$, RNG $\kappa-\varepsilon$ and $\kappa-\omega$), researchers have pointed out that these models are incompatible with the experimental data under stable atmospheric conditions. Therefore, there is an increasing interest in developing a robust mathematical model for heavy gas dispersion, especially in the field of turbulence modelling. This present study is to develop a CFD model with a two-equation turbulence model for heavy gas dispersion over complex geometry in stable atmospheric conditions. This two-equation turbulence model is a modified $\kappa-\varepsilon$ turbulence model based on the Monin-Obukhov similarity theory (MOST). The calculations from the modified turbulence model can maintain the homogeneity of the flow properties. The calculations from the CFD model with the modified $\kappa-\varepsilon$ model is compared with the experimental data collected from the Kit Fox experiment under stable atmospheric conditions (Class F). A robust and reliable model can provide potential guidelines for emergency mitigation planning for heavy gas leakage incidents.

Keywords: Risk, Risk assessment, Emergency, Dispersion model

1. Introduction

Hazardous gases leakage accidents are likely to cause serious injury to human health and to harm the local environment (Sklavounos and Rigas, 2004), especially for heavy gases (e.g., CO_2, H_2S, LNG), which possess larger density than air. When heavy gases release to the atmosphere, they tend to move towards the ground, thereby increasing the threat to the local population (Markiewicz, 2012).

A robust and reliable quantitative model is crucial for risk assessment which can provide quick predictions of downwind concentration and minimize the negative influences to the people and the environment (Markiewicz, 2012). As the advancement of the computational technologies, the numerical methods using the Computational Fluid Dynamics (CFD) models, which can predict fluid flow in complex geometries, are popular in both academic researches and industrial studies (Scargiali et al., 2008; Liu et al., 2016).

However, in recent years, many studies showed that the CFD models are incompatible with the experimental data. Studies showed that the calculations from CFD model using Reynolds-Averaged Navier-Stokes (RANS) with standard turbulence closures do not agree well with the large-scale experimental data, especially under stable atmospheric conditions (Pieterse and Harms, 2013). Furthermore, researchers pointed out that the potential issue for the discrepancies between the calculations and the experimental data are due to the ways that the standard turbulence closure calculate the pressure and the velocity. Therefore, homogeneous profiles are not maintained in the flow domain (Yasin and et. Al., 2019).

This present study incorporates the Monin-Obukhov Similarity Theory (MOST), a universal acceptable assumption for stable atmospheric conditions, in the RANS CFD model and validates the model with the experimental data. To apply the MOST to RANS CFD models, turbulence kinetic energy profiles, the turbulence dissipation rate profiles and the temperature profiles are modified based on the MOST. Also, the experimental data from the Kit Fox experiment were collected from literature and compared with the calculations from the modified RANS CFD model. The results showed that the modified RANS CFD model is able to maintain the homogeneity of the flow properties. Also, the calculations from the modified RANS CFD model agree well with the maximum concentration observed in the experiment.

With better confidence on the model by validating this model with other experimental data, this model can provide potential guidelines for emergency mitigation planning for heavy gas leakage incidents in a complex terrain, such as chemical plants and urban area.

2. Numerical approach

Numerical simulations with the standards and the modified turbulence closures are performed in the commercial Computational Fluid Dynamics (CFD) codes, ANSYS Fluent. The calculations are based on finite volume method for the discretisation of differential equations.

2.1. κ–ε turbulence model

The standard κ–ε turbulent model is a widely used to estimate the fluid flow momentum due to turbulence. The fluid flow considered in this work has high Reynolds number, which is classified as turbulence flow. Turbulence flow is described as the chaotic characteristics of the fluid motion due to pressure and flow velocity. The standard κ–ε turbulent closure, for example, uses turbulent kinetic energy [m^2/s^2] and dissipation rate of turbulence kinetic energy [m^2/s^3] as velocity and length scale related variables. The shear stress is defined as following:

$$u'w' = -\nu_t \frac{\partial \bar{u}}{\partial z} \; with \; \nu_t = c_\mu \frac{\kappa^2}{\varepsilon} \tag{1}$$

Here, c_μ is the turbulent viscosity coefficient. In the standard κ−ε turbulent closure, the value for c_μ is 0.09. The turbulent kinetic energy, κ, and the dissipation rate of the turbulent kinetic energy, ε, are estimated by solving the nonlinear partial differential equations shown below:

$$\mu_j \frac{\partial k}{\partial x_j} = \frac{\partial}{\partial x_j}\left[\frac{\nu_t}{\sigma_k}\frac{\partial k}{\partial x_j}\right] + P - \in \tag{2}$$

$$\mu_j \frac{\partial \epsilon}{\partial x_j} = \frac{\partial}{\partial x_j}\left[\frac{\nu_t}{\sigma_\epsilon}\frac{\partial \epsilon}{\partial x_j}\right] + C_1 \frac{\epsilon}{\kappa} P - C_2 \frac{\epsilon}{\kappa} \in \tag{3}$$

where P is the shear production term and ∈ is the shear dissipation term. In standard κ−ε turbulence model, the closure coefficients are given below:

$(\sigma_k, \sigma_k, C_1, C_2) = (1.0, 1.3, 1.44, 1.92, 1.3)$.

2.2. Application of Monin-Obukhov Similarity Theory (MOST)

MOST is a universal accepted theory for determination of vertical profiles of mean flow within the surface layer. Stratification effects could be important near the ground (roughly within 2 meters above the ground), especially in stable atmospheric conditions. Monin and Obukhov (1954) developed the Monin-Obukhov similarity theory (MOST) which suggested that the vertical variation of mean flow and turbulence characteristics in the surface flow should depends on the height (z) and the friction velocity (u_*). In order to define the velocity and potential temperature profiles within the surface layer, dimensionless stability functions for momentum and heat, which are denoted by Φ_m and Φ_m.

$$\Phi_m\left(\frac{z}{L}\right) = \frac{kz}{u_*}\left(\frac{du}{dz}\right) \tag{4}$$

$$\Phi_h\left(\frac{z}{L}\right) = -\frac{kz}{\theta}\left(\frac{d\theta}{dz}\right) \tag{5}$$

Gradients of wind speed and potential temperature are given with the dimensionless stability functions based on full-scale observations from the 1968 KANSAS experiments.

$$u(z) = \frac{u_*}{\kappa}\left[\ln\left(\frac{z}{z_0}\right) + \Phi_m\left(\frac{z}{L}\right) - 1\right] \tag{6}$$

$$T(z) = T_o + \frac{T_*}{\kappa}\left[\ln\left(\frac{z}{z_0}\right) + \Phi_m\left(\frac{z}{L}\right) - 1\right] \tag{7}$$

where

$$\Phi_m\left(\frac{z}{L}\right) = 1 + 5\frac{z}{L}$$

$$\Phi_h\left(\frac{Z}{L}\right) = 1 + 4\frac{Z}{L}$$

$$T_* = \frac{u_*^2 T_o}{gL\kappa}$$

The turbulence kinetic energy and turbulence dissipation rate are estimated in following profiles based on the full-scale experiment.

$$\kappa(z) = \frac{u_*^2}{\sqrt{C_\mu}} \sqrt{\frac{\Phi_m\left(\frac{z}{L}\right)}{\Phi_h\left(\frac{z}{L}\right)}} \tag{8}$$

$$\varepsilon(z) = \frac{u_*^3}{\kappa z}\left[\Phi_h\left(\frac{z}{L}\right)\right] \tag{9}$$

3. Experimental data

The Desert Research Institute (DRI) and Western Research Institute (WRI) conducted the Kit Fox field tests at the Nevada test site on August and September 1995. These tests were designed to represent a heavy gas release in a typical refinery plant or chemical processing plant. Since it was not practical to construct a real plant or to test in a plant, arrays of obstacles were arranged in the field and all setups were scaled down to a ratio of 1:10 compared to a typical plant (Hanna and Chang, 2001). The dimension of the test field was 314 meters long and 120 meters wide. CO_2 gas was released vertically from a 1.5-meter-by-1.5-meter square area on the ground (shown in ***Figure 1***). Eighty-four fast-responding concentration monitors were arranged in four arrays, which were 25 m, 50 m, 100 m and 225 m away from the releasing source. 6600 rectangular plywood billboards (Uniform Roughness Array, or URA) with dimensions of 0.8-meter width and 0.2-meter height in 133 arrays were set within the test boundary (light blue area in ***Figure 1***). 75 square plywood billboards (Equivalent Roughness Pattern, or ERP) with sides of 2.4-meter in 13 arrays were installed in a 39m X 85m rectangular area near the releasing source (dark blue area in ***Figure 1***). Meteorological data were collected by instruments mounted on a tower (Met4).

The experimental data used in this study is the experiment KF0711. The meteorological conditions are summarized in Table 1.

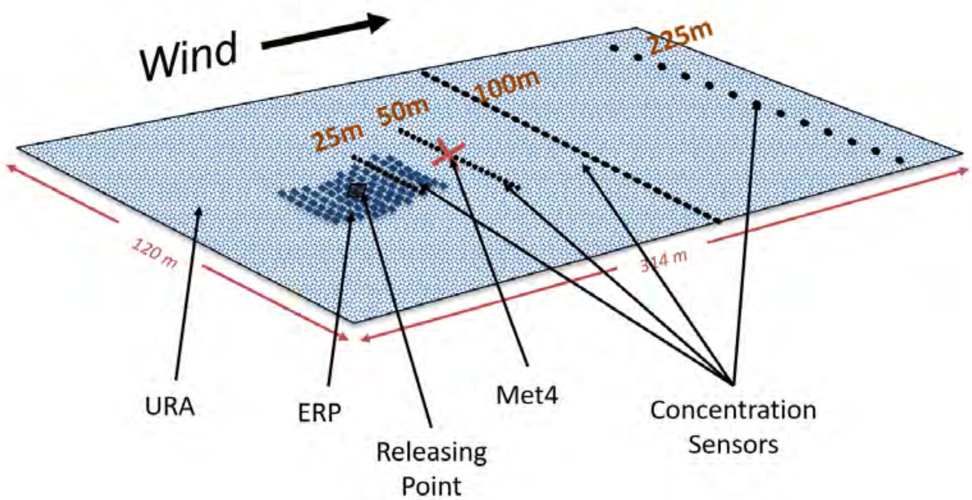


Figure 1. Layout of Kit Fox experiment showing locations of meteorological tower (Met4), concentration sensors, and releasing point.

Table 1. Summary of Experiment KF0711 including releasing source temperature (T_s), spill rate (Q), relative humidity (RH), duration (T_d) of the release, average wind speed (u) measured at 2m elevation, surface roughness values (z_o), inverse Monin-Obukhov length (1/L), and the atmospheric stability class (stab) during the tests.

	T_s (K)	Q (kg/s)	RH (%)	T_d (s)	u (m/s)	z_o (m)	1/L (m^{-1})	stab
0711	303	1.6	12	20	1.93	0.01	0.164	F

4. Parameterization in CFD simulation

In this section, detail descriptions of the 3-dimensional modelling setting in CFD code ANSYS Fluent are discussed. The boundary conditions for the top and the sides are symmetry boundaries, and bottom is ground boundary, the front is the wind inlet with velocity inlet boundary, the end is the wind outlet with pressure outlet boundary, and the gas inlet with velocity inlet boundary is located at the centreline on the ground and 1 meter away from the wind inlet boundary.

4.1. Equations solved

The equations solved in this study are the standard Reynolds Averaged Navier Stokes (RANS) equations with the assumptions that the fluids are not compressible and the Boussinesq assumption, which assumes the density is constant. Energy conservation equations are applied, and the potential temperature profile is considered with equation (7). The κ–ε turbulence closure was used in the form of equation (8) and (9).

4.2. Wind inlet condition

On the upwind boundary, vertical profile for wind velocity is given by equation (6), and the inlet turbulence condition for upwind boundary is given by equations (8) and (9).

4.3. Ground, top and side boundaries conditions

In order to preserve the momentum and heat fluxes through the domain, ground boundary is set to be zero heat flux. Also, a roughness constant of 0.01m represents the arrays of obstacles (0.8m width and 0.2m height) on the ground. Since the experiment is conducted in an open field, symmetry boundaries are set for top and sides boundaries. Symmetry boundaries represent zero normal velocity and zero normal gradients of all variables at the symmetry planes. Additionally, the symmetry plane has slip condition, which means zero shear stress at the symmetry plane.

4.4. Gas inlet condition

At the CO_2 inlet, vertical velocity profile modelled using User Defined Function (UDF) to represent the CO_2 gas flow at 0.21m/s for 20 seconds. The inlet turbulence conditions are given by equations (8) and (9).

4.5. Pressure outflow condition

Since the experimental setup is in a large-scale condition, fully developed flow is assumed in this modelling. Therefore, outflow boundary is utilized. Outflow boundary has zero diffusion flux for all variables at the exit direction.

5. CFD simulation results

Homogeneity of flow properties is examined in this study. This simulation domain used is a 3-dimensional of 250m length, 60m width and 100m height. In order to evaluate the homogeneity defined by equations (6), (7), (8) and (9), a model without CO_2 jet was simulated. Figure 1 illustrates that the equations (6), (7), (8) and (9) can well maintain the homogeneity of the flow properties in the domain. The average differences between the turbulence dissipation rate (ε), the turbulence kinetic energy (κ), and mean velocity profiles between the near-field (x=10m) and the far field (x=250m) are less than 18.50%, less than 29.02%, and less than 3.85%, respectively.

Additionally, the concentrations calculated from the CFD model with the modified turbulence closure are compared with the experimental data (shown in Figure 3). The results showed that the calculations were in good agreement with the experimental data. However, the results pointed out that the concentration peaks calculated from the CFD model generally arrived earlier than the ones that the experimental data showed. Also, the maximum concentration differences between the CFD model calculations and the experimental data were 16.49%, 24.70%, 20.99% and 16.92%, respectively. In other words, the maximum concentrations were within a factor of two of the observations.

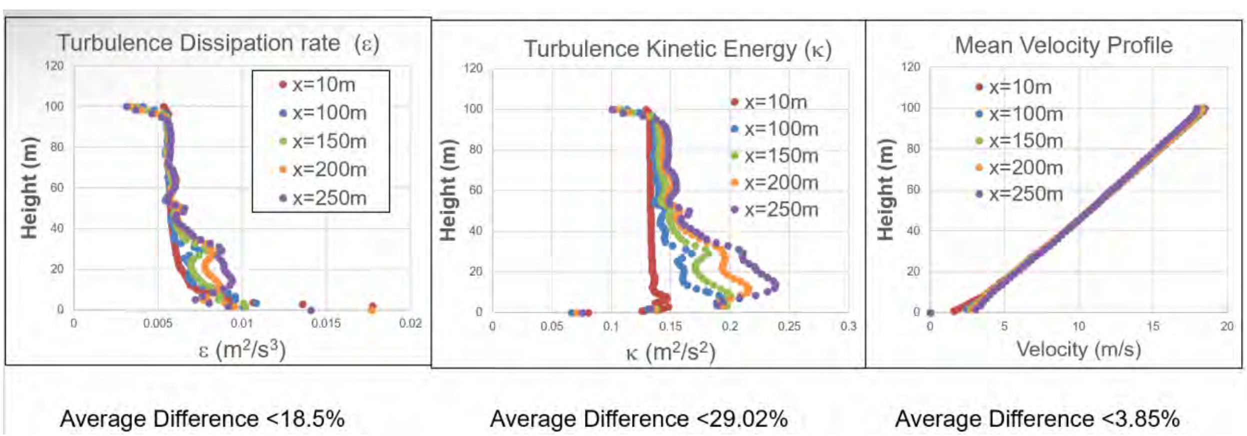


Figure 2. vertical profiles of turbulence dissipation rate, turbulence kinetic energy and mean velocity profile at different positions (10m, 100m, 150m, 200m, 250m)

6. Conclusion

In this work, we have investigated the application of RANS CFD approach with a modified $\kappa-\varepsilon$ closure to the stable atmospheric condition. This modified $\kappa-\varepsilon$ closure including modifications on turbulence kinetic energy equation, turbulence dissipation equation, velocity and temperature profiles were calculated with conservation equations in RANS. The results illustrate that the RANS CFD approach with modified $\kappa-\varepsilon$ closure can maintain the homogeneity of the flow properties well. Also, the concentration profiles calculated from this modified model have good agreement with the experimental data.

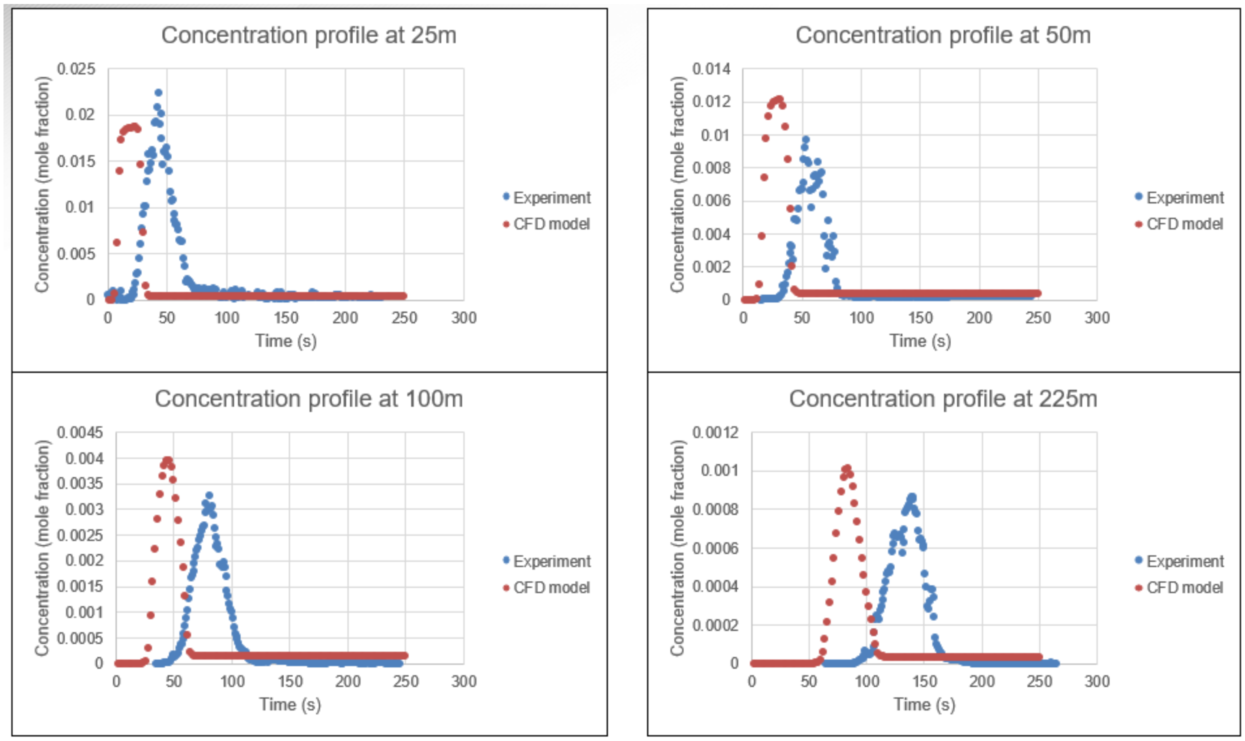


Figure 3. The concentration profiles of CFD calculations comparing with the experimental data at positions x=25m, x=50m, x=100m and x=225m.

7. References

Hanna, Steven R., and Joseph C. Chang. 2001.
Use of the Kit Fox Field Data to Analyze Dense Gas Dispersion Modeling Issues.
Atmospheric Environment. https://doi.org/10.1016/S1352-2310(00)00481-7.

Liu, Bin, Xiong Liu, Cheng Lu, Ajit Godbole, Guillaume Michal, and Anh Kiet Tieu. 2016.
Computational Fluid Dynamics Simulation of Carbon Dioxide Dispersion in a Complex Environment
Journal of Loss Prevention in the Process Industries.

Markiewicz. 2012, M. Markiewicz
A review of mathematical models for the atmospheric dispersion of heavy gases
Ecological Chemistry and Engineering, 19(2012), pp. 297-314

Pieterse and Harms, 2013., J.E.Pieterse, T.M.Harms
CFD investigation of the atmospheric boundary layer under different thermal stability conditions
Journal of Wind Engineering and Industrial Aerodynamics. 121. PP 82-97

Scargiali, et al., 2008 F. Scargiali, F. Grisafi, A. Brucato, M. Milazzo
CFD simulation of heavy pollutants in urban areas: the case study of Messina

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.604.4124&rep=rep1&type=pdf

Sklavounos, et al., 2004 S. Sklavounos, F. Rigas
Validation of turbulence models in heavy gas dispersion over obstacles
Journal of Hazardous Material, 1-2(2004), pp. 9-20.

Yasin and et. Al., 2019. Yasin Toparlar, Bert Blocken, Bino Maiheu, GertJan van Heijst
CFD simulation of the near-neutral atmospheric boundary layer: New temperature inlet profile consistent with wall functions
Journal of Wind Engineering and Industrial Aerodynamics. 19. PP 91-102

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

PSM Alarm Management – "It's Alarming"

Dana Cooper*
Cooper Hayes LLC
Stevensville, MI
*Presenter E-mail: dana@cooperhayesllc.com

Abstract

Improving Process Safety information through Alarm Performance. Alarm Management is applying the application of knowledge of human factors in the engineering of systems, instrumentation and establishing windows. Audible and/or visual means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response. Alarms should be set up if there is a relevant action connected, but ultimately the plant safety should not depend on the response. Understanding the why's behind the nuisance alarms can provide valuable insight to maintenance, process control, etc.

We will discuss how alarms must: 1). require an interactive operator response (make process changes, direct other to make changes, begin troubleshooting, increase monitoring 2). Contact other people, changing operating mode, logging conditions for later examination) 3). Be relevant to the operator role 4). Indicate what response is required 5). Be easy to understand 6). Be presented to operator at a rate that the operator can deal with it. Technology advancements are allowing us to expand in many ways.

The talk will review unique ways of utilizing computer human interactions to review and understand what is important, relevant and suitable for alarm set points. Most groups will want to revisit the optimal levels as well as utilize the information and set-points for training and truly understanding the chemistry, equipment and process. Monitoring alarms, alarm rate and relevant actions as key metrics for Process Safety Performance Indicators and your process safety culture.

Keywords: Alarms, PSM, Culture, Alarm Management, Technology

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Safeguards Verification

Abdullah AlMulla*
SADAF, A SABIC Affiliate
Jubail Industrial City, Kingdom of Saudi Arabia
*Presenter E-mail: mullaak@sadaf.sabic.com

Abstract

Process safety team within SADAF Affiliate established a proactive auditing that focuses on the verification of safeguards with the process units. The safeguards verification draws the attention of front-liners, engineers and their management towards evaluating the safeguards availability, functionality, reliability and independency. The audit divided into two categories, SAFER – SABIC Assurance For EHSS Risk (Risk Register of SABIC) safeguards verification and MOC process safeguards verification. Process Safety Engineer – PSE selects randomly an open significant or higher risk SAFER, where he engages with the front-liners auditing their awareness of the consequence and risk indicated in the SAFER along with the mitigations implemented. Moreover, PSE will request a front-liner to verify in the field the safeguards utilized as mitigation actions. Similarly, implemented MOCs audited by the PSE through his engagement with front-liners. The audit extends into validating the recommendations implemented in the field, management system and documentation. Both audits carried out on weekly basis every Thursdays, where every PSE selects randomly either a SAFER or an MOC. Observations and findings during the audits shared with the plant's owner to drive towards the improvement and progress of the pending actions or weak safeguards. Actions tracking included through Process Safety Field Engagement tracking list.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Data-Driven Prescriptive Maintenance Scheduling and Process Optimization

Baris Burnak[2], Christopher Kwadwo Gordon*[1,2], Melis Onel[2], and Efstratios N. Pistikopoulos[2]
(1)Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX,
(2)Texas A&M Energy Institute, Texas A&M University, College Station, TX
*Presenter E-mail: ckagordon@tamu.edu

Abstract

Maintenance refers to acts undertaken to improve the availability and integrity of ageing productive systems, and is at the nexus of the broader concepts of system resilience, system effectiveness, and complexity. Compromised system resilience can be catastrophic, with consequences such as cost to human life due to process safety incidents, lost revenue due to downtime, as well as damage to the system and the environment. Maintenance scheduling can improve system effectiveness, however due to system complexity, the optimal allocation of resources in selecting when and where to maintain process equipment is non-trivial. Existing approaches have focused on the use of equipment reliability models, degradation signal models, and fault detection models to help address this challenge. Limited attention has been given to future failure prediction in the literature, and efforts have typically focused on probability of failure prediction without consideration of process information, system resilience, or risk via inclusion of the consequences of equipment failure.

This research leverages the availability of data, and complex data-driven models to help guide the optimal allocation of resources in complex systems via the inclusion of information about process operations and equipment condition to obtain optimal maintenance schedules. Equipment data is fed to a non-linear machine learning regression model to determine the remaining useful life (RUL) distribution of equipment for future failure prediction. Knowledge of future failure is then used by a maintenance scheduling model to determine the optimal maintenance schedules via multi-objective optimization of system effectiveness and system resilience as quantified by safety metrics. The results of this research are a set of Pareto-optimal data-driven maintenance schedules from which the decision-maker can select. This research involves automated and dynamic assessment of the risks associated with process hazards, and can be used to help ensure system resilience.

Keywords: computing and systems engineering, plant operations, asset integrity and reliability

References

1. Onel, Melis, Chris A. Kieslich, and Efstratios N. Pistikopoulos. "A nonlinear support vector machine-based feature selection approach for fault detection and diagnosis: Application to the Tennessee Eastman process." AIChE Journal 65.3 (2019): 992-1005.
2. Jain, Prerna, Efstratios N. Pistikopoulos, and M. Sam Mannan. "Process resilience analysis based data-driven maintenance optimization: Application to cooling tower operations." Computers & Chemical Engineering 121 (2019): 27-45.
3. Baptista, Marcia, et al. "Forecasting fault events for predictive maintenance using data-driven techniques and ARMA modeling." Computers & Industrial Engineering 115 (2018): 41-53.
4. Yildirim, Murat, Xu Andy Sun, and Nagi Z. Gebraeel. "Sensor-driven condition-based generator maintenance scheduling—part II: Incorporating operations." IEEE Transactions on Power Systems 31.6 (2016): 4263-4271.
5. Bousdekis, Alexandros, et al. "Review, analysis and synthesis of prognostic-based decision support methods for condition based maintenance." Journal of Intelligent Manufacturing (2016): 1-14.
6. Van Horenbeek, Adriaan, and Liliane Pintelon. "A Dynamic Prognostic Maintenance Policy for Multi-Component Systems." IFAC Proceedings Volumes 45.31 (2012): 115-120.
7. Vassiliadis, Constantinos G., et al. "Simultaneous maintenance considerations and production planning in multi-purpose plants." Annual Reliability and Maintainability Symposium. 2000 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 00CH37055). IEEE, 2000.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

More effective use of Leading Indicators

Gregg Kiihne*
BASF Corporation
*Presenter E-mail: gregg.kiihne@basf.com

Abstract

Leading indicators are all the rage for managing not only Process Safety but all aspects of EHS performance. However; chances are, you are not truly harnessing the power of leading indicators because you do not clearly understand how leading indicators are best used to drive performance improvement. Misuse of leading indicators includes the choice of which indicators to measure / manage and how to use the information obtained from the indicators. This paper will explore the little-known purpose and best use of leading indicators including how to choose the right leading indicators for your facility and team to maximize the impact, how many indicators to measure, how long to use a specific leading indicator, and how to best drive performance improvement from the indicators.

Keywords: Leading Indicators, KPI

Brief Discussion of Indicators

"To measure is to know. If you cannot measure it, you cannot improve it." Lord Kelvin

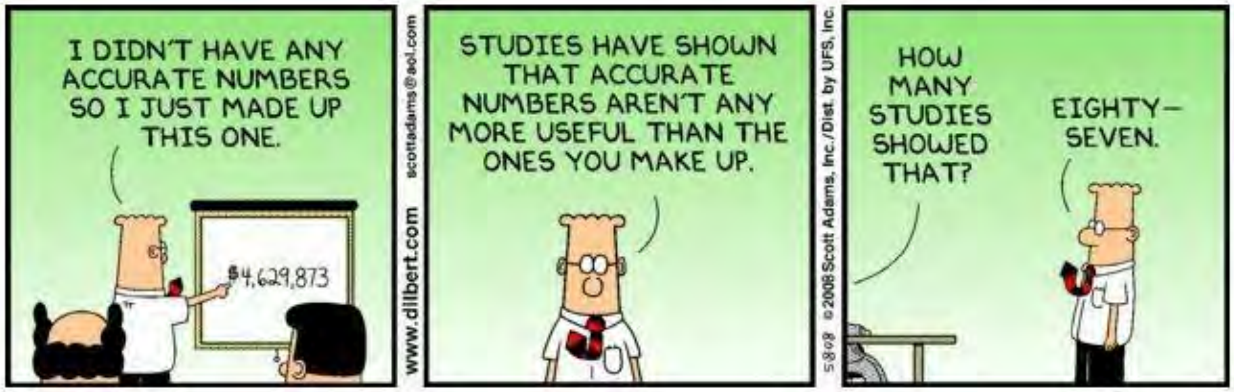
"You can't manage what you don't measure." Peter Drucker, Edwards Deming, et al.

If you don't measure it, you can't manage it.

If you don't measure it, you can't improve it.

If you don't measure it, you probably don't care.

If you can't influence it, then don't measure it. – Introduction to ITIL



Indicators, also known as Key Performance Indicators (KPIs), are those activities or results which people and organizations use to measure performance and/or progress toward a goal. For example, a car is equipped with a speedometer to give real time feedback regarding the car's speed. This is used by the driver to gauge compliance with speed limits (posted or enforced) and to determine approximate estimated time of reaching the destination. Alternatively, a person with a goal of losing weight might stand on a scale each morning to determine progress toward that goal. In the case of the speedometer, the feedback is almost instantaneous based on the actions taken by the driver, whereas the feedback from the scale is somewhat lagging and may not directly correlate to an individual action.

Based on the quotes above, since many managers want to be able to manage or improve every aspect of their operations, they may be using dozens of different indicators.

Within the field of Safety, lagging indicators such as OSHA's Total Recordable Incident Rate (TRIR) or the more international Lost Time Incident (LTI) Rate have been used for decades to rate and compare industrial safety performance. More recently, in the field of Process Safety, companies have been measuring the number of process related incidents, typically fires, explosions and releases (loss of containment events) also often expressed as a function of hours worked. This Process Safety Incident (PSI) rate has become the standard for measuring process safety performance with the publishing of API's Recommended Practice 754 and other international equivalents such as the guidance published by the International Council of Chemical Associations (ICCA).

API 754 has set the industry standard for classifying the types of process safety indicators into one of four buckets or Tiers.

- **Tier 1** events are significant process safety incidents that signify a greater potential for damage to people, plants, communities and reputation – analogous to a Lost-time injury or worse. These are the most lagging of the process safety related KPIs.
- **Tier 2** events are more minor process safety incidents analogous to a first-aid or recordable injury.
- **Tier 3** events are those upsets that challenge a safety system (layer of protection), but do not result in a fire, explosion or release. These are less-lagging indicators, but still lag the conditions that allowed the event to occur.

- **Tier 4** events are the true leading indicators, measuring operating discipline and management systems.

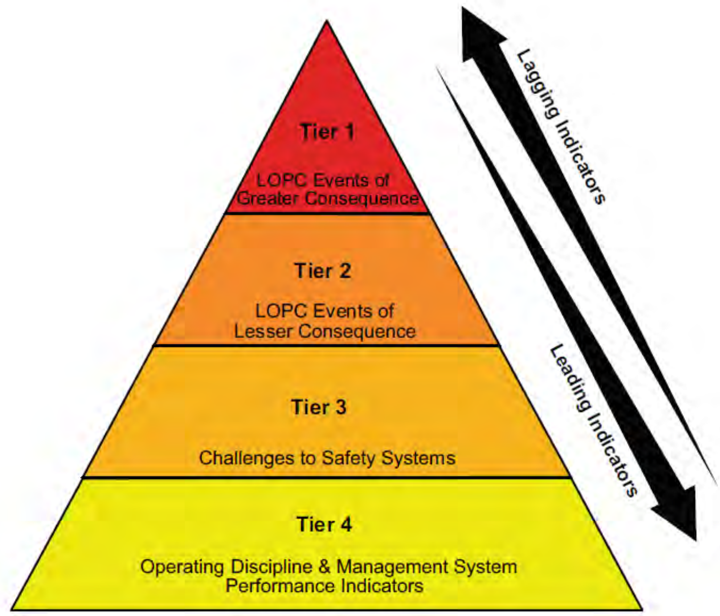


Figure 1 - Process Safety Indicator Pyramid

Typical Uses of Indicators

As with other indicators, Process Safety indicators are useful for identifying when and where attention is needed to correct negative trends in performance.

Lagging indicators are typically used to compare performance among different units, sites, and regions, as well as comparing a company's performance to industry or peer group averages. Often the most lagging indicators are used when a company is early in their journey to performance improvement, but as fewer Tier 1 incidents occur, then focus shifts to Tier 2 events.

Process Safety Incidents (PSIs) are a common measure of process safety performance. But what is it actually being measured…the number of times something fails, namely loss of containment events, fires and explosions. As a lagging indicator, PSIs only tell us when something already went wrong…so how do we use KPIs to help us improve?

Conventional wisdom tells us to use leading measures to more proactively manage performance, but what does that really look like? Tier 3 indicators such as activations or failures of protective devices are good measures, but still telling us what has already happened. These are 'less lagging measures.' Tier 3 events are useful for identifying weaknesses in specific layers of protection and directing efforts to remediate or improve those areas identified; however, Tier 3 events should not be used to compare separate units, especially when they operate different technologies, processes and equipment. This results in the proverbial Apples to Oranges comparison.

Tier 4 events or Leading Indicators are the focus of this paper. These typically measure specific aspects of a management system performance, often in terms of percentages of activities completed successfully or on time, or more pessimistically, the percentage of non-conformances, such as Mechanical Integrity Inspections, Action Item Closure, MOC system compliance. These are all very important activities, but how do you know if you are measuring the right action? How do you know when to act? Are you influencing the leading indicators?

Challenges to effective use of Leading indicators

Leading indicators are popular for performance management because if chosen properly, they measure activities which may effectively influence the outcome of important lagging performance measures. At the same time, many organizations struggle to use leading measures appropriately often due to a lack of understanding of how they should be used.

Many organizations, feeling pressure to measure leading indicators, will select a handful of leading indicators from an industry standard list, based on what information they can most easily measure or because the general topic, e.g. Action Items or Management of Change, seems to be important; however, they fail to understand what exactly is being measured and what to do with that information.

Some organizations will develop global leading indicators which are measured across every facility in the organization, then used to rate the performance of those facilities without understanding what the KPI is communicating. Inappropriate responses to the leading indicators are also common. One organization was measuring Loss of Containment (LOC) events in an effort to increase awareness and reporting. So theoretically, rising numbers of events reported would indicate that the indicator was having the desired effect. However, management decided to recognize sites with fewer LOC events as having better performance.

“Whatever is measured will be managed” …or put another way, “Whatever is measured will be manipulated.” Care should be taken to communicate the intent of leading measures so that facility and unit leadership can support the development of appropriate behaviors instead of only managing the numbers to look best in the KPI “beauty contest.”

A different way of using Leading indicators… to proactively shape Behaviors and Culture

- Identify the desired change / goal
- Determine specific desired Behaviors that will achieve the change / goal
- Develop Leading indicators to measure / encourage that behavior
- Set targets (Don’t make it easy!)
- Measure & communicate performance regularly (daily, weekly, monthly)
- Don’t be afraid to encourage competition

I submit that the best use of leading indicators is not just to measure activities, but to drive culture change by changing behaviors, by creating good habits and breaking bad ones. In other words, to disrupt the normalization of deviation and drive the normalization of excellence.

Leading Indicators Around Us

But how do we make this work in practice? A top down edict often fails because there is no engagement or ownership at the individual level. So how can this be achieved? Let's look at an example…

Years ago, one could track driving fuel economy periodically when refueling the vehicle, by dividing miles driven by gallons of fuel consumed, or more accurately, by gallons of fuel that it took to fill the tank. This only gave a lagging indication of the fuel economy achieved over the last days or even weeks of driving. Newer cars are equipped with a trip computer measuring real-time fuel consumption and vehicle speed to calculate and average or instantaneous fuel economy, but even this is a "less-lagging measure" as it measures results but does not specifically impact behaviors.

A recent rental car included an Eco-Display on the dashboard, which measured real-time and cumulative for the trip, three different behaviors that influence fuel economy on a constantly updated "scoreboard," see Figure 2. The behaviors were 1) Acceleration – how quickly or evenly the driver accelerated, 2) Constant velocity – how much the car's speed varied over the course of driving, and 3) Coasting – a measure of whether the driver braked hard or allowed the vehicle to slow down more before braking. By watching these three icons over the course of the business trip, I became aware of certain driving habits that negatively and positively influenced my fuel economy and was able to begin changing my driving habits. These measures were influenceable, that is, I could impact the outcome, and indicative, by changing this behavior, I could measurably impact the outcome.

Figure 2: ECO-Display Leading Indicators

Like this example, effective leading indicators are those which the individuals or team can *influence*, and which clearly *impact* the desired result. In addition, this example shows the importance of keeping a simple, relevant scoreboard. I became so engaged in the 'competition' to improve my Eco score, that I missed my freeway exit.

Examples in Process Safety

How does this translate to the world of Process Safety and reducing the number of PSIs? Plants with a high number of PSIs often demonstrate a lower level of employee discipline, which often results from low levels of engagement and ownership. We found that one successful means of improving performance is to focus on the employees, making them aware of the issues. Several sites successfully implemented two simple leading indicators: Reporting all spills and Extreme Housekeeping.

Reporting All Spills

Employees are trained to report significant spills that occur during the course of their work; however, many other spills, such as small leaks and drips were common place and failed to register in their awareness. When implementing this KPI, our leaders were careful to point out that not only significant spills should be reported, but literally every time material left primary containment. Even minor drips were to be reported. At first, there was a general disbelief and feeling that this was another flavor of the day. However, one operator came across a gasket leak that had resulted in just a few drips. He reported the 'spill' to see if anything would be done. The plant leader took the report seriously and had the gasket replaced and flange retorqued at the first available opportunity. Immediately, the operators engaged and began 'hunting' for other leaks.

Within a few months, the spill reports were overwhelming the reporting system, so the plant had to modify the system. At the same time, they gathered information as never before about plant condition and leak causes. This information proved vital to proactively address weaknesses in the plant's systems, both operational and mechanical. In addition, the employees became hyper-aware of leaks and often spotted and stopped leaks long before they reached the tier 2 level. Plant leadership tracked the spills reported and regularly recognized employees for reporting.

Extreme Housekeeping

Another plant was experiencing a relatively high number of LOC events. The plant had a comprehensive 5S system used to manage plant condition and housekeeping, but plant tours showed minor issues with spills, leaks and cleanliness. The plant used a relatively relaxed set of criteria for the 5S scoring, and in the end, got what they expected. A new plant manager decided to significantly raise the expectations for the 5S scoring, and previous satisfactory scores were no longer acceptable. The scoreboards were updated with the new criteria and showed that much work was needed. In addition, the plant manager would at least weekly walk through the plant with a clipboard and trash bag, picking up zip-ties, bolts, bags and other trash, while making notes of plant condition. The employees quickly took notice and began cleaning the plant before the manager's routine walk throughs. In time, the employees started meeting the new 'extreme' 5S standards and developed a much greater sense of pride in the plant.

Both of these plants experienced a significant reduction in Process Safety Incidents because the leaders found a way to engage the employees and encourage greater ownership of the facility.

A Leader's Work

This sounds like a quick and easy way to reduce spills; however, it was anything but easy. This type of change always requires a significant amount of effort by the leaders, although the results are worth it.

For example, when requiring that employee report all spills, the leader must be willing to act on the spills that are reported and on the learnings from those spill reports. This must be a priority for you if you wish to make it a priority for your workers. One plant even adapted their spill reporting system because it was overwhelmed by the 10-fold increase in reporting. If the systems were not adapted, reporting likely would have returned to previous levels.

If you decide to require extreme housekeeping, the leader must be willing to join in the work. Setting the example and modeling the desired behavior. An improvement in housekeeping will often expose existing issues. The leader must be willing to address (fix) these issues as they are identified. Doing so will further encourage housekeeping improvements…but failing to fix issues will lead to a quick death of employee engagement.

Regardless of which measures are chosen, the leader must be dedicated to driving accountability by setting high expectations and routinely (weekly) following up, measuring, inspecting results and by requesting input for further improvements or actions.

In addition, leaders must be willing to take action from the learnings, involving the entire team: what did we learn, what can we do about it, and what should we do next?

Creating the momentum needed to bring about a significant change in performance is difficult, and just as challenging to maintain the focus and the momentum once the initial targets have been achieved. You and your teams are capable of significantly better performance, but you must be willing to find the levers to change the behaviors and ultimately the culture of your teams.

Conclusion

In summary, leading indicators are valuable tools for driving performance improvement, but only if appropriate indicators are chosen and used properly.

- Identify measures that
  - challenge the team
  - impact the performance goal,
  - can be directly influenced by the individuals or team.
- Visibly track progress with the teams and celebrate successes.
- Actively support the team's progress.
- Inspect, measure and follow-up at least weekly.

References

American Petroleum Institute. (2016, April). Process Safety Performance Indicators for the Refining and Petrochemical Industries, RP 754. API Publishing Services.

McChesney, C., Covey, S., & Huling, J. (2012). *The 4 Disciplines of Execution.* New York, NY: Free Press.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Procedural Systems as Independent Layers of Protection: Are We Giving More Credit Than is Due?

S. Camille Peres*
Environmental and Occupational Health Department
Mary Kay O'Connor Process Safety Center
Texas A&M University System
College Station, Texas, USA
*Presenter E-mail: peres@tamu.edu

Abstract

Analysis for incidents in high-risk process industries (e.g., petrochemical, oil and gas) have often identified "human error" as the root cause for the incidents. Many researchers and practitioners have begun to point out that human error cannot be a root cause for incidents—that the root cause instead is the condition that caused the human to make the error. In the last 10 – 15 years, incident analyses have begun to elaborate a bit on what may have caused any human error and many times "procedural issue" was the identified root cause. However, although more specific than human error, procedural issue still does not provide sufficient clarity regarding the root cause to allow for the identification of prevention or mitigation efforts. For instance, if procedural issue is identified, what was the issue? What the procedure wrong? Was the procedure hard to follow? Did the worker ignore the procedure? Each of these circumstances requires very different approaches in order to resolve the issue.

The Next Generation Advanced Procedures Consortium has been conducting multi-disciplinary, multi-methodological research on procedural systems in high-risk process industries for the last 4 years. As part of this effort, we have identified several variables associated with procedure comprehension, use, and adherence. Further, we have identified that while the design of the procedure documents is important and necessary for a good procedural system, well designed documents are not sufficient for an effective procedural *system.* Most importantly, we have identified that effective procedural systems are a necessary part of process safety and the implementation of inherently safer design. However, how procedures can be used as an Independent Layer of Procedure is currently not sufficiently understood. As part of this paper, we will share some relevant empirical findings regarding procedural systems and offer industry partners and researchers potential paths forward.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Analysis of the Low Perception of Risk: Causes, Consequences, and Barriers

Cassio Brunoro Ahumada[2], Salvador Ávila Filho[1]*, and Lucas Menezes Pereira[1]
Federal University of Bahia – UFBA; Texas AM University - TAMU
*Presenter E-mail: avilasalva@gmail.com

Abstract

The principles of risk, danger, and sociability depend on cognitive limitations and the social work environment. Subjects are linked in binaries or multiples where they can establish causal relationships or influences that lead to informal rules of behavior in the workplace. A group that understands what positively influences the organizational goal of avoiding accidents and losing energy will know the importance of keeping the fundamentals of work alive. Understanding the principles is the basis for research into safe, alert, and resilient behavior. From the characterization of the principles adopted in the form of relationships, from the established standards of good practices, they present hypotheses about safe behavior. The hypotheses may indicate gaps in the difference between what is expected for a risk activity (good practices) and what is detected from the observation scenarios of this industrial routine. In the cognitive analysis based on the models that indicate perception, attention, and memory are initial stages for the construction of the mental scheme of execution of preformatted procedures or elaboration of procedures in unusual situations. A comparative analysis for a group indicates which aspects considered as priorities for decision and common sense allow a more complex preparation that requires a new concept. In the job search are the physical, cognitive (information flow and type of communication) and organizational situations that can cause human error and equipment failure. Working criteria can decrease or increase human error. This work aims to test the principles and indicate the hypotheses through the analysis of scenarios and confirm the relationships of the lack of perception of risk, with the analysis of the work station indicating which factors of performance that influence the human error. When designing interventions, it is important to suggest the influence of competence level and quality of communication tools in a stressful environment with specific leadership. Interventions depend on the type of human error, therefore, on the application of intellectual capital, operational groups for situations under stress, change of habits and educational campaigns.

Keywords: Work Station - Risk Perception - Human Error - Behavior - Industry

1 Introduction

Sensitizing teams to change behavior and preparing preliminary diagnosis on the motives of lack of risk perception. To achieve these goals, appropriate methodologies were developed that seek to break down social paradigms about accidents through training work teams. Reflections in crisis situations assist in the elaboration of hypotheses for future interventions in operational mass and environments, reinforcing personal, organizational and regional safety policies. The choice of interventions depends on their validation in later work. It is important to distinguish the elements that induce unsafe behavior and the human-organizational-technical (HOT) factors that cause human error, losses, and accidents. The managerial, human-social and technological aspects can create an environment for unsafe behavior, in which they allow the flow of danger energy across barriers. The human and organizational factors elaborate, by events, the condition for the transfer of social hazard towards the physical realization of the accident or incident.

It is crucial for the industry to focus on ways to improve their workers' risk perception. Accidents may cause from small material losses (in which production is needed to stop for a while) to disasters involving harms to human beings or even human losses, incurring fines to the company. Adopting adequate safety culture always represent economic advantages for companies regardless the period of time for analysis, because an accident may occur at any time, not only in mid and long-terms.

The work done by the authors and reported in this paper implemented a manner to calculate and diagnose human reliability levels in workstations. By using principles from the C4t (Communication, Commitment, Competence and Cooperation) tool and some industrial safety policies widespread, it was intended to know whether divergencies would be found on operational mass' opinions about actions considered scientifically in favor of safety. Besides, if they could put them into practice when necessary, otherwise, get to know what prevents them to do so. High dispersion on responses would mean trouble in team consensus, and then a high possibility of workers' arbitrary decision-making and their actions to have mutual interference, may leading to ineffectiveness, especially in emergency situations. Also crucial to diagnose on human reliability is to find whether there is training that simulates a large number of possible abnormal conditions at work (as hard failures on productive systems) to teach and simulate how everyone should act in order to the practical procedures to be the same as those taught with great efficiency and effectiveness.

1.1 Risk and Accident Perception

1.1.1 Risk and Accident Perception overview

Risk and accident perception is a fundamental aspect of any person's life, for safety in the workplace, at home, in leisure time, etc. It is defined as the ability to detect real signs of danger or even to predict the occurrence of a negative situation. The perception is often influenced by context, individual's subjectivity, experience, trust, the way a problem is communicated and then analyzed (the Framing Effect), and even by heuristics, that are defined as cognitive processes used in decision-making required to be faster, in which part of not so relevant information is ignored. Kahneman and Tversky (1974) found that people overestimate results (considering the triggers as high-risk) from more recent and extraordinary events, for example, murders instead of thefts.

In some cases, one may refuse to face a certain risk situation because of fear, need for protection or believing that the possible benefits do not make it worth risking, and then, there is no need to do it. The concept associated with this early evaluation is Risk Tolerance, that is, the degree of risk severity that a person agrees to undergo. The relationships established by people in a group also influence their risk perception and risk tolerance. At work, for example, influencing factors divide into three groups and are related to the following theories [1].

Table 1 - Factors that Influence Human Risk and Accident Perception

LEVEL	FACTOR	ASSOCIATED THEORY(IES)	DESCRIPTION	ASSOCIATED RESEARCHERS
Macro-level Factors (institutional and structural)	1. Organization's Safety Culture	Social Action Theory	Society's perception that a certain activity is low risk.	Harding & Eiser (1984); Cooper (2003); Mullen (2004).
		Social Control Theory	Connect to the organization's policies to decrease unnecessary high-risk attitudes.	Hirschi (1969); Neal et al. (2000); Garcia et al. (2004); McNeely & Falci (2004); Clarke & Ward (2006); Ford & Tetrick (2011); Chapman et al. (2013).
	2. Enforcement and Organizational Trust.	Social Control Theory	The same as in item 1 of this table.	The same as in item 1 of this table.
Meso-level Factors (in general, by civil society groups)	3. Peer and Society pressure	Social Action Theory	The same as in item 1 of this table.	The same as in item 1 of this table.
		Situated Rationality Theory	Do not consider any high-risk attitude as irrational and safe attitudes as rational without previous analysis.	Rhodes (1997); Finucane et al. (2000); Mullen (2004); Vernero & Montanari (2007); Choudry and Fang (2008); Cafri et al. (2008); Keating & Halpern-Felsher (2008); Hambach et al. (2011).
	4. Inadequate leadership and Informal groups	Social Action Theory	The same as in item 1 of this table.	The same as in item 1 of this table.
Micro-level Factors (individual's psychological level)	5. Level of knowledge about the risk	Protection Motivation Theory (PMT)	People protect themselves when they predict that negative events may happen.	Becker & Maiman (1975); DeJoy (1996); Mearns et al. (1998); Gucer et al. (2003); Sheeran et al. (2013); Glendon & Walker (2013).
	6. Optimism bias + overconfidence	Risk Compensation Theory	Engaging in higher-risk situations by the feel of being safer because of safety equipment.	Wilde (1994); Aschenbrenner & Biehl (1994); Janssen (1994); Klen, (1997); Bridger & Freidberg (1999); Morrongiello et al. (2007).
		Habituated Action Theory	Risk perception decreases over time when no negative events occurred from high-risk attitudes.	Kasperson et al. (1988); Weyman & Kelly (1999); Weller et al. (2013).

1.1.2 Perception of traffic risk

Since attention is one of the requirements for good risk perception, it is known that performing certain activities with insufficient and/or diverted attention may cause harm. We can cite road transportation, in which some studies on risk perception were made in Europe by ESRA (European Survey of Road users ' safety Attitudes) [2]. More than 17000 respondents from 17 European countries participated. By the results, it was concluded that the main risk factors for road accidents were: driving under the effect of alcohol and drugs and lack of attention, rather than fatigue (ESRA, 2016). The survey also showed a remarkable characteristic of people: the feeling that the risk imposed by another person is more serious than the one in which the individual decides to face himself/herself without external influence. It was concluded from the results that for all three age groups interviewed (18-34, 35-54, and above 55 years) the scores attributed to the feeling of safety (which could range from 0 to 10) had around 0.5-higher mean value for people who were car drivers instead of car passengers.

1.2 Industry operation requirements for workstation project and operations control

The chemical industry has specific characteristics of technology, complexity in the tasks and risk of accident indicated by Figure 1. The plant project needs to meet physical-technological, cognitive and human requirements for the development of the tasks [3], otherwise, a human error should probably occur. After meeting them, it is crucial to set the criteria of the workstation for the best operation in routine in order to get better control of the task.

Due to the dynamics of processes, people and organizations, human error may also happen by behavioral (subjective and social aspects) deviances by the feeling of uncertainty in some work situations. It is possible to find what is the "level of adherence" (aimed in this paper) to safe procedures when those conditions are faced. The prediction of this behavior requires the measurement and monitoring of cooperation, commitment, communication, competence and stress levels, discussed in the C4T tool [4]. The operational control depends on the processes of standardization, communication, and analysis of the task and its failures. It is important to analyze their network relations, in addition to the way they affect or are affected by low risk perception. These factors are the basis for systemic (sociotechnical) failure [5], and they indicate the level of system reliability by function or region of process.

The conclusions may indicate informal rules adopted by the operator. In this investigation, according to Ávila [6], it is useful to find: (a) The difficulty/ease in installing informal communicational and technological barriers; (b) The way in which the group is aligned with good practices and principles of risk and reliability; (c) The issues of organizational cooperation and commitment; (d) The analysis of safety leadership and safety culture; (e) Cognitive gaps, workstation criteria and human performance factors management.

1.3 Risk in operating routine

The research group on dynamic risk needs to measure the subjective factors in the operational routine to project future behavior and the quality of risk perception. It is essential to check the safety principles and a good sense of leadership. It is important to analyze the scenarios and priorities [7], in addition to indicating gaps in cognitive processing and weaknesses in the workstation. This investigation intends to discuss the most appropriate interventions to adjust the safety culture by improving the team's risk perception, the most important input in cognitive processing. The C4t tool indicates the opening or closing of doors that allow the transit of danger energy in the human performance factors [4]. It must be considered that certain environments can set inadequate behavior for safety, quality, energy and cost control.

1.4 New Dynamic Risk Decision Tools

It was redefined not only reliability (human being, operation, process and equipment), sociotechnical reliability and reliability mapping, but also: factors affecting human performance (management, organization and operational culture), man's behavioral elements, deviances, failures and cultural phenomena that establish a safety culture. Figure 1 tries to represent that complex analysis. Letters from A to G were positioned on Figure 1 and their whole explanation is on Table 2.

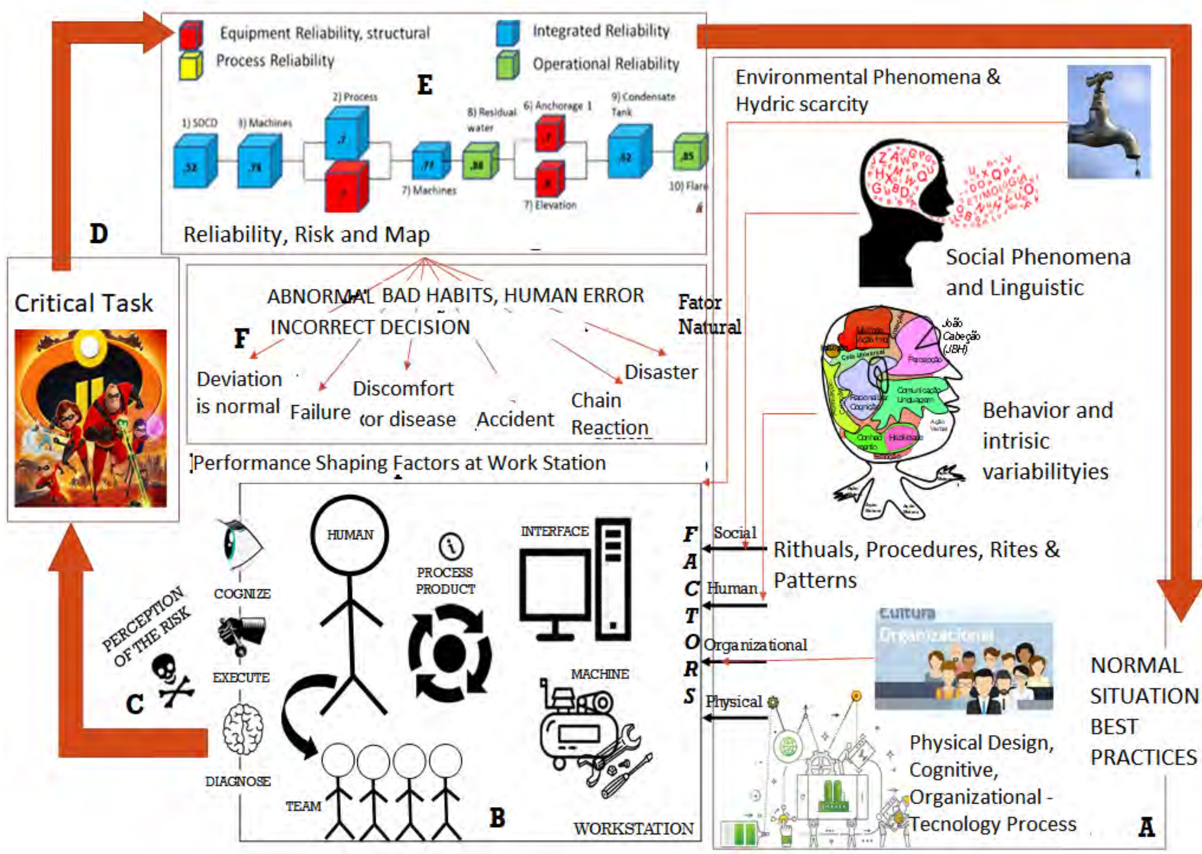


Figure 1 - Reliability and human factors in workstation design. Adapted from [6].

Table 2 – Auxiliary table to explain Figure 1

ITEM	DESCRIPTION
A	Requirements/guidelines for industrial and technological layout design should be found through analysis balancing: organizational principles; safety conditions; and workers' decision-making, performance, and limits.
B	Adequate interfaces should be provided to ensure clear and objective communication, avoiding conflicts between production-technology and workers' social phenomena. Interface examples: computer screens, written procedures, general feedback.
C	Risk perception must follow great safety guidelines to hinder the flow of danger energy and avoid interrupting the task/production due to human and material losses.
D	Safety-based procedures (how to act) must be taught and followed more seriously at critical tasks. A multidisciplinary view is needed to find root/main cause(s) and system limitations.
E	To calculate and diagnose human reliability, it is useful to construct a diagram including equipment, process, operation, etc.
F	All risks must be mapped. If deviances in safety procedures are accepted and the flow of danger energy is not controlled, it may happen failures, hazardous chain reactions, occupational diseases, and disasters.
G	Simple attitudes can bring great results in risk perception and preventing accidents in order to ensure good work conditions. Some of them are: changing leadership, giving feedback and improving man-machine interface. A multidisciplinary view is a must!

2 Methodology

A human risk perception improvement program led by the research group presented content about different elements of behavior and HOT factors to avoid the accident. A lecture lasting up to 8 hours was firstly presented in a chemical industry for the operational mass. It was like a training with the goal of sensitizing the operational mass. The concepts issued were divided into: Principles to spiritualizing safety; Investigating cognitive gaps in practices; Discussing the workstation criteria; and analyzing how to manage human factors.

The first block of content discusses the principles and concepts of risk, danger, reliability, behavior and human factors. By using examples of practical cases and routine situations, barriers to social, human and technological hazards are elaborated.

In the second block, cognitive models were presented to identify where and how failures of perception can occur in routine practices and/or accidents. Thus, the elaboration of a mind map for the decision and also physical and communicational actions was considered.

In the third block, discussions on workplace situations that can cause human errors are initiated. In addition, an analysis of the best criteria for the workstation is performed to identify the main constraints in the task and the main physical, cognitive and organizational factors. Related to these concepts, socio-human risk tools are presented, besides the importance of attention in industrial control.

The fourth block finished the training by a discussion on how to manage and intervene to change unsafe behavior. Among the tools reported, there were: the socio-human risk analysis; the C4T technique (measurement in human factors); the classification of cultural biases, bad habits, human errors and incorrect decisions; and the interventions on factors and human elements.

The preliminary diagnosis deals with the discussion of the principles and the respective hypotheses that should be validated in later work: cognitive gaps, risk perception, workstation criteria that cause errors, and management of indicators on human factors.

A transnational chemical industry, that adapts to local cultures, allows the existence of differences and seeks to improve safety standards. Handling behavioral aspects in consonance with technological aspects is a challenge, once considered the current characteristics of the hazardous energy environment and the complexity of the technologies. Probably because of this, the CCPS (Center for Chemical Process Safety) is concentrated in the discussion about what causes normalization of deviances and how to avoid the accident after organizational changes.
The different regions, leaderships, technologies, and organizations drive danger energy in the direction of the accident. The work of adjusting: the safety culture and the organizational culture, the interfaces involving the worker and the production, the quality of communication, cooperation levels and the level of commitment, require confirmation through routine (operator's discourse) or a poll during moments of sensitization.

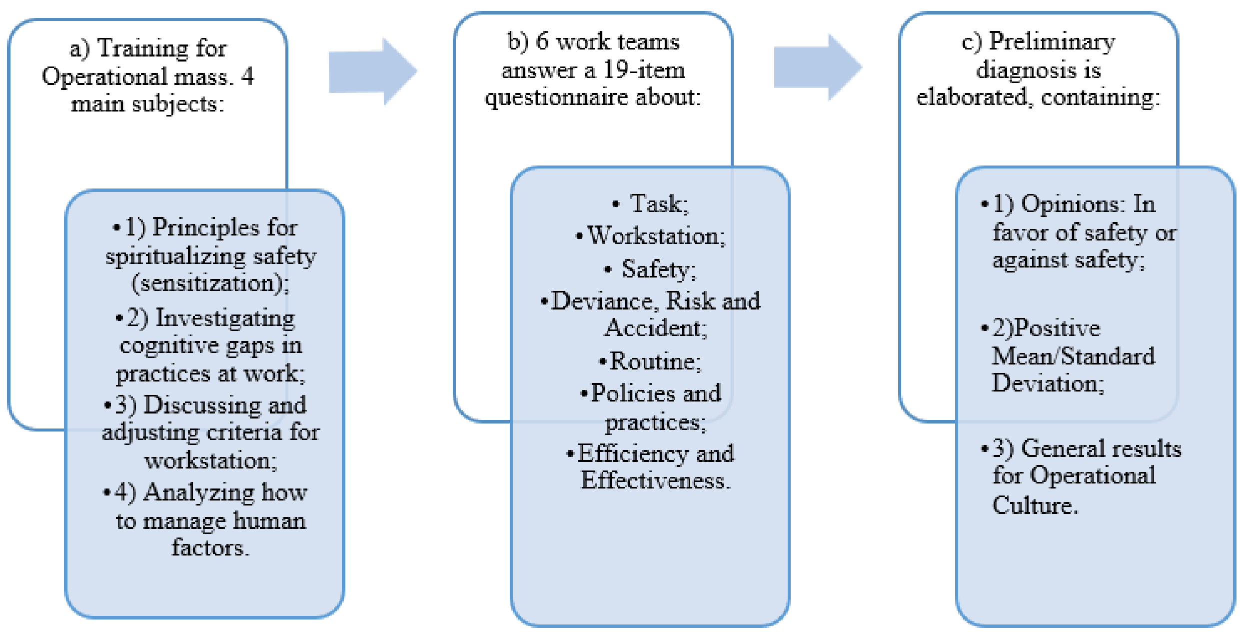


Figure 2 – Steps used for training, testing and diagnosing an industrial operational mass

3 Application

A diagnosis of general and specific aspects that affect the behavior of the work team was performed and interventions were needed to get out of the unsafe behavior. The diagnosis was based on the first stage of the 4-stage training.
The preliminary diagnosis in Figure 2 should be validated with additional safety data and multivariate data processing, and complementary discussion on cognition, workstation and Human factors.
The interventions depend on the validation of the hypotheses. They may be related to rituals, training, educational processes, operative groups, knowledge against failure, adjustments of HMI (Human Machine Interface), alarm system or other tools in Human Reliability Analysis (HRA) and Human Factors Analysis (HFA). It may be necessary to set an investigators team.
The training performed in the operational mass, divided into 6 groups (5 shift and one administrative work teams), during weekdays. The participation of the group must be active and adapted to limited time to provoke a break of paradigms in order to raise awareness. The "Insite"

course for safety brings difficulties because of the intense operational routine. The questionnaires should not be revised, in order to avoid lack of representativeness in the statistical processing. An evaluation of the type of leadership and quality of attention should be done.

4 Discussion

4.1 Spiritualizing safety

Through 19 statements involving informal practices, principles and rules, it was intended to find relationships between behavioral aspects and intrinsic human performance factors or those resulted from managerial, organizational and operational relationships. The statements were related to keywords that indicate factors and elements (some showed in the most left-hand column in Table 3): communication, competence, avoiding production-safety conflict, leadership, procedures, good practices, human stress, political-practical conflict, communication and feedback, task and excessive self-confidence. Operating mass answers were treated statistically, making them possible to indicate getting closer or getting away in relation to the best practices in operational safety. The indicators can describe behaviors that represent operational culture, shift team leadership, informal shift rules, and some specific cases. These indicators can also show how danger energy circulates through the HOT (human-organizational-technical) elements and factors that build the Human Factors Bayesian Network. Other important elements and factors that have been indirectly discussed were: risk perception, economic bias, work training, standardization and work memory, information flow, selection and development, risk aversion, regional and global culture, opportunism, deviance normalization, centralizing management, social conflicts (generation, gender, multiculturism), control devices, alarm management, PLC (Programmable Logic Controller) or interface, instruments and PSV (Pressure Safe Valve).

Table 3 – 6 of the 19 questionnaire items evaluated by the authors, industry managers and supervisors as in favor (F) of safety, in blue "1"; or against (A) safety, in red "-1"

SUBJECTS	3) F	3) A	8) F	8) A	11) F	11) A	13) F	13) A	17) F	17) A	18) F	18)A	SUM: 1) to 19)
Communication											1		2
Competence							1						2
Avoid Production-safety conflict	1												2
Leadership										-1			-1
Procedures				-1									-1
Good practices			1										1
Human Stress									1			-1	-1
Political-practical conflict						-1							-2
Communication and Feedback					1								1
Task								-1					-1
Excessive Self-confidence								-1					-1

4.2 Group of issues in subject classes

The 19 sentences, here sometimes called 'questions' (because it was questioned about operational mass' opinions afterwards), could be grouped into blocks of similar subjects: communication (questions 1; 11; 18), in which the answers showed a tendency to decrease the safety levels, demonstrating that the feedback is not enough and there may be a conflict between company policies and practice during routine and emergency. Competence (2, 13 and 15) had a high level of safety, indicating employees' good competence, but the drop at question 15 showed a certain level of excessive self-confidence. Results from the conflict of priority between production and safety (items 3 and 6) demonstrated a tendency to normalization of deviance. Guilt culture and feedback in the procedure (7 and 8) results showed that culture is a strong factor in the company, which hinders the execution of good practices There was a low percentage that had perception about the need to "pay attention " in the context. Other results from the study appear after colon punctuations. Stress management by leadership (items 10 and 17): high positive percentage, a good perception for the influence of human factors by everyone, although dispersion on the answers resulted also high. Cooperation and Leadership (4, 12 and 14): despite demonstrating a leadership profile with active listening, the low percentage in favor of safety in questions 12 and 14 may indicate conflicts in leadership relations or between the staff and the shift teams, and a lack of adequacy at the workstation, task, and team. Commitment and fair culture (5, 9, 16 and 19): there was a fair culture, with employees committed to safety, and it is needed that the use of PPE (Personal Protective Equipment) by people becomes a habit in everyday life.

4.3 Question, sense and statistics for safety response

Before showing and commenting on the data collected from the questionnaire applied to a Brazilian chemical industry company, it is necessary to say that they represent correctly what is seen in most of chemical and other industries, although the data are not exactly the same because of their right of confidentiality**.** For this same reason, the region where it is located and also the technology used in their processes cannot be unveiled.

The 19 questions were grouped according to the 4.2 topic and the operational mass' answers for some of them were described in Table 4, where blue means the percentage of opinions in favor of safety; those in red, against safety.

Some of the 19 sentences had their meaning been inverted before the questionnaire was given to the workers. These sentences are signaled by an asterisk in the end (Table 4). The inversion was due for not asking their opinions always the same way. That is, if a person sees many sentences scientifically in favor of safety, his/her first positive opinions about them tends to influence the other questions answers by the reason of being already accustomed to response positively. Once a sentence was inverted, by for example, putting the word 'NOT' in the middle (as on item 13 in Table 4), when a worker considered it against safety, the answer was registered at that table as in favor of safety, and vice-versa.

The key words indicating the subject are in the last column of the right. The positive (in blue) answers were statistically treated. Sentences evaluated by around and/or above 70% of respondents as favorable to safety, partially favorable and against safety were highlighted as following. In favor: competence, perception, emergency task, routine patterns, control stress; Partially favorable: workstation and operator's function; Against: operational culture and guilt culture.

Table 4 – Averages of 6 operational mass groups' opinions for statements (items) as in favor, partially in favor or against safety

ITEM	STATEMENT	MEANING INVERTION?	Favor safety (F)	Partially favor (P)	Against safety (A)	ITEM KEYWORDS
11	Policies and practices are compatible in operation. There is no feedback without them.	No	**45%**	**23%**	**32%**	**Conflict between policies and practices; communication and feedback.**
18	Communication and action must be repeated as risk level increases.	No	**48%**	**24%**	**28%**	**Perception of risk; communication and stress (routine and emergency).**
13	The knowledge necessary to perform the activity does not include aspects of task identification and attitude-action in urgent situations. *	Answers A were considered F and vice-versa, due to the inversion of original statement meaning.	**92%**	**5%**	**3%**	**Routine; emergency (stress), competence and task.**
3	Competition between service measurement and quality hinders cooperative and safe work.	No	**48%**	**23%**	**29%**	**Conflict between production and security; Cooperation.**
8	Revise the patterns in time for correct routine management.	No	**93%**	**7%**	**0%**	**Procedure and standards; good practice.**
17	The operator should work under high stress level because his perception and safe acting remain the same. *	Answers A were considered F and vice-versa, due to the inversion of original statement meaning.	**70%**	**23%**	**7%**	**Stress (routine and emergency) and leadership.**

4.4 General behavior and comparison by teams in classes (Shift or staff)

The chart above, with the average of the 6 groups' opinions, was compared with the chart per training class for each one of the 19 questions. The discussion is about specific or general behaviors detected when the results from different teams are compared, in each question, to the mean values showed in Table 4. Some conclusions were as follows.

Questions 11 and 18 obtained from 18 to 45% of conviction of all classes interviewed that they had unsafe behavior. This fact indicated that problems use to occur between policies and practices not compatible with routine, besides low feedback. In addition, communication and action are not redundant as the risk increases.

Question 18 approaches communication and action. With the proposal that redundancy in communication and action raises attention to prevent deviance, it was obtained in all groups from 5 to 35% of the opinions as being against safety. In the average for all groups, the result was 28%.

Question 3, which stated that the "competition between measurements adopted in services and their quality hinders cooperative and safe work". The opinions obtained in each class range from 15% to 58% against security (29% for the mean value from all the classes).

The statement in item 13 was clearly linked to safe behavior. In all classes, 87% or 100% agreed that adequate knowledge to develop the activity includes attitude and action in the urgency task, and this would make the work safer.

Questions 13, 2, 18 are about issues in communication and competence. Although there were more answers in favor of safety, there were also other responses. Those questions were about policies and practices, observing deviances and communicating, etc.

The comparison involving results from an average for the 6 groups (those in Table 4) and 2 specifics of them, is shown in Figure 3. The 6 items detailed were, in sequence, 17, 8, 3, 13, 18 and 11, the most critical on conclusions and future work.

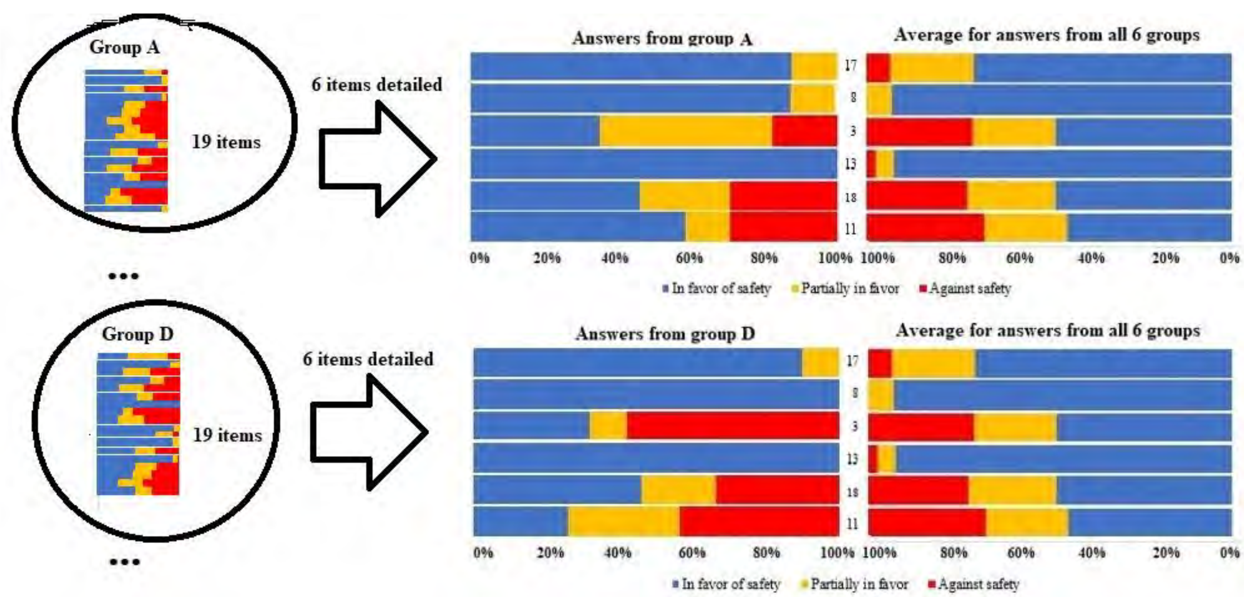


Figure 3 – Comparison between some groups' opinions and the average for 6 of 19 items evaluated by operational mass as in favor, partially or against safety.

4.5 Positive responses and Standard Deviation: an analysis by group and by question

In this analysis, it is important to establish the following criteria. An average of high results in favor of safety (close to 100%) with a low dispersion, that is, less variability in questionnaire answers indicates higher values for the ratio between positive mean and dispersion (positive mean/standard deviation), which indicates high safety. The smallest results for that ratio indicate the worst safety (these answers show the non-effectiveness of leadership in the safety culture). Thus, the best results were for Q1 (To ask in doubt), Q4 (active listening vs pressure for results), Q13 (sufficient knowledge for emergency tasks) and Q19 (commitment). The items with worst scores follow: Q11 (compatible policies and practices), Q18 (redundancy in communication and signs of deviance), Q12 (operator's social and family roles versus operator's function), Q14 (positioning in workstation due to supervision). Table 5 shows some notes about specific results. Group E was divided into Group E(1) and Group E(2) parts because it was originally the biggest among all teams.

Table 5 – Some comments on the results for average and Standard Deviation

Worst results	Medium results	Best results
Question 11: All classes.	Questions 9 for Group E(2).	Q1 (ask in doubt)
Question 18 (except class E, part 2).	Questions 8; and 17 (procedures; and stress) scored mid result for group A.	Q13 (sufficient knowledge for emergency tasks.
In question 2: class E (part 1) and class D had low values.		Q4 and 19 (leadership, commitment)

Considering all the questionnaire, the following risk map could be constructed:

Table 6 – Risk map for the results from average/SD

Mean value for safety	0 – 25				Q11, Q12, Q14
	25.1 – 50	Q5, Q9, Q16	Q2		
	50.1 – 75			Q4, Q8, Q10, Q17	
	75.1 – 100	Q1, Q4, Q13, Q19			
		0 – 25	25.1 – 50	50.1 – 75	75.1 – 100
	Standard Deviation from safety value.				

It may also be interesting to see the values for positive mean/SD for each of the 6 teams in each question. Figure 4 shows:

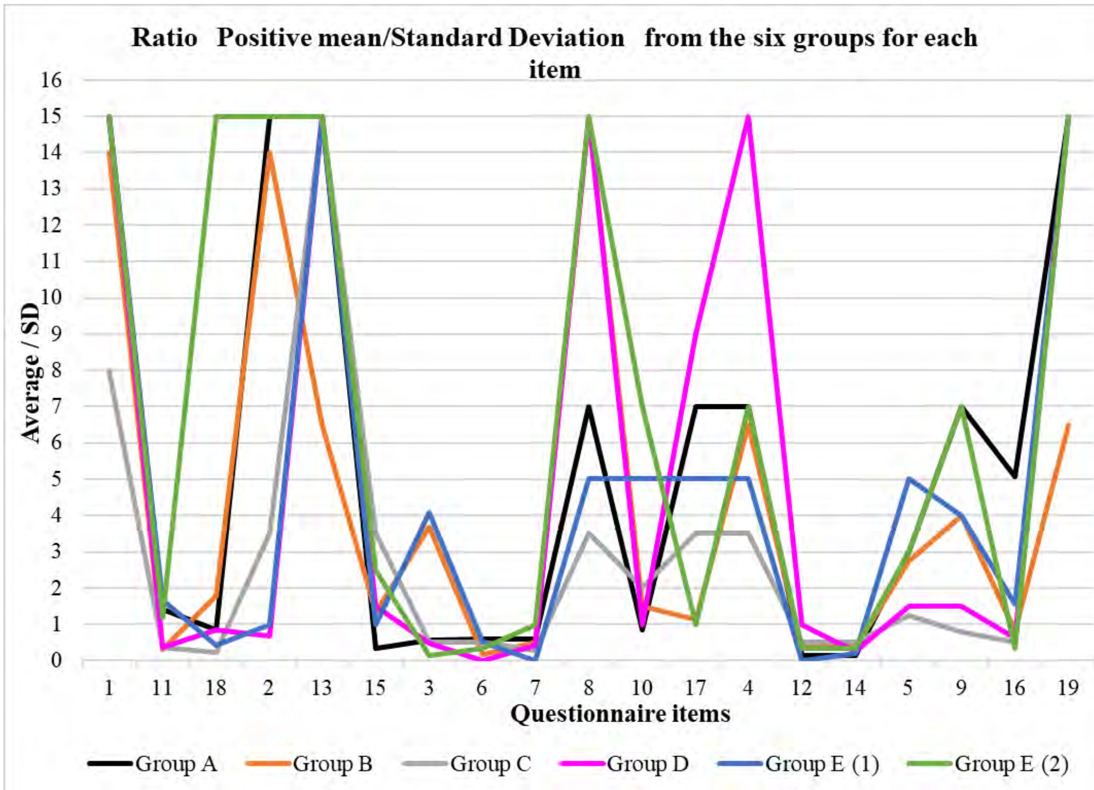


Figure 4 – Ratio Positive Mean/SD per group and per item plot

4.6 General results for Operational Culture

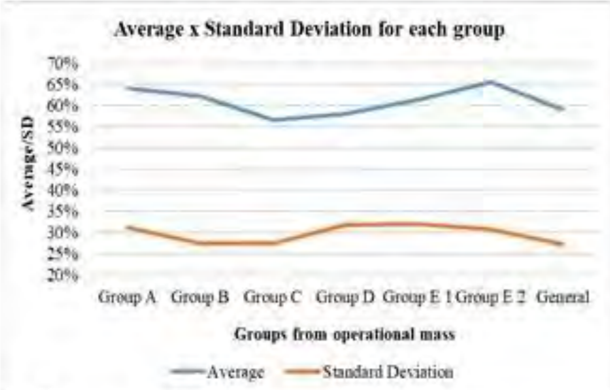
Figure 5 shows that for all the 19 items evaluated, each group had from 56% to 61% of positive opinions (they perceived them as in favor of safety). For a well-established safety culture, it is expected values above 75%. In terms of uniformity in response, around 27 to 32% in the standard deviation (SD). Thus, considering the groups mean value for F (favorable responses) and SD, the ratio F/SD = 58.5/29.5 = 1.98. Best results would range from 2.5 to 3.

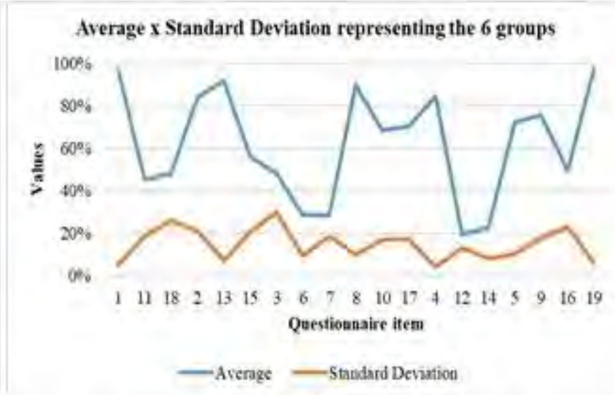
Team C had the worst performance in favor of safety and the teams A and E2 had very good results.

In Figure 5, by the plot for positive mean and SD for each question, it is noted that the highest score in favor of safety and the lowest standard deviation is the best result. Thus, in terms of positive responses, the highest were: Q1 (communication), Q13 (competence), Q19 (Commitment), Q8 (procedure), Q4 (cooperation), Q5 (commitment) and Q9 (fair culture) are the best results. The worst results: Q6 (conflict between production and security), Q7 (Procedures), Q12 (lack of cooperation), Q14 (cooperation and leadership).

In terms of standard deviation, smaller results indicate higher certainty, then: Q1, Q13, Q4, Q19. Higher results for SD indicate much dispersion in the group when commenting on the statements, thus, Q18, Q3, Q16. The dispersion results for other questions were normal, around 10%.

By dividing the positive responses by standard deviation, we have the following result: Q1, Q13, Q4, Q19 with very high values in favor of safety (above 10.0). The following questions scored badly, under 5.0: Q11 (communication), Q18 (communication), Q2 (competence), Q15 (competence), Q3 (priority production versus security), Q6 (priority production versus security), Q7 (procedure), Q12 (cooperation), Q14 (cooperation).





Aggregation parameter	Questions			
Communication	1	18	11	
Competence	2	13	15	
Conflict between production and safety	3	6		
Guilt culture /procedures	7	8		
Leadership/Stress	17	10		
Leadership relationship and Profile	4	12		
Commitment/Fair culture	5	9	16	19

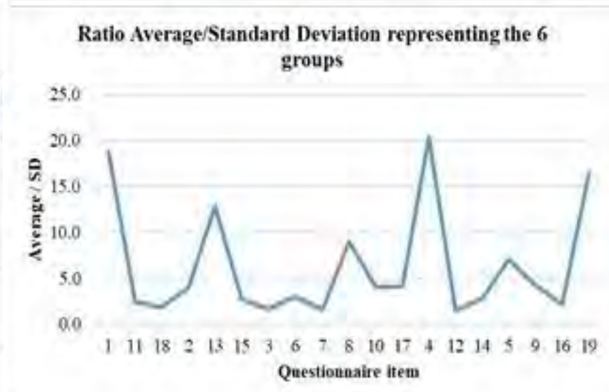


Figure 5 – General results for Operational Culture per item and per group. The word 'Average' at the plots titles means the same as 'Positive Mean', said before

4.7 New Concept: Intrinsic Relationship, Work Network, Graphs and Perception

Inadequate safety conditions that can cause incidents may incur problems of higher severity, that is, accidents. The chemical industry, in general, has decreased the number of incidents throughout the last years, but there is almost no reduction of accidents with or without lost days. There is, apparently, no connection between the various risks that might trigger situations of danger in routine, which makes no sense. It is noted, therefore, that results like above are caused by cases of no notification for serious problems, because of guilt culture, no priority in safety, and others. There is a gap between the safety asked by organizations, as in policies adopted, and the safety seen in practice.

The behavior present in many industries nowadays can be called as 'reactive', that is, it only starts to react in terms of safety and organizational culture after an accident occurs. The goal to be achieved by any organization that seeks to work well by balancing production, safety and human factors, is a proactive behavior with good leadership(s). Protective actions to avoid accidents all the time, especially when it is seen any deviation of conduct or even signs indicating a possibility of danger in the future, commonly known as predictive behavior. It is useful the following to activate that behavioral model: enhancing the safety culture, improving the availability and quality of trainings, make security and operation work together, promoting better active listening and clear communication, acknowledge good practices, managing risks, changes and incidents, and effectively integrating actions in different organizational areas to improve risk perception.

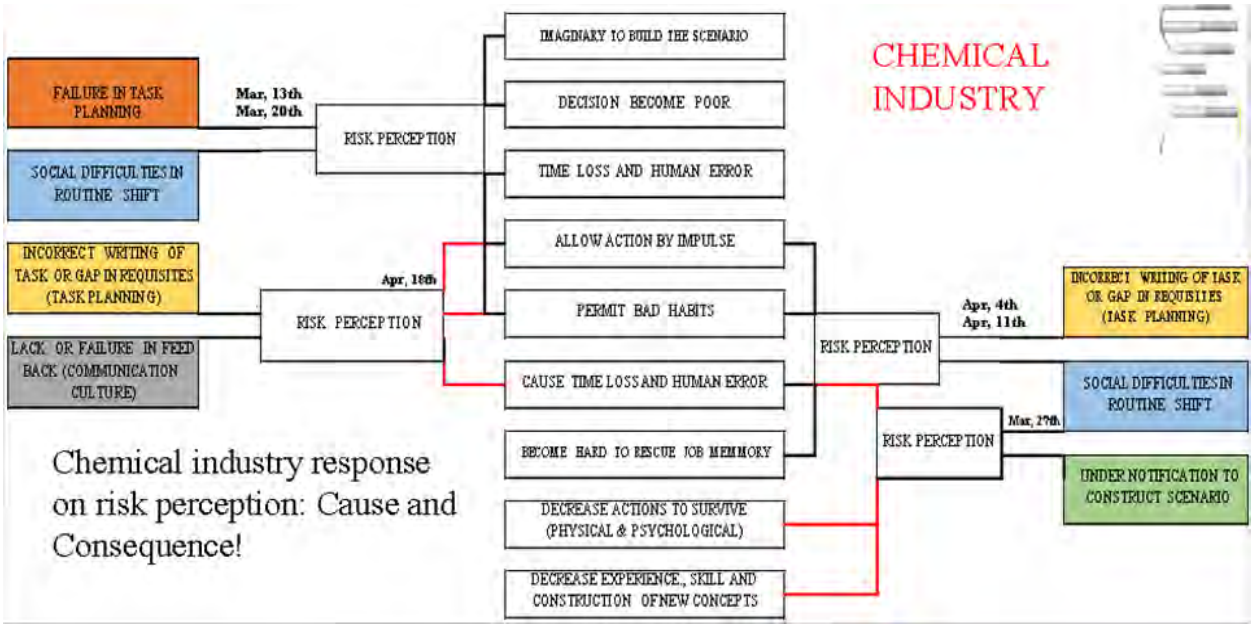


Figure 6 - Reliability and human factors in workstation design

5 Conclusions & Future Work

Some important points collected from the results of the diagnosis were: (1) Change the idea of the best work team for the one that reviews and respects the safety-based procedure; (2) Do not inspire fear for delay or possibility of failure; (3) Get to know how to discuss conflicts and priorities through good practices and giving feedback; (4) To understand that communication must be redundant because there might be some incorrect information; (5) Observe the real scenario before critical actions; (6) Take care when accelerating services and seek to set a climate of cooperation. Besides, it is important to intensify strong points bonds as: (7) emergency knowledge; (8) in doubt, always ask; (9) communicate any deviations; (10) Keep the stress controlled; (11) Active listening; (12) The patterns for the routine; and (13) avoid losses.

Risk and Human factors are often subjective, which hinders the application of appropriate techniques that can see the present moment and then design the future. Resilient organizations need to develop tools to confirm the risk perception in industrial critical tasks. Many companies with stable safety programs have encountered behavioral changes and unexpected accidents, confirming the lack of perception of changes over time in teams and leadership. Thus, low risk perception should be diagnosed from different perspectives that include: culture (principles), operation (cognition and practices), design (criteria for the workstation) and management (identification and measurement of human factors quality). This work was done in a real case of the chemical industry and complex process from questions elaborated after research on human factors. It intends, in the future, to help build the Bayesian Network indicating the regions, functions, appropriate subjects for corrective and preventive actions.

6 References

1 Inouye, J. Risk Perception: Theories, Strategies, And Next Steps. Campbell Institute. National Safety Council, 2014.

2 Furian, G.; Brandstätter C.; Kaiser S.; Witzik, A. ESRA thematic report no. 5: Subjective safety and risk perception. European Survey of Road users' safety Attitudes (ESRA), 2016.

3 Ávila, S.; Sousa, C. R.; Carvalho, A. C.: Assessment of complexity in the task to define safeguards against dynamic risks. In: 6th International Conference on Applied Human Factors and Ergonomics (AHFE) and the Affiliated Conferences, Las Vegas. Conference Proceedings; International Conference on Applied Human Factors and Ergonomics, (2015).

4 Cerqueira, I.; Drigo, E.; Ávila, S.; Gagliano, M.: C4t: Safe Behaviour Performance Tool. In: Karwowski, W., Trzcielinski, S., Mrugalska, B., Di Nicolantonio, M., Rossi, E. (eds.) Advances in Manufacturing, Production Management and Process Control. AHFE 2018. Advances in Intelligent Systems and Computing, vol .793, pp. 343--353, Springer, Cham (2019).

5 ÁVILA, S.F. A Excelência Operacional através da Confiabilidade Integrada. 1º Congresso Brasileiro de Confiabilidade, Risco e Segurança de Processos. ABRISCO. 2013b.

6 Ávila, S.; Mrugalska, B.; Wyrwicka, M.; Souza, M.; Ávila, J.; Cayres, E.; Ávila, J.: Cognitive and Organizational Criteria for Workstation Design. In: 10th International Conference on Applied Human Factors and Ergonomics (AHFE) and the Affiliated Conferences, Washington D.C. Conference Proceedings Springer; International Conference on Applied Human Factors and Ergonomics, (2019).

7 Souza, L.; Ávila, S.; Brito, R.; Cerqueira, I.; Ávila, J.: Discussion About Criteria for the Management of Alarms and Cognitive Limits for the Chemical Industry. Springer International Publishing AG, part of Springer Nature 2019 W. Karwowski et al. (Eds.): AHFE 2018, AISC 793, pp. 1–13, 2019.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Enhancing Safety Through strengthening Human Barrier

Abdulla Al-Azmi, Abdulrahman Al-Hajri, Bala Siva Srikanth Adivi, Sridhar Ketavarapu*, and Vishal Sawlikar
Kuwait Oil Company, Kuwait
*Presenters E-mails: sketavarapu@kockw.com, vsawlikar@kockw.com

Abstract

It is a well-known fact that up to 80 % of industrial incidents are caused wholly or partly by human actions. "Machines on its own does not cause any Incidents but human intervention does" is the well know based on incident investigations. To reduce the Incidents and its consequence, it is imperative to have knowledge, know-how, authority & controls be given to all front line personnel making them a reliable and competent barrier.

Based on the learnings from events, it was observed that for every incident there are several factors which had contributed to the event. Outcome of the findings suggest enhancing the robustness of preventive measures and this was the top priority within KOC – It includes workforce involvement through Competency Enhancement, further enabling them to identify the underlying hazards and follow the company procedures and standards. The process is chalked on a routine basis as a Plan Do Check Act (PDCA) activity to improve the inherent human reflexes. This plan/campaign was audited periodically to ensure that workforce can be included as a barrier.

It was observed that PDCA where planning was based on the inspection & Audit gaps identified. The gaps suggested the diversity of training and awareness session required and competency enhancement at various levels to ensure that personnel act as a critical barrier reducing the human error. It is imperative to suggest that unfamiliarity/skill & knowledge, planning (time shortage or hasting up) and understanding the hazards present along with supervision and feedback stood out as the top human factors which weakens the Human Barrier. The various sessions had motivated the frontline workforce to voice upon the concerns to their superiors for ensuring a safer operation prevail in the oil field. Further the Human factors play a significant role and this is to be given priority at all levels to include safety behavior and safety culture. The Human factor along with the feedback forms the base of the safety pyramid. It was also observed from the quarterly trends which focused on developing a significant improvement in the safety integrated policy concept for enhancing safety through strengthening human barrier.

The concept of Human and Human factors being a reliable barrier in the past has not been given significant weightage in design and operation. The idea of this paper is to showcase the approach where the reliability has increased and can consider personnel as a barrier and ensure a reliability operation/ activity. Workforce with a significant support can transform into efficient preventive and mitigative barrier.

Keywords: Human Barrier, Workforce Safety, Natural Safety, Culture Enhancement

Introduction

Safe and sustainable operability have been a key challenge in all process industries where time, material and resources (including human resources) are evaluated on a monetary base line inputs. The foundation for newer technology and associated complex equipment is to ensure better efficiency and operating margins. Considering the number of controls, inherent safe design and safeguards, included in the modern technology/equipment, it is still observed that the incidents tend to rise in the organization. Further the modern incidents are powerful to wipe out the facility and to the extent of determining the sustenance of the organization.

When discussing process safety, it is of the general opinion that the operability and process upsets are the key to understand process safety aspects and that the personnel involved are included under umbrella of occupational (personal) safety. The key understanding is that the entire operations is being operated and managed by personnel working in the frontline. Also it is imperative to note from the process safety incidents that "Machines on its own does not cause any Incident but human intervention does". As a result, it is important that we understand the significant contribution by the front line workforce and to ensure how they can manage to become a reliable barrier in the process safety.

It is also required that an organization develops tailor made programs to ensure that workforce is significantly on-guard to assimilate the hazards associated in the activities performed, the process involved and evaluate risks with all the available tools and mitigate in a timely manner to avoid incidents – appropriate risk management.

Concept of Human Barrier

The Risk Based Process Safety approach by CCPS defines the twenty (20) Elements classified under the Four (4) Pillars of Process Safety. On evaluating each of the element, on both macro level and micro level, it is evident and clear that human activity/ human element presents as the key input driver. It is vital that due weightage is given for each of the element's underlying knowledge to ensure that there is a robustness built into the system.

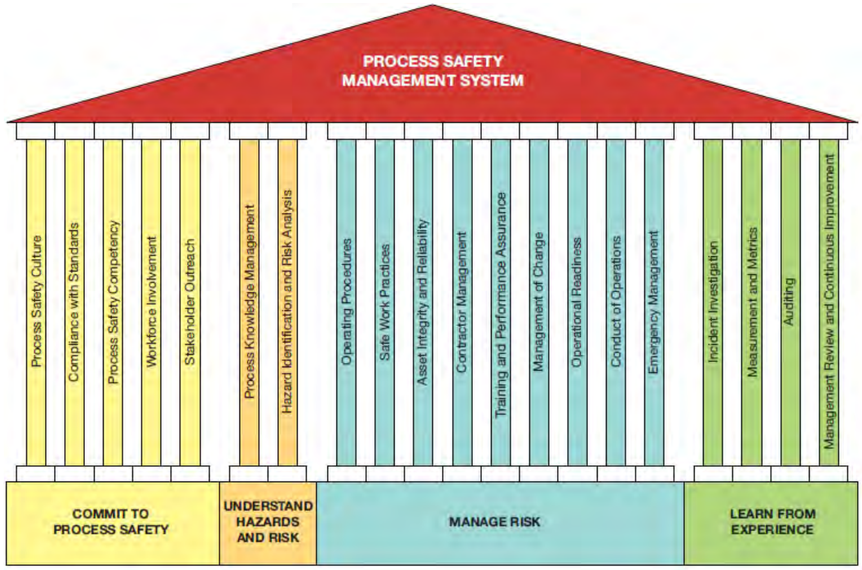


Figure 1 Pillars (Foundational Blocks) and associated Elements that constitute a sturdy RBPS Management System Pillars (CCPS)

The Process Safety Elements as well as, working personnel at all levels have revealed that, every sane human being in general is committed to self -safety- generally known as naturally safe, however the degree of commitment varies. The commitment is motivated by several methods - many analysis and theories have been developed on that subject. The knowledge (procedural & practical, risk evaluation), training (regular, critical and emergency) and act to work appropriately in a timely manner ensures that the robustness is built into the Universal Process Safety System.

“Human Barrier of Process Safety” comprises of the overall thought process and logical response of personnel to handle and contribute across the Process Safety Elements.

As part of company PHA requirements (possible technical safety studies such as HAZID, HAZOP, SIL, FMEA, etc.), Simulations (SIF, Model reviews, QRA’s, F&G Mapping etc.), knowledge levels along with safer and reliable systems are developed, it can be stated that the Engineering has emerged competitively over time considering that the engineering decisions is resourced and well aided. As a result, this area of concern where human functional impact and critical decision making, under the time bound circumstances is moved towards the operations and maintenance phase.

The workforce at the site, interacting with the machines/equipment and reviewing the process on minute to minute scenario, are to take well informed step and are considered as the “Front Line Human Barrier”.

Process Safety and Barrier Management – A Hierarchical Approach

It is the top of the pyramid in process safety pyramid or top event in case we refer to the bow tie model that is to be avoided.

As the hierarchy suggests, the process safety incident is the top of the Process Safety Metric Pyramid (Figure 2) - the top being Major process safety incident and second level is the process safety incident with lesser severity. Understanding the process safety pyramid, it is evident that incident is a culmination of failure of the Layer of Protection concept with a lesser significance. Also, the near miss incident is a forewarning of process safety (near- miss) incidents. These near miss incidents could be due to process upset/ failure or improper guideline or procedure or unsafe behavior resulting into near miss incidents. However, the bottom most part of the pyramid is generally considered the unsafe behavior, acts or insufficient operating discipline which is to be considered as process safety near miss incident at par with respective level.

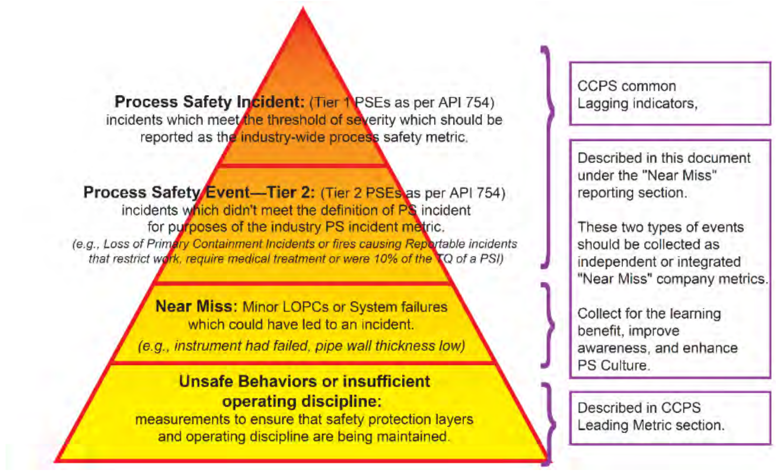


Figure 2 Process Safety Metric Pyramid (CCPS)

To elucidate the same in a swiss cheese model or using the bow-tie, the hazards are contained by multiple protective barriers and it is certain that any barrier may have weakness or holes, when all these holes are aligning the hazard passes through the barrier resulting in the potential for adverse consequences. Barrier may be physically engineered in the design of the system; however, the behavior control depends on the people, especially the front line workforce. The holes can be latent/ incipient or actively opened by the people.

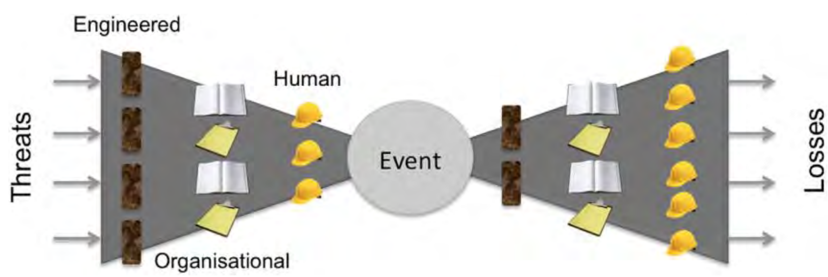


Figure 3 Conceptual bowtie showing the relationship between threats, events and losses and different types of Generic Controls (McLeod, R.W)

As the process safety pyramid (Ref: Figure 2 Process Safety Metric Pyramid) is explained above, failure of protection layers is directly or indirectly responsible under the personnel working in the field. The actual safety and operability of the facility and/or field falls in the hands of the operational and maintenance workforce. In other words, organizations shall implement the management of leading indicators because appropriate interpretation of the leading indicators matters in the process safety management.

This idea of having a robust front line human barrier is important. Stressing on this, Kuwait Oil Company management has established a robust management system that includes reporting of leading indicators such as near miss, hazardous condition and in-house developed behavioral safety tool- SOC (Safety Observation and Conversation) and mechanism to implement the corrective actions from the leading indicators. This systems ensure that all unsafe conditions are reported for a quick rectification and enhancement in the respective systems.

Besides the leading indicators, the lagging indicators are also documented in the management systems and they are reviewed and investigated as per procedures.

It is from the leading and lagging indicators, a continual improvement is ensured through updating manuals, procedures and learning from incidents (leading & lagging). The Quarterly Performance Review (QPR) of the HSSE is conducted to see how the indicators are performing and evaluating the safety triangle bottom. Also to understand the performance of frontline workforce in terms of reporting the hazardous condition observed and to review the number of conditions corrected. This tracking is to ensure that the observed hazardous conditions does not lead to incidents. Also during the review, analysis of the number of SOC reported, wherein how many worked was intervened to correct the behavior/ activity is also included.

Based on the leading indicators & lagging indicators of the past, a detailed program was conceived to strengthen the front line workforce personnel who act as a human barrier of controlling the risk and consequence. For the emergency response, a realistic training based on the NORSOK - CRIOP (Crisis Intervention and Operability) was imparted to the front line operation and maintenance workers as it defines the hierarchy during emergency operations.

Plan Do Check Act (PDCA) Program on Human Barriers

It is observed across all process industries that an incident has a direct correlation where some of the final signals/checks were either missed or critical signals not addressed at the right stage to avoid the accident or negate the consequence. The goal is to ensure that such scenarios are addressed and that workforce personnel are prepared for such contingencies within the organization.

Within KOC, to understand the gaps available in the frontline workforce, initially a course discussion with operational & maintenance frontline workforce was undertaken to understand that there is a gap existing – This is important a detailed protocol may not lead into appropriate responses. This is then followed by a streamlined audit by developing a specific audit protocol – this is to be done with the task of operational teams. The protocol focused on the following: Knowledge (Procedures), Practical Response during scenario, Behavior and Cultural Impact, Management support (Expectation).

Inside KOC, the HSSE Management System Framework Guide suggest the utilization of Plan Do Check Act guideline at its core, is to encourage and facilitate continual improvement on all its HSSE parameters. The below KOC HSSE Quality model shows the 13 HSSE elements used in KOC and how they are interlined to each other. Each of the element has a set of guidelines and procedure including the process safety procedures.

Figure 4 KOC HSSE Quality Model and Relationship to Elements

The Planned Program: The commitment of the leadership had suggested to identify the process safety/ human barrier gaps. These requirements have been identified based on the Audits/inspections, following which a Performance Indicator system was developed. The performance indicator included all the leading indicators identified by the frontline workforce, identifying process safety hazards, suggesting the management of change with justification of how it can support maintenance and operations, Trainings and awareness session required on the Process Safety risk assessment (including behavioral aspects) and Training and awareness session related to Operational and Maintenance activities and Emergency Response readiness.

The Worked out Program: A clear strategy consisting of bridging the gap was developed by creating a modular training package for each of the target group considering the diversity and training needs. During the training and awareness session, the frontline workforce was mooted to voice their concerns and brainstorming of the cases of incidents in the process industry was discussed. Also included topic was "What Can Be Done Better for Their Facility". The session took feedback and reciprocated it to the management at the end of every quarter along with additional training needs identified during the sessions.

The training aspect shall start with identification of the hazard, critical signs and signal from the unit/equipment. The key for accident prevention evaluation is the key to understand the prevailing hazard and how it had started to take shape. The overall theme of the awareness session was "Any unfamiliarity/ skill for not identifying a hazard senses disaster". This was also included by showing and discussion various incidents from within the company and the industry.

It was also made clear to the frontline workforce that however robust the design and engineering is, and capability of the equipment, it is not all information has been included on your control panel or included in the operational manual or based on a risk based maintenance program. As a result, the operators and maintenance personnel who are looking at the facility, and listening to the physical response of the equipment, a balanced approach has to be can be taken on the total operations and inform the concerned team for their expert evaluation of the scenario. It was emphasized that taking support of including different subject expert opinion is the best way to utilize the company knowledge resources to enhance the better operability of the plant.

For example, considering some of the older plants, there shall be several generation difference units and controllers which are to interact. The awareness session included that the field operator shall also be in a position to distinguish between the hardware and software issues as it is always important to ensure the maximum utilization of the equipment/ facility. This is first line of evaluation and identification. The awareness session shall be followed up as an incremental part of the training. The training focused on how to identify the Leading Process Safety Indicators, and how operational intervention is required or as to when the Maintenance activities would be more advised to make it an advantage.

The advantage of an awareness session shall always mean that there is a recap of the earlier session as well as to include an incremental information to the participants. Further the competency enhancement at various levels is conducted to ensure that field personnel act as a critical barrier reducing the human error.

Similar to a STOP system, KOC had included Safety Observation and Conversation system where every working aspect is included and peer review is done to ensure that the job is done in the safest manner. It is different when it comes to emergency response and management where CRIOP based training is imparted. Right from identification and stopping the process requires many inputs and quick decision making capabilities. The functional administrative capability of evaluating and decision making of the front line workforce be enhanced by periodically conducting a CRIOP based discussion coaching and facility/ field based action response training.

The Evaluation of the Program: Competition session between teams were conducted with frontline supervisors and their team to come with ideas "What Can Be Done Better for Their Facility" and this helped in the supervisor gain confidence on his/her team and how the other team defends on not having it in place. These session made teams more competent and number of Management of Change (MoC) had resulted in the event/ competition. They were further evaluated on technical merits – this was scored on the performance on the program.

During the competition and during the program, it was recommended to check on motivation of the frontline workers and also with supervisor evaluations – this is done on observing and feedback and response to interactions. This concept of the motivation, support from the management, supervisor evaluation and positive support is combined and described as Human Barrier Maintenance – when evaluating the human barrier, it is important that the last line is well connected and well informed of the decision to be made. The performance indicators developed act as evaluation of the program. The program was reviewed every first week of every month and during the management meetings the results were discussed.

Review of the program: Reports were generated on both monthly and quarterly basis. The monthly report was on the indicators identified the base line requirement and on the new requirements identified based on the training/awareness session conducted. Quarterly reports were generated to review the performance of the program on overall basis. The modular training planned and its basis was suggested to the top management by showing the performance and scope of coverage.

The feedback from the management was discussed in the following awareness sessions to encourage the frontline workforce personnel. A two way feedback from the management to the frontline workforce and the workforce perception to the senior management, resulted in an increase of mutual trustworthiness. Further the program was a welcome on all fronts to enhance the reliability of the frontline workforce as a human barrier.

Result and Inferences

The results have been satisfactory as the frontline personnel were involved in the discussion on procedural control and operability issues after implementation of the program. It was made clear that barrier management in the process safety management has been assigned as Key Performance Indicators. API RP-754, Process safety performance indicators for the refining and petrochemical industry and KOC internal guidelines and procedures for process safety management (under KOC HSSE Management System) are considered in identifying the leading and lagging performance indicators.

Inclusion of the operation and maintenance workforce and involving at all stages as well as conducting CRIOP based discussion has been beneficial for the frontline workforce as well as for the management as a reliable barrier is been formed. It is to be clearly noted that this barrier is a last line of contingency and cannot be included for operational planning of emergencies.

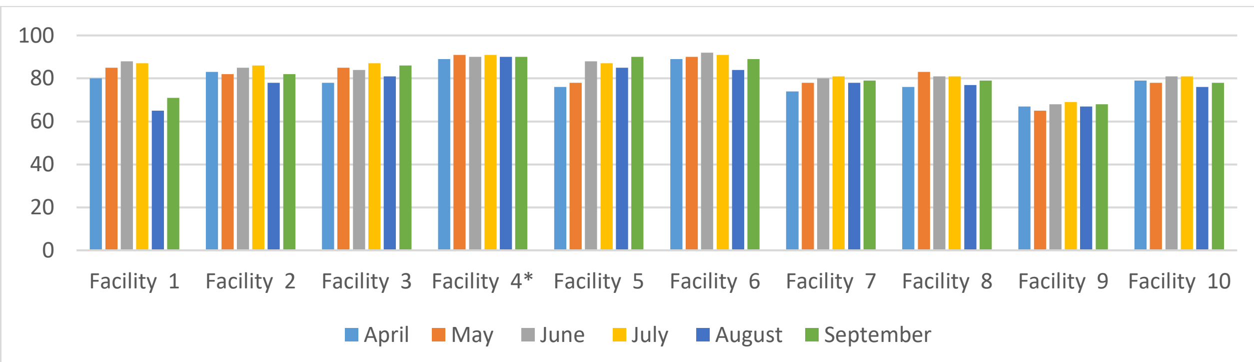


Figure 5: KPI Performance - Human Barrier & Emergency Response Evaluation

The training/ awareness session for this program include the following as indicators for evaluation:

- Leading indicators
- Process Safety Hazards
- Trainings and awareness session – Process/ Behavior/Occupation Safety/Guidelines/Standards
- Training and awareness session related to Operational and Maintenance – MoC/Procedure
- Emergency Response readiness

Scoring was predominantly based on the training and awareness session conducted. The objective is to train and evaluate rather than evaluate on an overall aspect. As there was a fresh inclusion of new frontline workforce and considering the partial staff rotation in August as a result, most of the scoring had dropped a little in the month of August. It was observed that Facility 4 had no rotation of staff and as a result the scoring on the parameters were maintained.

As described in the Hierarchical approach (Refer Section Process Safety and Barrier Management – A Hierarchical Approach), all kinds of barriers shall be audited and focused to enhance and ensure program is on track to reach the goal. The Key Performance Indicators for operational and maintenance workforce shall include operating the equipment in critical efficiency zone to ensure optimum production is maintained in the highly volatile crude market besides adhering to HSE standards and procedures.

It is to note that however, adept they are with facility procedures and protocols, a constant training and encouragement with support for management (Human Barrier Maintenance) is required to ensure that they are able to deliver the knowledge received.

The maximum visibility of process safety management (including barrier management) is achieved by the adequate awareness and incorporating the risk mitigation measure into the system by design and by following the HSEMS standards & procedures of the company. Further training and behavior based vision on the risk, consequence of the various hazards which have been identified during the various studies would support and ensure clarity.

Conclusions

The operational & maintenance personnel act as the most important line of control in the Safety Management Program (both Process Safety as well as Occupational Safety) and for its implementation. The core concept is to continually develop the frontline personnel and enhance their competence in responding to any process safety deviations in a safe and sustainable manner to avert incidents.

The program is generally an ongoing and continuous in nature. It is important to have a compatible digital concept for better tracking of the continual improvement in case of workforce spread across different area for such programs - considering the size of the organization by virtue of the changes in workforce, locations and complexity.

It is important that the frontline personnel are considered as a barrier and are included right during design, startup and commissioning and all Management of Change (MoC) activities. They shall also be trained for appropriate response during operating and maintenance (operational phase) for managing the safety critical elements only to suggests the holes of the Swiss-cheese model can shrunk / barrier in the bowtie can be strengthened by creating a better control, by the strong knowledgeable and capable workforce who act as a barrier by holding the risk and not escalating it further.

The human barrier act in a most significant manner and work wonders within the safe operating framework defined. Further, the operational and maintenance workforce along with a comprehensive system to report hazardous conditions, near miss items, and safety observations in the field supports in strengthening the preventive barrier and support the overall all safety in the industry.

Acknowledgements

The authors acknowledge the support and permission granted by Kuwait Oil Company, especially the South & East Kuwait Senior Management team, for their support and guidance and for

approving of sharing the information accumulated information during the concept, planning and execution of this Program to the Process Safety Management fraternity through this paper.

The Authors are basically from the Conventional Oil background along with experience from several projects on process safety management and barrier management. This journey where many man hours have been invested to enhance and develop the frontline of workforce by making them a reliable human barrier and in their view it has been a very humbling journey.

The authors also, acknowledge the other teams in the organization who had supported them in this program.

References:

1. CCPS Book "Guidelines for Risk Based Process Safety"
2. KOC HSEMS Procedures and Standards
3. CRIOP: A scenario method for Crisis Intervention and Operability analysis by SINTEF
4. KOC "Enhancing Safety Through strengthening Human Barrier" Program
5. Swain, A.D., Guttmann, H.E., 1983. NUREG/CR – 1278. Handbook of Human Reliability Analysis. U.S. NRC
6. McLeod, R.W., 2015. Designing for Human Reliability – Human Factors Engineering in the Oil, Gas, and Process Industries. Gulf Professional Publishing, Massachusetts.
7. HSE (Health and Safety Executive), 2009. Review of Human Reliability Assessment Methods. Research Report RR679. United Kingdom.
8. API RP-754 Process Safety Performance Indicators for the Refining & Petrochemical Industries
9. CCPS Book "Process Safety Leading and Lagging Metrics"
10. KOC Enhancing Safety Through strengthening Human Barrier program

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Crosswalk of Human Reliability Methods for Offshore Oil Incidents

Ronald L. Boring*, Jooyoung Park, Thomas A. Ulrich
Human Factors and Reliability Department
Idaho National Laboratory
P.O. Box 1625, MS 3818
Idaho Falls, Idaho 83415, USA
*Presenter E-mail: ronald.boring@inl.gov

Abstract

Human reliability analysis (HRA) has long been employed in nuclear power applications to account for the human contribution to safety. HRA is used qualitatively to identify and model sources of human error and quantitatively to calculate the human error probabilities of particular tasks. The nuclear power emphasis of HRA has helped ensure safe practices and risk-informed decision making in the international nuclear industry. This emphasis has also tended to result in a methodological focus on control room operations that are very specific to nuclear power, thereby potentially limiting the applicability of the methods for other safety critical domains. In recent years, there has been interest to explore HRA in other domains, including aerospace, defense, transportation, mining, and oil and gas. Following several high profile events in the oil and gas industry, notably the Macondo well kick event in the U.S., there has been a move to use HRA to model and reduce risk in future oil drilling and production activities. Organizations like the Bureau of Safety and Environmental Enforcement are adapting the risk framework of the U.S. Nuclear Regulatory Commission for offshore purposes. In this paper, we present recent work to apply HRA methods to the analysis of offshore activities. We present the results of retrospective analyses using three popular HRA methods: SPAR-H, Petro-HRA, and CREAM. With the exception of Petro-HRA, these HRA methods were developed primarily for nuclear power event analysis. We present a comparison of the findings of these methods and a discussion of lessons learned in applying the methods to offshore events. The objective of this paper is to demonstrate the suitability of HRA methods for oil and gas risk analysis but also to identify topics where future research would be warranted to tailor these HRA methods.

Keywords: Risk Assessment, Human Error Assessment, Human Reliability Analysis, Standardized Plant Analysis Risk-Human Reliability

1 Human Reliability Analysis Methods

1.1 General Overview of Quantification Approaches

Human reliability analysis (HRA) methods have historically been developed to account for and mitigate human errors in nuclear power applications. Recently there is increased use of HRA outside the nuclear domain such as to support quantitative risk assessment for oil and gas settings. As HRA is generalized to new areas, it is important that existing HRA methods are validated to a broader range of uses. Where there are shortcomings in existing HRA methods, the methods should be adapted to support these new domains, or new HRA methods should be developed. This validation and evolution of methods ensures that HRA identifies and thereby minimizes risk.

HRA methods serve the twofold purpose to classify the sources of errors qualitatively and to estimate the human error probability (HEP). Qualitative error classification serves as the basis for quantification. Of the roughly 60 HRA methods created, most are centered on quantification [1]. Boring [2] proposed the following ways of classifying HRA quantification methods:

- *Scenario Matching Methods:* This approach, used by the original HRA method, the Technique for Human Error Rate Prediction (THERP) [3], entails matching the human failure event (HFE) to the best fitting example scenario in a lookup table and using the HEP associated with that template event as the basis for quantification. See Table 1(a).
- *Decision-Tree Methods:* Methods like the Cause-Based Decision Tree (CBDT) [4] follow a decision tree (similar to an event tree), which guides the quantification along a number of predefined analysis decision points. See Table 1(b).
- *Performance Shaping Factor (PSF) Adjustment Methods:* In these methods, exemplified by approaches like the Standardized Plant Analysis Risk-HRA (SPAR-H) method [5], the PSFs serve as multipliers on nominal error rates. For example, a PSF with a negative influence would serve to increase the HEP over a nominal or default error rate. A list of PSFs and associated multipliers is provided by the method. See Table 1(c).
- *Expert Estimation Methods:* In these approaches, subject matter experts including risk analysts will estimate the likelihood of the HFEs. A Technique for Human Error ANAlysis (ATHEANA) [6] uses a structured expert estimation approach to arrive at HEPs. Such approaches often provide anchor values for quantification to assist subject matter experts in producing the relevant HEP, but the specific method used to derive the HEP and the factors that may influence the quantification are largely left to the subject matter experts. Because expert estimation methods typically do not specify how to decompose the factors shaping the quantification but rather look at the HFE as a whole, they are often referred to as holistic approaches [7]. See Table 1(d).

The wide availability of HRA methods may leave the analyst overwhelmed at which methods to select for which applications. Recent method comparisons exist for nuclear (e.g., [1,8]), and they provide helpful benchmarks in considering the advantages and disadvantages of each method. The National Aeronautics and Space Administration's (NASA's) HRA method guidance [9] serves as another helpful template for downselecting HRA methods. Across multiple selection criteria, NASA selected four primary HRA methods to be used individually or in combination. Table 2 lists the four methods selected by NASA and a summary of their primary strengths and weaknesses in a generalized form (e.g., without consideration of specific NASA domain applications). While this downselection is helpful, it does not necessarily represent optimal methods with respect to offshore oil applications.

Table 1 - Examples of Common HRA Quantification Approaches

(a) Scenario matching lookup table from THERP [3], which provides the HEP and the error factor (EF) for uncertainty.

Table 20-13 Estimated HEPs for selection errors for locally operated valves (from Table 14-1)

Item	Potential Errors	HEP	EF
	Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is		
(1)	Clearly and unambiguously labeled, set apart from valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.001	3
(2)	Clearly and unambiguously labeled, part of a group of two or more valves that are similar in <u>one</u> of the following: size and shape, state, or presence of tags*	.003	3
(3)	Unclearly or ambiguously labeled, set apart from valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.005	3
(4)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in <u>one</u> of the following: size and shape, state, or presence of tags*	.008	3
(5)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.01	3

(b) Decision tree from CBDT [4] provides HEPs for the event-tree end states.

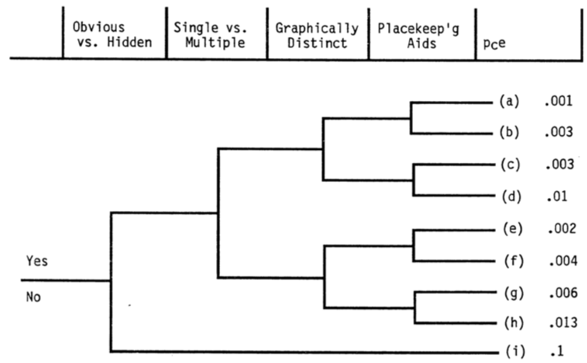


Figure 4-6. Decision tree Representation of P_{ce}, Skip a Step in Procedure

(c) Example PSF multipliers on the nominal HEP (0.001) for diagnosis tasks in SPAR-H [5].

PSFs	PSF Levels	Multiplier for Diagnosis
Available Time	Inadequate time	P(failure) = 1.0 ☐
	Barely adequate time (≈2/3 x nominal)	10 ☐
	Nominal time	1 ☐
	Extra time (between 1 and 2 x nominal and > than 30 min)	0.1 ☐
	Expansive time (> 2 x nominal and > 30 min)	0.01 ☐
	Insufficient information	1 ☐
Stress/ Stressors	Extreme	5 ☐
	High	2 ☐
	Nominal	1 ☐
	Insufficient Information	1 ☐
Complexity	Highly complex	5 ☐
	Moderately complex	2 ☐
	Nominal	1 ☐
	Obvious diagnosis	0.1 ☐
	Insufficient Information	1 ☐

(d) Example anchor HEPs for expert elicitation in ATHEANA [6].

Table 3.8-2. Suggested Set of Initial Calibration Points for the Experts

Circumstance	Probability	Meaning
The operator(s) is “Certain” to fail	1.0	Failure is ensured. All crews/operators would not perform the desired action correctly and on time.
The operator(s) is “Likely” to fail	~ 0.5	5 out of 10 would fail. The level of difficulty is sufficiently high that we should see many failures if all the crews/operators were to experience this scenario.
The operator(s) would “Infrequently” fail	~ 0.1	1 out of 10 would fail. The level of difficulty is moderately high, such that we should see an occasional failure if all of the crews/operators were to experience this scenario.
The operator(s) is “Unlikely” to fail	~ 0.01	1 out of 100 would fail. The level of difficulty is quite low and we should not see any failures if all the crews/operators were to experience this scenario.
The operator(s) is “Extremely Unlikely” to fail	~ 0.001	1 out of 1000 would fail. This desired action is so easy that it is almost inconceivable that any crew/operator would fail to perform the desired action correctly and on time.

Table 2 - The Four HRA Methods Selected for NASA Use

Method	Approach	Strengths	Weaknesses
THERP	Lookup table	Widely used original HRA method. THERP specifies a complete process model for HRA. It has good coverage of errors related to human actions.	Little coverage of cognitive factors. Method may have limited generalizability beyond the nuclear-specific human interactions in the lookup tables.
CREAM[a]	Task types (lookup table) and PSF multipliers	Good coverage of cognitive factors and detailed task decomposition approach for qualitative insights into errors.	Method is complex in practice (e.g., involving many steps for basic quantification) and tends to produce similar HEPs regardless of performance drivers.
NARA[b]	Task types (lookup table) and PSF multipliers	Good use of human factors literature as data source to validate HEPs for task types.	The task types are aligned to nuclear power plant operations, and specialized variants need to be developed for air traffic control and rail domains. The method remains proprietary.
SPAR-H	PSF multipliers	Simplified method that can be used without extensive HRA background. PSFs allow generalizability beyond predefined task types.	Quantification-only approach that assumes HFEs defined in the probabilistic risk assessment (PRA). PSF multipliers are not calibrated to non-nuclear techniques.

a. Cognitive Reliability Error Analysis Method [10]

b. Nuclear Action Reliability Assessment [11]

1.2 HRA Methods for Oil and Gas

Two HRA methods have been developed specifically for oil and gas, and they are briefly noted below.

1.2.1 Barrier and Operational Risk Analysis (BORA)

Despite information suggesting major accident sequences may be attributed to several risk influencing factors classified as technical, human, operational and organizational, the majority of quantitative risk analyses of offshore oil and gas production platforms has been directed at technical safety systems. The Barrier and Operational Risk Analysis (BORA) of hydrocarbon releases (BORA-Release) is a method for carrying out the qualitative and quantitative risk analysis of platform specific hydrocarbon release frequency [12]. In finer detail, the method assesses the effect of risk reducing measures and risk increasing changes within operations. BORA affords the ability to analyze both the effect of safety barriers put in place to impede the release of hydrocarbons as well as how platform specific conditions such as the aforementioned technical, human, operational and organizational factors influence the performance of the barrier. Analysis of hydrocarbon release risk via the BORA method is executed with the use of barrier block diagram/event trees, fault trees, and risk influence diagrams.

The BORA-Release method is made up of eight steps:

1. Development of a basic risk model including release scenarios
2. Modeling for the performance of safety barriers
3. Assignment of industry average probabilities/frequencies and risk quantification based on these probabilities/frequencies
4. Development of risk influence diagrams
5. Scoring of risk influencing factors
6. Weighting of risk influencing factors
7. Adjustment of industry average probabilities/frequencies
8. Recalculation of the risk in order to determine the platform specific risk related to hydrocarbon release.

Many of these steps overlap basic HRA processes found across HRA methods like [3,4,5,6,10,11]. BORA focuses on the breakdown of barriers designed as part of defense in depth to prevent accidents in oil and gas production facilities. These barriers, however, may omit many of the HFEs that can precipitate accidents at the facility. HRAs centered on barriers may overlook important precursors to many types of accidents. Additionally, BORA's emphasis on prevention of accidents may limit some of its application as a risk analytic tool for as-built systems and processes.

1.2.2 Petro-HRA

The Norwegian Research Council and the Norwegian state oil company, Statoil (now called Equinor), recently sponsored development of an HRA method to aid human factors analysts in completing HRAs for oil and gas applications. The approach, named the Petro-HRA method [13], features seven steps that mirror much of what is outlined in the IEEE-1082 HRA guide [14]:

1. Scenario definition
2. Qualitative data collection
3. Task analysis
4. Human error identification
5. Human error modeling
6. Human error quantification
7. Human error reduction.

Quantification in the Petro-HRA method is based on SPAR-H [5], offering some refinement to PSFs and multipliers to make them more oil and gas industry specific. SPAR-H was selected as the basis method because other HRA methods that had been used in the Norwegian oil and gas industry were found to generate unreasonably high HEPs or have low interrater reliability [15]. Because SPAR-H is primarily a quantification approach, additional guidance was developed to aid analysts in completing the qualitative portion of HRA, including translating a task analysis to HFEs when they are not already defined by a PRA. Because HRAs are performed to support the safety evaluation of new technologies in the Norwegian oil industry, specific guidance is provided to improve the system design or operations process to minimize human errors when they are identified.

2 Example Human Reliability Analysis for Well Kick

2.1 Selection of HRA Methods

In this section, we provide a review of the same well blowout event using three different HRA methods: SPAR-H [5], Petro-HRA [13], and CREAM [10]. The selection of these methods is based on the widespread use of SPAR-H and CREAM for non-nuclear applications, including many completed analyses for oil and gas. Petro-HRA, which is a derivative method of SPAR-H tailored to petroleum applications, serves as a useful benchmark. The same HFEs are analyzed using all three methods, and a brief explanation is provided on how the analyses are completed. The explanations of the analyses provide tutorial details, but analysts should ensure they refer back to the source guidance for the methods for a better understanding of how to apply the methods.

2.2 Human Failure Events

SPAR-H and CREAM assume the HFE has been defined in the PRA, while Petro-HRA provides guidance on how to define the HFE. For the present purposes, we have characterized three primary HFEs related to the well kick as depicted in Figure 1. As can be seen in Figure 1, HFE_1 refers to the detection of the well kick, HFE_2 refers to responding to the well kick by actuating the annular of the blowout preventer (BOP), and HFE_3 refers to performing the emergency well disconnect. A brief description of the well-kick related accident is necessary for those who are not familiar with the human activities pertaining to the well-kick event or the Deepwater Horizon accident.

Figure 1 - Example Human Failure Events in Sequence

An excellent and detailed chronological account of the specific events can be found in Chapter 2 of the Transocean Investigation Report titled *Macondo Well Incident* [16]. All event details are not necessary for demonstrating the HRA methods; therefore, here only a brief description is provided for context to the analysis. The event began on April 20, 2010, when an oil and gas blowout incident at the Macondo Oil Well caused an explosion and fire that resulted in 11 fatalities, 17 seriously injured personnel, the sinking of the Deepwater Horizon drilling rig, and the release of millions of gallons of oil into the Gulf of Mexico. The event can be attributed, in part, to a failure to detect the well kick and subsequent blowout or uncontrolled release of oil and gas hydrocarbons from the well. The backpressure drove the hydrocarbons through the drilling apparatus to the rig, in which it was ignited in an explosion that subsequently set fire to the rig. The rig had finished the exploratory drilling phase of operations and was in the process of performing temporary well-abandonment activities to prepare the well for the production phase of operations which another rig was scheduled to perform.

The well-abandonment activities entail plugging the well with cement, ensuring the integrity of the cement plugs via a negative pressure test, and then retracting the drilling apparatus. The negative pressure test circulates chemically treated mud that serves as the primary barrier to prevent the hydrocarbon from traveling through the well and into the drilling apparatus. The negative pressure created by circulating the mud simulates the low pressure sea floor atmosphere in order to verify the cement plug is properly sealing the well. Pressure and flow indications were available to the drilling team, though due to urgency to finish the drilling phase of operations, they went unnoticed until the negative pressure test was performed. A supervising representative from British Petroleum overseeing the drilling operation did raise a concern to the driller; however, any concern was improperly alleviated by more experienced drilling team members stating the odd pressure values were not uncommon and did not merit any significant concerns. Operations resumed, even though the undetected kick had occurred up to an hour prior and was continuing to worsen over time.

The drilling crew closed the upper annular of the blow out preventer (BOP) at 9:34 PM in attempt to arrest the kick. The high pressure and volume of hydrocarbon flow caused the piping within the BOP annular to shift such that a joint between two pipes impeded the closing mechanism and the annular failed to seal the well. Mud began to flow onto the drilling floor, and in response the flow was diverted to the mud-gas separators at 9:45 PM. The volume of flow quickly exceeded the mud-gas separators' capacity, and the blowout alarm sounded at 9:47 PM. Shortly thereafter, at 9:49 PM, the rig lost main power followed quickly by two explosions. At 9:56 PM, an emergency well disconnect was attempted in which the BOP was designed to sever the pipe to eliminate flow to the rig. The bridge team received indication that the disconnect mechanism was activated; however, the pipe was not successfully severed, and flow continued. The order to abandon ship was issued at 10:00 PM.

2.3 A Brief Note on Retrospective HRA

The following HRA walkthroughs are examples of retrospective HRA. Retrospective HRA is an analysis that looks at an event that has already happened. Of course, the probability that the event happened is 1.0, because it actually did occur. The purpose of a retrospective analysis is to determine the likelihood that the event should have happened given its context. In colloquial terms, was the event simply bad luck, or was it the systematic product of circumstances that could have been prevented? In identifying the causes of the event, a retrospective analysis looks at the probability that such an event could occur again, given the same circumstances. Retrospective analyses are crucial for establishing corrective actions and preventing recurrence of similar events.

It should be noted that a retrospective analysis will have greater and more specific insights than would a typical prospective analysis. A prospective analysis, such as an HRA conducted when a system is being designed or built, must rely on the normal course of operations. In other words, the context must be kept general to cover a variety of operating contexts. It is not typical to assume the confluence of multiple poor factors during a prospective analysis. In contrast, a retrospective analysis would feature all known mitigating factors that caused the event to transpire. As such, a retrospective analysis will inherently be more conservative than a prospective analysis. It is assumed that for an extreme event like the Deepwater Horizon accident, the retrospective HEP generated by most HRA methods would be close to 1.0. This represents a much more severe form of the well blowout than would be modelled in a prospective analysis.

2.4 Example Analysis Using SPAR-H

2.4.1 Overview

Here, we demonstrate SPAR-H [5] as a simplified method to help understand how to quantify the three HFEs. A SPAR-H quantification requires several steps:

1. Define the HFE (completed by PRA and a prerequisite for the SPAR-H analysis)
2. Determine the appropriate SPAR-H worksheet
3. Determine the appropriate SPAR-H nominal HEP
4. Evaluate the PSFs
5. Calculate the product of the nominal HEP and the PSF multipliers
6. Apply correction factor for dependence.

These steps are walked through in separate subsections below. The first step—defining the HFEs—was detailed in the previous section.

2.4.2 Determine the Appropriate SPAR-H Worksheet

SPAR-H contains two types of analysis worksheets:

- *At power* (NUREG/CR-6883, Appendix A [5])
- *Low power and shutdown* (NUREG/CR-6883, Appendix B [5]).

The origin of SPAR-H as an HRA method for nuclear power applications is clear here. The basic difference between these two worksheets involves whether the plant is producing electricity (i.e., at power) or in maintenance or refueling mode (i.e., low power and shutdown). It is assumed that there is more opportunity for high consequence events and tighter time windows to take recovery actions during at-power operations. An offshore analogy for at power would be during drilling activities.

For the well kick scenarios, we assume the SPAR-H at-power worksheets are applicable.

2.4.3 Determine the Appropriate SPAR-H Nominal HEP

The SPAR-H worksheets for at-power and low-power-and-shutdown each have two task types that are modeled. The task types determine the nominal or default HEP for the HFE:

- *Diagnosis:* This HFE primarily involves cognitive activities such as monitoring or decision-making. The nominal HEP for diagnosis HFEs is 1E-2 (0.01).
- *Action:* This HFE primarily involves carrying out physical activities such as manipulating equipment. The nominal HEP for action HFEs is 1E-3 (0.001).

Because an HFE may involve a series of activities by the human involved, it is not uncommon for the HFE to be classified as both diagnosis and action. In that case, the *joint HFE* can logically be thought to occur due to diagnosis *or* action errors. Mathematically, this means that the nominal HEPs for diagnosis and action are added together.

In our well kick example, all HFEs involve diagnosis and action components, since they require cognitive monitoring, decision-making, and interaction with equipment.

2.4.4 Evaluate the PSFs

SPAR-H uses nominal HEPs to represent the generic diagnosis and action tasks performed within the HFE. These nominal HEPs are then modified using multipliers corresponding to different levels of influence of the PSFs. SPAR-H makes use of eight PSFs, encompassing:

- Available time to complete the task (which is independent of any time pressure the personnel may experience)
- Internal stress and external stressors
- The complexity of the task and scenario
- The experience and training of the personnel completing the tasks under analysis
- The procedures—either written or oral—to guide the personnel in completing the task
- The ergonomics of the system being used and the human-machine interfaces available to the personnel
- The fitness for duty—including degraded fitness due to fatigue of long-duration events—of the personnel completing the task
- Work processes, including organizational factors, command and control, and communications.

Generally, the SPAR-H PSFs can have three types of effects:

1. *Negative:* A negative effect means that the PSF decreases human reliability and thereby increases the HEP. For example, to denote the negative effect of available time would mean to suggest that there was inadequate time available to complete the task.
2. *Nominal:* A nominal effect means that the default applies. Nominal time, for example, suggests that there's adequate time to complete the task without undue time pressure or extra time.
3. *Positive:* A positive effect means that the PSF increases human reliability and thereby decreases the HEP. A positive effects results in giving credit to the human actions. For example, positive available time means that there is extra time over what is needed to accomplish the task.

In the absence of information to inform the assignment, the analyst would denote "inadequate information," which simply assigns a nominal value.

To assign SPAR-H PSFs, it is useful for the human reliability analyst to consult with an operations specialist to answer the following questions:

- Which personnel are involved in this task?
- What indicators are available for the task?
- What are the timing constraints that could interfere with a successful outcome?
- Do personnel have adequate training and experience on the task?

- What’s needed to perform this task successfully?
- What can go wrong?
- What could influence personnel performance in terms of actions or decision-making?

For the three example HFEs, the following PSF effects could be noted:

- For detection of the well kick (HFE_1), the time available will vary from situation to situation, but once a kick occurs, there is a limited window of time before the formation fluid reaches the blowout preventer. As the available time erodes, the ability of the drilling crew to respond decreases proportionately to the decreasing time window. It may be assumed that limited available time to detect will adversely affect the HEP. The clock is ticking, so to speak, which can only operate negatively on the outcome of the event. All other PSFs are assumed to be nominal.
- The detection of a well kick triggers a change: response actions are needed in order to prevent a blowout (HFE_2) and ultimately disconnect the well from the oil rig (HFE_3). This operational shift will generally result in multiple elevated negative PSFs relative to nominal or normal operations. The time window is closing, but there may also be elevated negative stress and complexity, potentially diminished levels of experience for this type of situation, and potentially poor to incomplete procedures. Underlying the situation, negative work processes such as breakdowns in communication, coordination, or command and control may also manifest.

While detection of the well kick (HFE_1) can be seen as a mostly nominal influence of the PSFs, the transition to emergency operations to prevent blowout (HFE_2) and disconnect the well (HFE_3) will likely invoke multiple negative PSFs.

2.4.5 Calculate the Product of the Nominal HEP and the PSF Multipliers

When negative, nominal, or positive effects of PSFs have been determined, these are matched to the appropriate level in the SPAR-H PSF multiplier tables. If there is a negative or positive effect of a PSF, this phase involves determining the degree of that effect, which corresponds to a multiplier. A summary of SPAR-H multiplier assignments for the well kick detection, response, and disconnect HFEs is found in Table 3. For the detection HFE, a single negative PSF—available time—is assumed. For the response HFE, three slightly negative PSFs—available time, stress, and complexity—are assumed. For the disconnect HFE, two negative PSFs—available time and stress—are assumed.

The basic HEP is defined in SPAR-H as the nominal HEP multiplied by the product of all PSF multipliers:

$$\text{Basic HEP} = \text{Nominal HEP} \times \prod \text{PSF Multipliers} \qquad \textit{(Eq. 1)}$$

For HFE_1 related to well kick detection, the PSF is calculated separately for diagnosis and action:

$$HFE_1 \text{ Diagnosis Basic HEP} = 1E\text{-}2 \times 10 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 1E\text{-}1 = 0.1 \qquad \textit{(Eq. 2)}$$

$$HFE_1 \text{ Action Basic HEP} = 1E\text{-}3 \times 10 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 1E\text{-}2 = 0.01 \qquad \textit{(Eq. 3)}$$

Table 3 - SPAR-H Assignments for Well Kick Detection, Response, and Disconnect

PSFs	PSF Levels	HFE_1: Well Kick Detection		HFE_2: Well Kick Response		HFE_3: Well Disconnect	
		Diagnosis Multiplier	**Action Multiplier**	**Diagnosis Multiplier**	**Action Multiplier**	**Diagnosis Multiplier**	**Action Multiplier**
Available time	Inadequate time	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0
	Barely adequate time	10	10	10	10	10	10
	Nominal time	1	1	1	1	1	1
	Extra time	0.1	0.1	0.1	0.1	0.1	0.1
	Expansive time	0.01	0.01	0.1 to 0.01	0.01	0.1 to 0.01	0.01
	Insufficient info	1	1	1	1	1	1
Stress/stressors	Extreme	5	5	5	5	5	5
	High	2	2	2	2	2	2
	Nominal	1	1	1	1	1	1
	Insufficient info	1	1	1	1	1	1
Complexity	Highly complex	5	5	5	5	5	5
	Moderately complex	2	2	2	2	2	2
	Nominal	1	1	1	1	1	1
	Obvious diagnosis	0.1	N/A	0.1	N/A	0.1	N/A
	Insufficient info	1	1	1	1	1	1
Experience/ training	Low	10	3	10	3	10	3
	Nominal	1	1	1	1	1	1
	High	0.5	0.5	0.5	0.5	0.5	0.5
	Insufficient info	1	1	1	1	1	1
Procedures	Not available	50	50	50	50	50	50
	Incomplete	20	20	20	20	20	20
	Available, but poor	5	5	5	5	5	5
	Nominal	1	1	1	1	1	1
	Diagnostic/symptom oriented	0.5	N/A	0.5	N/A	0.5	N/A
	Insufficient info	1	1	1	1	1	1
Ergonomics/ HMI	Missing/ misleading	50	50	50	50	50	50
	Poor	10	10	10	10	10	10
	Nominal	1	1	1	1	1	1
	Good	0.5	0.5	0.5	0.5	0.5	0.5
	Insufficient info	1	1	1	1	1	1
Fitness for duty	Unfit	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0	HEP = 1.0
	Degraded fitness	5	5	5	5	5	5
	Nominal	1	1	1	1	1	1
	Insufficient info	1	1	1	1	1	1
Work processes	Poor	2	5	2	5	2	5
	Nominal	1	1	1	1	1	1
	Good	0.8	0.5	0.8	0.5	0.8	0.5
	Insufficient info	1	1	1	1	1	1

The joint basic HEP is simply the sum of the diagnosis and action basic HEPs:

HFE_1 Joint Basic HEP = Diagnosis Basic HEP + Action Basic HEP

$$= 1E\text{-}1 + 1E\text{-}2 = 1.1E\text{-}1 = 0.11 \qquad \textit{(Eq. 4)}$$

The same general form of the equation applies to HFE_2 related to the response to well kick and HFE_3 related to the well disconnect, but with one exception. Because it is possible to have a resultant HEP greater than 1.0 when there are more than three negative HEPs, SPAR-H prescribes a correction factor:

$$\text{Corrected Basic HEP} = \frac{\text{Nominal HEP} \times \Pi \text{ PSF Multipliers}}{\text{Nominal HEP} \times (\Pi \text{ PSF Multipliers - 1}) + 1} \qquad \textit{(Eq. 5)}$$

Thus, for HFE_2 we first calculate the product of the PSF multipliers, which in this case is identical for the diagnosis and action tasks:

$$\prod \text{PSF Multipliers} = 10 \times 2 \times 2 \times 1 \times 1 \times 1 \times 1 \times 1 = 40 \qquad \textit{(Eq. 6)}$$

This product is then applied in the corrected basic HEP equation for diagnosis and action:

$$HFE_2 \text{ Corrected Diagnosis Basic HEP} = \frac{1E\text{-}2 \times 40}{1E\text{-}2 \times (40 - 1) + 1} = 0.288 \qquad \textit{(Eq. 7)}$$

$$HFE_2 \text{ Corrected Action Basic HEP} = \frac{1E\text{-}3 \times 40}{1E\text{-}3 \times (40 - 1) + 1} = 0.0385 \qquad \textit{(Eq. 8)}$$

The joint basic HEP for HFE_2 is calculated by adding the two basic HEPs:

$$HFE_2 \text{ Joint Basic HEP} = 0.288 + 0.0385 = 0.326 \qquad \textit{(Eq. 9)}$$

HFE_3 is calculated identically to HFE2 but with different multipliers since stress is much higher while the complexity of activating the well disconnect is lower. We first calculate the product of the PSF multipliers, which in this case is identical for the diagnosis and action tasks:

$$\prod \text{PSF Multipliers} = 10 \times 5 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 = 50 \qquad \textit{(Eq. 10)}$$

HFE3 only has two negative PSFs. Thus, the basic (uncorrected) HEP is calculated:

$$HFE_3 \text{ Diagnosis Basic HEP} = 1E\text{-}2 \times 50 = 5E\text{-}1 = 0.5 \qquad \textit{(Eq. 11)}$$

$$HFE_3 \text{ Action Basic HEP} = 1E\text{-}3 \times 50 = 5E\text{-}2 = 0.05 \qquad \textit{(Eq. 12)}$$

The joint basic HEP for HFE_3 is calculated by adding the two basic HEPs:

$$HFE_3 \text{ Joint Basic HEP} = 0.5 + 0.05 = 0.55 \qquad \textit{(Eq. 13)}$$

There is nearly a threefold increase in the basic HEP between HFE_1 and HFE_2 due to the increased effects of negative PSFs for stress and complexity between well kick detection and response. A further increase in the basic HEP occurs between the HFE_2 and HFE_3 for the well disconnect.

2.4.6 Apply Correction Factor for Dependence

In the final stage of SPAR-H quantification, a correction factor is applied for dependence. Dependence in SPAR-H means that the second or subsequent HFE in sequence may result in greater likelihood of human error. If appropriate, a correction factor is applied to the basic HEP.

For sequences of two or more HFEs, SPAR-H considers four factors that influence dependence:

- Same (s) or different (d) *crew* between the HFEs
- Close (c) or not close (nc) in *time* between the HFEs
- Same (s) or different (d) *location* between the HFEs
- Additional (a) or no additional (na) *cues* (i.e., information available to crew) between the HFEs.

The more the HFEs share crew, time, location, and cues, the more likely there is to be dependence between them. SPAR-H uses a dependency condition table (see Table I-4) to classify dependence along a scale from *Zero*, *Low*, *Moderate*, *High*, to *Complete*.

Table 4 - SPAR-H Dependence Table (from [5])

Condition Number	Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or no additional)	Dependency	Number of Human Action Failures Rule ☐ - Not Applicable. Why?________________
1	s	c	s	na	complete	When considering recovery in a series e.g., 2nd, 3rd, or 4th checker If this error is the **3rd error in the sequence**, then the dependency is at least **moderate**. If this error is the **4th error in the sequence**, then the dependency is at least **high.**
2				a	complete	
3			d	na	high	
4				a	high	
5		nc	s	na	high	
6				a	moderate	
7			d	na	moderate	
8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17					zero	

HFE_1 is the first HFE in the sequence and by definition does not have dependence. We assume HFE_2 to have somewhat different crew responding to the well kick. HFE_2 and HFE_3 follow closely in time, have the same location, but also have additional cues. The resultant dependence level as traced (d-c-s-a) in Table 4 is *moderate dependence*.

The conditional HEP is the basic HEP corrected for dependence. SPAR-H features the following equations for levels of the conditional HEP:

- *Zero Dependence:* Conditional HEP = Basic HEP
- *Low Dependence:* Conditional HEP = (1 + 19 × Basic HEP) / 20

- *Moderate Dependence:* Conditional HEP = (1 + 6 × Basic HEP) / 7
- *High Dependence:* Conditional HEP = (1 + Basic HEP) / 2
- *Complete Dependence:* Conditional HEP = 1.0.

For HFE_2 and HFE_3 assuming moderate dependence, we have:

HFE_2 Conditional HEP = (1 + 6 × 0.326) / 7 = 0.422 *(Eq. 14)*

HFE_3 Conditional HEP = (1 + 6 × 0.55) / 7 = 0.614 *(Eq. 15)*

Moderate dependence resulted in the HEP for HFE_2 and HFE_3 each increasing by nearly 0.1 in our example.

Using the SPAR-H method, we quantified the HEPs for the three HFEs, arriving at:

Detect well kick: HEP_{HFE1} = 0.11 *(Eq. 16)*

Respond to well kick: HEP_{HFE2} = 0.422 *(Eq. 17)*

Well Disconnect: HEP_{HFE3} = 0.614. *(Eq. 18)*

A final note on SPAR-H is that it only provides the HEP, not a measure of uncertainty. Uncertainty is calculated using the constrained noninformative prior, a method for calculating parameters assuming a single input parameter on a beta distribution. Some PRA software feature the ability to calculate the uncertainty in SPAR-H if required by the analyst.

2.5 Example Analysis Using Petro-HRA

2.5.1 Overview

As noted, the Petro-HRA method [13] is a modified variant of SPAR-H developed specifically for applications in the oil and gas industry. As outlined in the brief introduction in Section 1.2.2, the activities involved with performing the analysis for the Petro-HRA method align closely with SPAR-H. The terminology is slightly different, and some additional guidance specific to the oil and gas industry is included. For example, the SPAR-H method relies on the PRA model to screen and identify HFEs, while the Petro-HRA method does not assume the HFE is defined by the PRA.

2.5.2 Performance Shaping Factor Definitions

Petro-HRA uses the same quantification framework as SPAR-H, but it uses modified PSFs that are tailored to address the context of oil and gas including offshore drilling and refinery operations. The modified PSFs for Petro-HRA include:

1. Time
2. Threat stress (equivalent to stress in SPAR-H)
3. Task complexity
4. Experience/Training
5. Procedures
6. Human-machine interface
7. Attitudes to safety, work and management support

8. Teamwork
9. Physical working environment.

The first six PSFs (i.e., time, threat stress, task complexity, experience/training, procedures, and human-machine interface) are nearly identical to the PSFs in SPAR-H. Petro-HRA has three different PSFs that replace the fitness for duty and work process PSFs from SPAR-H. The PSF entitled "Attitudes to safety, work and management support" reflects organizational aspects of the context surrounding the HFE. The teamwork PSF pertains to the level of coordination and the efficacy of the team to accomplish common and valued goals. The PSF for physical working environment is a more explicit evaluation of the ergonomics surrounding the work environment. In contrast to SPAR-H, physical ergonomics can play a more significant role in the oil and gas industry given the sometimes harsh working environments, and therefore it is defined by its own PSF.

2.5.3 Performance Shaping Factor Levels and Multipliers

A significant difference between SPAR-H and Petro-HRA is the how the levels of the PSF multipliers are treated. In SPAR-H, the levels for the multipliers of each PSF are uniquely defined. Petro-HRA simplifies the multiplier levels, such that each PSF has the same ranking system for impact on performance. The same categorical levels exist across all PSFs, ranging from two levels of negative effect, a nominal effect, and one level of positive effect. However, the assignment of a multiplier value itself has specific criteria and specific numerical values for each PSF. Table 5 provides examples of the multipliers for attitudes to safety, work and management support. Table 6 shows the same multipliers for the time PSF.

Table 5 - Petro-HRA PSF for Attitudes to Safety, Work and Management Support (from [13])

Multipliers	*Levels*	*Level descriptions*
50	Very high negative effect on performance.	In this situation safety is not at all prioritized over other concerns when it is appropriate or there are extremely negative attitudes to work conduct (for example the operators are not monitoring or awake when they should be). There is very low mindfulness about safety. The operators do not experience management support, for example in strong management pressure for production even if safety is clearly in question.
10	Moderate negative effect on performance.	In this situation it is not specified by management that safety should be prioritized when that is appropriate. The operators are uncertain if safety should be prioritized or not, or the operators are uncertain about rules and regulations that are important for performing the task.
1	Nominal effect on performance.	The operators have adequate attitudes to safety and work conduct and there is management support to prioritize safety when that is appropriate. The operator(s) shows mindfulness about safety. Attitudes to safety, work and management support have neither a negative nor a large positive effect on performance.
0.5	Moderate positive effect on performance	The operator(s) has very good attitudes to safety and work conduct and there is explicit management support to prioritize safety when that is appropriate. The operator(s) shows a very high degree of mindfulness about safety.
1	Not applicable.	This PSF is not relevant for this task or scenario.

Table 6 - Petro-HRA PSF for Time (from [13])

Multipliers	*Levels*	*Level descriptions*
HEP=1	Extremely high negative effect on performance.	Operator(s) does not have enough time to successfully complete the task.
50	Very high negative effect on performance.	The available time is the minimum time required to perform the task or close to the minimum time to perform the task. In this situation the operator(s) has very high time pressure or they have to speed up very much to do the task in time.
10	Moderate negative effect on performance	The operator(s) has limited time to perform the task. However, there is more time available than the minimum time required. In this situation the operator(s) has high time pressure, or they have to speed up much to do the task in time.
1	Nominal effect on performance.	There is enough time to do the task. The operator(s) only has a low degree of time pressure, or they do not need to speed up much to do the task. When comparing the available time to the required time the analyst concludes that time would neither have a negative nor a positive effect on performance.
0.5	Moderate positive effect on performance	There is extra time to perform the task. In this situation the operator(s) has considerable extra time to perform the task and there is no time pressure or need to speed up to do the task in time.
1	Not applicable.	This PSF is not relevant for this task or scenario.

2.5.4 Quantification Process

The process of quantifying the HEP for each human failure event is nearly identical to that of SPAR-H, and therefore a detailed explanation will not be repeated. An important distinction between SPAR-H and Petro-HRA is that Petro-HRA only features a single nominal HEP set at 1E-2 (0.01). This nominal HEP is equivalent to the higher nominal HEP associated with cognitive or diagnosis tasks in SPAR-H. Essentially, Petro-HRA does away with the separation of Diagnosis and Action in SPAR-H and assumes all HFEs contain elements of both. In some analyses, this may result in possible conservatism in Petro-HRA compared to SPAR-H.

The completed table for each of the three previously identified HFEs including detect well kick, respond to well kick, and disconnect well is shown in Table 7. The HFE evidence used to assign PSF levels for SPAR-H was also used to populate the PSF multipliers in this table. The assigned values are similar to SPAR-H and follow the same general pattern in which stress was elevated in both HFE_2, recovery from blowout event, and even more so during HFE_3, well disconnect. Complexity was higher in HFE_2 than either of the other HFEs. Unlike SPAR-H, which doesn't have a designated physical working environment PSF, here the physical working environment was significantly deteriorated during HFE_3, in which the fire from the blowout event made it difficult for the crew to reach the control room and activate the emergency disconnect function.

The basic HEPs for the three HFEs are calculated as the product of the nominal HEP and the PSF multipliers:

Detect well kick: $HEP_{HFE1} = 0.01 \times 100 = 1.0$ *(Eq. 19)*

Respond to well kick: $HEP_{HFE2} = 0.01 \times 400 = 4.0 \approx 1.0$ *(Eq. 20)*

Table 7 – Petro-HRA Assignments for Well Kick Detection, Response, and Disconnect

PSFs	PSF Levels	HFE1: Well Kick Detection Multiplier	HFE2: Well Kick Response Multiplier	HFE3: Well Disconnect Multiplier
Time	Extremely high negative	HEP=1	HEP=1	HEP=1
	Very high negative	50	50	50
	Moderate negative	10	10	10
	Nominal	1	1	1
	Moderate positive	0.1	0.1	0.1
	Not applicable	1	1	1
Threat Stress	High negative	25	25	25
	Low negative	5	5	5
	Very low negative	2	2	2
	Nominal	1	1	1
	Not applicable	1	1	1
Task Complexity	Very high negative	50	50	50
	Moderate negative	10	10	10
	Very low negative	2	2	2
	Nominal	1	1	1
	Moderate positive	0.1	0.1	0.1
	Not applicable	1	1	1
Experience/Training	Extremely high negative	HEP=1	HEP=1	HEP=1
	Very high negative	50	50	50
	Moderate negative	15	15	15
	Low negative	5	5	5
	Nominal	1	1	1
	Moderate positive	0.1	0.1	0.1
	Not applicable	1	1	1
Procedures	Very high negative	50	50	50
	High negative	25	25	25
	Low negative	5	5	5
	Nominal	1	1	1
	Low positive	0.5	0.5	0.5
	Not applicable	1	1	1
Human-Machine Interface	Extremely high negative	HEP=1	HEP=1	HEP=1
	Very high negative	50	50	50
	Moderate negative	10	10	10
	Nominal	1	1	1
	Low positive	0.5	0.5	0.5
	Not applicable	1	1	1
Attitudes to Safety, Work and Management Support	Very high negative	50	50	50
	Moderate negative	10	10	10
	Nominal	1	1	1
	Low positive	0.5	0.5	0.5
	Not applicable	1	1	1
Teamwork	Very high negative	50	50	50
	Moderate negative	10	10	10
	Very low negative	2	2	2
	Nominal	1	1	1
	Low positive	0.5	0.5	0.5
	Not applicable	1	1	1
Physical working environment	Extremely high negative	HEP=1	HEP=1	HEP=1
	Moderate negative	10	10	10
	Nominal	1	1	1
	Not applicable	1	1	1

Well Disconnect: $HEP_{HFE3} = 0.01 \times 25000 = 250.0 \approx 1.0$ *(Eq. 21)*

Note that the Petro-HRA guidance specifies that an HEP greater than 1.0 should be set as 1.0. This correction has been applied for HFE_2 and HFE_3.

2.5.5 Apply Correction Factor for Dependence

The same calculations and adjustments for dependence performed for the SPAR-H analysis are also performed here for the Petro-HRA method. The reader can refer back to the Section 2.4.6 on SPAR-H dependence for the equations. Note that where the basic HEP is 1.0, there is no change to the overall conditional HEP considering dependence. The results of the calculations are shown below for each HFE:

Detect well kick: Final (Conditional) $HEP_{HFE1} = 1.0$ *(Eq. 22)*

Respond to well kick: Final (Conditional) $HEP_{HFE2} = 1.0$ *(Eq. 23)*

Well Disconnect: Final (Conditional) $HEP_{HFE3} = 1.0$ *(Eq. 24)*

These HEPs are considerably more conservative than the HEPs produced for SPAR-H. As noted in a paper on a similar event analysis [17], whereas SPAR-H was developed for retrospective analyses, Petro-HRA was developed for prospective analyses. This difference may contribute to the conservatism of Petro-HRA.

2.6 Example Analysis Using CREAM

2.6.1 Overview

The Cognitive Reliability and Error Analysis Method (CREAM) method [10] provides a different approach from SPAR-H to quantify the HEP for each HFE. CREAM contains a basic and extended method. The basic method corresponds to an initial screening of the human interactions. The screening or basic method addresses either the task as a whole or major segments of the task. The extended method uses the outcome of the basic method to look at actions or parts of the task where there is a need for further precision and detail. The following sections describe how to use the basic and extended method using the same HFEs examined with the SPAR-H and Petro-HRA methods in the prior sections.

2.6.2 CREAM Basic Method

There are three steps to the CREAM Basic Method:

1. *Describe the task or task segments to be analyzed.* This task is analogous to defining the HFE and any subtasks associated with the HFE.
2. *Assess the Common Performance Conditions (CPCs).* The CPCs are essentially PSFs.
3. *Determine the probable control mode.* The CPCs are used to classify the control mode as either strategic, tactical, opportunistic, or scrambled.

Step 1 was already performed in defining the HFE in Section 2.2 and can be input directly into this analysis.

Table 6 - Summary of the CPC Level Assignments in CREAM

CPC name	CPC Levels		
	HFE_1: Well Kick Detection	**HFE_2: Well Kick Response**	**HFE3: Well Disconnect**
Adequacy of organization	Very efficient	Very efficient	Very efficient
	Efficient	Efficient	Efficient
	Inefficient	Inefficient	Inefficient
	Deficient	Deficient	Deficient
Working condition	Advantageous	Advantageous	Advantageous
	Compatible	Compatible	Compatible
	Incompatible	Incompatible	Incompatible
Adequacy of MMI and operational support	Supportive	Supportive	Supportive
	Adequate	Adequate	Adequate
	Tolerable	Tolerable	Tolerable
	Inappropriate	Inappropriate	Inappropriate
Availability of procedures / plans	Appropriate	Appropriate	Appropriate
	Acceptable	Acceptable	Acceptable
	Inappropriate	Inappropriate	Inappropriate
Number of simultaneous goals	Fewer than capacity	Fewer than capacity	Fewer than capacity
	Matching current capacity	Matching current capacity	Matching current capacity
	More than capacity	More than capacity	More than capacity
Available time	Adequate	Adequate	Adequate
	Temporarily inadequate	Temporarily inadequate	Temporarily inadequate
	Continuously inadequate	Continuously inadequate	Continuously inadequate
Time of day	Day-time (adjusted)	Day-time (adjusted)	Day-time (adjusted)
	Night-time (unadjusted)	Night-time (unadjusted)	Night-time (unadjusted)
Adequacy of training and experience	Adequate, high experience	Adequate, high experience	Adequate, high experience
	Adequate, limited experience	Adequate, limited experience	Adequate, limited experience
	Inadequate	Inadequate	Inadequate
Crew collaboration quality	Very efficient	Very efficient	Very efficient
	Efficient	Efficient	Efficient
	Inefficient	Inefficient	Inefficient
	Deficient	Deficient	Deficient

For Step 2, Table 8 represents a summary of the level/descriptors on each CPC for the three HFEs. CREAM maps well to the earlier SPAR-H and Petro-HRA examples, but differs on a few items. For example, the working conditions CPC is a factor uniquely considered in CREAM and is not covered as a standalone PSF in other HRA methods like SPAR-H or Petro-HRA. Table 9 shows the selected effects of each CPC for the three HFEs in this analysis. These effects are important for calculation of the HEP.

Table 7 - Summary of the CPC Level Assignments and Their Performance Effects in CREAM

CPC name	**HFE_1: Detect**		**HFE_2: Respond**		**HFE_3: Disconnect**	
	Level / descriptors	**Expected effect on performance reliability**	**Level / descriptors**	**Expected effect on performance reliability**	**Level / descriptors**	**Expected effect on performance reliability**
Adequacy of organization	Inefficient	Reduced	Inefficient	Reduced	Inefficient	Reduced
Working condition	Compatible	Not significant	Compatible	Not significant	Incompatible	Reduced
Adequacy of MMI and operational support	Supportive	Improved	Supportive	Improved	Supportive	Improved
Availability of procedures / plans	Inappropriate	Reduced	Inappropriate	Reduced	Inappropriate	Reduced
Number of simultaneous goals	Fewer than capacity	Not significant	Fewer than capacity	Not significant	Fewer than capacity	Not significant → Reduced
Available time	Adequate	Improved	Adequate	Improved	Adequate	Improved
Time of day	Night time	Reduced	Night time	Reduced	Night time	Reduced
Adequacy of training and experience	Adequate, limited experience	Not significant	Adequate, limited experience	Not significant	Adequate, limited experience	Not significant
Crew collaboration quality	Inefficient	Not significant → Reduced	Inefficient	Not significant → Reduced	Inefficient	Not significant → Reduced

As the last step, the combined CPC score expressed as the triplet [$\sum_{\text{Reduced}}$, $\sum_{\text{Not significant}}$, $\sum_{\text{Improved}}$] is calculated, whereby the total number of instances is summed for the negative, nominal, and positive effects, respectively. For example, in case of HFE_1, the triplet is estimated as [4, 3, 2], meaning four negative, three nominal, and two positive effects. The negative and positive effects are used to determine the control mode in Figure 2, whereby the negative (i.e., reduced reliability) number of CPCs is treated as the horizontal axis and the positive (i.e., improved reliability) number of CPCs is treated as the vertical axis. This process classifies the HFE into one of four control modes—scrambled, opportunistic, tactical, or strategic. Table 10 provides the reliability interval for the HEP for each control mode.

The reliability interval for the three HFEs is summarized in Table 11. In all cases, the Basic CREAM analysis produced an opportunistic control mode with in HEP reliability interval of 1.0E-2 < p < 0.5E-0.

Figure 2 – Relationship Between Improved and Reduced Performance and Control Modes in CREAM (adapted from [10])

	7	Strategic	Strategic	Strategic							
	6	Strategic	Strategic	Strategic	Tactical						
	5	Strategic	Strategic	Tactical	Tactical	Tactical					
	4	Strategic	Tactical	Tactical	Tactical	Tactical	Tactical				
Improve	3	Tactical	Tactical	Tactical	Tactical	Tactical	Opportunistic	Opportunistic			
	2	Tactical	Tactical	Tactical	Tactical	Opportunistic	Opportunistic	Opportunistic	Opportunistic		
	1	Tactical	Tactical	Tactical	Opportunistic	Opportunistic	Opportunistic	Opportunistic	Opportunistic	Opportunistic	
	0	Tactical	Tactical	Tactical	Opportunistic	Opportunistic	Opportunistic	Scrambled	Scrambled	Scrambled	Scrambled
		0	1	2	3	4	5	6	7	8	9

Reduce

Table 8 - Control Modes and Probability Intervals (adapted from [10])

Control mode	Reliability Interval
Strategic	0.5e-5 < p < 1.0e-2
Tactical	1.0e-3 < p < 1.0e-1
Opportunistic	1.0e-2 < p < 0.5e-0
Scrambled	1.0e-1 < p < 1.0e-0

Table 9 - HEPs Produced by the CREAM Basic Method

HFE	Triplet [∑Reduced, ∑Not significant, ∑Improved]	Control mode	Reliability Interval
HFE_1	[4, 3, 2]	Opportunistic	1.0e-2 < p < 0.5e-0
HFE_2	[4, 3, 2]	Opportunistic	1.0e-2 < p < 0.5e-0
HFE_3	[6, 1, 2]	Opportunistic	1.0e-2 < p < 0.5e-0

2.6.3 CREAM Extended Method

The Basic CREAM method produces a range of HEPs suitable for screening. In contrast, the Extended CREAM method produces a more specific HEP akin to other HRA methods. There are three steps of the Extended CREAM method:

1. *Build or develop a profile of the cognitive demands of the task.* This step entails classifying each step in the HFE according to its cognitive demands. Cognitive demands encompass observation, interpretation, planning, and execution. These are similar to the Diagnosis vs. Action distinction in SPAR-H, but at a finer level of granularity.

2. *Identify the likely cognitive function failures.* Cognitive demands lead to failures, and CREAM provides a table of possible failure types for each demand.

3. *Determine the specific action failure probability.* In this step, CREAM's equivalent of an HEP is calculated.

For Step 1, Table 12 indicates task steps or activities on each HFE, their basic cognitive activities, and cognitive demands. The cognitive activity consists of fifteen cognitive activity types—coordinate, communicate, compare, diagnose, evaluate, execute, identify, maintain, monitor, observe, plan, record, regulate, scan, and verify. These cognitive activities are matched to each of the four cognitive demands. Multiple demands may be present.

Table 10 - Task Steps or Activities of each HFE and Corresponding Cognitive Demands

HFE	**Task Step or Activity**	**Cognitive Activity**	**Cognitive Demand**			
			Observation	**Interpretation**	**Planning**	**Execution**
HFE_1: Detect Well Kick	Ensure return mud flow is rising	Monitor	✓	✓		
	Ensure BSR does not need be closed and sealed	Observe	✓			
	Ensure annulus are not sealed	Observe	✓			
	Ensure formation fluid does not rise	Monitor	✓	✓		
HFE_2: Respond to Well Kick	Remotely operated vehicle (ROV) intervention	Execute				✓
	Lower marine riser package disconnect	Execute				✓
HFE_3: Well Disconnect	Ensure BOP is unavailable	Observe	✓			
	Decision making for well disconnect	Diagnose		✓	✓	
	Push two buttons for well disconnect	Execute				✓

In Step 2, the analyst identifies the most likely cognitive function failures. The generic CREAM failure types are found in Table 13, while the specific ones identified for the HFEs are found in Table 14.

Table 11 - Generic Cognitive Function Failures (adapted from [10])

Cognitive Function	Potential Cognitive Function Failure	
Observation	O1	Observation of wrong object. A response is given to the wrong stimulus or event.
	O2	Wrong identification made, due to e.g. a mistaken cue or partial identification.
	O3	Observation not made (i.e., omission), overlooking a signal or a measurement.
Interpretation	I1	Faulty diagnosis, either a wrong diagnosis or an incomplete diagnosis.
	I2	Decision error, either not making a decision or making a wrong or incomplete decision.
	I3	Delayed interpretation, i.e., not made in time.
Planning	P1	Priority error, as in selecting the wrong goal (intention)
	P2	Inadequate plan formulated, when the plan is either incomplete or directly wrong.
Execution	E1	Execution of wrong type performed, with regard to force, distance, speed or direction.
	E2	Action performed at wrong time, either too early or too late
	E3	Action on wrong object
	E4	Action performed out of sequence, such as repetitions, jumps, and reversals
	E5	Action missed, not performed (i.e., omission), including the omission of the last actions in a series ("undershoot")

Table 12 - Potential Cognitive Function Failure Modes for the Task Steps for Each HFE

HFE	Task Step or Activity	Potential Cognitive Function Failure Mode	
HFE_1: Detect Well Kick	Ensure return mud flow is rising	O2	Wrong identification made
	Ensure BSR does not need be closed and sealed	O2	Wrong identification made
	Ensure annulus are not sealed	O2	Wrong identification made
	Ensure formation fluid does not rise	O2	Wrong identification made
HFE_2: Respond to Well Kick	ROV intervention	E3	Action on wrong object
	Lower marine riser package disconnect	E3	Action on wrong object
HFE_3: Well Disconnect	Ensure BOP is unavailable	O2	Wrong identification made
	Decision making for well disconnect	I3	Delayed interpretation
	Push two buttons for well disconnect	E3	Action on wrong object

In Step 3, the HEP is calculated. In CREAM terminology, this is called the cognitive failure probability (CFP). A nominal HEP lookup table is provided by CREAM for each function failure mode, as depicted in Table 15. Table 16 provides the nominal HEPs specific to the three HFEs. Table 17 provides the weighting factors for the CPCs. Each task's nominal HEP (i.e., CFP in

CREAM terminology) is multiplied by the sum of the CPC weighting factors, and the largest overall task HEP is retained as the HEP for that HFE. Table 18 shows the CPC weightings for each HFE, and Table 19 summarizes the final result.

Table 15 - Nominal CFP Values and Uncertainty Bounds for Cognitive Function Failures (adapted from [I-10])

Cognitive function	**Generic failure type**	**Lower bound (.05)**	**Basic CFP value**	**Upper bound (.95)**
Observation	O1	3.0E-4	1.0E-3	3.0E-3
	O2	1.0E-3*	3.0E-3*	9.0E-3*
	O3	1.0E-3*	3.0E-3*	9.0E-3*
Interpretation	I1	9.0E-2	2.0E-1	6.0E-1
	I2	1.0E-3	1.0E-2	1.0E-1
	I3	1.0E-3	1.0E-2	1.0E-1
Planning	P1	1.0E-3	1.0E-2	1.0E-1
	P2	1.0E-3	1.0E-2	1.0E-1
Execution	E1	1.0E-3	3.0E-3	9.0E-3
	E2	1.0E-3	3.0E-3	9.0E-3
	E3	5.0E-5	5.0E-4	5.0E-3
	E4	1.0E-3	3.0E-3	9.0E-3
	E5	2.5E-2	3.0E-2	4.0E-2

*Corrected from erroneous values in the original CREAM documentation [10]

Table 16 - Summary of Basic CFP Value of Each Potential Cognitive Function Failure

HFE	**Task Step or Activity**	**Potential Cognitive Function Failure Mode**	**Basic CFP Value**
HFE_1: Diagnosis of Well Kick	Ensure return mud flow is rising	O2	3.0E-3
	Ensure BSR does not need be closed and sealed	O2	3.0E-3
	Ensure annulus are not sealed	O2	3.0E-3
	Ensure formation fluid does not rise	O2	3.0E-3
HFE_2: Recovery Activities after Well Kick	ROV intervention	E3	5.0E-4
	Lower marine riser package disconnect	E3	5.0E-4
HFE_3: Well Disconnect	Ensure BOP is unavailable	O2	3.0E-3
	Decision making for well disconnect	I3	1.0E-2
	Push two buttons for well disconnect	E3	5.0E-4

Table 17 - Weighting Factors for CPCs (from [I-10])

CPC name	Level / descriptors	Cognitive Function			
		Observation	Interpretation	Planning	Execution
Adequacy of organization	Very efficient	1.0	1.0	0.8	0.8
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.2	1.2
	Deficient	1.0	1.0	2.0	2.0
Working condition	Advantageous	0.8	0.8	1.0	0.8
	Compatible	1.0	1.0	1.0	1.0
	Incompatible	2.0	2.0	1.0	2.0
Adequacy of MMI and operational support	Supportive	0.5	1.0	1.0	0.5
	Adequate	1.0	1.0	1.0	1.0
	Tolerable	1.0	1.0	1.0	1.0
	Inappropriate	5.0	1.0	1.0	5.0
Availability of procedures / plans	Appropriate	0.8	1.0	0.5	0.8
	Acceptable	1.0	1.0	1.0	1.0
	Inappropriate	2.0	1.0	5.0	2.0
Number of simultaneous goals	Fewer than capacity	1.0	1.0	1.0	1.0
	Matching current capacity	1.0	1.0	1.0	1.0
	More than capacity	2.0	2.0	5.0	2.0
Available time	Adequate	0.5	0.5	0.5	0.5
	Temporarily inadequate	1.0	1.0	1.0	1.0
	Continuously inadequate	5.0	5.0	5.0	5.0
Time of day	Day-time (adjusted)	1.0	1.0	1.0	1.0
	Night-time (unadjusted)	1.2	1.2	1.2	1.2
Adequacy of training and experience	Adequate, high experience	0.8	0.5	0.5	0.8
	Adequate, limited experience	1.0	1.0	1.0	1.0
	Inadequate	2.0	5.0	5.0	2.0
Crew collaboration quality	Very efficient	0.5	0.5	0.5	0.5
	Efficient	1.0	1.0	1.0	1.0
	Inefficient	1.0	1.0	1.0	1.0
	Deficient	2.0	2.0	2.0	5.0

Table 18 - Summary of the CPC Weightings for Task Steps Included in Each HFE

HFE	CPC name	Level / Descriptors	Task Step # 1	Task Step # 2	Task Step # 3	Task Step # 4
HFE$_1$	Adequacy of organization	Inefficient	1	1	1	1
	Working condition	Compatible	1	1	1	1
	Adequacy of MMI and operational support	Supportive	0.5	0.5	0.5	0.5
	Availability of procedures / plans	Inappropriate	2	2	2	2
	Number of simultaneous goals	Fewer than capacity	1	1	1	1
	Available time	Adequate	0.5	0.5	0.5	0.5
	Time of day	Night time	1.2	1.2	1.2	1.2
	Adequacy of training and experience	Adequate, limited experience	1	1	1	1
	Crew collaboration quality	Inefficient	1	1	1	1
	Total influence of CPCs		9.2	9.2	9.2	9.2
HFE$_2$	Adequacy of organization	Inefficient	1.2	1.2		
	Working condition	Compatible	1	1		
	Adequacy of MMI and operational support	Supportive	0.5	0.5		
	Availability of procedures / plans	Inappropriate	2	2		
	Number of simultaneous goals	Fewer than capacity	1	1		
	Available time	Adequate	0.5	0.5		
	Time of day	Night time	1.2	1.2		
	Adequacy of training and experience	Adequate, limited experience	1	1		
	Crew collaboration quality	Inefficient	1	1		
	Total influence of CPCs		9.4	9.4		
HFE$_3$	Adequacy of organization	Inefficient	1	1	1.2	
	Working condition	Incompatible	2	2	2	
	Adequacy of MMI and operational support	Supportive	0.5	1	0.5	
	Availability of procedures / plans	Inappropriate	2	1	2	
	Number of simultaneous goals	Fewer than capacity	1	1	1	
	Available time	Adequate	0.5	0.5	0.5	
	Time of day	Night time	1.2	1.2	1.2	
	Adequacy of training and experience	Adequate, limited experience	1	1	1	
	Crew collaboration quality	Inefficient	1	1	1	
	Total influence of CPCs		10.2	9.7	10.4	

Table 19 - The Adjusted CFP for Each Task Step and the Final CFPs for HFEs

HFE	Task step or activity	Basic CFP Value	Total Influence of CPCs	Adjusted CFP	Final CFP (i.e., HEP)
HFE_1	Ensure return mud flow is getting high.	3.0E-3	9.2	2.76E-2	2.76E-2
	Ensure BSR does not be closed and sealed.	3.0E-3	9.2	2.76E-2	
	Ensure annulus does not sealed.	3.0E-3	9.2	2.76E-2	
	Ensure formation fluid does not rise.	3.0E-3	9.2	2.76E-2	
HFE_2	Remotely operated vehicle (ROV) intervention	5.0E-4	9.4	4.70E-3	4.70E-3
	Lower marine riser package disconnect	5.0E-4	9.4	4.70E-3	
HFE_3	Ensure BOP is unavailable.	3.0E-3	10.2	3.06E-2	9.70E-2
	Decision making for well disconnect.	1.0E-2	9.7	9.70E-2	
	Push two buttons for well disconnect	5.0E-4	10.4	5.20E-3	

3 Method Comparison and Summary

Here, we offer brief insights on the methods, based on the example analysis for the three HFEs. The final HEPs for the three HFEs across the three HRA methods are found in Table 20. As can be seen, Petro-HRA exhibits an overall very conservative tendency across the HFEs. SPAR-H and CREAM exhibit slightly less conservatism but do not offer good inter-method agreement. Generally SPAR-H proved more conservative than Extended CREAM, but the SPAR-H HEPs were comparable to the screening values produced by Basic CREAM. SPAR-H and Petro-HRA proved easier to estimate than CREAM, with fewer steps toward quantification, but CREAM provided greater consideration of factors to consider in the analysis, potentially offering a more nuanced account of the event.

Table 20 - Final HEPs Produced by the HRA Methods for the Three HFEs

HRA Method	HFE_1: Detect	HFE_2: Recovery	HFE_3: Disconnect
SPAR-H	1.10E-1	4.22E-1	6.14E-1
Petro-HRA	1.0	1.0	1.0
CREAM	2.76E-2	4.70E-3	9.70E-2

This article stops short of providing recommendations to use specific HRA methods. The example retrospective analysis is a single snapshot of the methods, and a large-scale benchmark of HRA methods for oil and gas applications has not yet been performed. As part of a benchmark, no comparison has been performed to demonstrate consistency of analysts using these methods for offshore applications, meaning the inter-analyst variability is not well understood. Moreover, the HEPs have not been validated, and it is not possible to say that a particular method has more accurately quantified the event. Still, some recommendations can be extracted from the sample application of the methods:

- For quick analysis, SPAR-H and Basic CREAM provide a succinct and seemingly conservative approach to quantify the HEP.
- There is still limited application of Petro-HRA for retrospective analyses of events that have occurred, and more experience and guidance are warranted.
- Petro-HRA provides the most complete guidance on formulating the HFE compared to SPAR-H and CREAM. If no HFE has been defined in the underlying PRA, the Petro-HRA guidance should be consulted.
- All three HRA methods considered here use some form of PSFs to quantify nominal HEPs. While these PSFs may be slightly different in wording, it is easy to crosswalk the PSFs to account for the main performance drivers in comparable ways.
- Petro-HRA has only a single nominal HEP, SPAR-H has two, and CREAM has multiple. Where consideration of nominal conditions is important, a more nuanced version of the nominal HEPs may be helpful to the analyst such as is found in CREAM.
- The terminology in SPAR-H is the most nuclear specific of the three methods and may require some degree of interpretation and extrapolation to match to petroleum contexts.
- Petro-HRA is well aligned with petroleum tasks, but it proved very conservative, producing HEPs equal to 1.0 for all three HFEs.
- CREAM proves a flexible method that works well in the oil and gas domain.

Thus, the use of particular HRA methods represents tradeoffs. Analysts should be aware of these tradeoffs and ensure that HRAs performed with these methods are credible in their outputs. Likely, no HRA method serves all oil and gas applications equally. Thus, the selection of the particular HRA method must be based on analyst insights into the best method for that analysis. Additionally, there clearly remains research to be done on the use of HRA methods for retrospective analysis in the oil and gas industry. The findings of this comparison point to the need to validate and refine HRA methods for petroleum purposes. Still, there is considerable value in the methods, and they can be readily used to support retrospective analysis with varying degrees of conservatism.

4 Disclaimer

 Idaho National Laboratory is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517.

5 References

1 Bell, B.J., Holroyd, J., Review of human reliability assessment methods, RR679, Health and Safety Executive, Buxton, UK, 2009.

2 Boring, R.L., Adapting human reliability analysis from nuclear power to oil and gas applications, in Podifilini et al. (Eds.), Safety and reliability of complex engineered systems, pp. 2853-2860, Taylor & Francis, 2015.

3 Swain, A.D., Guttmann, H.E., Handbook of human reliability analysis with emphasis on nuclear power plant applications, final report, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

4 Electric Power Research Institute, An approach to the analysis of operator actions in probabilistic risk assessment, TR-100259, Palo Alto, 1992.

5 Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., The SPAR-H human reliability analysis method, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Washington, DC, 2005.

6 U.S. Nuclear Regulatory Commission, Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA), NUREG-1624, Rev. 1, Washington, DC, 2000.

7 Boring, R.L., Gertman, D.I., Atomistic and holistic approaches to human reliability analysis in the U.S. power industry, Safety and Reliability Journal, Vol. 25, No. 2, (2005), pp. 21–37.

8 Forester, J., Kolaczkowski, A., Lois, E., Kelly, D., Evaluation of human reliability analysis methods against good practices, NUREG-1842, U.S. Nuclear Regulatory Commission, Washington, DC, 2006.

9 Chandler, F.T., Chang, Y.H.J., Mosleh, A., Marble, J.L., Boring, R.L., Gertman, D.I., Human reliability analysis methods: Selection guidance for NASA, NASA Office of Safety and Mission Assurance Technical Report, Washington, DC, 2006.

10 Hollnagel, E., Cognitive reliability and error analysis method – CREAM, 1st ed., Elsevier Science, 1998.

11 Kirwan, B., Gibson, H., Kennedy, R., Edmunds, J., Cooksley, G., Umbers, I., Nuclear action reliability Aasessment (NARA): A data-based HRA tool, Safety & Reliability Journal, Vol. 25, No. 2 (2005), pp. 38-45.

12 Aven, T., Sklet, S., Vinnem, J.E., Barrier and operational risk analysis of hydrocarbon releases (BORA-Release), Part I, Method description, Journal of Hazardous Materials, Vol. A137, (2006) pp. 681–691.

13 Bye, A., Laumann, K., Taylor, C., Rasmussen, M., Øie, S., van de Merwe, K., Øien, K., Boring, R., Paltrinieri, N., Wæro, I., Massaiu, S., Gould, K, *The petro-HRA guideline,* The Research Council of Norway, Lysaker, Norway, 2017.

14 Institute for Electrical and Electronics Engineers, Guide for incorporating human reliability analysis into probabilistic risk assessments for nuclear power generating stations and other nuclear facilities, IEEE-Std-1082, New York City, 2017.

15 Gould, K.S., Ringstad, A.J., van de Merwe, K., Human reliability analysis in major accident risk analyses in the Norwegian petroleum industry, Proceedings of the 56th Annual Meeting of the Human Factors and Ergonomics Society, (2012), pp. 2016-2020.

16 Transocean Investigation Report, Macondo well incident, Volume I, June 2011.

17 Boring, R.L., Rasmussen, M., Ulrich, T.A., Blackman, H.S., Retrospective application of human reliability analysis for oil and gas incidents: A case study using the Petro-HRA method, Proceedings of the 61st Annual Meeting of the Human Factors and Ergonomics Society, (2017), pp. 1653-1657.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

How Dynamic Simulation Helped Mitigate Vapor Disposal System

Kartik Maniar* and Omi Soni*
Siemens Energy, Inc.
4615 Southwest Fwy, Suite 900
Houston, TX 77027
*Presenter E-mails: kartik.maniar@siemens.com, omi.soni@siemens.com

Abstract

Siemens recently completed a refinery wide pressure relief and flare analysis for two major refineries in the United States. Major deficiencies were identified on the existing flares if the relief loads calculated using steady state methods were relieved. The calculated relief loads based on the steady state method were overly conservative and resulted in relief devices and vapor disposal systems with inadequate capacities. A systematic approach to reduce the relief loads to the flare was conducted, which included performing dynamic simulation on major contributors to the flare. This systematic approach reduced the conservative assumptions and improved the predictions of the relief loads. Guidance for dynamic simulation was in line with approaches allowed per API-521[1].

The governing case was determined and analyzed for the dynamic analysis. Validation of the results from the dynamic study helped to understand the reason behind the reduction in relief load. The study also predicted potential reduction in relief load that can be achieved prior to running dynamic simulation which is dependent on type of distillation tower (i.e. tower with conventional steam reboiler vs atmospheric towers with feed furnaces) and global release (i.e. boil up vs loss of overhead cooling). Combined credits from dynamic simulation, instrumentation and Quantitative Risk Analysis (QRA) enabled the client to understand the risk, thus helping find the most feasible and economical engineering solution to address the concern. This paper will highlight results, benefits, basis and assumptions of the detailed dynamic simulation study.

Keywords: Mitigation, Vapor Disposal System, Dynamic Simulation, Mitigation, Flare

Introduction

API STD 521 §4.3.3 allows for doing dynamic simulation for calculating relief loads [1]. Conventional methods for calculating relief loads using steady-state approach are conservative and may result in concerns for existing plant relief systems, especially when there are throughput changes being made and plant is operating higher than their original design. Furthermore, API STD 521 §4.2.6 also allows for the favorable responses of conventional instrumentations in the design of relief system components such as flare header, flare knockout drum and flare tip [1].

1 Steady-State Results

After detailed pressure relief analysis and flare analysis, it was determined that Total Power Failure is the governing scenario for the relief system. This resulted in concerns related to excessive relief valve backpressures, radiation and inadequacy of flare disposal system. Table 1 below represents relief loads calculated for governing case for all participating systems to the flare.

Table 1: Steady-State Relief Loads

Steady State Relief Loads, lb/hr											
System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8	System 9	System 10	System 11	Total Relief Load to Flare (lb/hr)
168,763	907,294	1,185,736	427,570	277,852	349,843	138,380	117,532	21,707	50,276	34,469	3,679,422

Mitigating the concerns related to excessive flare radiation was the highest priority. Therefore, we needed to account for all the potential credits and engineering methodology that could help to minimize overall relief load to the flare, before any additional mitigation or solution is recommended to reduce the radiation levels within acceptable limits.

2 Dynamic Simulation Modeling

Based on the above results, six of eleven contributing systems (e.g. systems 1 through 6) were picked for the detailed dynamic simulation study. These six systems were the major contributors to the flare for governing scenario.

The most significant difference between steady-state and dynamic simulation is that steady-state assumes that variables are constant with respect to the time. This means that in steady-state there is no accumulation in the system, so the overall mass and energy input matches its output. Conversely, dynamic models consider the mass and energy rate of accumulation within the system, which allows one to determine the how long it would take to reach a stable condition starting from a specified initial state. Since there are many variables that goes in to developing the dynamic model, it was very important for the team to ensure that behavior of dynamic model is aligned with the equipment operation in field, while at the same time it is conservative from relief load prediction standpoint. Main focus of this paper is to highlight the reduction obtained in relief loads by performing detailed dynamic simulation. Overall methodology, guidelines and assumptions on developing dynamic simulation should be developed by project team based on standard industry practices.

2.1 Results of Dynamic Simulation

Detailed Dynamic simulation was performed on systems 1 through 6 for the governing case Total Power Failure. Tables below summarizes various results obtained from the dynamic simulation.

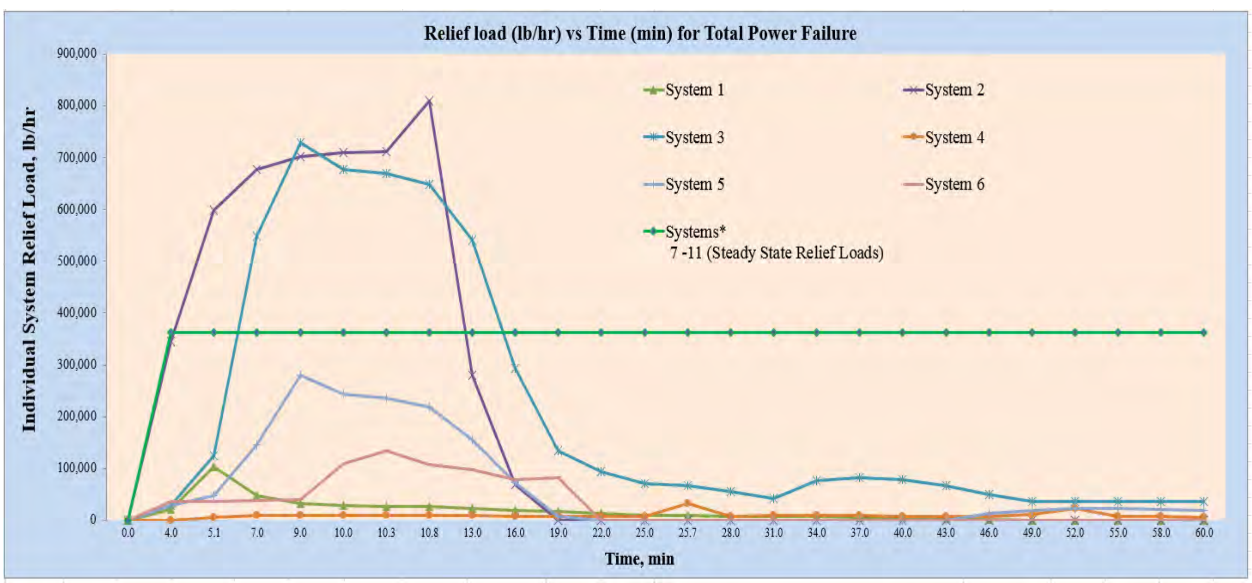
Table 2 below summarizes the individual peak relief loads calculated from the dynamic simulation for systems 1 through 6. Dynamic simulation on systems 7 through 11 was not performed and therefore, relief loads are kept same as calculated using steady-state approach (per Table 1 above). This resulted in reduction of total relief load going to the flare by 33% (in comparison with total load calculated using steady-state approach as mentioned under Table 1 above).

Table 2: Peak Relief Loads from Dynamic Simulation

Peak Relief Loads from Dynmic Simulation, lb/hr											
System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8	System 9	System 10	System 11	Total Relief Load to Flare (lb/hr)
102,857	809,146	729,339	31,912	280,623	133,365	138,380	117,532	21,707	50,276	34,469	2,449,605

Note that each system that is studied for the detailed dynamic simulation is different and unique when it comes to the equipment configuration, dimensions, instrument response time and process/operating conditions. Therefore, when initiating event is triggered in the dynamic model, time to overpressure the system, time to reach peak relief load, magnitude of peak relief load and time at which relief ends was observed to be different for different systems. Peak relief from each individual system does not occur simultaneously; as a result of this, total relief load going to the flare system is not sustained but varies over the period depending on starting and ending duration of release for each individual system releasing to the flare. Please refer to Plot 1 below, which summarizes the relief load vs time data obtained from the dynamic simulation for systems 1 through 6, and sum of total relief load for systems 7 through 11 is represented via straight line.

Plot 1: Relief load vs Time Data Calculated from Dynamic Simulation



As seen in the plot above, duration and magnitude of peak relief is different for all six systems studied and peak relief from each individual system do not occur simultaneously. Therefore, credit for the staggering of the relief load can be taken to further reduce total relief load going to the flare. Table 3 below summarizes the relief load calculated from the dynamic simulation for systems

1 through 6 at the instance when peak flare load occurs accounting credit for the relief load staggering. This resulted in further reduction of total relief load going to the flare by 11% (in comparison with total load mentioned under Table 2 above).

Table 3: Relief Load from Dynamic Simulation When Peak Flare Load Occurs

Relief Loads from Dynmic Simulation When Peak Flare Load Occurs, lb/hr											
System 1	**System 2**	**System 3**	**System 4**	**System 5**	**System 6**	**System 7**	**System 8**	**System 9**	**System 10**	**System 11**	**Total Relief Load to Flare (lb/hr)**
26,269	809,146	648,923	9,230	218,805	107,658	138,380	117,532	21,707	50,276	34,469	2,182,394

As mentioned earlier, dynamic simulation on systems 7 through 11 was not performed and therefore, relief loads are kept same as calculated using steady-state approach (per table 1 above).

2.2 Credit for the Existing Instrumentations and Safeguards

As noted earlier, API STD 521 §4.2.6 allows taking credit for the favorable responses of conventional instrumentations and safeguards in the design of relief system components. Based on this, credit for the existing instruments and safeguards (i.e. triconex trips, APS on spare pump etc.) was applied to further reduce relief load going to the flare. Table 4 below summarizes relief loads from each individual system after taking credit for the existing safeguards.

Table 4: Relief Load with Credit for Existing Safeguards

Relief Load After Taking Credit for All But Two Existing Safeguards, lb/hr											
System 1	**System 2**	**System 3**	**System 4**	**System 5**	**System 6**	**System 7**	**System 8**	**System 9**	**System 10**	**System 11**	**Total Relief Load to Flare (lb/hr)**
102,857	809,146	729,339	31,912	12,048	133,365	34,608	117,523	5,446	16,094	34,458	2,026,795

Note that each safeguard is assigned a probability of failure on demand (PFOD) which indicates the safeguard's reliability. As a result of this, failure of certain number of safeguards needs to be accounted, which depends on the safeguard's reliability, its PFOD, and client-specific guidelines. In current study, credit for a total of six safeguards (on systems 2,3,5,7,9 and 10, one per system) was considered between total of eleven participating systems, and based on the client-specific guidelines, two of six safeguards which provide the largest reduction in relief load needed to be failed. Note that failure of safeguard was based on the probability theory for the safeguards that are 98 percent reliable on demand, with no more than a 1 in 1000 chance that more than two safeguards will fail out of the total six safeguards as per the client-specific guidelines. As shown in Table 4 above, credit for safeguards for systems 2 and 3 (highlighted in red) was removed, as they provided largest reduction in the relief load. Therefore, relief loads for these two systems were updated to be same as calculated from the detailed dynamic simulation study, such that no credit is taken for safeguards. Credit for the remaining four safeguards was considered to continue (on systems 5,7,9, and 10). This resulted in further reduction of total relief load going to the flare by 8% (in comparison with total load mentioned under Table 3 above).

As part of the sensitivity study, total relief load to the flare was calculated accounting credit for all six existing safeguards. As result of this, relief loads accounting credit for the safeguards on system 2 and system 3 was calculated and documented under Table 5 below.

Table 5: Relief Load with Credit for All Existing Safeguards

Relief Load After Taking Credit for All Existing Safeguards, lb/hr											
System 1	**System 2**	**System 3**	**System 4**	**System 5**	**System 6**	**System 7**	**System 8**	**System 9**	**System 10**	**System 11**	**Total Relief Load to Flare (lb/hr)**
102,857	**202,256**	**7,218**	**31,912**	**12,048**	**133,365**	**34,608**	**117,541**	**5,436**	**16,103**	**34,471**	**697,815**

It can be observed that when all six existing safeguards functions as intended, total relief load going to the flare has reduced significantly.

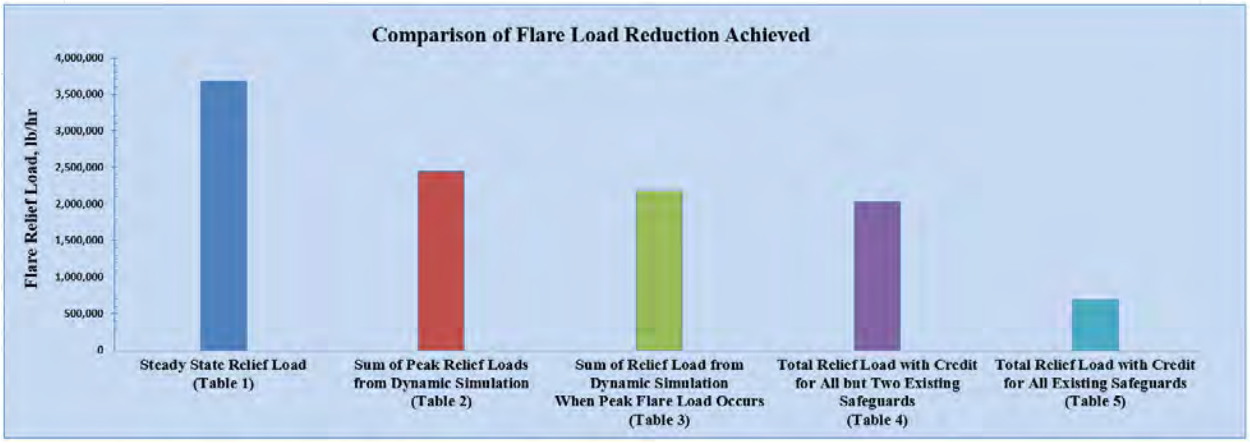
3 Recommendation and Conclusions

Results of the sensitivity study (as mentioned under previous section), which accounts for the credit of all existing safeguards can be utilized during the mitigation stage, to determine if reliability on existing safeguards is increased to the level such that either less number of safeguard failure or no safeguard failure can be achieved (i.e. SIL-3 reliability), to further reduce relief load going to the flare and mitigate various concerns related to excessive back pressure and radiation. If safeguards are less or greater than 98 percent reliable or greater or lower number of safeguard credits are present, the total number of safeguard failures are different based on the client specific guidelines. An option of recommending new safeguard/s of specific reliability can also be considered and reduction in the total flare load can be determined. This data then can be taken to the next step, which is performing a Quantitative Risk Assessment (QRA). QRA may help determine if the results comply with local regulations, API STD 521, and the owner's risk tolerance criteria, whichever is more restrictive [1]. Note that the risk acceptance criteria are the sole responsibility of the owner. Please refer below paper as reference, which details Flare QRA [2].

Based on the reduction in the flare load calculated using various approaches as mentioned above, it can be concluded that steady-state relief loads are often conservative. While these are utilized for relief valve sizing purposes, they should not be taken as the basis to check the adequacy of the vapor disposal system.

Bar chart below summarizes the reduction in the total flare load which was achieved using systematic approach of detailed dynamic simulation study with credit for the existing instruments and safeguards.

Plot 2: Comparison of Flare Load Reduction Achieved



As a result of above-mentioned systematic approach, overall reduction in the flare relief load was calculated to be 45% (in comparison with total load mentioned under Tables 1 and 4 above). As mitigating the concerns related to excessive flare radiation was the goal of the study, radiation was re-run for the reduced flare load calculated per Table 4 above and as a result of this, significant reduction in flare radiation was also achieved.

Acronyms A-Z	
API	American Petroleum Institute
QRA	Quantitative Risk Assessment
PFOD	Probability of failure on Demand
APS	Automatic Pump Start-up

References:

1. *Pressure-relieving and Depressuring Systems, API Standard 521 6th edition.*
2. *Ben Pratt and Nancy Faulk, "What is My Flare Capacity, Really? Best Practices for Flare QRA Tools," 15th Global Congress on Process Safety (April 2019), New Orleans, LA*

Disclaimer:
The information contained in this document represents the current view of the authors at the time of publication. Process safety management is complex and this document cannot embody all possible scenarios or solutions related to compliance. This document is for informational purposes only. Siemens makes no warranties, express or implied, in this paper.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Fire and Gas Hazard Mapping Continues to Require Engineering Judgment

James McNay BSc MIFireE CFSP MIET[2] and William Pittman, PhD*[1]
[1]Fire and Gas Detection Consultant, Micropack (Detection) Americas
[2]Managing Director, Micropack (Engineering) Ltd
*Presenter E-mails: williampittman@micropackamericas.com

Abstract

It is becoming increasingly common to use computer applications and software tools to aid engineers in designing fire and gas detector layouts. These tools help designers optimize layouts as well as verify, quantify and document the level of performance the system can be expected to achieve. The process of designing and assessing layouts in this way is called hazard mapping.

In an age where "optimization" is increasingly becoming associated with computerized approaches that seek to minimize or maximize objective functions, many in the industry see these software tools and assume or wonder if the layout is generated automatically by the mapping software. Upon learning that a human engineer must still design the detector layout and place the detectors in the facility model, many ask why it hasn't been automated and how the system can be considered optimized if it isn't designed with the assistance of an algorithm.

Fire and gas detector layout design requires the use of a great deal of engineering judgement which cannot currently be replicated or replaced by optimization algorithms. There are many practical concerns that must be addressed in the design of such systems that are difficult to model and automate. There are many rules of thumb, soft restrictions and best practices that are sometimes bent or broken to address the specific need of an application or facility. This paper reviews many of these issues in an attempt to make the case that the expert judgment of a human engineer is and will continue to be essential to the design of truly optimized fire and gas detection systems.

Introduction

Ever since fire and gas detectors were first brought to market the industry has faced the challenge of designing detector layouts and assessing, either qualitatively or quantitatively, the coverage achieved by the system. Two important and inter-related questions must always be addressed:

1. How much coverage is need? Alternatively: What level of coverage is adequate or acceptable?
2. Does the detector layout currently in use or planned for installation deliver that level of coverage?

Fire and gas hazard mapping studies, so-called "coverage assessments," attempt to help engineers and operators answer the second question, but the answers generally are not straight-forward and do not lend themselves to "cookie-cutter" approaches.

The goal of a design engineer is, as always, to design an "optimized" system, with "optimized" in this case usually meaning that the system provides an acceptable level of coverage - as defined by whoever or whatever answered the first question - with the lowest possible number of detectors. In principle, this should deliver the system that fulfills the requirements of the facility or operator at the lowest possible cost.

The problem with "optimized" these days is that, when most people hear it, they tend to assume that the entire design process is being handled by a computer with an objective function, an algorithm or some weighted set of criteria that it's trying to minimize or maximize. When discussing fire and gas hazard mapping, it is not uncommon for some to ask, "are the detector locations being chosen by a human designer or by a computerized optimization approach." The answer to this is, the detectors are placed by a human design engineer.

The question that inevitability follows is usually some form of "why not have the computer do it?" or "then how can you be sure that the system is optimized?"

For flame detection coverage assessments, the approach is generally to calculate the percentage of the volume with different levels of coverage. The designer specifies the volume(s) or space(s) where-in flame detection is expected or required. Software tools are then used to model the coverage provided by a detector layout and determine if one or more detectors have a clear line of sight to that volume, if the volume is within a detector's field of view, and if the detector is close enough to detect a fire of the specified size. This information is used to calculate what percentage of the volume of interest has coverage and at what level - usually 1ooN or 2ooN.

At first glance it might seem to most that this problem would lend itself to computerized optimization programs. All the system must do is to either take a fixed number of detectors and arrange them in a way that maximizes coverage. Alternatively, the system can start from nothing and add detectors at the location that incrementally improves the coverage the most until the coverage target is met or exceeded. That sounds easy. Right? Not exactly.

Is a target percentage coverage, in and of itself, excluding other considerations, an appropriate test of effectiveness or acceptability? No.

The design for flame detector layouts requires an appreciation of many practical concerns that are not necessarily easy to factor into computer-based optimization systems. This paper reviews and discusses some of these issues, sometimes illustrating the point using example 3D coverage assessments and results. Because of these issues, the authors regard it as unlikely in the near term that any computerized system or algorithm will be able to provide an effective and reliable substitute for an experienced engineer using sound judgement to design a fire and gas detector layout. Some of these issues will impact the design of both flame and gas detector layouts, some are more limited to flame detection.

What Optimization Criteria are Used and How are They to be Ranked?

For flame detection coverage assessments, most guidance documents currently in use assign a rank or "grade" to equipment based on the perceived fire risk associated with it - usually into "low", “medium,” “high” and / or “special” categories. The standards put forward target coverage levels and performance targets for each risk rank or grade. The Performance Targets will usually include a target fire size that the detector layout should be able to detect in a timely manner (usually 10s or less) for each risk grade - smaller target fire sizes are selected for higher risk equipment with 50 KW RHO being typical for high risk equipment, 250 KW RHO being typical for medium risk equipment, and 500-1000 kW RHO being typical for low risk equipment.

Many operators will design a FGS to generate an alarm in response to “unconfirmed,” 1ooN, detection and take an automated control action in response to “confirmed,” 2ooN, detection.

The combination of voting schemes and risk ranking means, in an area where-in equipment with all three risk grades are present, a designer will not have a single coverage value consider. Rather, there could be eight values to consider - 1ooN and 2ooN coverage for high, medium, and low risk equipment, and the module overall. This forces a designer to ask, which value should we optimize based on? If we rank and prioritize the different values in a fixed hierarchy, how do we arrange them? Is 1ooN coverage more important or 2ooN? If two detector locations are being considered and one improves 1ooN coverage more but the other increases 2ooN coverage more, which do you select?

To illustrate how this can happen, consider the situation shown in Figure 1 below where there are 3 vessels in an area with a medium risk grade assigned: Figure 1 and all subsequent figures in the paper have been generated using HazMap3D, a hazard mapping and coverage assessment application developed and used by Micropack.

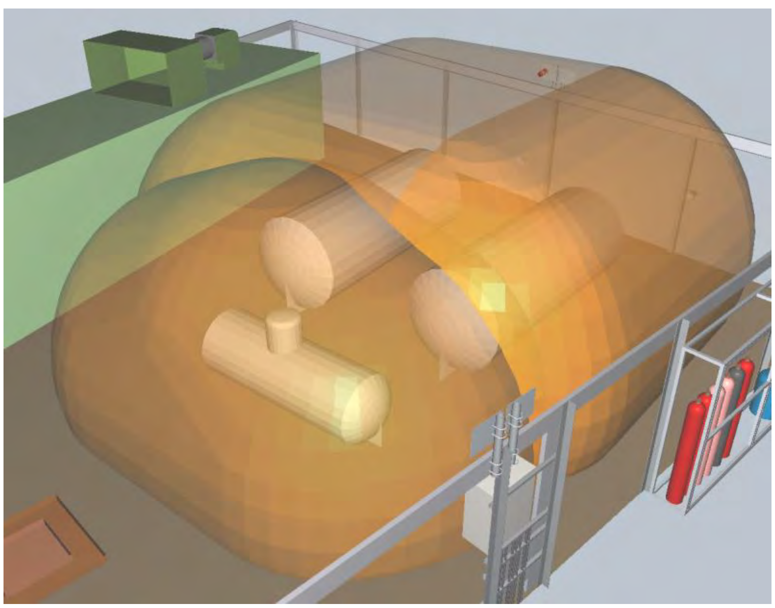


Figure 1: Three vessels assigned a “medium risk” grade.

To provide coverage in this case, the design engineer might choose to recommend a detector layout using 3 detectors. An assessment of such a 3-detector layout, assessed in a manner consistent with TR 84.00.07, indicated that the layout would give 81% 2ooN coverage, giving the 80% control action coverage recommended in ISA TR 84.00.07 for medium risk assets. Alarm-only 1ooN coverage was assessed at about 98%.

Table 1 provides a summary of the coverage levels achieved for 1ooN, 2ooN and 3ooN voting. Table 2 also shows, in the "individual" column, what percentage of the graded volume each detector can see, and, in each row, what coverage is reduced to for 1ooN, 2ooN and 3ooN voting if the detector named on that row fails.

Table 1: Summary of voted coverage and detector coverage contributions for the three vessels using a three-detector layout.

	Individual	1ooN	2ooN	>2ooN
All Detectors		98.2	81.1	50.1
Det01	81.1	93.0	55.3	0.0
Det02	74.2	92.1	63.0	0.0
Det03	74.1	92.4	62.9	0.0

From this, we can see a few things. Det03 covers the smallest percentage of the graded volume, although it comes in only slightly lower than Det02. Unconfirmed 1ooN coverage increases more when Det02 is added to the layout (rising from 92.1 to 98.2) but confirmed 2ooN detection rises more when Det 03 is added to the other 2 (rising from 62.9 to 81.1%). Det01 sees the largest fraction of the graded volume (81.1%) and is clearly the most important detector for providing 2ooN coverage, but it adds the least amount of the three to 1ooN coverage. So even this simple example, where-in only one risk grade is present, shows that choosing where to add another detector or the next detector to a layout may not be obvious when only looking at % coverages to see which one gives you more coverage.

What is more important? Coverage for equipment and assets that are deemed "High Risk" (HR), "Medium Risk" (MR), or "Low Risk" (LR)? If two detector locations are being considered and one improves HR coverage more but the other increases MR coverage more, which do you select? It might seem easy to say, "choose the one that increases HR coverage more, it's HR!" However, what if one option gives you 0.1% higher HR coverage where the other gives you 2.0% higher MR coverage? Most would likely take 2.0% MR coverage over a paltry 0.1% increase in HR coverage, all else equal. How would one program an algorithm to make a choice between options like that?

This is not to say that different optimization systems cannot be ranked or that a weighting system cannot be developed and programmed into a computer program. However, the complexity of the considerations may make designing and implementing such a system extremely difficult with detector coverage and hazard mapping. A design produced in such a manner also would not represent a true, objective, global optimum. It would simply represent the optimum using that weighting system for the selected criteria. It is not credible to think that such a system would always develop a layout that experienced designers would universally agree is truly optimized.

Concerns regarding prioritizing 1ooN coverage or 2ooN coverage will impact flame detector and gas detector layouts. Designers are far more likely to encounter issues arising from multiple risk grades being present in an assessment area with flame detection than with gas detection. In flame detection the individual pieces of equipment are assigned risk grades where, with gas detection, the entire assessment is usually assigned a single risk grade based on the levels of congestion and / or confinement.

Overall Coverage Levels Say Little about the Nature of The Gaps

A percent coverage alone says nothing about the size, number, or location of the gaps. When the full volume of an area is considered at once (coverage across the entire volume shown simultaneously), percentage coverage results can appear lower than expected while the area appears to have suitable coverage overall. This can result from having a large number of small gaps that collectively add up to a significant fraction of the graded volume. These gaps may be in small blind spots that are located adjacent to areas with good coverage and which are not large enough to hide a fire that is likely to occur in that unit or likely to cause significant damage.

Even where gaps exist that are large enough to conceal a large fire, not all such gaps area equally problematic. A large gap in coverage on the back side of a storage tank, where there are no pumps or pipe connections, is not as concerning as a coverage gap where transfer pumps and pipe connections are located next to the tank. A gap in coverage behind the driver of a pump is not as concerning as a coverage gap on the liquid handling side of the pump. Oftentimes, the dominant fire scenario in such situations is a liquid pool fire and the decks around tanks and pumps is usually slightly sloped. This will cause the liquid pool to flow and expand, often out of the gap in detector coverage, into an area of the deck where detection will occur with minimal delay.

In these cases, it is of critical importance to analyze the areas of low coverage and make a judgement upon the suitability of the detection arrangement, based upon knowledge of the area and equipment, identified fire scenarios, the size of the coverage gaps relative to the size of fires expected in the area, and the location of the gaps. For gas detection coverage assessments, designers may also need to consider issues like whether an area is naturally ventilated or subject to forced ventilation. If forced ventilation is used in an enclosed space and air-flow patterns are more predictable, a designer may be able to excuse or accept some coverage gaps on that basis.

Achieving Target Coverage Levels is Often Very Difficult in Some Environments

As the foregoing example in the previous section shows, achieving high levels of 1ooN or 2ooN coverage with flame detectors is often easy in areas that are very open and where there is not a high degree of congestion. However, on offshore facilities space is at a high premium and even at some onshore facilities congestion is quite high, sometimes because the available land area was small or because equipment was clustered together to lower the amount of piping that had to be installed in the unit.

Where congestion is high and there are many large and small visual obstructions in the process area, providing high levels of flame detector coverage is often quite difficult when conducting assessments with detailed, accurate 3D models. Small and large diameter piping, manifolds, decking and steel supports combine in such spaces to severely limit a detectors ability to achieve a clear line of site over long distances. In such process areas and facilities, it quickly becomes difficult, if not practically impossible, to achieve the 70-90% coverage that is usually specified in company-specific performance targets, even with only 1ooN coverage.

For an example of this, consider the following figure, which shows images of a process area in a 3D model of an offshore platform:

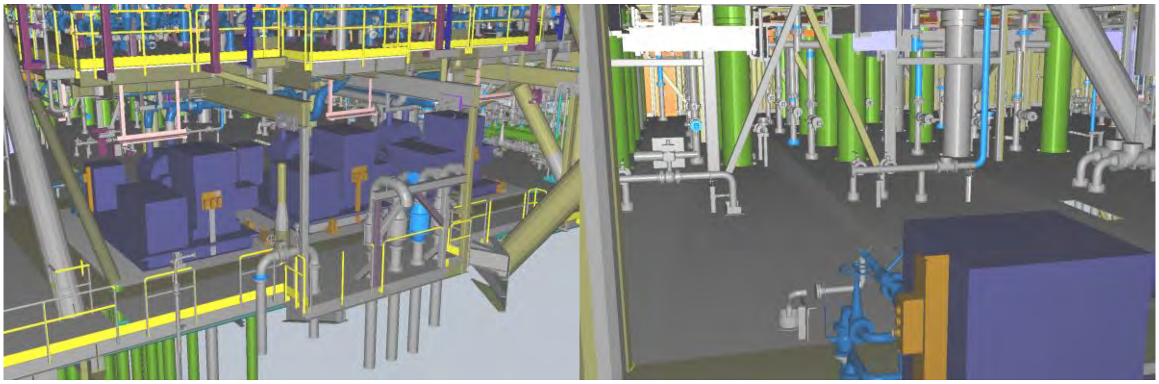


Figure 2: Screen shots of a coverage assessment area in a 3D model of an offshore platform.

Figure 3 is provided to give the reader an idea of the flame detection / fire risk grading that was applied in this area.

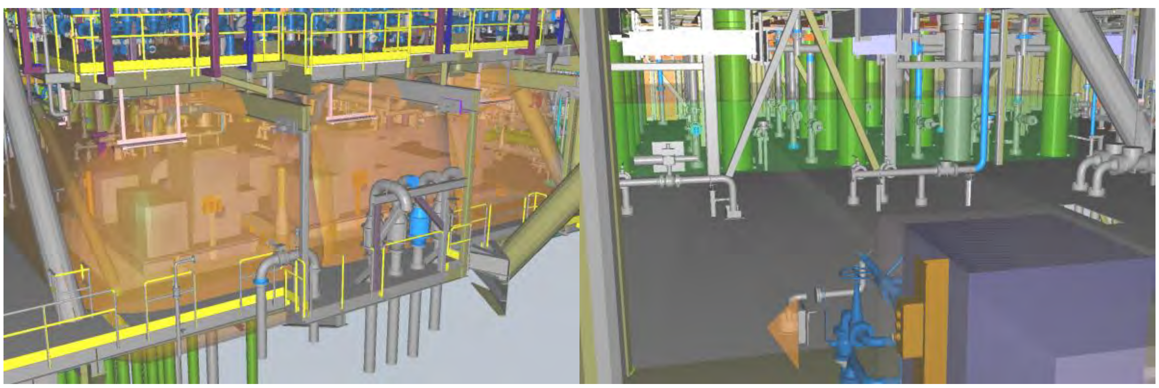


Figure 3: Screen shots showing the grading applied to a section of an offshore platform

The tight confines and high level of congestion is a kind of nightmare scenario for flame detection design. The process area shown in Figures 2 and 3 contains only medium and low risk equipment and measures only 32 meters by 17.5 meters with a deck height of about 3.5 meters. Based on the grading applied and the size of the space alone, one might think that such a space could easily be covered with 3-4 detectors, similar to the situation with the three tanks above. However, because of the very high level of congestion within this area, and because the detectors cannot be set back, away from the equipment being covered as with the prior example, a layout using nine (9) detectors still produces lower coverage than what is achieved in the previous example, and this nine-detector layout achieves coverage that is still far from what many would consider "ideal." Table 2 summarizes the coverage achieved by that nine-detector layout.

Table 2: Summary of voted coverage by risk grade for the nine-detector layout.

	Green	Orange	Brown	Red
MR	62%	22%	2%	15%
LR	48%	31%	0%	21%
Overall	58%	25%	1%	16%

Table 3 gives the contributions of each detector to the overall layout, similar to Table 1 in the previous example:

Table 3: Summary of voted coverage and detector coverage contributions for the nine-detector layout.

	Individual	1ooN	2ooN	>2ooN
All Detectors		82.5	57.7	30.6
Det01	5.2	80.7	56.2	29.3
Det02	1.7	81.8	57.0	30.3
Det03	37.7	78.7	45.0	18.9
Det04	27.3	79.6	51.1	21.2
Det05	23.3	79.8	52.3	23.8
Det06	33.4	79.8	47.7	20.0
Det07	33.1	77.2	48.8	20.9
Det08	11.3	80.1	53.7	27.3
Det09	12.0	79.7	53.3	27.5

It is worth noting that, while in the previous example each flame detector covered 70-80% of the graded volume, in this area, 20-35% is more typical and some detectors cover only 5-12% of the covered volume. That these nine detectors were placed in what the designer felt were the most promising locations. Each incremental detector would therefore be expected to, on average, add less to the assessed coverage than the nine used here.

The nine-detector layout only achieved 2ooN coverage for 58% and 1ooN for 83% of the module overall. How many additional detectors might be required to raise 2ooN coverage for the LR equipment from 48% to the 70-90% that many operators list as a target? How many additional detectors might be required to raise MR 2ooN coverage to 80%? A human designer knows when a point of diminishing returns has been reached and when it is no longer practical, feasible, necessary or wise to keep adding detectors in a space. A computer program would keep adding detectors until the target coverage was achieved unless logic were built in to make it stop adding detectors if adding another detector would increase coverage by less than a pre-specified critical amount - perhaps 1.0% of the graded volume. A human designer would likely look at Table 3, realize that Det01 and Det02 aren't doing much, remove them, and recommend the installation of a seven-detector layout that provides coverage that is as good as is reasonably achievable. Depending on the operator's risk tolerance, Det08 and Det09 might be eliminated as well, leaving only the five detectors which individually cover 23% or more of the graded volume.

For gas detection, a designer might design a system to detect a certain percentage of scenarios assessed as part of a CFD dispersion study within a certain period of time after the release starts. Depending on the number of scenarios assessed and the results of the CFD analysis, the allowed time to detection and the targeted coverage percentage a computer algorithm tasked with designing that system could propose a very large number of detectors.

Coverage targets in the range of 70-90% were developed when operators assessed coverage based on a single 2D slice or plot plan rather than a full, detailed 3D model. Using this approach, accounting for the impact of small diameter piping and similar obstructions was difficult and the high coverage factors were specified to add a layer of conservatism. As assessments using 3D models become more common, this layer of conservatism and reliance on % coverage as a measure of the quality of coverage provided by a system may no longer be necessary or appropriate.

The Challenge of Mounting Location Selection

Detectors should not be mounted an any random location that isn't currently occupied by other equipment. One of the most important things to consider in designing a detector layout - whether or not the mounting location is appropriate - is not necessarily easy to program into a computer program, in part because of the number of considerations that must be made in deciding if a location is "suitable."

Detectors ideally should not be positioned randomly hanging in space in a model. Yes, this is done sometimes on the assumption that a new post or support is or can be placed in that location to allow the detector to be mounted in that location. However, designers tend to prefer to mount detectors on existing structures where the layout is being designed for an existing facility. Where a layout is designed for a green-field unit, operators are still not going to want to build extra supports and run extra wiring solely for the FGS. The goal will always be to use existing or otherwise already planned / required structures as much as possible.

There are other instances where a computer program might, out of "ignorance," if we can call it that, propose mounting a detector in a disallowed or otherwise reserved space. Operators will also not be thrilled if a computer algorithm designs a layout that puts a detector on or next to a railing that it can't be used for because that railing is required for maintenance activities.

Detectors cannot be mounted to an object / surface that vibrates too much. Flame detectors ideally should not be too close to the floor - they will be blocked too easily by workers, temporary equipment and other temporary obstructions. Flame detectors ideally should not be too high above the deck. This makes them much harder to access for testing and maintenance when needed. Because of all of this, most standards indicate that detectors should be situated between two and four meters above the local deck (ALD). The tilt on a flame detector should ideally be within the range of 20-30 degrees. However, these are not hard and fast rules. Flame detectors are sometimes installed only 1.5 meters above the deck. At other times they may be 6-8 meters above the deck when used in spaces with very high ceilings. Many manufacturers and operators allow 10-40 degrees when needed and in some cases 45-50 degree down-angles are used - but only when deemed truly necessary. It's generally wise to position gas detectors so that they are unlikely to be splashed, clogged, or otherwise fouled by liquid sprays or other contaminants.

If 2ooN coverage is desired or required, designers might catch a computer algorithm placing two or more detectors right on top of each other with maybe a one- or two-meter difference in elevation (stacking detectors), or placing detectors very close to each other, with flame detectors facing in the same or similar directions. On the surface, this is an easy way to get 2ooN coverage in a process area, which is why one might see it happen. The problem with this practice is that having two flame detectors so close together with nearly identical fields of view drastically increases the odds of both detectors being blocked by a temporary obstruction and the risk of both flame detectors being triggered by the same false alarm stimulus. If there is an automated suppression system triggered by the flame detection system, this could lead to large numbers of spurious activations. It might be possible to overcome this with a requirement that two detectors cannot be placed within, say, 5 or 10 meters of each other, or that two detectors placed within 5 to 10 meters of each other must have at least a 60° or 90° difference in their "pan" or compass orientation. The problem with this, however, is that there may be special or unique circumstances where-in a designer might feel it best to ignore or loosen this restriction - especially if the assessment area is relatively small.

Many of these rules of thumb need to be flexible, with designers allowed to “break the rules” a little in some cases to deal with the nuances and unique needs of a specific application and facility. How do you make a computer understand all of this?

There have been optimization approaches that allow a user to program in acceptable / allowed mounting locations for detectors.[2] This approach still does not really create an exhaustive list of all possible mounting locations. It just gives a list of mounting locations that the designer thought were promising enough to enter in as options. It would also be difficult to allow the computer to consider the possibility of adding new posts or structures to mount to, where absolutely needed, because the designer would then be tasked with somehow telling the computer what voids or open spaces it can suspend detectors in. All of this immediately destroys the prospect of having a truly 100% computer optimized design. Whether this is accomplished by telling the computer what locations, surfaces, or areas are allowed or by marking disallowed locations, this is potentially time consuming.

If all of that could somehow be overcome or if a designer simply decided that whatever list of mounting locations they provided would be “good enough” for the computer to choose from, how would a user or programmer get the computer to consider the relative desirability of a location? How would this be factored into the design? What happens if a situation arises in which one additional detector is needed to reach the specified target coverage level and there are three detector locations where adding a detector will increase coverage by the necessary amount? What if, hypothetically, one of these locations is significantly easier or safer to access for maintenance purposes - possibly because of noise levels, toxic gas hazards, elevation relative to grade, or some other consideration, but this location gives marginally lower / worse coverage than the other two locations? Most operators would rather have a detector in a location where it is easier to clean and maintain, but how do you make the computer understand this and select that mounting location? Even if mounting detectors only in locations that would be relatively easy to access for testing and maintenance would require the addition of two detectors rather than just 1, many operators would rather spend more on CAPEX to install the system in order to reduce future OPEX.

Effective Flame Detection Distance is Not a Single, Fixed Value

It was previously noted that many operators will specify different target fire sizes which the FGS will be tasked with detecting depending on assessed or assigned risk levels. Owing to the inverse square law that governs the intensity of light sources in relation to distance to the source, this means that a flame detector can be farther away from a low risk asset than it can be to a high-risk asset while still providing effective coverage.

To use an example, an operator might set the target fire size for “high risk” assets at 50 KW RHO and the target fire size for low risk assets at 500 KW RHO. In this case, with the target fire size for a low risk asset being 10 times larger, a detector will be able to provide coverage for low risk assets from more than three times the distance at which it can cover high risk assets.

To show how this might look, we can consider the hypothetical case of a set of three vessels with two flame detectors monitoring them from a distance of about 15-21 meters. The generic detectors have a range to a 1 sq. ft test fire (roughly 40 kW RHO) of 17.5 meters.

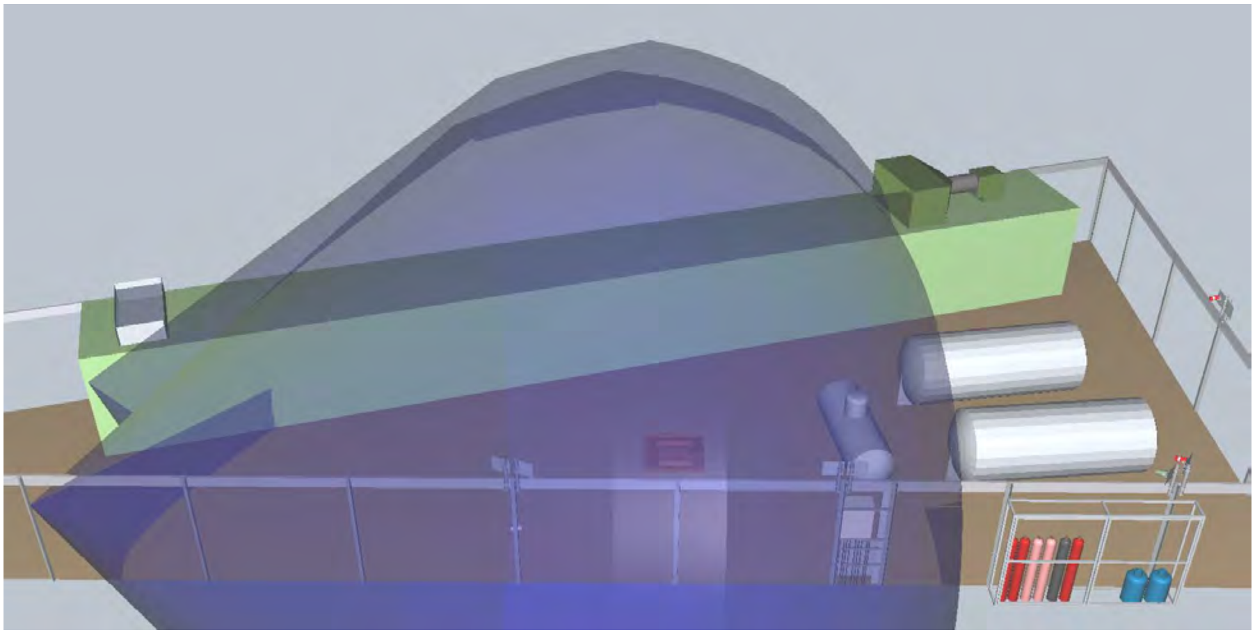


Figure 4: Image depicting the location and orientation of two detectors relative to the three vessels.

These vessels may be graded as HR, MR, or LR, as shown below.

a) b) c)

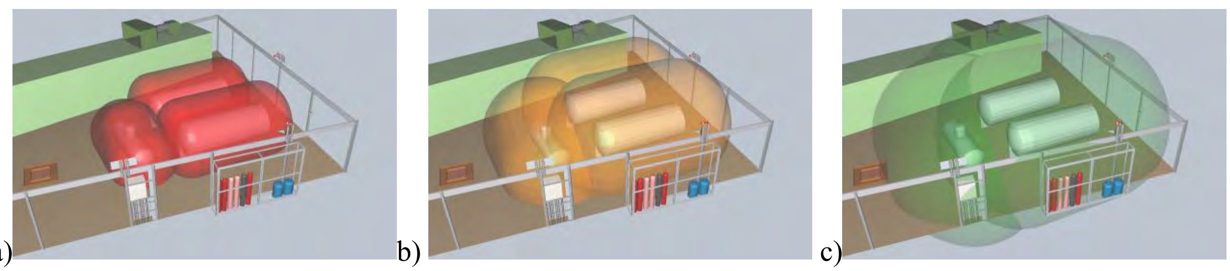


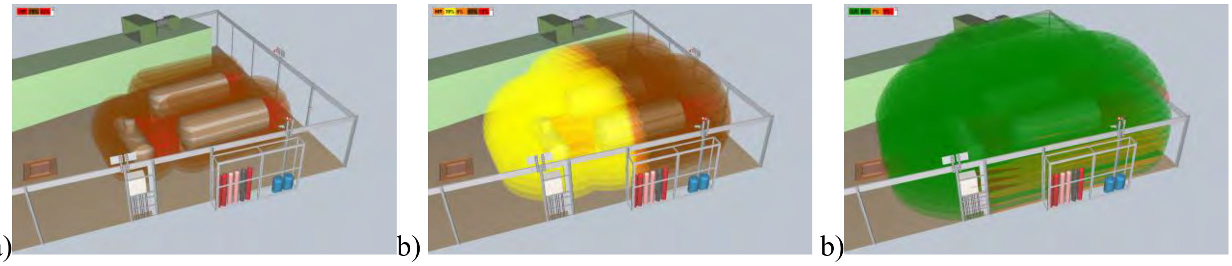
Figure 5: Images depicting the three vessels graded a) "high risk," b) "medium risk," and c) "low risk."

The operator might set target fire sizes for alarm and control action as outlined in the table below with two voting detectors required for control action.

Table 4: Grade definitions for the geographic coverage assessments

Grade	Grade Color	Fire Size		Votes Required	
		Alarm	Control Action	Alarm	Control Action
HR		10	10	1	2
MR		10	50	1	2
LR		100	250	1	2

Figure 6 and Table 5 below summarize the results obtained using the two detector layout in Figure 4 with the three different grading schemes shown in Figure 5.



a) b) b)

Figure 6: Results of the geographic coverage assesments where-in all three vessels are graded a) “high risk,” b) “medium risk,” and c) “low risk.”

Table 5: Summary of results for the geographic coverage assesments conducted with the three vessels.

	Coverage Sufficient for Control Action	Coverage Sufficient for Delayed Control Action	Coverage Sufficient for Alarm	Coverage Sufficient for Delayed Alarm	No Coverage
All HR	-	-	-	78%	22%
All MR	-	39%	6%	43%	12%
All LR	85%	-	7%	-	9%

The results clearly show the impact that risk-based performance targets and target fire sizes can have on the suitability or adequacy of a proposed layout. The detectors are easily able to provide coverage for LR assets at this range but cannot provide any coverage for HR assets at the same distance.

This would, again, further complicate any attempt to generate an optimization algorithm. It may prove simple enough for an algorithm to consider a single, variable target fire size and a single effective detection range for a detector. However, would such a program be able to deal with several different target fire sizes and effective ranges simultaneously? This could occur in an area where there are pieces of equipment with different assigned risk grades, as shown in Figure 7, or it could result from an operator using more than one make and model of detector with different effective ranges, as sometimes happens.

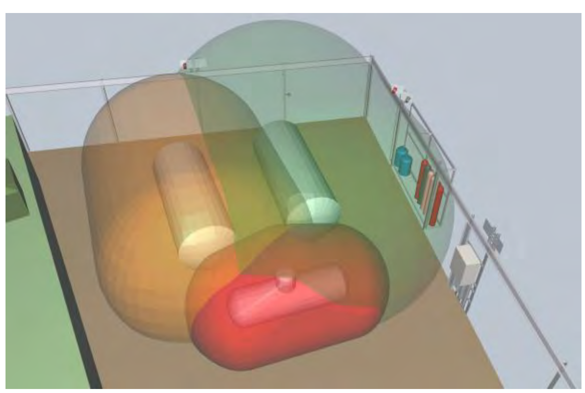


Figure 7: Image depicting an alternative grading scheme where-in all three vessels have been assigned different risk grades.

Conclusion

The authors have presented and reviewed a list of practical considerations involved in the design of fire and gas detection systems - particularly flame detection. These considerations, which include rules of thumb and recommendations that are flexible and not always tightly enforced in the design process, are difficult, if not impossible, to model using current technology and algorithms. A computerized design optimization algorithm is not going to understand or have an awareness of the reasons these rules or guidelines exist and will not be able to exercise judgement in deciding when it is okay to bend or break these guidelines in the way that a human engineer can. At the present time and for the foreseeable future, computer-based sign using optimization algorithms cannot and should not be used as a substitute for the nuanced judgment of an experienced fire protection engineer. Machine learning and artificial intelligence systems may eventually enable a computer to approach the level of judgement required to allow for fully computer-generated flame detector layouts, but such technology is not available today.

References

1. ISA TR 84.00.07. Guidance on the Evaluation of Fire and Gas System Effectiveness.
2. Benavides-Serrano, AJ; MS Mannan, CD Laird. “A quantitative assessment on the placement practices of gas detectors in the process industries.” Journal of Loss Prevention in the Process Industries. 35 (2015) 339-351.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Inherent Safety as a driver for business success in the Oil & Gas Industry

Hari Attal*, Noma Ogbeifun
ETC, Chevron, Houston TX

*Presenter E-mail: Hari.Attal@Chevron.com, Noma.Ogbeifun@Chevron.com

Abstract

Inherent safety is not a new concept and is recognized in the oil and gas industry following the works of Trevor Kletz [1] and others dating back to the 1970s. However, despite the progress made to date in the process safety management arena, incidents have occurred resulting in a renewed focus by regulators to follow-up with more stringent regulations. Two recent studies, covering a span of 20 years (1998-2018), revealed that 19-36% of these incidents could have been avoided if an Inherent Safer Design approach was utilized [2]. Some barriers to adoption and implementation of inherent safety include lack of full understanding of Inherently Safer Design (ISD) principles, lack of assessment tools to showcase ISD benefits, and lack of ISD application framework. This paper will demystify ISD definition, examine the barriers to ISD application, propose a framework to overcome them and share recent successes in application of ISD at Chevron.

Keywords: Inherently Safer Design (ISD); inherent safety; barriers

Introduction

Over the last 40 years, there have been incidents that highlighted the importance of process safety awareness and management to protect people and environment. Noteworthy incidents include Flixborough, UK 1974 (Explosion – 28 Fatalities), Bhopal, India 1984 (MIC release – 4,000-20,000 fatalities), Piper Alpha, UK 1988 (Explosion – 167 fatalities), Pasadena, US (Explosion - 23 fatalities), Texas City, US (Explosion – 15 fatalities), and Deepwater Horizon, US (Explosion – 11 fatalities and catastrophic environment damage). Possible causes include increase in scale and complexity of new plants; complex relationships between people and automation; limitations of current probabilistic risk assessments.

Despite the technological advancements in process safety engineering and management processes, the re-occurrence of these process safety incidents questions the assumptions and notions of progress in terms of hazard reduction. This begs the question “How can we build safer plants while satisfying overarching project objectives? Hence, the concept of inherently safer design.

What does Inherently Safer Design mean?

Inherently safer design is a design philosophy that prioritizes hazard elimination or reduction in hazard likelihood or severity of occurrence rather than addition of layers of protection to prevent and minimize hazards. This is accomplished by means that are inherent in the process design such that it is permanent and cannot be removed. A system may be defined as Inherently Safer if – after an upset – it stays or returns to a safe and stable state without involving human intervention or automatic controls. The expectation is to focus on what can be done to eliminate the hazard before considering how to control the hazard. In some instances, we recognize that application of some of the ISD strategies may prove challenging because of the chemical nature of hydrocarbons, e.g. flammability, is often what makes the commodity valuable. Consequently, it may be infeasible to eliminate all hazards.

A report by the Centre for Chemical Process Safety (CCPS) [3] in 2010 for the U. S. Department of Homeland Security (DHS) Chemical Security Analysis Centre (CSAC) emphasizes that ISD evaluation and selection decision process must consider the entire life cycle, the full spectrum of hazards and risks, and the potential for transfer of risk. Technical and economic feasibility of options must also be considered.

ISD Strategies

Approaches to inherently safer design have been grouped into five major strategies and summarized below:

Strategy	How?
Elimination	Eliminate the hazardous material or activity
Substitution	Replace a hazardous material or process with an Alternative that reduces or avoids the hazard; e.g. Replace Hot oil with Hot water as a heat media
Minimization	Use small quantities of hazardous substances or reduce inventory or energy; e.g. Reduce pipe, equipment size
Moderation	Use dangerous materials in their less dangerous form or identify options with less severe conditions; e.g. optimization of production separation pressures
Simplification	Designing processes equipment and procedures to Eliminate unnecessary complexity and human error; e.g. Containment within process equipment (design for maximum pressure and full vacuum)

It is important to understand that there is no hierarchy in terms of risk reduction potential within the different strategies except elimination is considered First order and other four strategies are considered second order [3].

What are the barriers to adoption of ISD approach in the industry?

There are barriers to its full adoption by practitioners due to following reasons:

1. One of the major problems related to the adoption of ISD principles is the perception that the only way to make a plant safer is to add more systems to it. As facilities become more complex, there is a need to focus on eliminating/reducing hazards rather introducing more avenues for failures.
2. Limited knowledge of Inherently Safer Design strategies and their role in achieving the key objectives of hazard management principles (Prevention, Control and Mitigation) during Engineering has made adoption of ISD approach difficult. However, many installations incorporate some ISD principles initiated through 'good ideas' or cost reduction initiatives rather than a deliberate application of principles throughout the project life cycle. This means systematic application of the principles could lead to a widespread adoption and implementation of ISD.
3. Lack of development of structured design review techniques in oil and gas industry to identify Inherently Safer Design Opportunities has been a challenge in consistent application of ISD strategies [4]. In comparison, PHA and QRA risk analysis techniques have been sufficiently developed and applied in the oil and gas industry. However, current literature [5][6] shows examples of successful application of ISD techniques/methodologies to the design of offshore platforms. For example, on an offshore project, the operator implemented ISD strategies through a series of workshops from concept level to operations.

Framework for implementing ISD

Effective application of ISD strategies requires a structured and multifaceted approach. This involves broad alignment and support from key stakeholders, integration of ISD principles into project and design philosophies and solid understanding and acceptance of ISD strategies among practitioners. This will require creating a workflow and process with methodology and tools to achieve desired ISD goals and objectives, as well as providing a platform for showcasing ISD successes and contributions to decision making. The steps involved in systematic application is given in Figure 1.

Figure 1: Steps for systematic ISD application

1. Role of Leadership

Strong leadership is the foundation on which ISD success is built. Business leaders, project leaders and engineering leaders need to define the approach to safety early during the concept selection phase.

Figure 2: Opportunities to implement ISD [5]

It is worth noting that the greatest benefits of applying ISD thinking are derived early in the design process (concept stage). However, there are more benefits from maintaining this hazard elimination/reduction mindset throughout the design process although with diminishing returns.

Successful cultivation of ISD mindset and culture begins leaders charting a clear set of expectations relating to design safety; a continuous interest in the hazard identification by project leaders; and a visible commitment to risk reduction, will set a visible example which will permeate through the different phases of the design process.

On a past project, the ISD project vision was to deliver an inherently safer design that satisfies the following tenets:

- Reduced probability of unwanted events
- Reduced facility attendance
- Reduced damage potential
- Reduced scope for smaller incidents to escalate and overwhelm the facilities
- Clear focus on simplicity, reliability and longevity to reduce exposure

Leaders challenged the project teams to start the hazard management process with the mindset of hazard elimination rather than using risk analysis techniques to aim for an ALARP solution. Project teams were challenged to justify adding any equipment or instrumentation to the design. A similar approach was successfully applied by Woodside during the design of the Angel Platform and resulted in significant CAPEX reduction [7].

Leaders are responsible for driving a cultural change that encourages innovation. This involves strengthening ISD awareness and fluency via subject matter presentations, training, campaigns and workshops; incorporating ISD into all layers of design decision making – For example, ISD lunch and learns exercises where leadership provide examples that demonstrate how the incorporation of ISD in early phases of projects have minimal cost impacts as well as lessons learned from missed opportunities which resulted in add-on safeguards.

2. People

Incorporating an ISD objective in each project team member's performance expectations have proven effective towards focusing the wider team to actively adopt and steward the routine application of ISD. On a recent project, project leaders nominated ISD champions within the respective disciplines to help identify ISD opportunities, track the opportunities to action and communicate ISD application examples to wider stakeholders to increase overall fluency. During workshops, standing meetings, and model reviews, ISD champions asks probing questions to challenge the design teams to consider ISD alternatives. The ISD champion provides broad support across the project but should have focused engagements with the process and mechanical engineering and operations representative's teams as most of the ISD opportunities lay in those functions.

3. Process

One of the challenges leaders must overcome is creating the ability among practitioners to consistently apply ISD principles in a reproducible manner. This will involve creating a process/workflow to identify ISD opportunities and measurement and verification. On a past project, the project team identified ISD opportunities via a series of strategically timed design evaluation workshops where the team critically examined the selected design to identify opportunities to reduce risk during the early phases through the application of ISD strategies. The workshops are facilitated sessions with a cross functional team. The facility under review was divided into nodes and critically examined for opportunities to apply ISD principles. When an ISD opportunity was identified, the team discussed the benefits and potential trade-offs to assist in further evaluation of the opportunity during the facility lifecycle. ISD opportunities were recorded in an ISD Opportunities Register and tracked to closure on a frequent (weekly to monthly) basis. Table 2 gives an example of the structure of an ISD Opportunities Register [8].

- *Table 2: ISD Opportunities Register - Example*

Hazard	ISD Principle	Description (concern – options – benefit – trade-offs)	Owner	Status
Pressure	Simplification	Current design: Acid stimulation is a practice to improve well productivity in deep water subsea environment. Spent acid is often sent to topsides prior to disposal. The topsides manifold is not designed to handle acid flowback. Consider eliminating acid flowback to topsides with a safer alternative Benefit: Eliminating a hazardous activity and operations exposure. Tradeoff: Evaluate the feasibility and cost of acid flowback alternatives.	John Doe	Pending

On another project, the design team adopted the strategy leveraging from a popular sit-com series to implement ISD strategies to identify and track removal of redundant equipment and/or instrumentation from an offshore platform in order to achieve weight and cost objectives [5]. The integrated (company and EPC) design team were encouraged to submit their ideas for weight and cost reduction to project leaders and monthly prizes are awarded to selected ideas. This resulted in significant weight savings and 15-20% reduction in associated costs.

ISD application examples

This section lists examples from offshore oil & gas projects demonstrating how ISD strategies were incorporated for meeting project vision for inherently safer facility.

Eliminate

(i) Elimination of high-pressure gas handling hazard: Enhanced Oil Recovery (EOR) through gas injection, chemical injection or water injection is one of the strategic decisions during concept select for offshore field development projects. In one greenfield project, EOR by gas injection, was preferred alternative for improved recovery of oil. This process includes additional equipment, such as gas compressors for generating the high pressures needed and requires buy-back of flammable gas to the facility. Handling high flowrate of high-pressure gas increases the risk to personnel on board which leads to addition of active and passive safeguards like high integrity instrumented protection system and blast resistant walls. Through ISD application, the project team eliminated high pressure flammable gas handling hazard by electing not to pursue EOR by gas injection despite an expected reduction in total oil recovery.

(ii) Elimination of asphyxiation hazard: Fire suppression is an important mitigative safeguard and can be achieved with multiple technologies, including water mist, chemicals or foams, and carbon dioxide (CO_2). The use of CO_2 for fire suppression introduces an asphyxiation hazard for personnel due to the potential for spurious activation of the CO_2 system in enclosed areas like equipment cabinets or electrical rooms. The design philosophies prohibited the use of CO_2 fire suppression systems in enclosures. By not allowing the use of CO_2 systems, the projects eliminated the potential asphyxiation hazard while still ensuring fire suppression can be achieved by other technologies.

Substitute

(iii) Substitution of flammable chemical: Hydrates, which occur due to the presence of water and gas in production fluids and the high pressures and low temperatures of the systems, can block flowlines and create operational and flow assurance concerns. The project planned to use a highly flammable chemical that is injected in the production flowlines to prevent hydrate formation. Storage and handling of the chemical introduced flammable hazards requiring area classification, additional fire and gas detectors and fire suppression system. Through ISD application the design team substituted the hydrate inhibition system with a less hazardous (non-flammable) chemical. Risk reduction achieved without impact to production and saved cost of installing and maintaining the safeguards related to flammable chemical.

Minimize

(iv) Minimization of hazardous inventory: Initial project design specified storage of thousands of barrels of diesel in the hull to support power generation to meet facility availability targets. The estimated diesel storage volume could be met only by utilizing multiple pontoons of the hull requiring complex piping network for the diesel storage and handling. Through application of ISD minimization strategy, the project team was able to reduce the diesel storage needs by 75% through power use optimization effort and by choosing duel fuel alternative for power generation. The selected design option had some impact on the operational flexibility (in the event of a fuel gas system disruption), but significantly reduced the risk and simplified the design.

Moderate

(v) Moderation of hazardous drain system: Bilge water in the hull is typically routed to the hazardous drain system on the topsides as the waste stream can accumulate small quantities of hazardous spilled material. The project designed a dedicated hazardous drain system that will collect potential hazardous spills from equipment in the hull and routes to the hazardous drain system on the topsides. The hazards associated with the bilge system, which manages a large waste stream, have been moderated and the flows can be routed to the non-hazardous drain system.

(vi) An example of application of the moderation principle for an onshore, greenfield liquified natural gas MCP is provided. Molecular sieve beds are used to remove water from natural gas prior to export and these beds must be periodically regenerated to remain effective. Regeneration can be done using a high pressure or low-pressure system options. Dewatering natural gas using sieve beds regenerated with a high-pressure system is a more energy efficient process but requires operation of the entire dewatering system at very high temperatures and pressures. The team selected a low-pressure regeneration system that allows the dewatering system to operate at much lower temperatures and pressures and the severity of a potential incident are reduced.

Simplify

(vii) Simplification with reduction in human performance dependence: Chemical injection into production flowlines or into the well-bore is a common operational activity to manage the impurities in the oil (e.g. hydrates, waxes) and provide other critical flow assurance functions. On one MCP, the proposed strategy for distributing chemicals consisted of using one pump and multiple valves to allow for multiple chemicals to be injected using the same piping configuration. The team identified that misalignment of the valves and inadvertent introduction of the wrong chemical was a credible concern. The design was reconfigured to provide dedicated pumps and piping networks to simplify the operations procedures and minimize the potential for human error.

(viii) Simplification by enhancing the design rating: Subsea production flowlines can be subject to immense pressures during the initial phases of production in a reservoir or as the result of pressure buildup if subsea pumping is anticipated. High Integrity Protection System (HIPS), a complex and expensive instrument and control system, is often used for controlling pressure surges. A greenfield MCP elected to fully rate the subsea flowlines for the maximum expected pressures with incremental costs associated with the procurement and installation of thick-walled pipe. Through ISD application the risk was significantly reduced, and the complexity in maintenance of HIPS was avoided. In this example, the application of ISD provided a cost benefit for both Capital Expenditure and Operational Expenditure during the facility life.

4. Conclusion

This paper demonstrated risk management through a systematic application of the concepts of Inherently Safer Design through project design stages. It highlights the importance of project leadership and the relevance of approaching ISD as a mindset rather than a one-time risk assessment activity. The relevance of ISD training for project personnel and the value of an ISD opportunity tracker is discussed. Examples in this paper demonstrate that the maximum value of ISD application is realized when applied early in the project (before the layout is finalized and decisions on choice of equipment / process is made). Though ISD application yields benefits, the paper discusses trade-offs that need to be considered.

References

1. Trevor Kletz, 1978, “What you don’t have, can’t leak, Jubilee Lecture, Chemistry and Industry
2. Paul Amyotte, et al, 2018, Chemical Safety Board investigation reports and hierarchy of controls: Round 2, American Institute of Chemical Engineers 2018 Spring Meeting, 14th Global Congress on Process Safety, Orlando, Florida
3. Homeland Security, 2010, Final Report: Definition for Inherently Safer Technology in Production, Transportation, Storage, and Use
4. Health and Safety Executive, 1996, Improving Inherent Safety OTH 96 521
5. Kevin Stevenson, 2012, Care and Concern for People We’ll Never Meet – Process Safety in the Design of the Wheatstone Platform, APPEA International Conference
6. M.M Oakden et al., 2008, The Application of Inherently Safer Design Principles to the Design of a New Offshore Gas Processing Platform
7. Gordon B. et al., 2013, Delivering operationally Efficient Platforms Using Inherently Safer Design, SPE 167384, SPE Middle East Intelligent Energy Conference and Exhibition
8. Nair S. R, et al, 2019, Achieving World Class Performance in Oil and Gas Industry Using Inherently Safer Design, 75, Chemical Engineering Transactions

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Studying the Inherent Safety of Flare Utilization Alternatives during Abnormal Operations

Fadwa Eljack[a*], Vasiliki Kazantzi[b], Nikolaos K. Kazantzis[c], and Monzure-Khoda Kazi[a]
[a]Qatar University, Department of Chemical Engineering, College of Engineering, Doha, Qatar, P.O. Box-2713
[b]University of Thessaly, 41110 Larissa, Greece
[c]Worcester Polytechnic Institute (WPI), Department of Chemical Engineering, Worcester, MA 01609-2280, USA
*Presenters e-mails: Fadwa.Eljack@qu.edu.qa; kazantzi@teilar.gr

Abstract

Flare management constitutes a major issue in industrial practices and draw lately significant research interest, since it has been shown that economic, safety and sustainability performance of industrial systems can be substantially improved by effectively managing their flaring streams (Kazi et al., 2018). This work aims at applying ***I***nherently ***S***afer ***D***esign ***T***ool (*i*-SDT) for managing process safety and resilience risk analysis during implementation of flare recovery alternatives under uncertainty.

A recently developed ***I***nherently ***S***afer ***D***esign ***T***ool (*i*-SDT) (Eljack et al., 2019) that enables safety evaluation of process systems during the early design stage utilizing limited process data is here extended to encompass safety parameters related to flaring behavior that typically exhibits discrete and highly uncertain occurrence characteristics. Flaring can happen either routinely and during unexpected situations to prevent process from running under unsafe conditions, or emerge abruptly during abnormal process operations. A comparative estimation of the flaring implications on the overall safety process performance and at the same time a reflection on the potential to reduce this impact by properly manage them (recover and utilize) is presented and discussed here. The formerly developed characteristic equations of the safety parameters were now enriched by incorporating available flaring information under certain operating conditions, while the cluster safety parameter score (C_{SP}) as the resulting metrics of the *i*-SDT, enables the direct identification of the resulting safety consequences associated with the distinct flaring incidents, and offers insights on incremental changes in safety profiles of various flare management alternatives.

In this work, we investigate the influence and exploitation of the pertinent flaring historical data on the implementation of the recovery systems in relation to their inherent safer design and operational bottlenecks. Flare streams suitable as feed candidates for the flare recovery systems has been characterized and identified by a predictive, systematic and effective flare management approach. Thus, an advanced property based formulation, the *i*-SDT, has been utilized to intensify the concepts, analytical methods and mathematical tools derived from dynamical systems for characterizing the dynamic behavior of flare recovery systems over a wide range of operating conditions in the presence of nonlinearity and uncertainty. The proposed safety evaluation approach when directly consider flaring incidents in process performance may result in a more comprehensive safety metrics development, especially for industrial systems with many such flare occurrences. These systems seem prone to safety uncertainties and need to associate them with specific stream- and unit- risk characteristics for safety improvement using an a priori inherently safer design. Furthermore, the comprehensive tool is recommended to be embedded into a techno-economic analysis framework for a simultaneous cost and safety evaluation approach.

Keywords: Resilience Risk Analysis; Managing Process Safety; Safety Evaluation; Safety Analysis; Industrial Flares; Inherently Safer Design

References:

Eljack, F., Kazi, M.-K., Kazantzi, V., 2019. Inherently safer design tool (i-SDT): A property-based risk quantification metric for inherently safer design during the early stage of process synthesis. Journal of Loss Prevention in the Process Industries 57, 280-290.

Kazi, M.-K., Eljack, F., Amanullah, M., AlNouss, A., Kazantzi, V., 2018. A process design approach to manage the uncertainty of industrial flaring during abnormal operations. Computers & Chemical Engineering 117, 191-208.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Impact of particle density on dust cloud characteristics in the minimum ignition energy testing apparatus using high-speed digital in-line holography

Pranav Bagaria[1,2], Purvali Chaudhari[1,2], Waruna Kulatilaka[3], Chad Mashuga[1,2], Ankit Saini[2], and Christian Schweizer*[3]

[1]Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122

[2] Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX 77843-3122

[3]J. Mike Walker '66 Department of Mechanical Engineering Texas A&M University, College Station, TX, 77843

*Presenter E-mail: schweizer@tamu.edu, ankit.saini06@tamu.edu

Abstract

Dust explosions continue to be an industrial hazard with the probability of ignition estimated by the measurement of minimum ignition energy (MIE), typically in a Kühner MIKE3 device. For optimal MIE measurements, the dust cloud generated in the 1.2L Hartmann tube shall be in a uniform and a non-transient state. However, achieving it is difficult due to the turbulence induced by the air-driven dust dispersion system employed in such devices. Since particle densities of combustible dust vary considerably, the dynamics of dust clouds generated by a constant dispersion pressure, at a typical ignition delay of 120ms, will be dissimilar. In this study, two dust samples: poly(methyl methacrylate) and soda lime glass of different particle density are dispersed in the Kühner MIKE3 MIE device and a digital in-line holography (DIH) imaging system is employed to capture high-speed images. The DIH imaging system reveals real-time particle behaviour within the dust cloud ignition zone including particle velocity, concentration and particle size. At a given ignition delay, a variance is observed among these cloud characteristics for different dust density. The quantitative data obtained shows the cloud dynamics at ignition for different dust densities are not the same and can require selection of a different ignition delay for a consistent and quiescent dust cloud.

Keywords: Dust ignitability, Minimum ignition energy, Particle density, Kühner MIKE3

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Modelling of the plume rise phenomenon due to warehouse fires considering penetration of the mixing layer

Hans Boot and Sonia Ruiz Pérez*
Gexcon AS – Fire and Explosion Consultants
Utrecht, The Netherlands
*Presenter E-mail: sonia.ruiz.perez@gexcon.com

Abstract

The present paper describes the theory behind the "plume rise from warehouse fires model" as implemented in the software package EFFECTS. This model simulates the rising of buoyant plumes due to the density difference between the hot combustion products and the ambient air. The plume rise model calculates the maximum height at which the released material will be in equilibrium with the density of the air, and presents the resulting trajectory of the plume, including hazard distances to specific concentration threshold levels. These parameters will be determined depending on the windspeed, atmospheric stability class and the fire's convective heat production, leading to potential penetration of the mixing layer.

Additionally, the 'penetration fraction' is assessed which expresses the amount of plume penetrating the mixing layer. If the convective heat of production is sufficient to penetrate the mixing layer, the smoke plume will be trapped above the mixing layer. When this occurs, the (potentially toxic) combustion products do not disperse back below the mixing layer, thus, the individuals at ground level are not exposed to the harmful combustion products. If the convective heat of production is not sufficient to penetrate the mixing layer, the smoke plume may experience the so-called reflection phenomena which will trap the smoke plume below the mixing layer. This could have more dangerous consequences for individuals who then might be exposed to harmful combustion products at ground level.

Moreover, this paper includes the validation of the model against experimental data as well as to other widely validated mathematical models. The experiments and mathematical models used for the validation are described, and a detailed discussion of the results is included, with a statistical and graphical comparison against the field data.

Keywords: Consequence Analysis, Modeling, Combustion, Dispersion, Effects, Emission, Gas Dispersion, Plumes, Safety.

1 Introduction

Smoke plumes containing toxic combustion products resulting from warehouse fires, will initially rise due to the density difference between the hot combustion products and the ambient air. This density difference is caused by the fact that the temperature of the plume is significantly higher than the temperature of ambient air. The theory behind this plume rise phenomenon foresees that there will be a height at which the released material will be in equilibrium with the density of the air at that height, leading to a maximum plume height. The trajectory of the plume and the hazard distances to specific concentration threshold levels will be mainly influenced by the windspeed, atmospheric stability class and the fire's convective heat production, where the combination of these parameters lead to potential penetration of, or even reflection by the mixing layer.

Typical models that describe the mathematics behind rising of hot plumes include the effects of atmospheric turbulence, as described by the Pasquill stability class. However, the plume's potential penetration of the mixing layer should also be considered. The importance of the plume penetration is that all mass that has risen above the mixing layer, will never disperse back into the mixing layer. Therefore, toxic combustion products will be trapped above the mixing layer height and will never create chemical exposure at ground level. The reason for this is that at the boundary of the mixing layer (at the temperature inversion height) there is no vertical turbulence. Only the stronger chimney emissions are likely to penetrate upwards due to their greater buoyancy forces. Apart from penetration of the mixing layer height, the potential reflection of the plume should also be considered, which can play a role for plumes that remain below the mixing layer height.

The present study has led to the implementation of a dedicated model, implemented in Gexcon's software package EFFECTS, to simulate the plume rise phenomenon due to warehouse fires. This model calculates the maximum height and plume path of the plume and includes reporting of a 'penetration fraction'. Additionally, the reflection phenomenon is also considered. The model also presents concentration threshold contours of toxic combustion products at any height level.

The model provides safety professionals with valuable information for hazard identification, safety analysis and emergency planning. For instance, if a warehouse fire has enough convective heat production, a toxic smoke plume may rise high enough and even penetrate the mixing layer, not providing any danger at ground level. Trying to extinguish the fire, would decrease the heat production, leading to more danger of toxic exposure at ground level.

Because harmful concentrations may reach very large distances, where the assumption of a homogeneous wind-field is no longer realistic, the plume rise model has also been extended to account for the meandering of the plume (due to time and location dependent meteorological conditions). This model extension uses real-time meteorological data retrieved from the internet, which results in time dependent concentration contours of the plume and a real time view of the meandering plume path. This extension has not been made commercially available but could – when properly integrated into control rooms – provide valuable information to emergency services during interventions.

2 Methodology

2.1 Plume rise modelling

The “plume rise from warehouse fires model” as implemented in the software package EFFECTS is based on Briggs’ study of the plume rise phenomenon [1], the theory in the Yellow Book [2] and uses Mill’s correction for burning fires [3].

2.1.1 Briggs model

The rising of the plume with distance and the maximum height of the plume can be calculated in two different ways, depending on the atmospheric stability.

For Pasquill stability class A, B, C and D, the rising of the plume with distance and the maximum height of the plume can be calculated with Equation 1, Equation 2 and Equation 3, respectively. The corresponding distance to the maximum height of the plume (x_f) can be calculated with Equation 4 and Equation 5, depending on the value of the initial heat flux (Q_0).

if $x < x_f$ $$h_{BRIGGS} = z_s + 1.6 \cdot Q_0^{\frac{1}{3}} \cdot u_w(z_s)^{-1} \cdot x^{\frac{2}{3}}$$ Equation 1

if $x \geq x_f$ $$h_{BRIGGS} = z_s + 1.6 \cdot Q_0^{\frac{1}{3}} \cdot u_w(z_s)^{-1} \cdot x_f^{\frac{2}{3}}$$ Equation 2

$$h_{max} = z_s + 1.6 \cdot Q_0^{\frac{1}{3}} \cdot u_w(z_s)^{-1} \cdot x_f^{\frac{2}{3}}$$ Equation 3

$$x_f = 49 \cdot Q_0^{\frac{5}{8}} \qquad \text{for } Q_0 < 55$$ Equation 4

$$x_f = 119 \cdot Q_0^{\frac{2}{5}} \qquad \text{for } Q_0 \geq 55$$ Equation 5

For Pasquill stability class E and F, the rising of the plume with distance and the maximum height of the plume can be calculated with Equation 6 and Equation 7, respectively. The Brunt-Vaisala frequency (N) is described in paragraph 2.3.2. The 2/3 relation results from treating the time average profile of the bent over plume as an extension of the model of Morton, 1956 [4].

$$h_{BRIGGS} = z_s + 2 \cdot Q_0^{\frac{1}{3}} \cdot u_w(z_s)^{-\frac{1}{3}} \cdot N^{-\frac{2}{3}} \cdot \left(1 - \cos\frac{N \cdot x}{u_w(z_s)}\right)^{\frac{1}{3}}$$ Equation 6

$$h_{max} = z_s + 2.52 \cdot Q_0^{\frac{1}{3}} \cdot u_w(z_s)^{-\frac{1}{3}} \cdot N^{-\frac{2}{3}}$$ Equation 7

2.1.2 Mills correction for burning fires

According to Zonato et al, 1999 [5] the assessment of the rising of smoke plumes resulting from free burning fires would be appropriate by implementing a series of relations as suggested by Mills, 1987 [3]. Mills suggested altering the Briggs formula as shown in the equation below, where

h_{BRIGGS} corresponds to the plume rise due to buoyancy effects as described in the Briggs model (see paragraph 2.1.1).

$$h_{MILLS} = \left[(h_{BRIGGS})^3 + \left(\frac{D}{2 \cdot \gamma}\right)^3\right]^{\frac{1}{3}} - \frac{D}{2 \cdot \gamma} \qquad \text{Equation 8}$$

Additionally, Mills described the initial heat flux (Q_0) as follows:

$$Q_0 = (1 - 0.3) \cdot 0.037 \cdot Q_H \qquad \text{Equation 9}$$

Mills assumes that the 30% of the heat released in the combustion is dispersed as thermal radiation in the surrounding area and that the 70% of the heat combustion is devoted to the plume rise. Consequently, the term $[(1 - 0.3) \cdot Q_H]$ corresponds to the convective heat flux. Moreover, the term $[D/2 \cdot \gamma]$ is inserted in the Briggs formula (where $\gamma = 0.6$ is the entrainment coefficient for a buoyant plume rise) to account for the initial diameter of the plume, which is considered equal to the extent of the fire.

2.2 Calculation of the plume concentration

In order to calculate the concentration of the plume, it is necessary to know not only the position of the plume centerline but also the way in which the material is distributed through the plume's width and height. A rising plume entrains air into its own volume, thereby, increasing its radius. A rising plume is also subject to the normal processes of turbulent diffusion which acts to increase the plume size. The standard deviation of the distribution should allow for the effects of plume rise and passive diffusion on plume growth (as described in paragraph 2.2.3).

The Gaussian Plume Model as described in the Yellow Book [2] can be applied to describe passive dispersion if the dispersing cloud is either neutral or positively buoyant. Therefore, the Gaussian Plume Model is selected to calculate the dispersion phenomena for all scaling regions in the mixing layer. The Gaussian Plume Model is valid for dispersion calculations over flat, uniform terrain. The gaussian mathematical equations have been extended to account for reflection of the plume material in the mixing height (as described in paragraph 2.2.1).

The general expression to calculate the plume concentration (in kg/m^3) for continuous releases is:

$$C(x, y, z) = \frac{q_F}{u_w(z_c)} \cdot F_y(x, y) \cdot F_z(x, z) \qquad \text{Equation 10}$$

Where q_F is the formation rate of the chemical of interest (i.e. C, CO_2, HBr, HCl, HF, NO_2 or SO_2) and $u_w(z_c)$ the wind velocity at the plume centerline. The expression $F_y(x,y)$ accounts for lateral (crosswind) dispersion (see paragraph 2.2.1) and $F_z(x,z)$ accounts for vertical dispersion (see paragraph 2.2.1). Because of the importance of the source rate of a specific toxic combustion product, this formation rate of the chemical of interest can be calculated with the EFFECTS model "combustion and toxic combustion products". This combustion model allows for the calculation of the combustion of solid and liquid products due to warehouse fires, based on a gross chemical structural formula and burning area.

2.2.1 Lateral (crosswind) dispersion

The expression $F_y(x,y)$ accounts for the lateral (crosswind) dispersion and it is calculated as shown in Equation 12 and Equation 13. The calculation of lateral dispersion depends on the initial source half dimension in the lateral direction (b_{oy}), which is assumed to be the initial radius of the fire.

$$b_{oy} = \frac{D}{2} \qquad \text{Equation 11}$$

If $b_{oy} = 0$…

$$F_y(x,y) = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_y(x)}\cdot e^{-\frac{y^2}{2\cdot\sigma_y^2(x)}} \qquad \text{Equation 12}$$

If $2\cdot b_{oy} > 0$…

$$F_y(x,y) = \frac{1}{4\cdot b_{oy}}\cdot\left\{\mathrm{erf}\left(\frac{b_{oy}-y}{\sqrt{2}\cdot\sigma_y(x)}\right)+\mathrm{erf}\left(\frac{b_{oy}+y}{\sqrt{2}\cdot\sigma_y(x)}\right)\right\} \qquad \text{Equation 13}$$

2.2.2 Vertical dispersion

The expression $F_z(x,z)$ accounts for the vertical dispersion and it is calculated as shown in the equations below. The calculation of vertical dispersion depends on the source half dimension in the vertical direction (b_{oz}), which is also assumed to be the initial radius of the fire.

$$b_{oz} = \frac{D}{2} \qquad \text{Equation 14}$$

The calculation of the vertical dispersion depends on several parameters:

- **Penetration fraction:**
  The penetration fraction P(x) is the fraction of mass that has risen above the mixing layer height and it is calculated assuming a gaussian distribution of mass in the vertical direction. The penetration fraction might increase with distance until the maximum plume height h_{max} is reached. Additionally, the penetration fraction will reach its maximum value at the distance where the maximum height of the plume is reached. The significance of the penetration fraction is that this mass fraction can never expose a risk a ground level. A value of P = 0.5 implies that half the plume is above the mixing layer height, whereas P = 1 implies full penetration. It is assumed that at the top of the mixing layer, there is a region (at the temperature inversion height) where there is no vertical turbulence. That means that there is no turbulent exchange of mass through this inversion layer height.

$$P(x) = \frac{1}{2}+\frac{1}{2}\cdot\mathrm{Erf}\left(\frac{h_{max}-MH}{\sqrt{2}\cdot\sigma_z(X_d)}\right) \qquad \text{Equation 15}$$

The vertical dispersion parameter of the smoke plume (σ_z) needs to be calculated for the distance at which the height of study is reached by the cloud. Therefore, the expression in Equation 16 can be used where X_d corresponds to the addition of the distance at which the height of study of the plume is reached (x_f) to the distance of a virtual source (V_z). See paragraph 2.3.1 for more information about the virtual source.

$$X_d = x_f + V_z \qquad \text{Equation 16}$$

- **Reflection**:
  Reflection is the phenomenon in which concentrations get "bounced back" against a non-penetrable boundary, such as the ground level or temperature inversion layer. For plumes near the ground level, the reflection against the ground (R_G) needs to be accounted for. For plumes near the mixing layer height the reflection against the mixing layer (R_{MH}) needs to be considered. The mixing layer acts as a ceiling for the smoke plume.

The calculation of the vertical dispersion needs to consider two different situations: (1) vertical dispersion when the plume is no longer rising, hence, it has reached its maximum height (see paragraph 2.2.2.1); (2) vertical dispersion when the plume is still rising, and has not yet reached its maximum height (see paragraph 2.2.2.2).

2.2.2.1 Plume has reached its maximum height

Once the plume has reached its maximum height, the plume center line can be situated either below or above the mixing layer height.

<u>If $h_{max} < MH$</u>

If the maximum height of the plume is situated <u>below the mixing layer height</u>, the penetration fraction is expected to be small (as shown in the left picture of Figure 1) or 0 (as shown in the right picture of Figure 1). This is typically because the plume does not have sufficient momentum to penetrate the mixing layer due to its heat of combustion. In this situation the reflection of the plume against the mixing layer height needs to be accounted for.

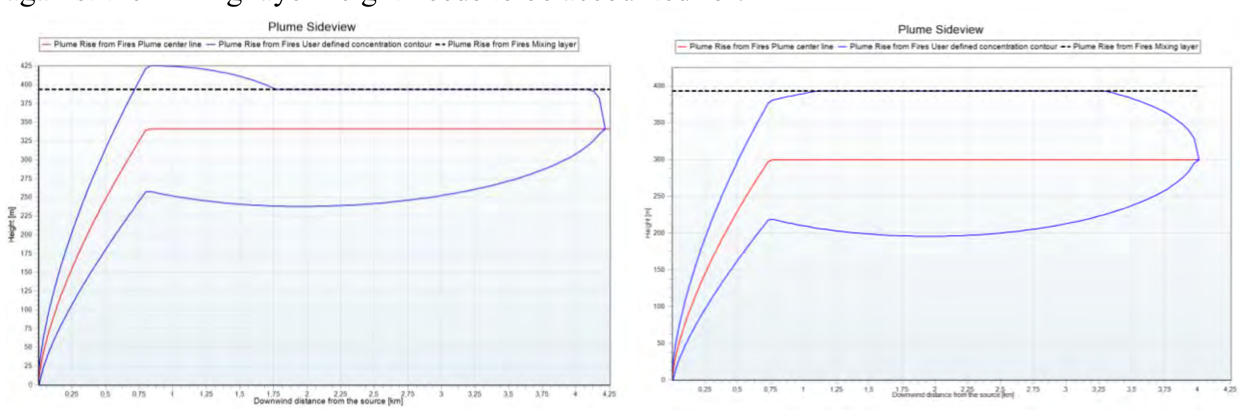


Figure 1. Plume with a maximum height situated below the mixing layer height with a very small penetration fraction (left) and with no penetration (right)

In order to be able to describe the full trajectory of the plume, the calculation needs to include two different approaches to calculate the vertical dispersion depending on whether the vertical coordinate of study is below or above the mixing layer height for every distance evaluated.

- If $z < MH$

  When the vertical coordinate of study is situated below the mixing layer height, and $P < 1$, the plume will not fully penetrate the mixing layer. In this case, the reflection from the mixing layer height (R_{MH}) and from the ground (R_G) need to be incorporated.

$$F_z(x,z) = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\exp\left[-\frac{(z-z_c)^2}{2\cdot\sigma_z^2(x)}\right] + R_G + CF\cdot R_{MH} \qquad \text{Equation 17}$$

Where:

$$R_G = \frac{1}{4\cdot b_{oz}}\cdot\left\{\operatorname{erf}\left(\frac{b_{oz}-z-z_c}{\sqrt{2}\cdot\sigma_z(x)}\right) + \operatorname{erf}\left(\frac{b_{oz}+z+z_c}{\sqrt{2}\cdot\sigma_z(x)}\right)\right\} \qquad \text{Equation 18}$$

$$CF = P(x) - P(x_f) \qquad \text{Equation 19}$$

$$R_{MH} = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\left\{\exp\left(-\frac{\left(z-z_{c,reflected}\right)^2}{2\cdot\sigma_z^2(x)}\right) + \exp\left(-\frac{\left(z+z_{c.reflected}\right)^2}{2\cdot\sigma_z^2(x)}\right)\right\} \qquad \text{Equation 20}$$

$$z_{c,reflected} = 2\cdot MH - h_{max} \qquad \text{Equation 21}$$

- If $z \geq MH$

  When the vertical coordinate of study is situated above the mixing layer height, and the plume has partly penetrated the mixing layer, a different situation occurs. In this case, the reflection from the mixing layer height (R_{MH}) and from the ground (R_G) does not need to be included, because the upper part of the plume will only dilute upwards.

$$F_z(x,z) = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\exp\left[-\frac{(z-z_c)^2}{2\cdot\sigma_z^2(x)}\right]\cdot CF \qquad \text{Equation 22}$$

$$\text{If } P(x) > 0 \quad CF = \frac{P(x_f)}{P(x)} \qquad \text{Equation 23}$$

$$\text{If } P(x) \leq 0 \quad CF = 0 \qquad \text{Equation 24}$$

<u>If $h_{max} \geq MH$</u>

If the maximum height of the plume is situated <u>above the mixing layer height</u>, then $P > 0.5$. In this case, the penetration fraction needs to be evaluated, because it is highly relevant for the dilution of the plume concentration. In the situation where $P = 1$, the smoke plume will be fully trapped above the mixing layer (see left picture in Figure 2), hence, the (toxic) combustion products will not disperse back below the mixing layer. However, in some other cases the plume will not fully penetrate the mixing layer ($P < 1$). Therefore, for the mass fraction below mixing layer, reflection against the ground needs to be taken into account (see right picture in Figure 2).

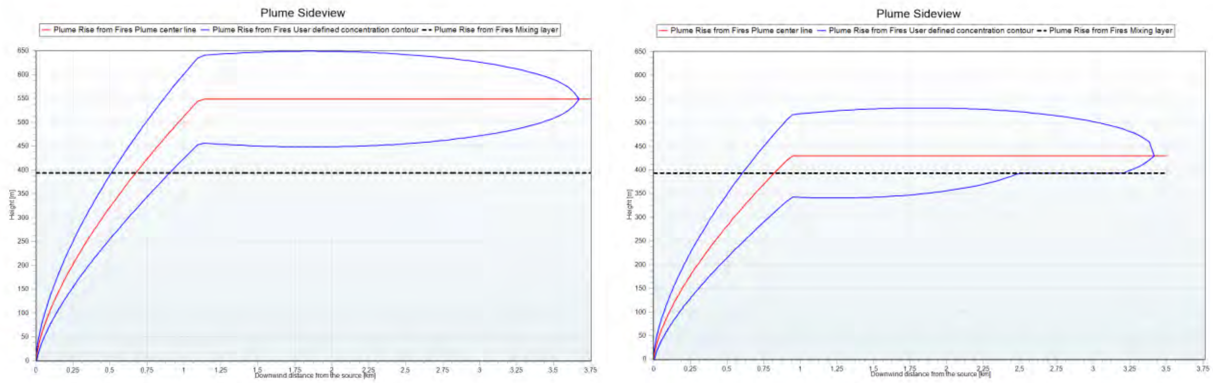


Figure 2. Plume with a maximum height situated above the mixing layer height with full penetration (left) and partial penetration (right)

In order to be able to describe the full trajectory of the plume, the calculation needs to include two different approaches to calculate the vertical dispersion depending on whether the vertical coordinate of study is below or above the mixing layer height for every distance evaluated.

- If $z < MH$

  When the vertical coordinate of study is situated below the mixing layer height and $P < 1$, the plume will not fully penetrate the mixing layer. In this case, the reflection from the ground (R_G) need to be evaluated for the mass fraction that has not penetrated the mixing layer. However, the reflection from the mixing layer height (R_{MH}) does not need to be included because the maximum height of the plume is already above the mixing layer height, where this reflection phenomena will not occur.

$$F_z(x,z) = CF \cdot \left(\frac{1}{\sqrt{2 \cdot \pi} \cdot \sigma_z(x)} \cdot \exp\left[-\frac{(z - z_c)^2}{2 \cdot \sigma_z^2(x)} \right] + R_G \right) \quad \text{Equation 25}$$

$$\text{If } P(x) < 1 \quad CF = \frac{1 - P(x_f)}{1 - P(x)} \quad \text{Equation 26}$$

$$\text{If } P(x) \geq 1 \quad CF = 0 \quad \text{Equation 27}$$

- $z \geq MH$

  When the vertical coordinate of study is situated above the mixing layer height, the plume will fully or partly penetrate the mixing layer. This is typically because the plume does have enough momentum to penetrate the mixing layer due to its heat of combustion. In this case, the reflection from the mixing layer height (R_{MH}) needs to be evaluated because it is possible that not all the plume penetrates though the mixing layer. However, the reflection from the ground (R_G) does not need to be considered because the vertical coordinate of study is above the mixing layer height, hence, this phenomenon is not relevant.

$$F_z(x,z) = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\exp\left[-\frac{(z-z_c)^2}{2\cdot\sigma_z^2(x)}\right] + CF\cdot R_{MH} \qquad \text{Equation 28}$$

In this case, the correction factor (CF) is calculated in the same way as expressed in Equation 19, the height of the reflected centerline of the plume ($z_{c,reflected}$) is calculated as expressed in Equation 21, and the reflection against the mixing layer height (R_{MH}) is calculated as indicated in the equation below.

$$R_{MH} = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\left\{\exp\left(-\frac{\left(MH+z_{c,reflected}\right)^2}{2\cdot\sigma_z^2(x)}\right) + \exp\left(-\frac{\left(MH-z_{c,reflected}\right)^2}{2\cdot\sigma_z^2(x)}\right)\right\} \qquad \text{Equation 29}$$

2.2.2.2 Plume is rising

While the plume is rising, the penetration fraction might still be increasing as a function of distance. The only correction required in the calculation of vertical dispersion is the reflection against the ground (R_G). This is because any part of the plume reaching this mixing layer boundary, will always penetrate through the mixing layer height due to the density differences.

Additionally, a calculation approach is used when the vertical coordinate of study is below the centerline of the plume. This allows the plume rise model to separate the penetrating behavior of the fraction of the plume that is below the centerline of the cloud, from the fraction of the plume above the centerline of the cloud.

$$F_z(x,y) = \frac{1}{\sqrt{2\cdot\pi}\cdot\sigma_z(x)}\cdot\exp\left[-\frac{(z-z_c)^2}{2\cdot\sigma_z^2(x)}\right] + R_G \qquad \text{Equation 30}$$

2.2.3 Crosswind and vertical wind dispersion parameters

The purpose of the crosswind (σ_y) and vertical wind (σ_z) dispersion parameters of the smoke plume is to account for dilution in the crosswind and vertical wind directions. The reflection of the plume at the ground can be accounted for by assuming an image source at distance "x" beneath the ground surface. These dispersion parameters can be calculated as follows.

$$\sigma_y(x) = \left(\frac{t'}{600}\right)^{0,2}\cdot a\cdot {X_d}^{b} \qquad \text{Equation 31}$$

$$\sigma_z(x) = (10\cdot z_0)^{0,53\cdot {X_d}^{-0,22}}\cdot c\cdot {X_d}^{d} \qquad \text{Equation 32}$$

For a, b, c and d the values according to the following table are applicable [2]:

Pasquill Class	a	b	c	d
Very unstable (A)	0.527	0.865	0.28	0.90
Unstable (B)	0.371	0.866	0.23	0.85
Slightly unstable (C)	0.209	0.897	0.22	0.80
Neutral (D)	0.128	0.905	0.20	0.76
Stable (E)	0.098	0.902	0.15	0.73
Very stable (F)	0.065	0.902	0.12	0.67

Table 1. Value of the parameters a, b, c and d depending on the Pasquill stability class

2.3 Ad-hoc formulas

2.3.1 Virtual source

The concept of virtual source is included in the plume rise model to account for the initial area of the warehouse fire. The virtual source corresponds to a point located below ground level and back from the actual source location that gives an equivalent horizontal cross-sectional area to the actual source (V_y) and an equivalent vertical cross-sectional area to the actual source (V_z). The parameters a, b, c and d can be chosen as described in paragraph 2.2.3.

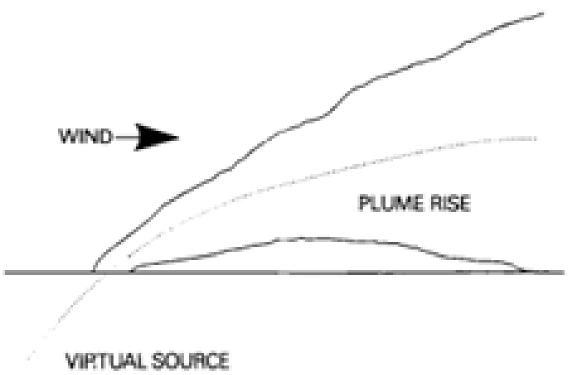


Figure 3. Graphic representation of a virtual source as depicted in Carter, 1989 [6]

$$V_y = \left(0.5 \cdot \frac{D}{a}\right)^{\frac{1}{b}}$$ Equation 33

$$V_z = \left(0.5 \cdot \frac{D}{c}\right)^{\frac{1}{d}}$$ Equation 34

2.3.2 Brunt-Vaisala frequency

The Brunt-Vaisala frequency (N) can be calculated for Pasquill stability class E and F using the data in Table 2.

$$N = \sqrt{\frac{g}{T_a} \cdot \left(\frac{\partial T_a}{\partial z} + 0.01\right)}$$ Equation 35

Pasquill stability class	$\delta T_a/\delta z$ ($K \cdot m^{-1}$)	Average N
E	-0.005 to 0.015	0.005
F	Bigger than 0.015	0.028

Table 2. Average Brunt-Vaisala frequency according to the Pasquill stability class

2.3.3 Inverse Monin-Obukhov length

The Inverse Monin-Obukhov length (1/L) can be calculated for different stability classes using the data in Table 3.

$$\frac{1}{L} = \frac{1}{L_{MO}} \cdot \log_{10}\left(\frac{z_0}{Z_{MO}}\right)$$ Equation 36

Pasquill stability class	L_{MO} [m]	Z_{MO} [m]
A	33,162	1117
B	32,258	11,46
C	51,787	1,324
D	∞	Not applicable
E	-48,330	1,262
F	-31,325	19,36

Table 3. Constants needed for the calculation of the inverse Monin-Obukhov length

2.3.4 Mixing layer height

The atmospheric mixing layer height (MH) is usually capped by a sharp elevated inversion which blocks dispersion of substances emitted near the ground from mixing further upwards.

Pasquill stability class	1/L	MH [m]
E, F	>0	$0.4 \cdot \sqrt{u_* \cdot L/f}$
D	0	$\min(0.2 \cdot u_*/f, 500)$
C	<0	1000
B		1500
A		1500

Table 4. Calculation of the mixing layer height according to the Pasquill stability class

Where Equation 37 is used to calculate frequency and Equation 38 to calculate friction velocity.

$$f = 2 \cdot \Omega \cdot \sin \phi$$ Equation 37

$$u_* = k \cdot \frac{u_w(z_{10})}{f\left(\frac{z_{10}}{z_0}, L\right)}$$ Equation 38

The velocity functions are calculated as follows. Note that if z>100m then z=100m must be used.

$$\begin{cases} f\left(\frac{z_{10}}{z_0}, L\right) = \ln\frac{z_{10}}{z_0} + 5 \cdot \frac{(z_{10} - z_0)}{L} & \text{for } \frac{1}{L} > 0 \\ f\left(\frac{z_{10}}{z_0}, L\right) = \ln\frac{z_{10}}{z_0} - \Psi\left(\frac{z_{10}}{L}\right) + \Psi\left(\frac{z_0}{L}\right) & \text{for } \frac{1}{L} \leq 0 \end{cases}$$ Equation 39

$$\Psi\left(\frac{z}{L}\right) = 2 \cdot \ln\left(\frac{1 + \Psi'}{2}\right) + \ln\left(\frac{1 + \Psi'^2}{2}\right) - 2 \cdot \arctan(\Psi') + \frac{\pi}{2}$$ Equation 40

$$\Psi' = \left(1 - 16 \cdot \frac{z}{L}\right)^{\frac{1}{4}}$$ Equation 41

2.3.5 Wind speed at height of study

According to the Nieuw Nationaal Model [7] the wind speed at a height of study can be calculated as follows.

$$u_w(z) = u_w(z_{10}) \cdot \frac{\ln\left(\frac{z}{z_0}\right) - \Psi\left(\frac{z}{L}\right) + \Psi\left(\frac{z_0}{L}\right)}{\ln\left(\frac{z_{10}}{z_0}\right) - \Psi\left(\frac{z_{10}}{L}\right) + \Psi\left(\frac{z_0}{L}\right)}$$ Equation 42

Depending on whether the inverse Monin-Obukhov length (1/L) is positive or negative, the empirical functions are described differently.

- If $L < 0$

$$\Psi\left(\frac{z}{L}\right) = 2 \cdot \ln\left(\frac{1 + \Psi'}{2}\right) + \ln\left(\frac{1 + \Psi'^2}{2}\right) - 2 \cdot \arctan(\Psi') + \frac{\pi}{2}$$ Equation 43

$$\Psi' = \left(1 - 16 \cdot \frac{z}{L}\right)^{\frac{1}{4}}$$ Equation 44

- If $L \geq 0$

$$\Psi\left(\frac{z}{L}\right) = -17 \cdot \left(1 - e^{\frac{-0.29 \cdot z}{L}}\right)$$ Equation 45

The value of z in the empirical function ψ (z/L) can be substituted by the surface roughness length (z_0), a stack height of 10 m (z_{10}) or the height of study (z), depending on which empirical function needs to be used.

3 Validation

The validation of the “plume rise from warehouse fires model” is performed by comparing the results given with EFFECTS with measurements from field experiments and with other already validated mathematical models. The validation includes a description of each validation experiment and a detailed discussion of the results obtained from a statistical and graphical comparison against the field data.

Each experiment set is statistically evaluated to determine the accuracy and precision of the “plume rise from warehouse fires model” model predictions versus the observed data. The fraction of predictions within a factor of two of the measurements is analyzed and represented in a scatter plot. Note that the quantitative acceptance criteria for FAC2 is that $0.5 \leq \mathrm{FAC2} \leq 2$ (see Equation 46).

$$0.5 \leq \left(\mathrm{FAC2} = \frac{C_p}{C_m}\right) \leq 2 \qquad \text{Equation 46}$$

3.1 Validation of the concentration

The investigation presented by Hall, Kukadia, Walker & Marsland [8] is used to validate the concentration of the rising plume as implemented in EFFECTS. This investigation examines a variety of fire plume discharges in a small-scale wind tunnel. For more information about the experimental conditions please refer to the original literature as presented by Hall, Kukadia, Walker & Marsland [8].

The following figure shows experimental ground level concentrations downwind of the source for discharges with buoyancy only, where S, T, U, V, W, and X correspond to different experimental data which represent different buoyancy conditions. The validation in Figure 4 shows that the simulation of S, T, U, V and W present good agreement with the experimental data. The simulation of X shows over-predicted values for downwind distances very close to the source.

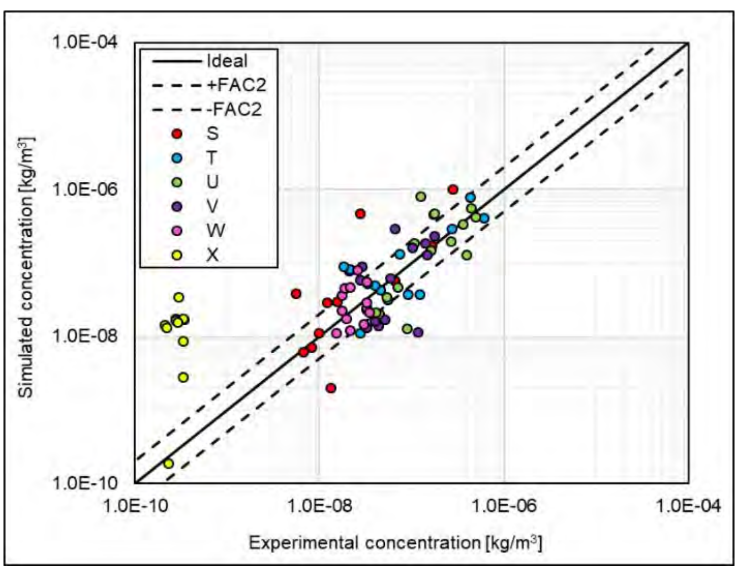


Figure 4. Validation of the Gexcon’s model against Hall’s experimental data. Buoyancy only

The following figure shows experimental ground level concentrations downwind of the source with a combination of buoyancy and discharge momentum. W1, W2, W3, W4, X1, X2, Y1, and Y2 correspond to different experimental data which represent different conditions of buoyancy and momentum flux. The validation in Figure 5 shows that the simulation of W1, W2, W4 and X1 present good agreement with the experimental data. The simulation of W3, X2, Y1 and Y2 show under-predicted values for downwind distances relatively close to the source.

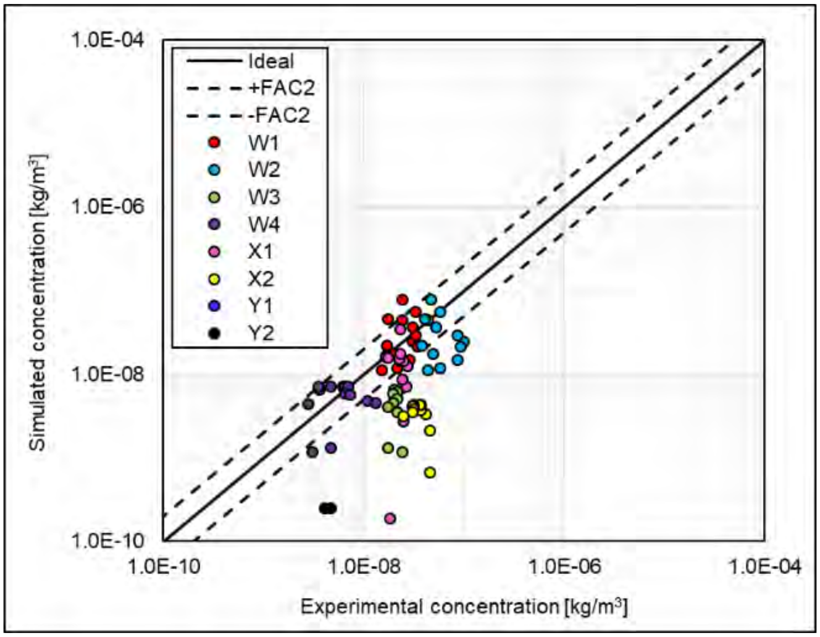


Figure 5. Validation of Gexcon's model against Hall's experimental data. Buoyancy & momentum

3.2 Validation of the plume height

Briggs [1] collected a series of experimental data for rising plumes, namely: Harwell, Bosanquet, Darmstadt, Duisburg, Tallwarra, Lakeview, CEGB plants, Earley, Castle Donington, Northfleet, TVA plants, Shawnee, Colbert, Johnsonville, Widows Creek, Gallatin and Paradise. The already validated theoretical formulas listed below, are used to assess EFFECTS' performance against this experimental data and compared with other validated theoretical formulas to calculate the maximum height of the plume.

- Moses & Carson, 1967

  Moses & Carson [9] developed a formula for ten different stacks. The least-squares fit was given by the empirical equation described in the equation below.

$$h_{\mathrm{max}} = 1.81\left[\frac{\mathrm{ft}^2/\mathrm{s}}{(\mathrm{cal/s})^{1/2}}\right]\cdot\frac{Q_H^{\frac{1}{2}}}{u_w(z_s)} \qquad \text{Equation 47}$$

- Stümke, 1963

  Stümke [14] derived the empirical formula described in Equation 48, on the basis of data from four stacks, namely, the Harwell stack [10-11], Moses and Strom's experimental stack [12], and the two stacks reported by Rauch [13].

$$h_{max} = 1.5 \cdot \left(\frac{w_0}{u_w(z_s)}\right) \cdot D + 118 \left[\frac{m^{\frac{1}{2}}}{s}\right] \cdot D^{\frac{3}{2}} \cdot \left(1 + \frac{\Delta T}{T_s}\right)^{\frac{1}{4}} \cdot u_w(z_s)^{-1} \qquad \text{Equation 48}$$

- Holland
  The equation for the calculation of the plume rise phenomenon developed by Holland was developed based on photographs taken at three steam plants near Oak Ridge, Tennessee [15]. Holland found the best fit to the data with the empirical equation detailed in Equation 49.

$$h_{max} = 1.5 \cdot \left(\frac{w_0}{u_w(z_s)}\right) \cdot D + 4.4 \cdot 10^{-4} \left[\frac{ft^2/s}{cal/s}\right] \cdot \frac{Q_H}{u_w(z_s)} \qquad \text{Equation 49}$$

- Priestley
  Priestley [16] developed Equation 50 which assumes that atmospheric turbulence dominates the mixing while plume rise occurs.

$$h_{max} = 2.7 \left[\left(\frac{ft}{s}\right)^{\frac{1}{4}}\right] \cdot F^{\frac{1}{4}} \cdot u_w(z_s)^{-1} \cdot x^{\frac{3}{4}} \qquad \text{Equation 50}$$

- Lucas, Moore & Spurr
  Lucas, Moore & Spurr [17] fitted observed plume rises at two of their plants with Equation 51. The formula is based on a simplification of Priestley's theoretical plume-rise model.

$$h_{max} = 258 \left[\frac{ft^2/s}{(cal/s)^{\frac{1}{4}}}\right] \cdot \frac{Q_H^{\frac{1}{4}}}{u_w(z_s)} \qquad \text{Equation 51}$$

- Lucas
  Lucas [18] noted some correlation with stack height and suggested a modification of the equation developed by Lucas, Moore & Spurr. This equation (see Equation 52) is not suited to plants with heat emission less than 10 MW because it predicts continued plume rise to almost 1 km downwind regardless of source size.

$$h_{max} = (134 + 0.3 \cdot z_s) \left[\frac{ft^2/s}{(cal/s)^{\frac{1}{4}}}\right] \cdot \frac{Q_H^{\frac{1}{4}}}{u_w(z_s)} \qquad \text{Equation 52}$$

- Briggs, 1969
  Briggs developed a theoretical model to predict penetration of a sharp elevated inversion of height through which the temperature increases. For the first stage of the rise, the bent-over model predicts the centerline for buoyant plumes in neutral conditions and it is given by the expression in Equation 53. This equation, which corresponds to Equation 4.32 in Briggs' publication [1], can be used up to the distance at which atmospheric turbulence dominates entrainment.

$$h_{max} = 1.8 \cdot F^{\frac{1}{3}} \cdot u_w(z_s)^{-1} \cdot x^{\frac{2}{3}} \qquad \text{Equation 53}$$

Once the distance at which atmospheric turbulence dominates entrainment is reached (x^*), the following equation can be used to simulate the complete plume centerline. This equation should not be applied beyond $x = 5 \cdot x^*$, because so few data go beyond this distance. This equation corresponds to Equation 4.34 in Briggs' publication [1].

$$h_{max} = 1.8 \cdot F^{\frac{1}{3}} \cdot u_w(z_s)^{-1} \cdot x^{*\frac{2}{3}} \cdot \left[\frac{2}{5} + \frac{16}{25} \cdot \frac{x}{x^*} + \frac{11}{5} \cdot \left(\frac{x}{x^*}\right)^2\right] \cdot \left(1 + \frac{4}{5} \cdot \frac{x}{x^*}\right)^{-2} \qquad \text{Equation 54}$$

The validation in the figure below shows that the simulation of the plume rise phenomenon with the "plume rise from warehouse fires model" as implemented in EFFECTS present very good agreement with experimental data. Moreover, from all the theoretical formulas collected in the publication of Briggs [1] and described in the present study, the equations implemented in EFFECTS (described in chapter 2**Error! Reference source not found.**) present the best agreement with experimental data.

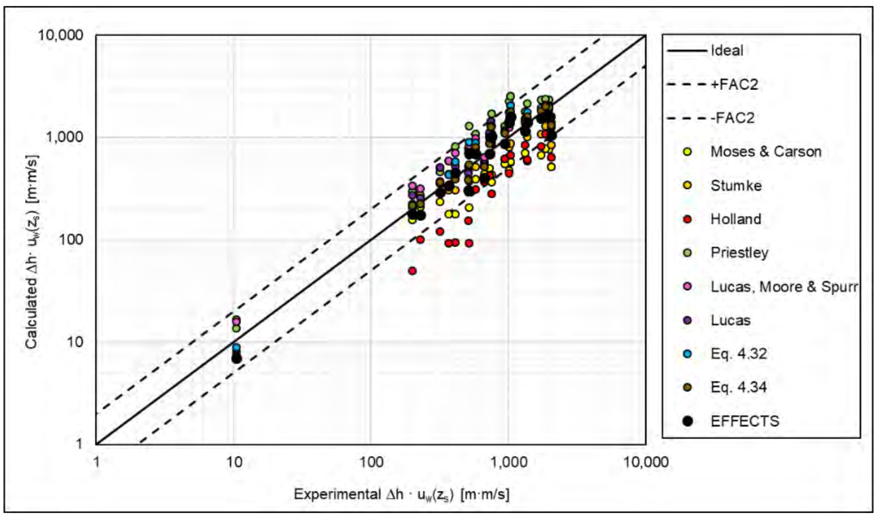


Figure 6. Validation of Gexcon's model against the already validated theoretical formulas

On the other hand, the formulas of Moses & Carson (Equation 47), Stümke (Equation 48) and Holland (Equation 49) are completely empirical and do not allow for the effect of distance of measurement on plume rise as the other formulas do. Consequently, these three formulas give poorer agreement with data. The Holland formula (Equation 49) shows a high percentage of scatter. Priestley's formula (Equation 50) is an asymptotic formula which predicts a rise proportional to $x^{3/4}$. This is a transitional-rise formula which shows less scatter compared with observations than the formulas of Moses & Carson, Stümke and Holland. Lucas, Moore & Spurr's formula (Equation 51) includes both a transitional and a final-rise stage and gives a little better agreement with experimental data. When Lucas, Moore & Spurr's formula is multiplied by the empirical stack-height factor suggested by Lucas (Equation 52), the agreement is considerably better. Brigg's formula (Equation 53) is based on the "2/3 law", which is another transitional-rise formula, and agrees well with the experimental data. The other Brigg's formula (Equation 54), which includes both a transitional-rise and a final-rise stage, gives both improved numerical agreement and much less percentage of scatter.

4 Results

In this chapter the results obtained with the "plume rise from warehouse fires model" as implemented in the software package EFFECTS are presented. For all the figures included in this chapter, the **black dashed line** corresponds to the mixing layer height, the **red line** corresponds to the centerline of the rising plume and the **dark green line** corresponds to the side view contour for a threshold concentration of 1 mg/m^3. The **dark blue line**, **light green line** and **pink line** correspond to the side view contour for a threshold concentration corresponding to PAC-1, PAC-2 and PAC-3 of Carbon (soot); respectively.

4.1 Plume penetrating the mixing layer

In the left picture of Figure 7 an example is given for a fully penetrating plume (P = 1) calculated with EFFECTS. In this case, soot is the pollutant being evaluated which comes from a fire with a convective heat of production of 30 MW. The soot formation rate at those conditions is 0.28 kg/s. The Pasquill stability class evaluated is D2 (neutral). The roughness length description is based on scattered large objects.

In the right picture of Figure 7 an example is given for a fully penetrating plume (P = 1) calculated with EFFECTS which experiences reflection from the mixing layer which prevents the (toxic) combustion products to disperse below the mixing layer. In this case, the same conditions as the previous example are used, except from the fire's convective heat of production which is reduced to 20 MW.

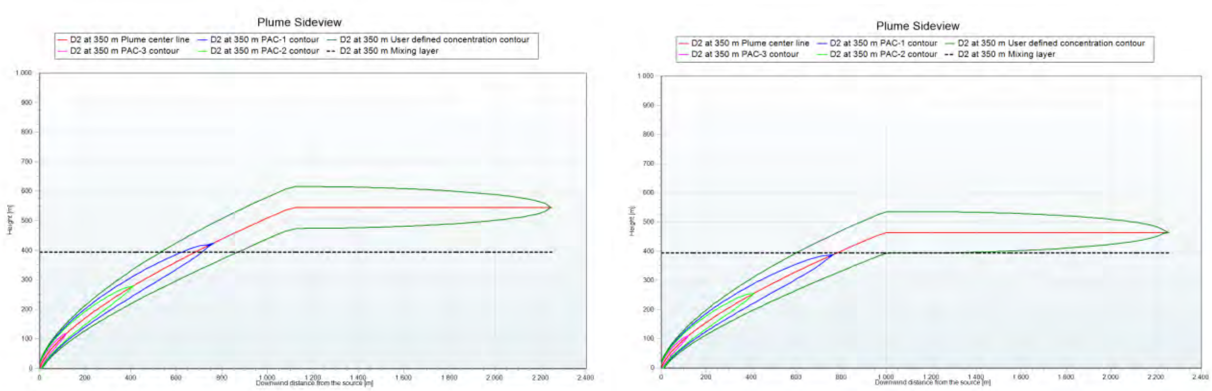


Figure 7. Plume fully penetrating the mixing layer (P = 1) without R_{MH} (left) and with R_{MH} (right)

In the left picture of Figure 8 an example is given for a partly penetrating plume (P < 1) calculated with EFFECTS which experiences reflection from the mixing layer upon penetration. In this case, the same conditions as the previous example are used, except from the fire's convective heat of production which is reduced to 5 MW.

In the right picture of Figure 8 an example is given for a partly penetrating plume (P = 0.5) calculated with EFFECTS which experiences reflection from the ground in the fraction of the plume that remains below the mixing layer height. In this case, the same conditions as the previous example are used, except from the fire's convective heat of production which is reduced to 4 MW. As it can be seen from the figure below the mixing layer is located at the same height as the plume centerline.

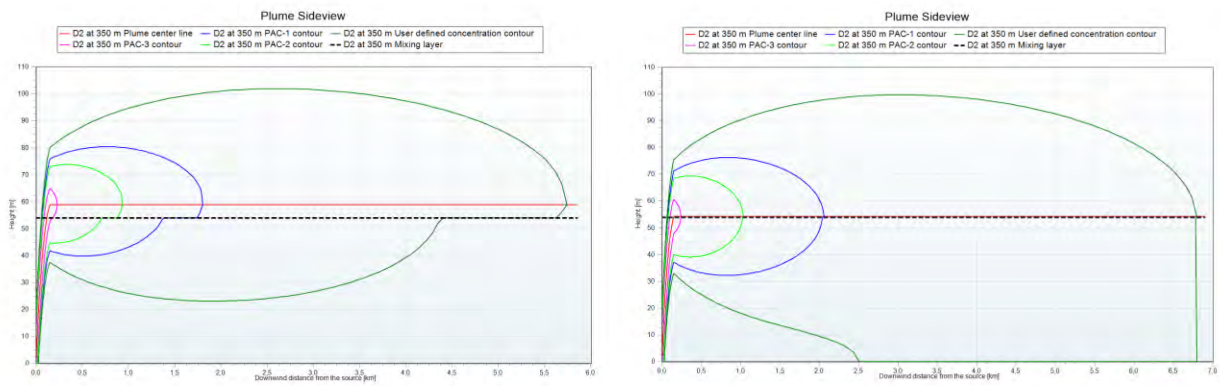


Figure 8. Plume partly penetrating the mixing layer (P < 1) with R_{MH} (left) and with R_G (right)

4.2 Plume non-penetrating the mixing layer

In the left picture of Figure 9 an example is given for a non-penetrating plume (P = 0) calculated with EFFECTS. In this case, the same conditions as the previous example are used, except from the fire's convective heat of production which is increased to 10 MW and the atmospheric stability is changed to D2 (neutral).

In the right picture of Figure 9 an example is given for a non-penetrating plume (P = 0) calculated with EFFECTS which experiences reflection from the ground. In this case, the same conditions as the previous example are used, except from the fire's convective heat of production which is reduced to 1 MW.

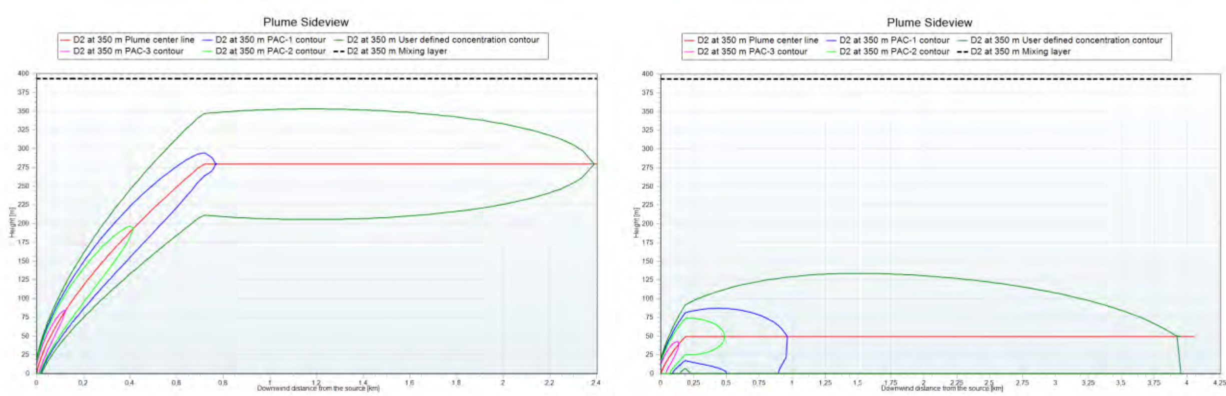


Figure 9. Plume not penetrating the mixing layer (P = 0) without reflection (left) and with R_G (right)

5 Conclusions and future work

5.1 Conclusions

The “plume rise from warehouse fires model” is a model implemented in the software package EFFECTS to calculate the plume rise phenomenon due to warehouse fires. The model is based on the theory presented on Briggs’ study [1], the theory in the Yellow Book [2] and corrected with Mill’s correction for burning fires [3].

Additionally, a mathematical approach for the calculation of the potential penetration of the plume through the atmospheric mixing layer has been developed by Gexcon and implemented in EFFECTS. This modelling approach allows the modeler to include in the calculations of plume rise, that all mass that has risen above the mixing layer, will never disperse back into the mixing layer. Therefore, for such conditions, (toxic) combustion products will never create chemical exposure at ground level.

Furthermore, another mathematical approach has been included to simulate the reflection phenomena which will “trap” the smoke plume below or above the mixing layer. This phenomenon is highly relevant because if the plume is “trapped” below the mixing layer, there could be more severe consequences for individuals at ground level exposed to toxic combustion products.

The “plume rise from warehouse fires model” has been extensively validated against experimental data and against other widely used and validated mathematical models. The results of the simulations with the “plume rise from warehouse fires model” as implemented in EFFECTS, present not only very good agreement with experimental data but also the best agreement compared to other already validated mathematical formulas.

5.2 Future work

The warehouse fire phenomenon creates a toxic combustion product plume that can affect a very large area. Nevertheless, the traditional “homogeneous wind-field” dispersion modelling of such a toxic plume can become unreliable because of the potential long distance of dangerous concentrations (>10 km). At these long distances, the wind direction and wind velocity may have changed, as these atmospheric parameters are not constant at every location and height.

The “plume rise from warehouse fires model” uses a homogenous wind field. However, the toxic plume will show a meandering behavior and may bend into different directions at different heights or after some time.

For this reason, the “plume rise from warehouse fires model” has been extended to account for the meandering of the plume due to time and location dependent meteorological conditions. This extension, called the “dynamic plume rise model”, uses on-line meteorological data and has been implemented as a web-based GIS tool, called RESPONSE.

RESPONSE is currently available as a demonstrator and uses real-time meteorological data to calculate actual and realistic hazard zones of a chemical accident. If properly integrated into control rooms, RESPONSE could allow emergency response organizations to immediately evaluate potential hazard zones, and to make well-founded decisions on alarming, evacuation and repression actions that will minimize social disruption, and potential damage to people, constructions and infrastructure.

Experimental data and previous experience with this phenomenon show that warehouse fires rarely produce hazardous concentrations at environment level. This is caused by the fact that the plume rise effect will usually force the fumes high up in the sky, potentially penetrating the mixing layer. This maximum height of the plume is highly influenced by the heat production and combustion efficiency of the fire. Firemen may try to extinguish the fire, which leads to less plume rise behavior. Therefore, feedback on the resulting plume height is very important to potentially correct the plume path and concentration predictions. In order to do this, access to sensor data, information from drones or observation reports could be connected to the modelling to make predictions more reliable.

The RESPONSE framework is intended for its integration as an additional module into existing Emergency Services GIS environments. Hence, it should be customized towards the specific user, who can define dedicated accident scenarios and use specific hazard level contours.

In the figure below, it is depicted the RESPONSE interface illustrating a meandering smoke plume, using location and time specific wind field.

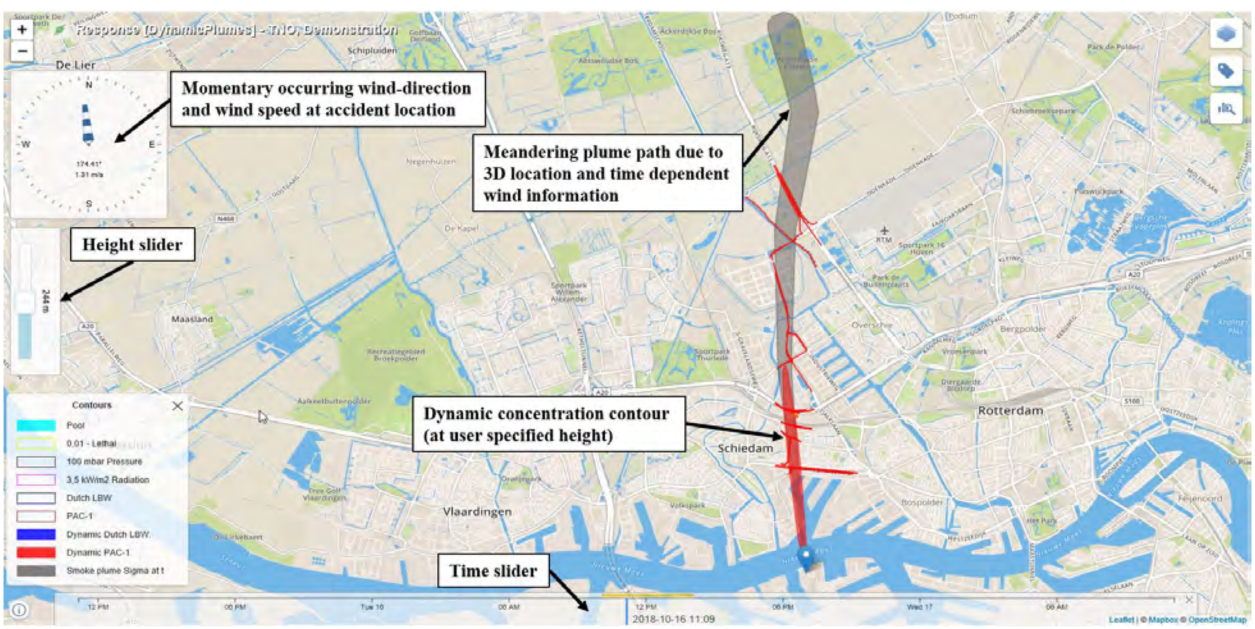


Figure 10. RESPONSE demonstrator showing a dynamic smoke plume using time specific wind field

6 Nomenclature

a, b, c, d	Constant parameters that depend on the Pasquill stability class (Table 1)	[-]
b_{oy}	Source half dimension in crosswind direction	[m]
b_{oz}	Source half dimension in vertical direction	[m]
C(x,y,z)	Downwind concentration at coordinate (x, y, z)	[kg/m^3]
CF	Correction factor	[-]
C_m	Measured (experimental) value	NA
C_p	Predicted (simulated) value	NA
D	Diameter of the fire / internal stack diameter	[m]
Erf	Gauss error function	[-]
f	Coriolis parameter	[s^{-1}]
F	Buoyancy flux parameter	[m^4/s^3]
F_y (x,y)	Parameter to describe the lateral (crosswind) dispersion	[-]
F_z (x,z)	Parameter to describe the vertical dispersion	[-]
g	Gravity	[m/s^2]
h_{BRIGGS}	Plume rise due to buoyancy according to Briggs	[m]
h_{max}	Maximum height of the plume	[m]
h_{MILLS}	Plume rise according to the Mills correction	[m]
k	Von Karman constant	[0.4]
L	Monin-Obukhov length	[m]
L_{MO}	Constant for the calculation of the Monin-Obukhov length	[m]
MH	Mixing layer height	[m]
N	Brunt-Vaisala frequency	[s^{-2}]
P(x)	Penetration fraction at distance x	[-]
P(x_f)	Penetration fraction at distance x_f	[-]
q_F	Formation rate	[kg/s]
Q_0	Initial heat flux	[kcal/s]
Q_H	Total heat rate	[kcal/s]
R_G	Reflection against the ground	[-]
R_{MH}	Reflection against the mixing layer height	[-]
t'	Averaging time	[s]
T_a	Ambient temperature	[K]
T_s	Average absolute temperature of gases emitted from stack	[K]
u_*	Friction velocity	[m/s]
u_w (z)	Wind speed at height of study	[m/s]

u_w (z_{10})	Wind speed at a height of 10 m	[m/s]
u_w (z_c)	Wind speed at the centerline of the plume	[m/s]
u_w (z_s)	Wind speed at stack height	[m/s]
V_y	Virtual source for vertical cross-section area equivalent to actual source	[m]
V_z	Virtual source for horizontal cross-section area equivalent to actual source	[m]
w_0	Efflux speed of gases from stack	[m/s]
x	Downwind distance	[m]
x^*	Distance at which atmospheric turbulence dominates entrainment	[m]
x_f	Downwind distance at which the plume reaches its maximum height	[m]
X_d	$x_f + V_z$	[m]
y	Crosswind horizontal coordinate	[m]
z	Vertical upward coordinate or height of study	[m]
z_0	Surface roughness length	[m]
z_{10}	Height of 10 m	[m]
z_c	Plume centerline	[m]
$z_{c,reflected}$	Height of the reflected centerline of the plume	[m]
z_s	Stack height	[m]
Z_{MO}	Constant for the calculation of the Monin-Obukhov length	[m]
ΔT	Temperature excess of stack gases	[K]
γ	Entrainment coefficient for buoyant plume rise	[-]
σ_y (x)	Crosswind dispersion parameter of the cloud	[m]
σ_z (x)	Vertical dispersion parameter of the cloud	[m]
ϕ	Earth's latitude	[°N]
$\Psi(z/L)$	Empirical function	[-]
Ψ'	Empirical function	[-]
Ω	Earth's rotational speed ($7.27\cdot10^{-5}$)	[s^{-1}]

7 References

[1] Briggs, G. Plume Rise. Air Resources Atmospheric Turbulence and Diffusion Laboratory. Environmental Science Services Administration. Oak Ridge, Tennessee. 1969.

[2] Yellow Book. Methods for the calculation of physical effects due to release of hazardous materials (liquids and gases). CPR14E. 2nd Edition, 1992. The Hague, The Netherlands.

[3] M.T. Mills. Modelling the release and dispersion of toxic combustion products from chemical fires. International Conference on Vapor Cloud Modelling. November 1987. Boston, Massachusetts.

[4] Morton, B., Taylor, G., & Turnen, J. Turbulent Gravitational Convection from Maintained and Instantaneous Sources. Proceedings of the Royal Society of London. 234: 1-23. 1956. London, UK.

[5] C. Zonato, A. Vidili, R. Pastorino and D.M. de Faveri. Plume rise of smoke coming from free burning fires. Journal of Hazardous Materials, 34: 69-79. 1993. November 28, 1991. Italy.

[6] Carter, D. Methods for estimating the dispersion of toxic combustion products from large fires. Chemical Engineering Research & Design. 67: 348-352. 1989.

[7] TNO Milieu, Energie en Procesinnovatie. Het Nieuwe Nationaal Model. Model voor de verspreiding van luchtverontreiniging uit bronnen over korte afstanden. Apeldoorn, 1998. TNO Rapportnummer RR 98/306.

[8] Hall, D., Kukadia, V., Walker, S., & Marsland, G. Watford. Plume dispersion from chemical warehouse fires. Building Research Establishment. UK, 1995.

[9] Moses, H., & Carson, J. Stack design parameters influencing plume rise. 60th Annual Meeting of the Air Pollution Control Association. 67-84. Cleveland, Ohio, 1967.

[10] Stewart, N., Gale, H., & Crooks. The atmospheric diffusion of gases discharged from the chimney of the Harwell Pipe (BEPO). British Report AERE HP/R-1452, R-1954.

[11] Stewart, N., Gale, H., & Crooks. The atmospheric diffusion of gases discharged from the chimney of the Harwell reactor (BEPO). International Journal of Air and Water Pollution. 87-102. R-1958.

[12] Moses, H., & Strom, G. A comparison of observed plume rises with values obtained from well-known formulas. Journal of Air Pollution. 455-466. 1961.

[13] Rauch, H. Zur Schornstein - Überhöhung. Beiträge zur Physik der Atmosphäre, 37: 132-158. Translated in USAEC Report ORNL-tr-1209. 1964.

[14] Stümke, H. Suggestions for an empirical formula for chimney elevation. Oak Ridge National Laboratory, 23: 549-556. Translated in USAEC Report ORNL-tr-977. 1963.

[15] A meteorological survey of the Oak Ridge Area: Final report covering the period 1948-1952. USAEC Report ORO-99. U.S. Weather Bureau. 554-559. 1953.

[16] Priestley, H. A working theory of the bent-over plume of hot gas. Quarterly Journal of the Royal Meteorology Society, 82: 165-176. 1956.

[17] Lucas, D., Moore, D., & Spurr, G. The rise of hot plumes from chimneys. International Journal of Air and Water Pollution, 7: 473-500. 1963.

[18] Lucas, D. Application and evaluation of results of the Tilbury plume rise and dispersion experiment. Journal of Atmospheric Environment, 1: 421-424. 1967.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Collision of Convex Objects for Calculation of Porous Mesh in Gas Explosion Simulation

Tatiele Dalfior Ferreira and Sávio Souza Venâncio Vianna*
University of Campinas
Albert Einstein 500. Campinas. SP – Brazil
*Presenter E-mail: svianna@unicamp.br

Abstract

We investigate the coupling of the flamelet combustion model with the collision distance algorithm for entertainment games. The collision algorithm is coded to calculate the porosity of the geometry based on the PDR (Porosity Distributed Resistance) approach for modelling of complex geometries. The turbulent field generated by the interaction of the flow with the porous objects is used to calculate the wrinkling length scale of the flame via the fluctuating velocities. The turbulent fluxes are amended in accordance with assigned porosities at the cell faces. The combustion and porosity models are implemented in the framework of an in house Fortran code that solves the full set of Navier-Stokes equations. Results are presented for non-reacting flows and reacting flows over a bluff body for Re=44,000 and Ka=1 (Reynolds and Karlovitz numbers, respectively). Numerical findings are compared with standard commercial CFD tools.

Keywords: Collision Algorithm, CFD, Vapor Cloud Explosion

1 Introduction

The numerical simulation of turbulent flows requires special attention to the so-called ”small scales” objects. Since such objects increase the generation of turbulence, they must be considered in the flow modelling, which poses an extra challenge when building the computational grid. Even if Reynolds averaged Navier - Stokes equations are solved, the capturing of all details of the complex geometry leads to extremely expensive cost from the computational point of view [1]. When considering reacting flows, such deflagrations and detonations, the problem is even worst as the wrinkling of the area of flame front is highly dependant on the generation of turbulence. To overcome this limitation, researchers have pursued the parametrisation of the geometry based on PDR (Porosity Distributed Resistance) approaches [1] [2] [3].

Unfortunately, the representation of a complex geometry, such those commonly found in real engineering problems, is not straightforward. Little documentation is found where details on how the porous is calculated is presented. Most of the research works are focused on the results rather than providing details on how the porous representation of the geometry has been built.
We reasoned that the flux through the face of the computational cells as well as the rate of change in the control volume can be amended based on the collision of two objects as if the objects are treated as collision parts in video games that consider the collision between players [4] [5]. In order to develop the method that accounts for all details of the geometry, the geometrical model was built in a CAD tool ensuring that all parts of the geometry are treated as a set of triangles.
The stereolithography (STL) CAD files are widely used for quick prototyping as well as for computer-aided manufacturing. The main advantage is that the STL files describes the geometry as unstructured triangulated surface by the normal and nodes of the triangles using the three dimensional Cartesian coordinate system. On the other hand, the computational mesh was considered as a set of cubes. We bring forward an effective procedure to check the collision between the elements of the geometry (triangles) and the computational mesh (cubes) based on the Minkowski addition.
In this work, the stereolithography (STL) CAD files are treated as an individual convex set at the same time that the computational mesh is also treated as a second convex set. Although no geometry is considered in the computational mesh, every face of the computational cell and its respective volume were amended to take into account the presence of an obstacle at the same region of the Euclidian space as if it was placed at the same coordinate of the computational cell. As result of this methodology, a porous mesh is created where the Navier-Stokes equations can be numerically solved and the explosion simulation is performed.

2 Methodology

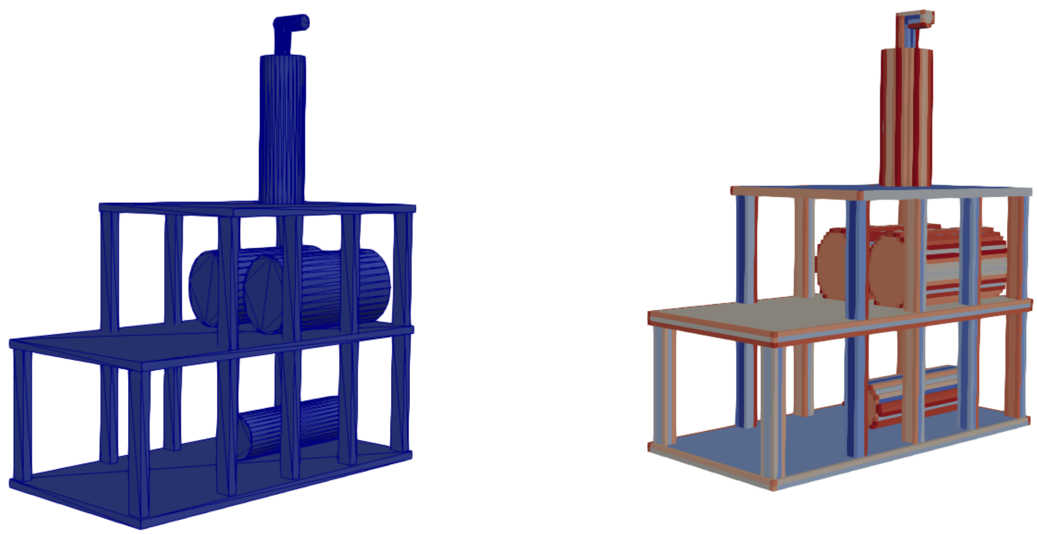
Considering two sets of vectors, say A and B, in the Eucledian space, the Minkowski sum can be defined by the sum of each vector in A to each vector in B leading to the following set:

The Minkowski addition concept was applied in a systematic manner to check whether there is collision between the elements of set A and elements of set B.
We first considered simple geometrical (Fig. 1a) model to examine if the details and contours of the geometry are well captured. We found that the porous (Fig. 1b) representation of the original geometrical model maintains the same dimensions and details of the faces and the edges that built up the topology of the geometry. The same is observed for the volume of the object. It is important to ensure that the faces of the computational cells are properly resolved as well as the volume of the computational since both entities will be used to calculate the flux of mass, moment and energy when solving the set of the equations governing the fluid flow.

(a) (b)

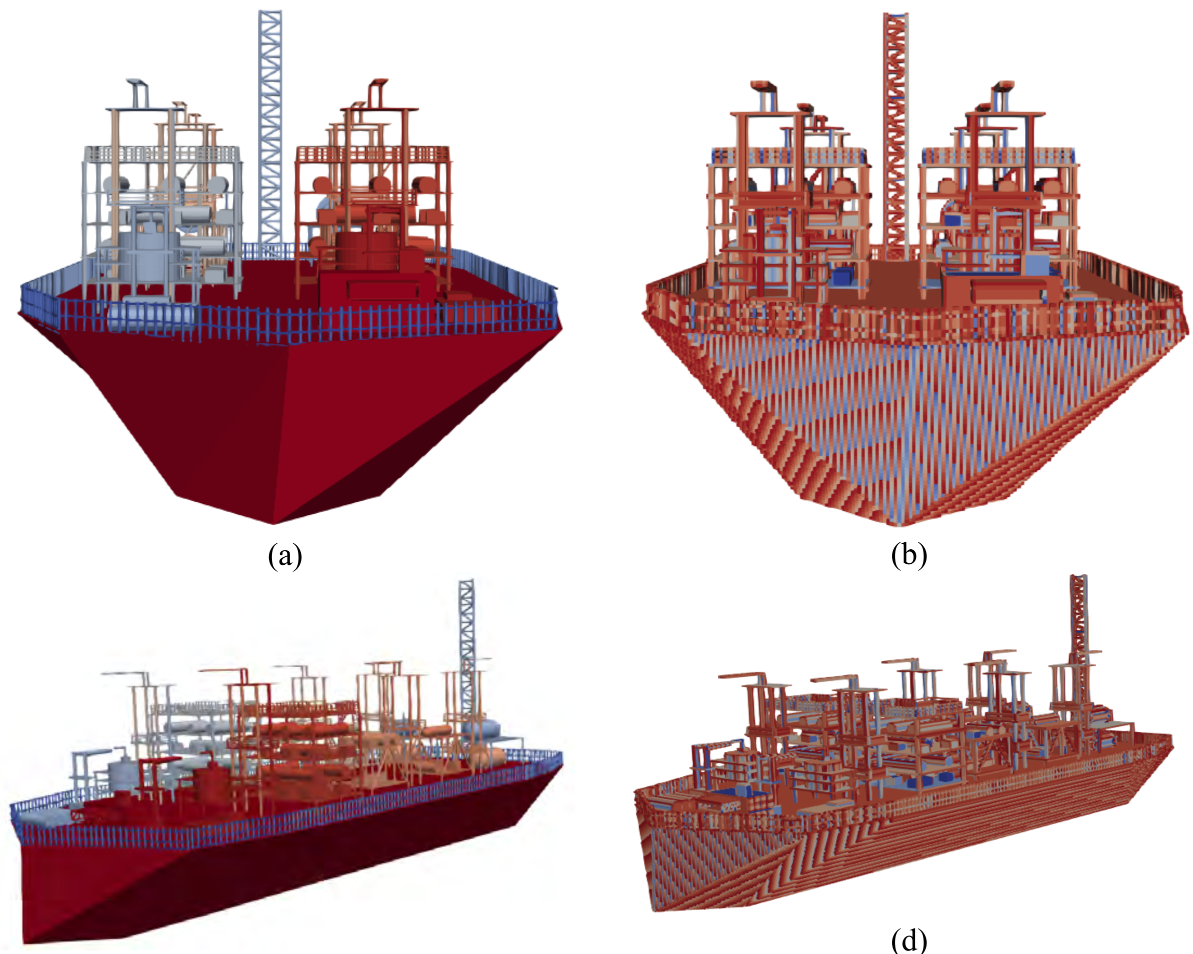
Figure 1: The geometrical STL model (a) for a simple cube and its respective porous (b) model calculated using the GJK algorithm. Threshold of the porosity is presented at the region of the computational domain where the porosity is slightly lower than unity.

We thus explored more complex geometries which resembles real engineering devices. A typical chemical processing module (Fig. 2a) has been considered. Details of the decks and the three rounded equipment are well resolved by the porosity procedure. In contrast to the results presented so far, a detailed geometrical model (Fig. 3a) comprising a significant amount of equipment and details such small pipes and trails has also been considered. The original STL - CAD front view (Fig. 3a) can be compared with its twin model (Fig. 3b) where every single detail is captured by the novel technique. The perspective view (Fig. 3c) shows details of even smaller pieces of the geometry which are also fairly mimic by the approach as shown in Fig. 3b.



(a) (b)

Figure 2: A chemical process module comprising two vessels and one heat exchanger at lower deck (a). Piping is omitted to ease the visualisation. The associated porous model (b) and details of the geometry well captured by the GJK algorithm applied to the STL model.



(a) (b) (c) (d)

Figure 3: STL model from front view (a) and perspective view (c) of a complex geometry comprising several equipment as well as small details, such as pipings and valves. The associated parametrised porous model of the STL models for front view (b) and perspective view (d).

We further combined the porous regions of the Euclidean space, as represented by the porous model (Fig. 1b, Fig. 2b, Fig. 3b, Fig. 3d), with the finite volume method for solution of the set of Navier-Stokes equations. For the discretised computational cells, all cell faces and the volumes were amended in accordance with the obstructions caused by the porous model. We have followed the reasoning line that if the cell is completed blocked no flow is allowed. Should the cell be 50% blocked it would therefore allow half of the flow expected for a full open cell.

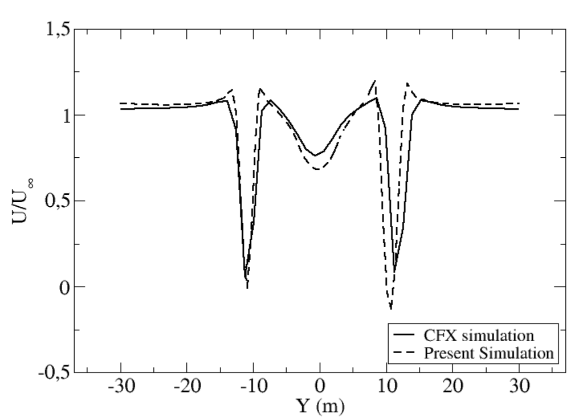
In doing so, porosity correction factors range from zero to unity. A blocked computational cell would be assigned zero porosity while a fully opened cell would be assigned unity porosity. The porosity values are used in the conservation equations to correct the fluxes through the computational cell. Extra terms are also added in the momentum equation, considering the drag, and in the turbulence source term in the k-epsilon equations. Full details of the implementation can be found elsewhere [6] [7].

3 Results

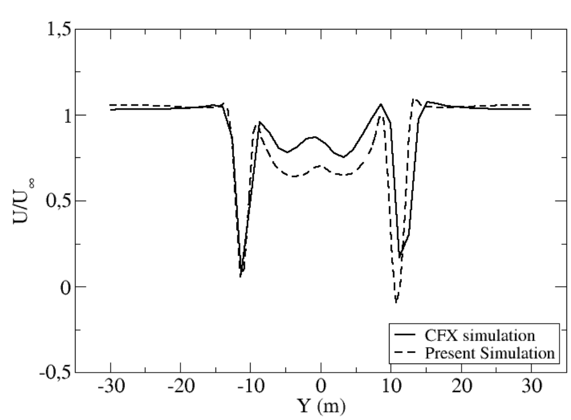
In the evaluation of the developed method to compute turbulent flows, in a first step we considered a cold flow simulation in a chemical process module presented in Figure 2. The velocity field have been calculated and numerical results were probed at 3 locations downstream the origin of the coordinate system and at 2 heights as listed below:

- Monitor Line 01: x = 3 m and z = 5 m.
- Monitor Line 02: x = 3 m and z = 22 m.
- Monitor Line 03: x = 18 m and z = 5 m.
- Monitor Line 04: x = 18 m and z = 22 m.
- Monitor Line 05: x = 50 m and z = 5 m.
- Monitor Line 06: x = 50 m and z = 22 m.

The numerical results from the numerical solution of the Navier-Stokes are shown in the plots as ”present simulation”. Since there is no experimental data for the cases considered the numerical findings obtained via the novel technique are compared with available CFD (Computational Fluid Dynamics) code, namely Ansys CFX. Comparison among the present simulation and the standard method for solution of the Navier-Stokes equations (Fig 4.a - Fig. 4f) shows good agreement.
As expected, the velocity drops significantly at regions behind the large equipment. Following the line transverse to the flow orientation shows a uniform flow where the normalised velocity is one.
At the regions inside the module the velocity drops due to the presence of obstacle dropping to values close to zero (Fig 4.a - Fig. 4e). At regions inside the module where the interference caused by the obstacle is less pronounced the velocity is reduced. However it does not reach value smaller than 50% of the bulk velocity. It is worth mentioning that it has also been observed regions in the module where the velocity increases due to the reduced area to the flow. This is in line with the principle of conservation of mass that ensures higher velocities at regions where the available area to the flow is reduced.



(a)



(b)

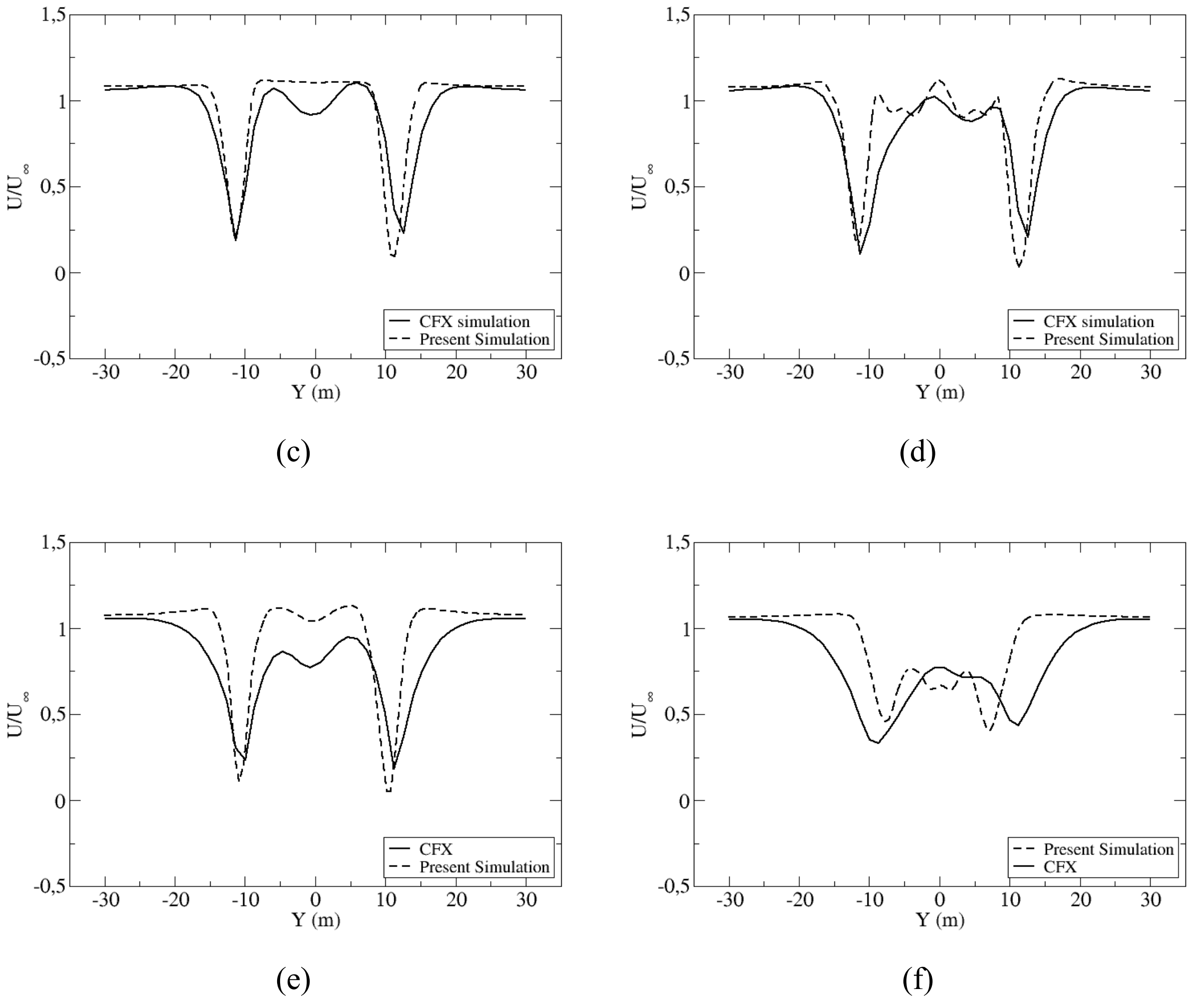


Figure 4: Velocity profile at six different locations inside a chemical process area (Figure 2): (a) monitor line 01, (b) monitor line 02, (c) monitor line 03, (d) monitor line 04, (e) monitor line 05, (f) monitor line 06. The numerical findings provided by the developed model presents good agreement with the standard CFD tool Ansys CFX [7].

We also investigate how the flamelet combustion model coupled with the collision distance algorithm reproduces turbulent reacting flows. In previous work, we have compared the numerical findings provided by the developed approach compare with experimental data for combustion scenarios in small scale geometry [6]. Here, two different combustion simulation were performed and the results were compared with the CFD commercial tool FLACS for gas explosion.

The first set of explosion analysis comprises a combustion chamber, measuring of 500 mm x 80 mm x 80 mm, filled with a flammable mixture of air and propane. Figure 5 presents the flame position into the chamber at different time steps. As expected for premixed combustion, the flame advances towards through the chamber in the reactant direction. The flame tip reaches the obstacle and its structure is changed to assume a finger shape. Similar behaviour is observed in both present and FLACS simulation.

(a)

(b)

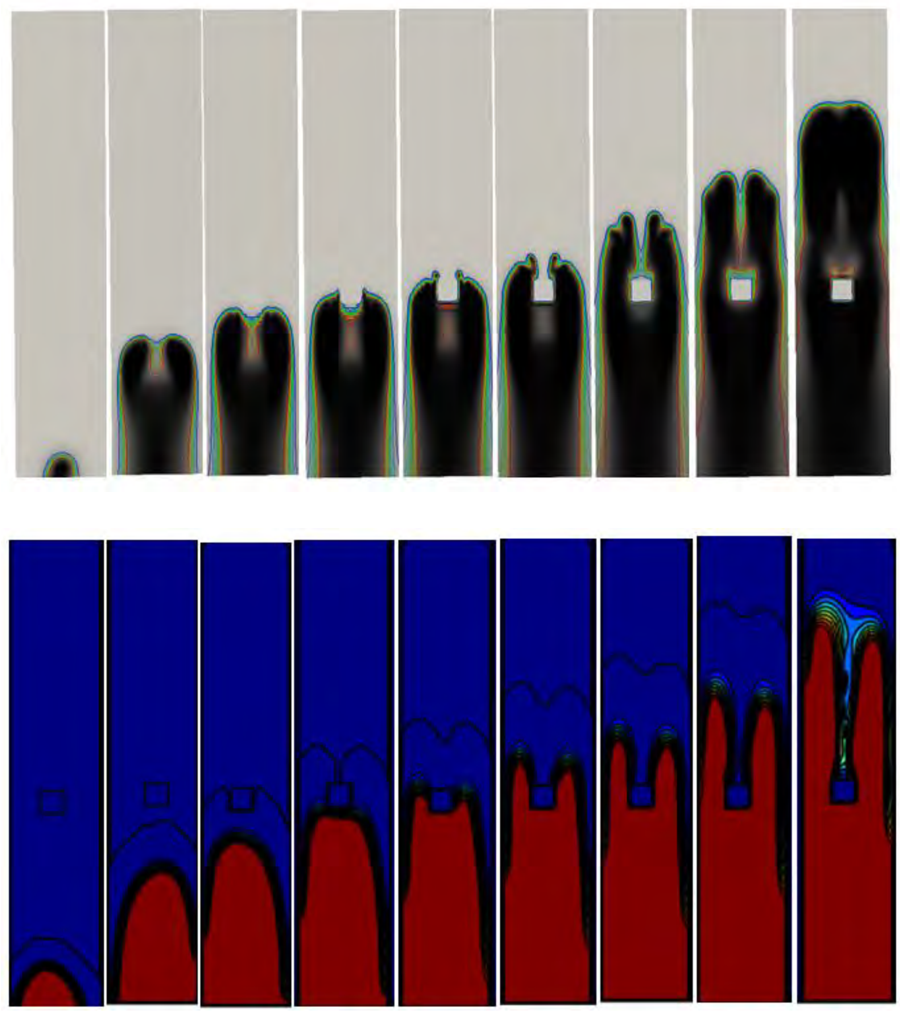


Figure 5: Flame position into a combustion chamber obstructed by a single square obstacle. The chamber was initially filled with a stoichiometric mixture of air and propane. The flame position is observed at different time steps considering numerical data provided by the developed approach (a) and FLACS CFD tool (b).

The second explosion analysis considers a real scale geometry with a chamber measuring 9 m x 4.5 m x 4.5 m. A set of 80 tubes with 0.5 m of diameter were placed into the chamber in order to make a congestion region. The chamber was filled with a stoichiometric mixture of methane and air. A ignition point was located in the beginning of the chamber and the flame behaviour was observed in different time steps after the ignition. Figure 6 presents the numerical results provided by the present approach and the FLACS CFD tool.

(a)

(b)

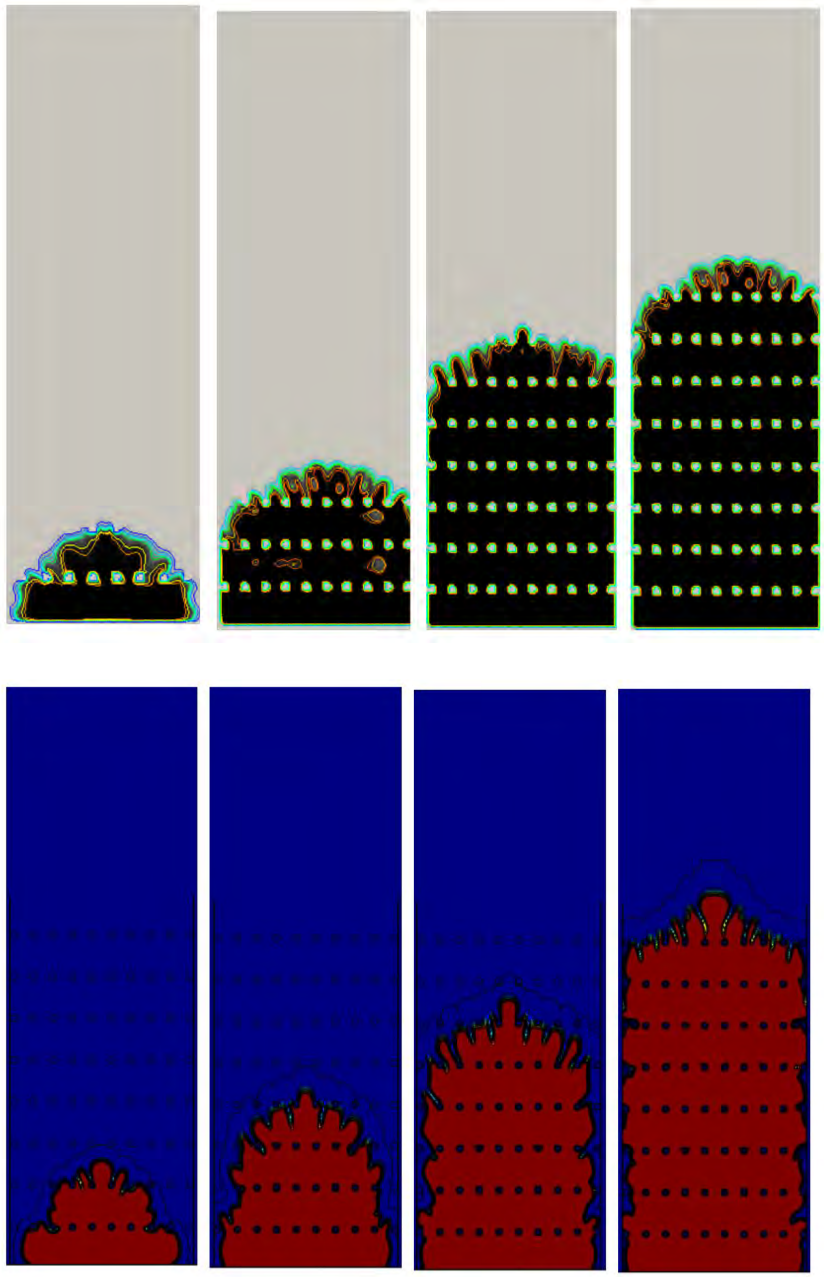


Figure 6: Progress variable advancement in a chamber congested by cylinders. The flame position is observed at different time steps considering numerical data provided by the developed approach (a) and FLACS CFD tool (b).

4 Conclusion and Future work

We have introduced a method for computation of turbulent flow in complex geometries. The new approach combines the finite volume method with Minkowski addition for correction of the flux through the area of the computational cell and its respective volume. The method is formulated as a convex combination of the simplex (simplex makes reference to a point, a line or any convex region) searching for the nearest reference point (The supporting point can be understood as the furthest point in a given direction). To demonstrate the approach we considered a simple geometry represented by a cube. The level of complexity was raised and two additional geometrical models have been considered. The first complex model was a chemical processing module and the second complex problem dealt with a full chemical process plant assembled on the topside of a vessel. Both complex geometrical models comprise details of the geometry ranging from a few inches to a few metres. We can correctly identify and map all the details of the geometry associated with the original CAD model using the Minkowski sum. Moreover, we have solved the set of Navier-Stokes using the modified formulation of the finite volume method using the Minkowski sum and the numerical finding agree with the selected benchmarking. We found that the numerical results obtained by the proposed method are in accordance with numerical findings provided by standard commercial CFD tools, even where the geometrical model has been considered in the simulations.

5 References

1. Vianna, S. and Cant, R. (2010). Modified porosity approach and laminar flamelet modelling for advanced simulation of accidental explosion. Loss Prevention in the Process Industries. 23, 3–14.
2. Savill, A. and Solberg, T. (1994). Some improvements to pdr/k − ε model predictions for explosions in confined geometries. In Procedings ER-COFTA/IMA Confined Flow Dispersion Through Groups Obstacles, Cambridge, UK, 227–247.
3. Forthergill, C., Chynowet, S., Roberts, P. and Packwood, A. (2003). Evaluation a cfd porous model for calculating ventilation in explosion hazard assessments. Loss Prevention in the Process Industries. v. 4, 16, 341–347.
4. Gilbert, E., Johnson, D. and Keerthi, S. (1988). “A fast procedure for computing the distance between complex objects in three-dimensional space”. Robotics and Automation. v. 2, 4, 193–203.
5. van den Bergen, G., Van, G. and Bergen, D. (1999). “A fast and robust gjk implementation for collision detection of convex objects”. Journal of Graphics Tools. 7–25.
6. Moreira, V.D., Ferreira, T.D., Santos, R.G., Vianna, S.S.V. (2015). A novel technique to obtain a mesh porosity based on the Gilbert-Johnson-Keerthi distance algorithm. 23rd ABCM International Congress of Mechanical Engineering. Proceedings, 1-9
7. Ferreira, T. D., Santos, R.G., Vianna, S.S.V. (2019). A coupled finite volume method and Gilbert–Johnson–Keerthi distance algorithm for computational fluid dynamics modelling. Computer Methods in Applied Mechanics and Engineering. 352, 417-436.
8. Ferreira, T.D and Vianna, S.S.V. (2019). The Gilbert Johnson Keerthi distance algorithm coupled with computational fluid dynamics applied to gas explosion simulation. Process Safety and Environmental Protection. 130, 209-220.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Effects of Non-uniform Blockage Ratio and Obstacle Spacing on Flame Propagation in Premixed H_2/O_2 mixtures

Cassio Brunoro Ahumada*[1], Eric L. Petersen[2], Qinsheng Wang[1]
[1]Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, Texas, USA
[2]J. Mike Walker '66 Department of Mechanical Engineering, Texas A&M University, College Station, Texas, USA
*Presenter E-mail: cassioahumada@tamu.edu

Abstract

Most of the current research in flame propagation and deflagration-to-detonation transition (DDT), including large and small-scale experiments, have analyzed the influence of obstacles uniformly distributed on the explosion severity. These uniform conditions are characterized by constant obstacle spacing, shape and blockage ratio (BR), and may not represent very well the layout of actual industrial facilities. Therefore, the objective of this study was to investigate the effects of varied BR in the peak overpressure and flame acceleration. A systematic analysis was conducted by varying layout parameters on a regular basis to examine what conditions favor the highest overpressure and minimal run-up distance when DDT is observed. Experiments were performed in a closed pipe with 38 mm internal diameter and an overall length to diameter ratio (L/D) equal to 73. The arrangement between two obstacles in the test vessel was varied in terms of blockage ratio (increasing, decreasing and equal) and obstacle distance (1D, 2D, and 3D). From the conditions tested, the increasing blockage ratio has a more significant impact on the overall maximum pressure and the DDT run-up distance.

Keywords: Explosions, Vapor Clouds, DDT, Blast Effects

1. Introduction

Understanding flame propagation and explosion characteristics of flammable mixtures is crucial for industrial explosion protection of power plants and chemical plants. From the practical point of view, safety professionals work towards estimating flame speeds and maximum overpressure build-up for a wide range of industrial releases scenarios. This information is later used to support safety design decisions and protective measure specifications. Defining the entire spectrum of plausible scenarios is not a straightforward task, it must address all affecting parameters including release locations, mixture concentration, the volume of flammable cloud, equipment density and disposition, and ignition position. This problem can be simplified by identifying and ranking conditions that are likely to lead to more severe explosion cases.

For several years it has been known that the presence of obstructions can give rise to substantial overpressure during combustion of premixed flammable gases[1, 2] . Therefore, researchers have proposed empirical correlations[3, 4] and numerical codes [5-7] to account for obstruction characteristics (equipment density and spacing) during explosion modeling analysis. Despite their usefulness, the majority of these methods were validated against uniform obstruction conditions that were far from the non-ideality encountered in industrial facilities. Such uniformity can be characterized by multiple obstacles with similar shapes and blockage ratio, distributed at equally spacing inside a combustion chamber, and may not be very representative on the actual industrial facilities layout.

To put into perspective, the authors created an obstacle complexity index (OCI) that can be estimated based on four factors: obstacle shape, BR, obstacle spacing, and uniformity. The following expression can be used to quantify OCI:

$$OCI = \prod_{i=1}^{4} F_i$$

Where

$$F_i = [1,3]$$

Table 1. Value for obstacle factor (F_i) based on test conditions.

Factor Value (F_i)	**Obstacle Shape**	**Obstacle Spacing**	**Blockage Ratio**	**Number of different obstacles**
1	Tests without obstacles	Tests without obstacles	Tests without obstacles	Tests without obstacles
2	Round obstacles (orifice plates and cylinders)	Tests with equally spaced obstacles	Continuous BR	At least 2
3	Obstructions with sharp edges	Tests with varied obstacle spacing	Varied BR	More than 2

Table 1 contains more detail on each factor value. Figure 1 shows the relationship between the flammable mixture volume and OCI of experiments listed in the literature. It can be observed that most of the industrial explosions are located in the upper-right quadrant, which represents the high complexity and large volume region; whereas the majority of the work on the literature are placed on the lower quadrants, including small and large volume regions with the exception of limited tests with propane and methane mixtures[8, 9]. In the later cases, authors analyzed the efficiency of venting panels on explosion mitigation inside obstructed enclosures simulating offshore installations. Although insightful observations on the effects of obstacle congestion in large-scale tests were obtained, only three distinct sets of layout displacement were studied giving limited conclusions on the influence of obstacle orientation and geometry.

The round points in red represent the capabilities of the current facility based on previous works [10, 11]. Even though the mixture volume is considerably lower than the ones experienced during an industrial explosion, our aim to towards understanding in more detail how obstacle characteristic play a role in turbulent combustion propagation and detonation onset. For that purpose, it is fundamental to conduct experiments in a controllable test environment. The data generated by this work can be used for validation purposes of current numerical models.

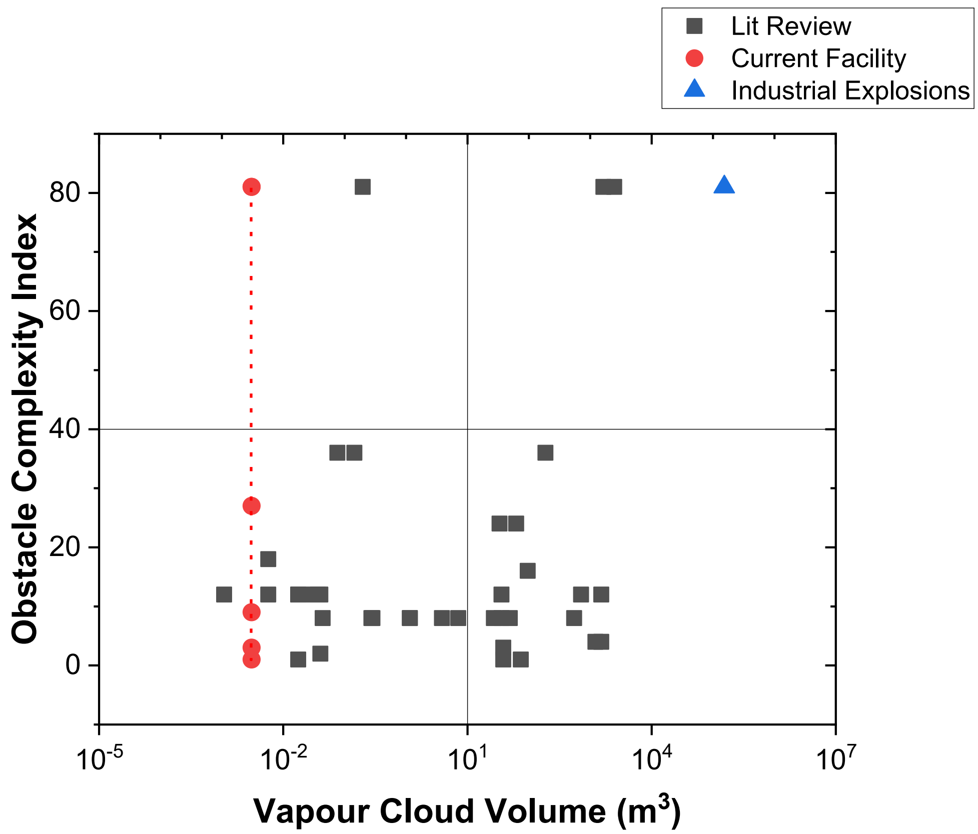


Figure 1. Variation of obstacle complexity index with flammable mixture volume

2. Experimental Details

Experiments were carried out in a horizontal tube with a length of 2.77 m and a 38-mm internal diameter, as shown in Figure 2. The tube is closed at both ends, and ignition was via a low-voltage, automotive glow plug operated at 10 A positioned centrally at the left-endplate. An expansion volume is located at the end-wall opposed to the ignition point, enabling the use of multiple spacers with different widths. A spacer with 25.4-mm width was maintained during all tests to minimize disturbances from reflected shocks propagating ahead of the flame. The pressure was recorded at seven different locations along the tube (P1 to P7) using piezoelectric pressure transducers, PCB 113B22, with a measurement range of 34.5 MPa, a rise time smaller than 1 μs, and a resonance frequency ≥ 500 kHz. Data were recorded using a PC oscilloscope board (GaGeScope) at a sampling rate of 1 MS/s.

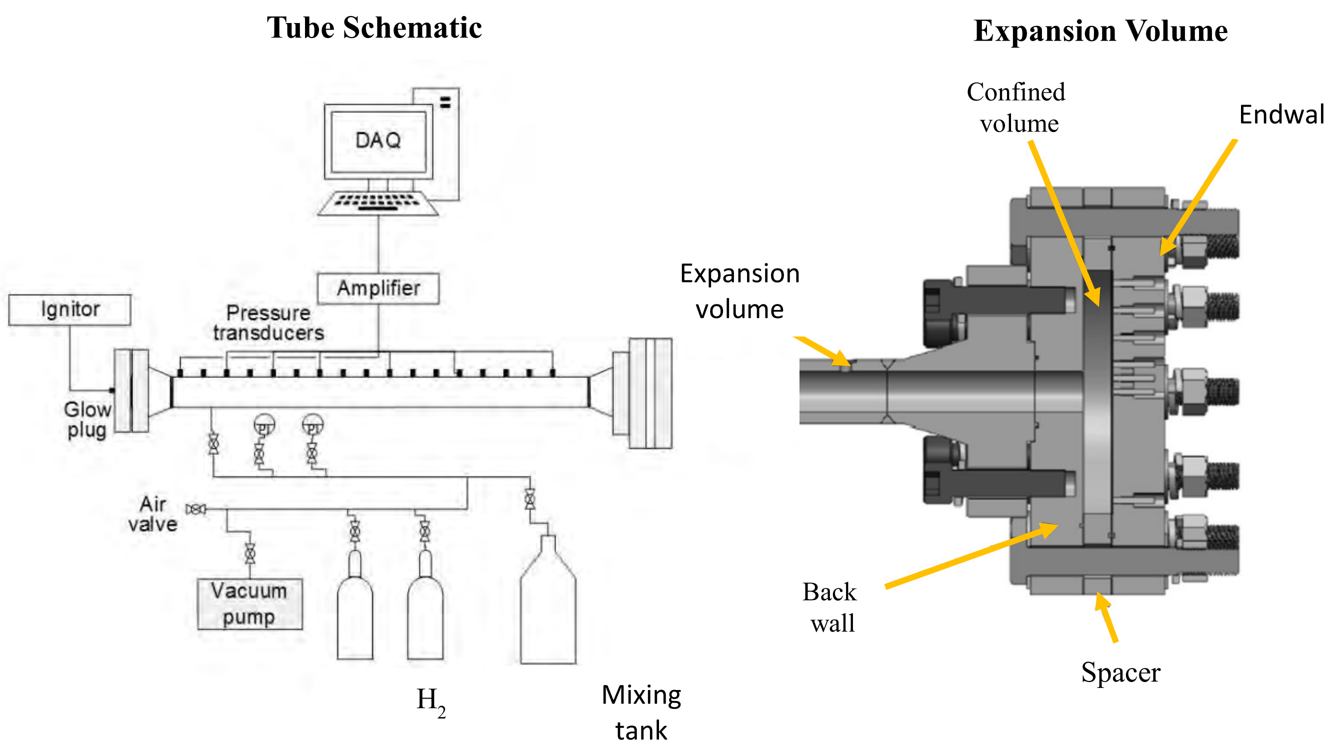


Figure 2. Schematic of the detonation tube utilized during experiments (left side) and the expansion volume located at endwall (right side)

All tests were conducted at ambient temperature, roughly 20°C. Stochiometric hydrogen/oxygen mixtures were prepared by the method of partial pressures in a separate mixing tank and left overnight. Two ring-shaped obstacles with 5-mm thickness were used during each test, with the first obstacle fixed at a distance of 80 mm from the ignition point. The arrangement between obstructions in the test vessel was changed in terms of blockage ratio (increasing, decreasing, and equivalent) and obstacle separation distance (38, 76, and 114 mm). Table 2 summarizes all conditions tested in this study. A full factorial design was conducted, resulting in 27 different experimental conditions. Each experimental condition was repeated at least three times. Figure 3 depicts obstacle shapes and displacement inside the tube during experiments.

Table 2. Summary of Experimental Conditions

Variable	Level 1	Level 2	Level 3
1st Obstacle BR	25%	40%	80%
2nd Obstacle BR	25%	40%	80%
Obstacle Spacing	38 mm	76 mm	114 mm

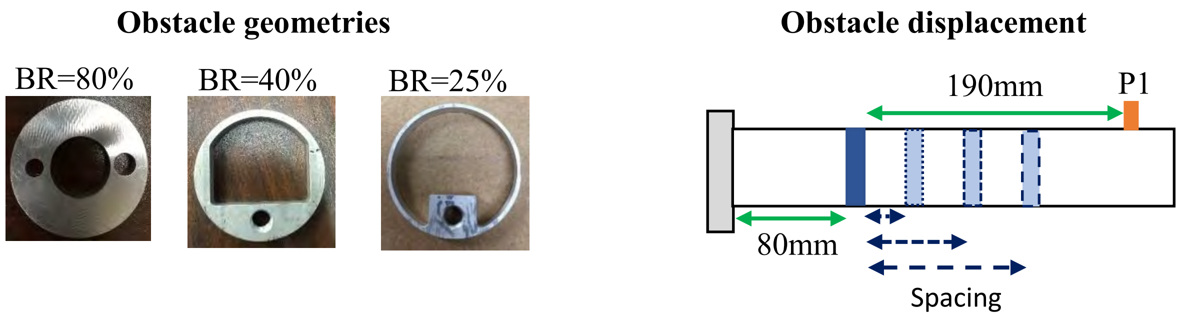


Figure 3. Illustration of the obstacles inserted inside the detonation tube.

3. Results and Discussion

3.1. Facility Characterization

A facility characterization study was performed with the tube emptied to analyze flame propagation without the presence of obstacles at initial pressure ranging from 30 to 300 Torr. Figure 4 shows the variation of the maximum shock wave speed (on the left) and the DDT time (on the right) with initial pressure. It can be observed that mixtures with initial pressure above 60 Torr experienced DDT whereas mixtures below 50 Torr did not ignite. Another interesting observation is the reduction in time when DDT was first identified in the facility – DDT time.

Figure 5 and 6 depict the overpressure profile with time along the tube at 50 and 150 Torr, respectively. Both cases experienced a leading shock wave traveling toward the right-end plate are observed, indicating an initial flame acceleration. For 150 Torr, a rapid transition to detonation takes place in the second half of the tube (between P10 and P13) creating overpressures around 4 bars. At 50 Torr (Figure 5), the precursor shock velocity remained above the sound speed at the reactants (540 m/s) but below the sonic velocity on the combustion products (~1,000 m/s). This is the characteristics of the "choke regime" [12]. Although flame arrival time was not measured directly, it can be inferred from the leading shock velocity profile that flame speed was near the local sound speed. The increase in shock velocity in the first half of the tube indicates that a flame front is propagating jointly behind the pressure front, forming a flame-shock structure.

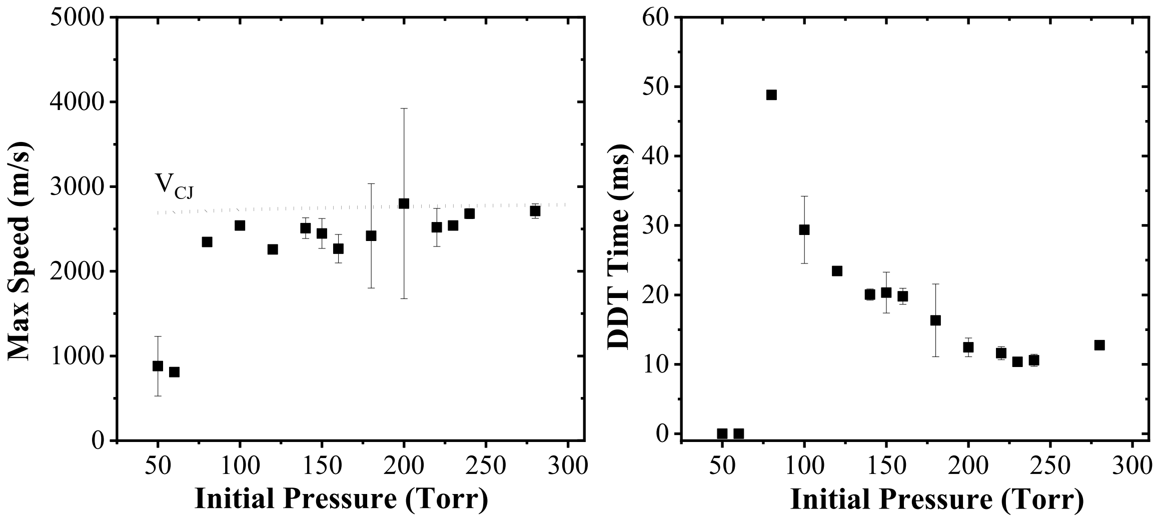


Figure 4. Variation of the maximum shock wave speed (on the left) and the DDT time (on the right) with initial pressure.

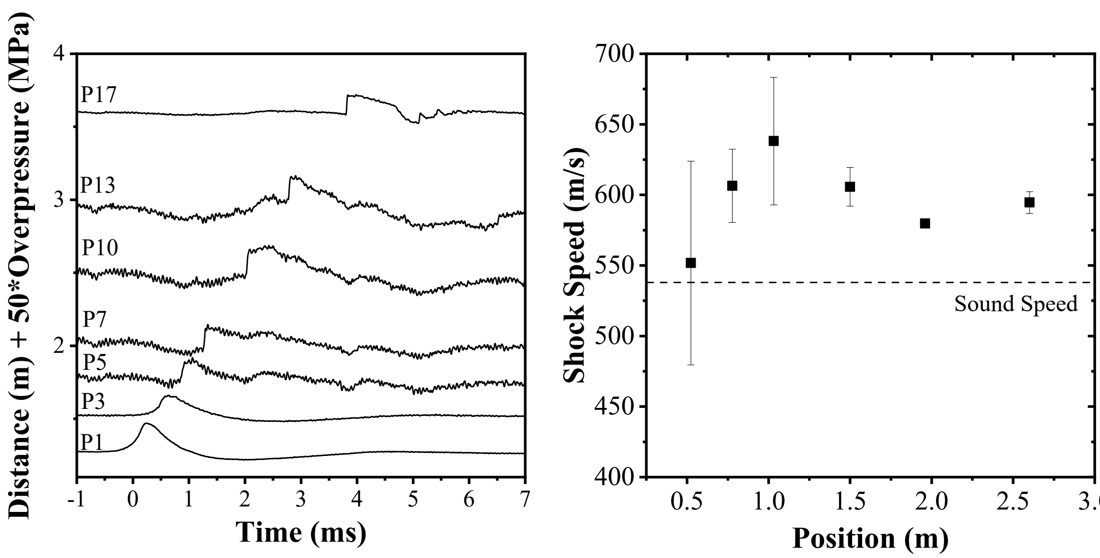


Figure 5. Pressure results obtained for a stoichiometric hydrogen-oxygen mixture initially at 50 Torr and with the tube emptied. Pressure is normalized by side-on pressure measured (MPa) multiplied by 50 and added the pressure sensor distance (m).

On the other hand, the mixture initially at 150 Torr demonstrates an entirely different behavior. An early acceleration creates a series of sonic waves traveling towards the right-endplate. Then, a rapid transition to detonation takes place in the second half of the tube (between P10 and P13). Even though DDT was not expected given the size of the internal tube diameter, the preceding waves increase the initial temperature of reactant mixture, increasing the reactivity of the mixture and propensity to detonation onset.

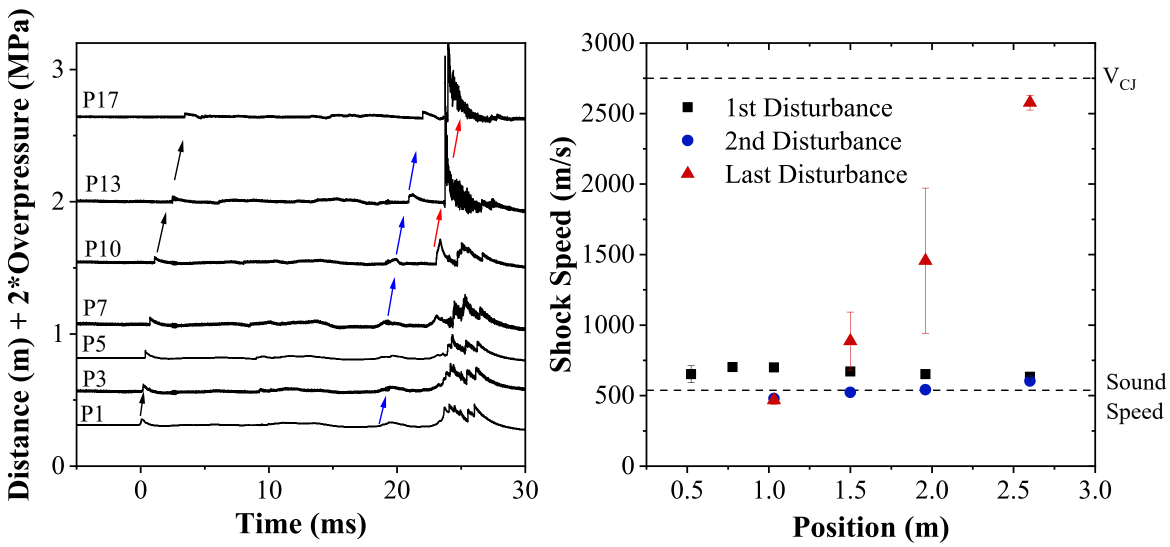


Figure 6. Pressure results obtained for a stoichiometric hydrogen-oxygen mixture initially at 150 Torr and with the tube emptied. Pressure is normalized by side-on pressure measured (MPa) multiplied by 2 and added the pressure sensor distance (m).

The facility characterization study showed that fast deflagrations and DDT are observed at the current set-up, The next section contains the results for the mixture at 150 Torr. Experiments with 50 and 100 Torr were completed, but at the current stage data analysis is still in progress and, therefore, will not be shown in this report.

3.2. Results for $H_2 + O_2$ mixtures at 150 Torr

After confirming that DDT is possible even with the absence of obstacles, experiments were carried out to investigate the effects of varied blockage on the explosion characteristics. As expected, deflagration-to-detonation transition was observed in all 27 experimental cases, but at different locations. Figure 7 shows the variation of maximum overpressure at the first sensor (P1) with average BR. Similar to the uniform condition case, Pmax increases as averaged BR changes from 0 to 60 %, most likely due to higher turbulence intensities. Then as BR changes to 80%, momentum losses become significant leading to a reduction in Pmax. One interesting observation is for the case of 40%-80% BR separated at 76 mm (2 internal diameters), in which detonation occurred before P1, reducing the run-up distance considerably. A possible explanation for the early detonation onset can be the reflection of the shock induced by the obstacle in the confinement wall as reported by Obara et al. [13]. Another reason could be the accumulation of multiple Mach stems generated by local explosions triggered by turbulent jet combustion near the confinement walls; this accumulation process creates stronger shocks that can trigger a detonation in hot-spots via shock focusing [14]. Currently, the absence of optical windows limits our ability for a detailed understanding of mechanisms behind detonation onset for this particular case. However, this behavior is very intriguing given that DDT was achieved using only two obstacles.

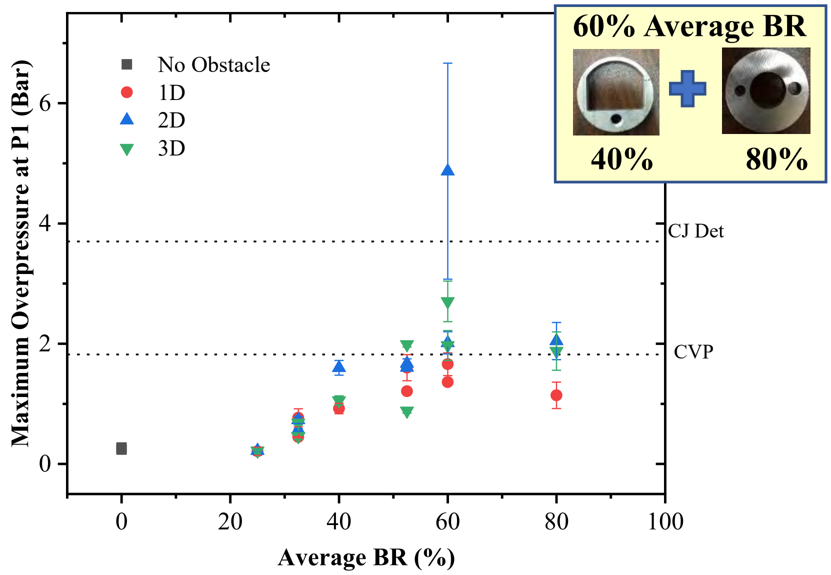


Figure 7. Variation of maximum overpressure with average BR at first pressure sensor (P1) in the wake of second obstacle.

In overall, four general propagation behaviors were identified (see Fig. 8) based on the time between the leading wave and the onset of DDT. In case I, a preceding wave continuously accelerates until it reaches a final speed near the Chapman-Jouguet detonation. This case can be further divided into two, I-A and I-B. The former, as mentioned earlier, consists of a strong shock that is created in the wake of the second obstacle and is detected early by sensor P1 or P3 located at 190 mm and 460 mm from the 1st obstacle, respectively. Since the detonation onset occurs earlier, there is no sign of retonation propagating backward towards the ignition point. In the case of I-B, DTT takes place within the second half of the tube near the leading shock front. For combustion type II, a shock wave is formed and accelerated up to speeds of 1500 m/s in the first half of the tube and later decelerated to final speeds around 800 m/s towards the closed end. The leading wave is not strong enough to ignite the mixture via shock compression and, as a result, the onset of DDT takes places after it passes. This behavior is typical for conditions when detonation onset occurs on the turbulent flame brush [15]. Case III is very similar to case II; however, in Case III, two major pressure waves are observed before the transition to detonation. The fact that the second pressure front is accelerating indicates that a flame-shock structure is formed and that detonation takes place after the flame passes. Gaathaug *et al.* [14] reported a similar phenomenon that was caused due to shock accumulation resulting from multiple local explosions. In case IV, on the other hand, numerous pressure waves are formed and travel near the sonic velocity in the medium; this indicates a slow flame acceleration followed by a sudden transition that takes place towards the end of the tube.

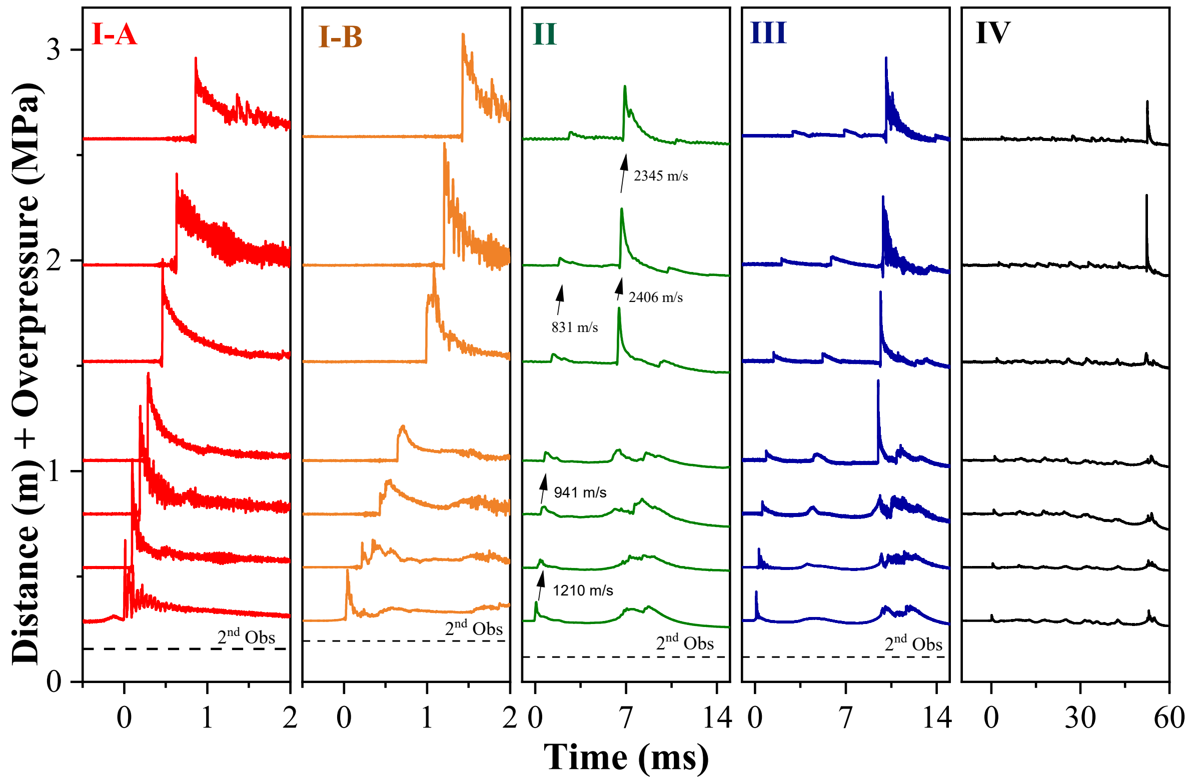


Figure 8. Representation of the four different types of combustion propagation behaviors identified.

Table 3 summarizes the predominant propagation behavior for each condition tested. The most robust combustion regime (Case I) occurred for obstructions with a higher blockage in the second obstacle (80-80, 40-80, and 25-80). It is reasonable to assume that narrower obstruction gaps may generate faster and stronger shocks as the flame front passes the solid obstruction. This strong shock can ultimately lead to detonation onset. Another important aspect is the distance between the obstacle and the ignition point — longer spacing results in faster flames before reaching the obstacle surface. For instance, cases with higher BR closer to ignition (80-40 and 80-25) resulted mostly combustion type III, in which leading shock front was significantly lower.

Table 3. Summary of prevailing propagation conditions for obstacle characteristic

Blockage Distribution	Average ABR	Obstacle Spacing 1D	2D	3D
80-80	80%	II	I-B	I-B
80-40	60%	III	III	I-B
40-80	60%	II	I-A	I-A
80-25	53%	III	III	III
25-80	53%	I-B	I-B	I-B
40-40	40%	III	II	II
40-25	33%	III	III	II

25-40	33%	II	III	III
25-25	25%	III	II	III
No obstacle	0%	IV	IV	IV

Another interesting observation is that obstacle pairs with the same average blockage ratio resulted in distinct combustion characteristics, especially when BR variation was more abrupt. For instance, comparing the results from the obstacle pair 40-80 with its equivalent on average blockage (but transposed), 80-40, one may observe that the increasing obstruction leads to a stable detonation within the first three sensors (see Figure 9). Conversely, in the decreasing blockage case, DDT takes place mostly within the second half of the tube (after P4), and it is preceded by two major pressure waves. Similar conclusions were obtained for obstacle pairs 80-25 and 25-80. Contrarily, obstacle pairs with smoothers changes in BR (40-25, 25-40) in general did not demonstrate significant differences in behavior.

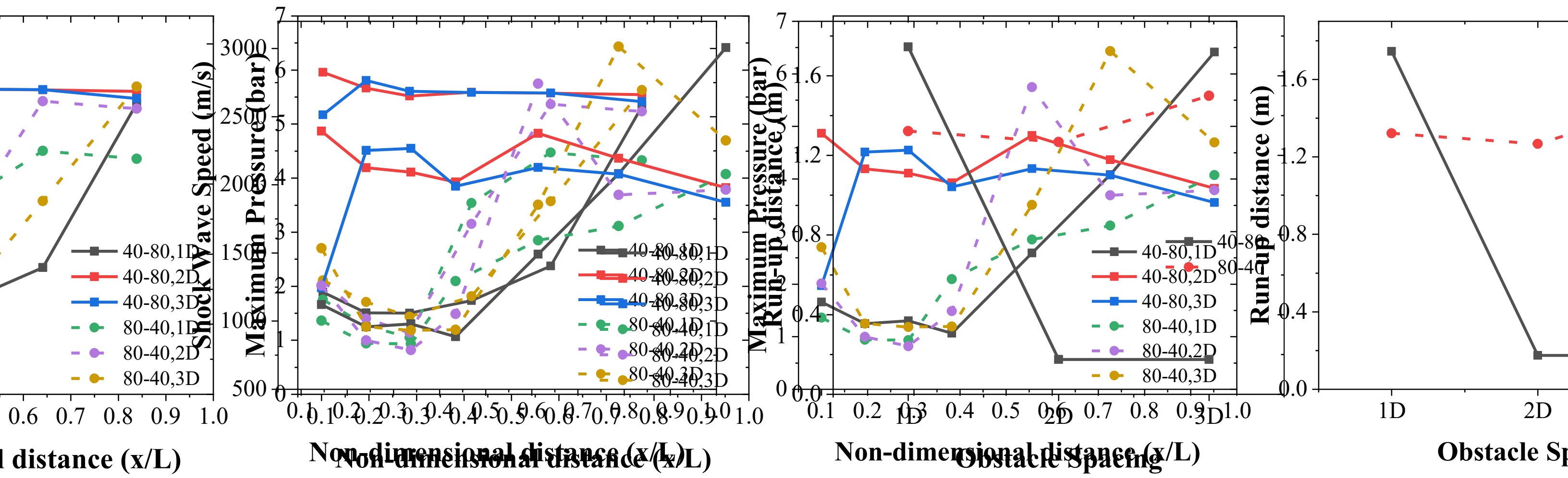


Figure 9. Comparison between obstacle pairs with an equivalent average blockage ratio.

Based on this study, we can conclude that the obstacle order does affect flame propagation and explosion severity for such high sensitivity mixture. This effect is more significant when a high degree of obstruction is present. For instance, for the 60% average BR case, the run-up distance was much shorter when 80% BR obstacle was locater after the 40% BR obstacle. Conversely, switching the obstruction displacement to 80-40 lead to longer run-up distances. This indicates that obstruction geometry should be considered when more than one obstruction shape is present and that looking only at the average BR may lead to underestimated results. The authors acknowledge that this is a preliminary result and further analysis will be conducted to investigate the isolated impact of obstacles with varied BR and similar shapes as well as obstacles with distinct shapes but identical BR.

4. Concluding Remarks

Experiments on flame propagation and DDT were carried out in stoichiometric, premixed hydrogen-oxygen mixtures at 150 Torr in a closed tube with two obstacles of varying configuration. Round-shaped obstacles with three different blockages (25%, 40%, and 80%) were used, and the arrangement between the obstacles was changed in terms of blockage distribution (increasing, decreasing, and equivalent) and obstacle distance (1D, 2D, and 3D). Four distinct propagation behaviors were identified based on the time between the leading wave and the onset of DDT. From the conditions tested, obstacle pairs with a higher blockage in the second obstruction lead to strong combustion. It was observed that obstructions with equivalent blockage resulted in distinct propagation characteristics and explosion strength. This study is still in progress, and additional experiments will be conducted to understand the mechanisms underlining these different behaviors.

References

[1] W. R. Chapman and R. V. J. J. o. t. C. S. Wheeler, "VI.—The propagation of flame in mixtures of methane and air. Part V. The movement of the medium in which the flame travels," pp. 38-46, 1927.

[2] I. O. Moen, "Transition to detonation in fuel-air explosive clouds," *Journal of Hazardous Materials,* vol. 33, no. 2, pp. 159-192, 2// 1993, doi: http://dx.doi.org/10.1016/0304-3894(93)85052-G.

[3] A. J. Pierorazio, J. K. Thomas, Q. A. Baker, and D. E. Ketchum, "An update to the Baker-Strehlow-Tang vapor cloud explosion prediction methodology flame speed table," *Process Safety Progress,* vol. 24, no. 1, pp. 59-65, 2005, doi: 10.1002/prs.10048.

[4] S. Dorofeev. "Flame acceleration and ddt: A framework for estimating potential explosion hazards in hydrogen mixtures." http://www.hysafe.org/science/eAcademy/docs/3rdesshs/presentations/ESSHS2008DorofeevSB.pdf (accessed 2016).

[5] B. Hjertager, K. Fuhre, S. Parker, J. J. P. i. a. Bakke, and aeronautics, "Flame acceleration of propane-air in a large-scale obstructed tube," vol. 94, pp. 504-522, 1984.

[6] O. R. Hansen and D. M. Johnson, "Improved far-field blast predictions from fast deflagrations, DDTs and detonations of vapour clouds using FLACS CFD," *Journal of Loss Prevention in the Process Industries,* vol. 35, pp. 293-306, 5// 2015, doi: http://dx.doi.org/10.1016/j.jlp.2014.11.005.

[7] G. Ciccarelli, C. T. Johansen, and M. Parravani, "The role of shock–flame interactions on flame acceleration in an obstacle laden channel," *Combustion and Flame,* vol. 157, no. 11, pp. 2125-2136, 2010, doi: 10.1016/j.combustflame.2010.05.003.

[8] B. Hjertager, K. Fuhre, and M. J. J. o. l. p. i. t. p. i. Bjørkhaug, "Gas explosion experiments in 1: 33 and 1: 5 scale offshore separator and compressor modules using stoichiometric homogeneous fuel/air clouds," vol. 1, no. 4, pp. 197-205, 1988.

[9] C. Selby and B. J. S. p. Burgan, "Blast and fire engineering for topside structures-phase 2: final summary report," 1998.

[10] C. A. Rosas Martinez, "Deflagration-to-Detonation Transition (DDT) Studies: Effect of Non-Uniform Obstacle Distribution on DDT," Doctoral, Material Science Texas A&M University, Internal report, 2016.
[11] N. L. Polley, M. Q. Egbert, and E. L. Petersen, "Methods of re-initiation and critical conditions for a planar detonation transforming to a cylindrical detonation within a confined volume," *Combustion and Flame,* vol. 160, no. 1, pp. 212-221, 2013/01/01/ 2013, doi: https://doi.org/10.1016/j.combustflame.2012.09.017.
[12] J. H. Lee, R. Knystautas, and C. K. Chan, "Turbulent flame propagation in obstacle-filled tubes," *Symposium (International) on Combustion,* vol. 20, no. 1, pp. 1663-1672, 1985/01/01/ 1985, doi: https://doi.org/10.1016/S0082-0784(85)80662-7.
[13] T. Obara, T. Kobayashi, and S. Ohyagi, "Mechanism of deflagration-to-detonation transitions above repeated obstacles," *Shock Waves,* vol. 22, no. 6, pp. 627-639, 2012, doi: 10.1007/s00193-012-0408-5.
[14] A. V. Gaathaug, D. Bjerketvedt, and K. Vaagsaether, "Experiments with Flame Propagation in a Channel with a Single Obstacle and Premixed StoichiometricH2-Air," *Combustion Science and Technology,* vol. 182, no. 11-12, pp. 1693-1706, 2010, doi: 10.1080/00102202.2010.497355.
[15] G. Ciccarelli and S. Dorofeev, "Flame acceleration and transition to detonation in ducts," *Progress in Energy and Combustion Science,* vol. 34, no. 4, pp. 499-550, 8// 2008, doi: http://dx.doi.org/10.1016/j.pecs.2007.11.002.

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Determination of Corrosion Velocity in Industrial Equipment Working under Dual Environments, Combustion and Steam. Case Study: ASTM A335 P91 Steel

Anibal Alviz-Meza[1]*, Adam Duong[2], Dario Y Peña-Ballesteros[3], Viatcheslav Kafarov[4]
[1]Grupo de Investigación en Desarrollo Humano, Tejido Social e Innovaciones Tecnológicas, GIDTI, Social Sciences, Coorporación Universitaria Minuto de Dios
[2]Institut de Recherche sur l'Hydrogène, IRH
Département de Chimie, Biochimie et Physique, Université du Québec à Trois-Rivières
[3]Grupo de Investigación en Corrosión, GIC
Escuela de Ingeniería Metalúrgica, Universidad Industrial de Santander
[4]Centro de Investigación para el Desarrollo Sostenible en Industria y Energía, CIDES
Escuela de Ingeniería Química, Universidad Industrial de Santander
*Presenter E-mail: anibal.alviz@uniminuto.edu, anibalalvizm@hotmail.com

Abstract

Taking as a reference point the scientific worldwide known problem about global warming and less cost energy requirement, the petrochemical sector has been implementing well-called eco-efficiency strategies, promoting the use of critical conditions throughout the traditional chain process of oil refining. So that, even causing the environment detriment, many industrial combustion processes are developed using as energy source a mixture of natural and recovery gases, refinery gases, which added to high temperatures and pressures generate potential corrosion atmospheres. Thus, this research effort tried to determinate the pipeline degradation that take place inside a boiler, evaluating for this purpose the ferritic ASTM A335 P91 (P91) steel.

P91 pipelines commonly are exposed to dual environments during boilers operation, where typically the external tube face remains in contact with water vapor while the internal part is reacting with flue gases. With this in mind, a device was built to hold P91 specimens inside an electric furnace, to expose each coupon face to different mixture of gases. The conditions selected to simulate real boilers operation were: a supplied molar flue gas composition, 650 °C and evaluation times between 1 and 200 h.

The main obtained results indicated that P91 steel form a duplex structure of oxide layers with considerable porosity and with an internal corrosion zone in both studied environments. The inner layer helped to determine the corrosion degradation velocity, which resulted in severe corrosion for both cases, although of greater magnitude in the flue gases atmosphere.

After 200 h of corrosion, the carburization effect could not be identified. Nevertheless, the carbon diffusion transport was discarded, which means that CO_2 responds to a direct mass transfer process, whose identification requires longer evaluation times.
These results showed the aggressive conditions under which the typically used steels at high temperatures processes are summited, highlighting some possible equipment integrity implications that can be generated if efficiency strategies do not take in consideration safety factors, to say nothing about environmental aftermath.

Keywords: Corrosion Velocity, Dual Environment, Fuel, Pure Vapor, Oxidation, Reaction Rate, High Temperature Corrosion

1 Introduction

The ferritic steel Fe-9Cr-1Mo (P91) and its latest derivatives, such as P92 or E911, belong to the group of materials of advanced resistance to corrosion and creep, which are used in equipment that normally work between 550 and 650 °C [1], [2]. The applicability of this steel in the power generation and petrochemical industry is due to its low coefficient of thermal expansion, good heat transfer and high corrosion resistance under stress in water vapor. However, above 700 °C the good mechanical properties of this steel decrease significantly over time, because of the multiple condensation of interstitial spaces in it. The foregoing translates into a decrease in the alloy hardness, its creep limit and its ultimate tensile strength [3]–[5].
In relation to the reported failures of P91 steel in the industry, researchers such as Fabricius and Jackson [3] have compiled several cases of premature failures of this alloy during its service in heaters, superheaters and steam generators. The main failures reported have been: local increases in stress and creep resistance reductions. These failures were related to poor steel finishes and their use outside design conditions.
On the other hand, in regard to the P91 corrosion resistance during its operation in the petrochemical sector, there is limited information available. Studies such as the one carried out by Ju *et al.* [6], allowed to identify drastic cases of carburization and hydrogen attack in a feed furnace from a dehydrogenation unit. The analysis developed by them pointed out that pitting and cracking of industrial extracted tubes are also related by the different corrosive phenomena involved in furnaces gaseous environment.
Likewise, there are studies conducted in controlled combustion environments, where researchers such as Peña-Ballesteros *et al.* [7] and Alviz *et al.*[8]–[11] reported the involvement of other corrosive effects. In the first study, it was demonstrated that in a mixture of gases composed of CH_4, CO, CO_2 and H_2, the simultaneous effects of carburation and oxidation could be presented at 550, 650 and 750 °C. While, in the others research efforts carried out *in situ*, in a furnace [8] from the Colombian refinery and a boiler [9], [10], the combined effects of oxidation, carburization and sulfurization were obtained. Therefore, many actors influence the final behavior of P91 steel during its operation in industrial equipment.
Another factor that should be considered in these investigations and that has been gaining strength in the scientific community, are the studies in dual environments, mainly of SOFC cells [12]–[14], which aim to simulate, as accurately as possible, the simultaneous effects to which metal parts and pipes are exposed into the different productive sectors. Thus, for example, in a boiler the P91 pipelines get the dual influence of water vapor at the outer face and flue gases at the inner face simultaneously.

In that sense, the contribution of this work went beyond checking separately the effect of water vapor [15]–[24] and carburization [7], [23], [25]–[28] on P91 steel, leading phenomena in the absence of sulfur compounds. The results presented below, seek to provide a more accurate explanation of P91 response to different environments and corrosive effects. Other similar research efforts have been developed in the past on the ferritic steels family 9-12% Cr [29], [30], but not in the simulated dual environment of H_2O/O_2-N_2-CO_2-H_2O, obtained based on the operating conditions used by some Colombian industrial boilers.

2 Experimental

2.1 Experimental Conditions

The experimental conditions were selected based on previous studies conducted by Alviz *et al.* [10] in which some industrial boilers operating conditions and the flue gases molar composition (calculated through simulation in Aspen HYSYS 8.6) were established (72.73 %N_2, 8.30 %CO_2, 3.37 %O_2, 15.60 %H_2O). Besides, other test variables were defined as: evaluation times between 1 and 200 h, 1 atm of pressure for each environment, a P91 critical temperature of 650 ºC, flue gases mass flow of 11.45 g/h and water vapor mass flow of 2.15 g/h. This last mass flow was the same in both streams, in order to be able to argue about the additional effect produced by the oxidizing species CO_2 and O_2 on the combustion side.

2.2 Material

The P91 steel samples used for the experimental tests were obtained by cylindrical machining and wire cutting, from a 15 cm long and 2.5 cm thick tube, whose composition was obtained by atomic emission spectroscopy (Table 1). The final dimensions of the coupons were 3 mm thick and 15 mm diameter, with an exposed area of 1.33 cm^2 per face. The different samples evaluated were sanded with silicon carbide paper until fine surface finishes were reached, to then be exposed to an ultrasonic bath with acetone, eliminating possible impurities contributions.

Table 1 – P91 steel weight elemental fractions as received

Element	**C**	**Mn**	**P**	**S**	**Si**	**Cr**
% Weight	0,106	0,316	0,013	0,003	0,768	8,439
Element	**V**	**N**	**Ni**	**Al**	**Nb**	**Mo**
% Weigtht	0,024	0,015	0,271	0,006	0,008	0,989

2.3 Experimental Setup

To carry water vapor into the experimental built system, an argon stream was humidified in a bubbler at 73 °C, whereas for the flue gas stream, the mixture of $86.2N_2/9.8CO_2/4.0O_2$ was the one that helped to drag the water vapor at the same temperature. The assembly flow network was assisted by electric heating cords to avoid condensation of water vapor before entering to the reactor. As can be followed in Figure 1, the main reactor (quartz tube) contained the device that allowed the coupons exposure (introduced by duplicate in each test) to the different study environments. The device was made up of 316L stainless steel for greater corrosion resistance, in addition, copper seals were used to prevent galvanic corrosion between the P91 samples and the dual reactor metal parts.

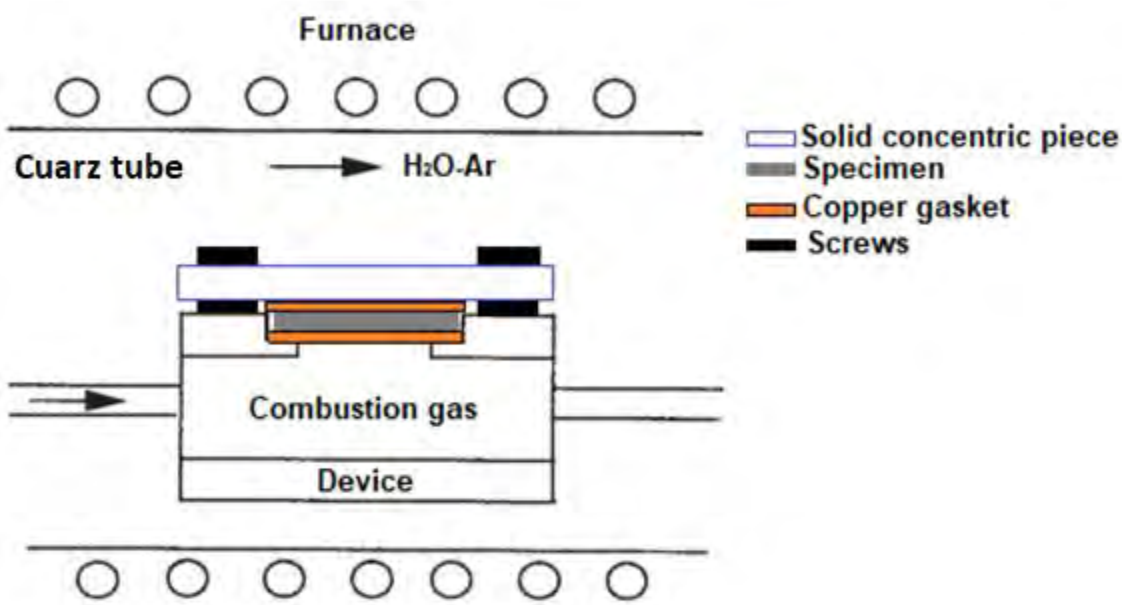


Figure 1 – Experimental dual reactor setup

2.4 Characterization Techniques

Prior to experimentation, the received steel was superficially characterized by X-ray photoelectron spectroscopy (XPS) to identify the stable chemical species at environmental conditions. Also, an initial P91 alloy microstructure inspection was performed, as much as its mechanical properties of hardness and microhardness through Rockwell A and Vickers tests.

After the experimental tests, the following techniques were implemented: Scanning Electron Microscopy with Energy Dispersive Spectroscopy (SEM-EDS), X-ray diffraction (XRD), atomic force microscope (AFM) and XPS. In their order, the equipment used were: a Quanta FEG 250 environmental scanning electron microscope (ESEM), a D8 ADVANCE BRUKER diffractometer operating in DaVinci geometry (equipped with a X-ray tube - CuKα radiation: $\lambda = 1.5406$ Å, 40 kV and 30 Ma - with a nickel filter and a detector one-dimensional LynxEye), a NanoScope IIIa AFM model and a High Resolution XPS-SPECS.

The XRD measurements had the following parameters: a scan range between 3.5 – 70.0 °2θ with a step size of 0.01526 ° and a counting time of 2 s per step. For flush type analysis, the incidence angle was selected as 0.1 ºθ. Whilst, for XPS analysis the reading conditions implemented were: a monochromatic Al-kα X-ray source operated at 100 W, a spectrometer pass energy fixed at 20 eV, for an estimated overall instrumental broadening of 0.75 eV. Furthermore, the background pressure during the data acquisition was 10^{-12} atm. Thereby, the regions studied were: O 1s, N 1s, C 1s, Fe 2p, Cr 2p Mn 2p and Mo 3d, setting the adventitious carbon peak at 284.8 eV.

Through the analysis of SEM-EDS, information about the corrosion layers morphology was obtained, both at the cross-section and superficial, as well as about the layers thicknesses and their growth speed. Moreover, AFM study helped to review uniformity aspects at the surface layers topography. For its part, the XRD readings revealed the crystalline phases present in the layers bulk. Finally, the XPS technique provided evidence about the chemical oxidation states present at surface level and possible adsorption phenomena.

Meanwhile, the kinetic study was carried out through the discontinuous gravimetric analysis, which was supported by SEM data to feed the discussion about the corrosion rate in each corrosion environment under evaluation.

3 Results and Discussion

3.1 P91 Microstructure as Received

After normalizing and tempering P91 heat treatments, the microstructure shown in Figure 2 was found.

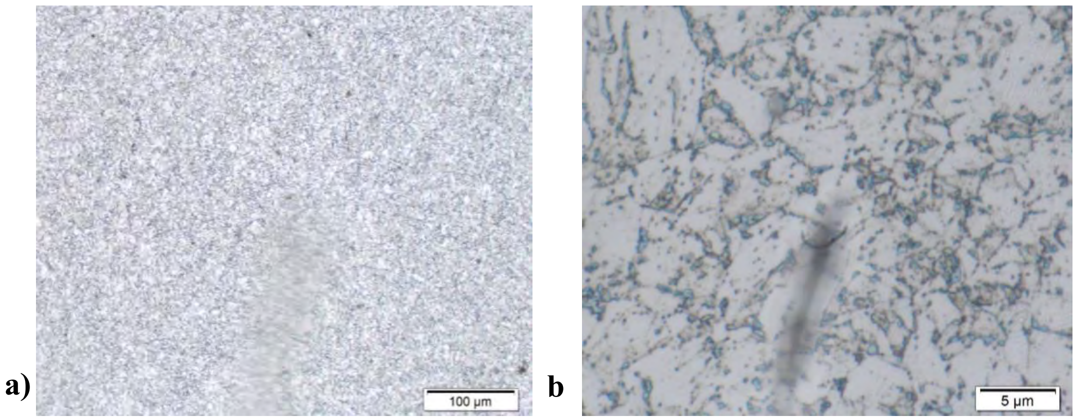


Figure 2 – P91 microstructure as received

Using the comparison method suggested by ASTM E112 [31] for stainless steels (considering the high Cr weight percentage in the alloy), a grain size (G) of 8 (Figure 1a) was observed, the smallest, which provides a good microstructure stability to the steel.
Additionally, taking as reference the Fe-Cr-C and isothermal transformation diagrams from Dunder *et al.* [32] and Durand-Charre [33], respectively, it was confirmed the presence of ferrite and carbides in the P91 alloy matrix (Figure 2b). These observed carbides were determined as $M_{23}C_6$ type, with M as: Cr, Fe, Mn, Mo, Nb and V; without ruling out the formation of carbonitrides of Nb,V(C, N), with molecular formula MX and M_2X: this time M as Nb and V, while X as C and N [34].
In addition, the values obtained through hardness and microhardness tests were in accordance with the magnitudes reported by the P91 steel fabrication sheet [4], 47 HRA and 229 Hv.

3.2 Initial P91 Oxidation State

The initial P91 surface inspection of deposited oxides, for short reaction times to environmental conditions, resulted in the determination of iron spinel ($FeO \cdot Fe_2O_3$) and chromium oxide (Cr_2O_3), which typically leads to Fe-Cr spinels. These binary mixed spinels are described as $Fe^{2+}(Fe_{1-n}Cr_n)_2O_4$, where $0 < n < 1$ denotes the mole fraction of chromite; n = 1 describes pure chromite, whereas n = 0 is magnetite [35]. Then, in Figures 2 and 3 the Fe 2p and Cr 2p regions are presented, respectively, relating the oxidation states found.

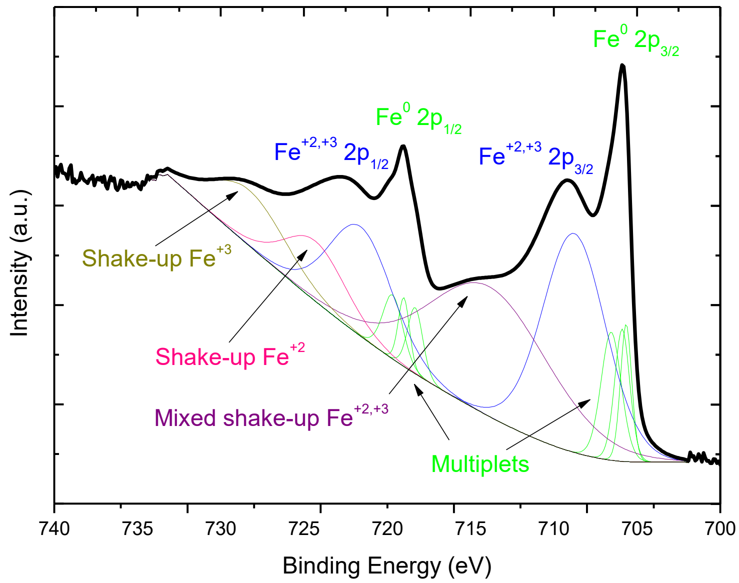


Figure 3 – Fe 2p deconvolution for P91 initial oxidation state

The binding energy for native Fe peak was fixed at Fe $2p_{3/2}$ ~ 706 eV, while its oxidation estates Fe^{+2} and Fe^{+3} at Fe $2p_{3/2}$ ~708,8 eV, according to Moulder *et al*. [36] XPS manual and the NITS database [37]. The Fe 2p energetic region commonly derives in complex arrangements, so strategies such as introducing multiplets are used to get acceptable fittings [38], in this case the Fe^{0} oxidation state was fixed by three pair of peaks (Figure 3). Otherwise, the Fe^{+2} and Fe^{+3} energy contribution were established based on their characteristic shake-ups; whose peaks follow the same oxidation states increasing order.

Similarly for the Cr 2p region, the oxidation states Cr^{0} and Cr^{+3} were identified, in their order, at Cr $2p_{3/2}$ ~ 573.3 eV and Cr $2p_{3/2}$ ~ 576.1 eV binding energies (Figure 4). The absence of other metal elements, such as Mn and Mo, was associated with both: the alloy composition and their higher required activation energy to be oxidized. In that sense, Figures 3 and 4 indicate that the predominant Cr 2p oxidation state is Cr^{+3}, while for Fe 2p is the pure metal contribution.

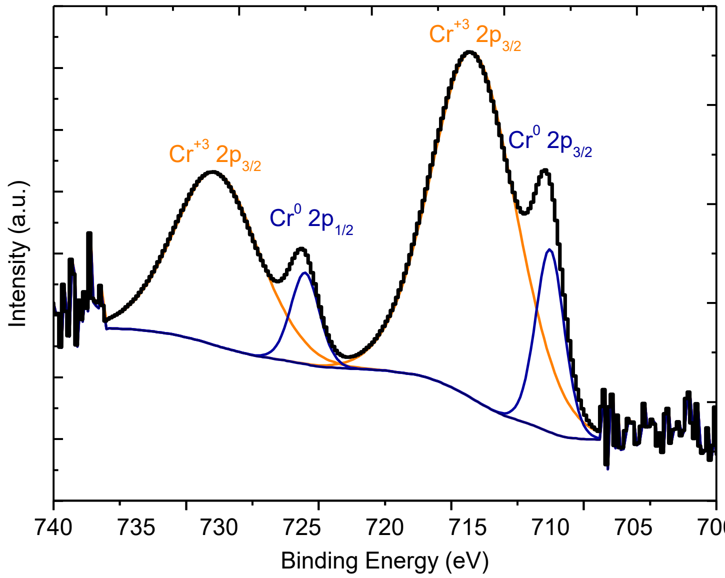


Figure 4 – Cr 2p deconvolution for P91 initial oxidation state

The discussion about the different effects caused by both the water vapor and combustion sides on P91 alloy are argued independently below, promoting a detailed analysis around the participating corrosive phenomena. Nevertheless, for the kinetic and corrosion rate studies, the total dual contribution by each environment was compiled.

3.3 Scale Composition in Water Vapor Side

When exposing P91 steel in highly oxidizing environments such as water vapor, even for a few minutes, a rapid conformation of nodules rich in Fe and Cr occurs, without forgetting the participation of other elements such as Mn, which has a high tendency towards oxidation at high temperatures (Figure 5).

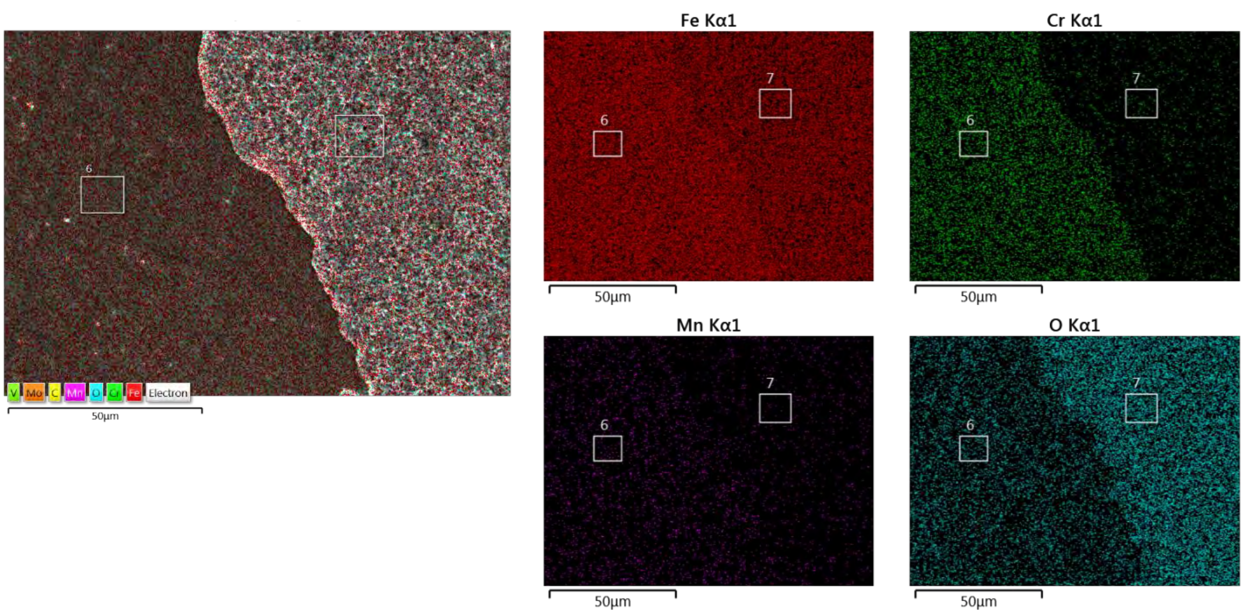


Figure 5 – Surface elemental composition after 1 h of testing at 650 ºC in water vapor

The Fe and Mn staging is frequently related to the limited Cr response capacity, which in turn, is the cause of its insufficient amount in the alloy [26]. This phenomenon is also known as breakaway oxidation [17], which is nothing more than the condensation of fissures through the chromium oxide layer, which favours the rapid diffusion and formation of poorly protective oxides, such as iron oxides.
Figure 6 shows the duplex structure of the oxide layer formed at 650 °C after 200 h of testing. The inner layer was fundamentally composed by Fe-Cr-O, possibly forming a binary mixed spinel, while the outer layer was made up of iron oxides. Traces of Mn and Mo between the layers could involve the precipitation of localized nodules of their oxides, then fed by intense diffusive processes.
P91 oxidation by water vapor has been the subject of multiple research papers, whose main contributions are associated with adverse effects on the typically reported duplex oxide layer structure [19], [21]. Thus, water vapor tends to reduce the depletion time of Cr at the metal matrix interfase and along the layers, due to the volatilization of iron and chromium oxides [39], [40], which release multiple vacant sites that give rise to pores, their coalescence, microcracks and macrocracks, finally increasing the steel corrosion rate.

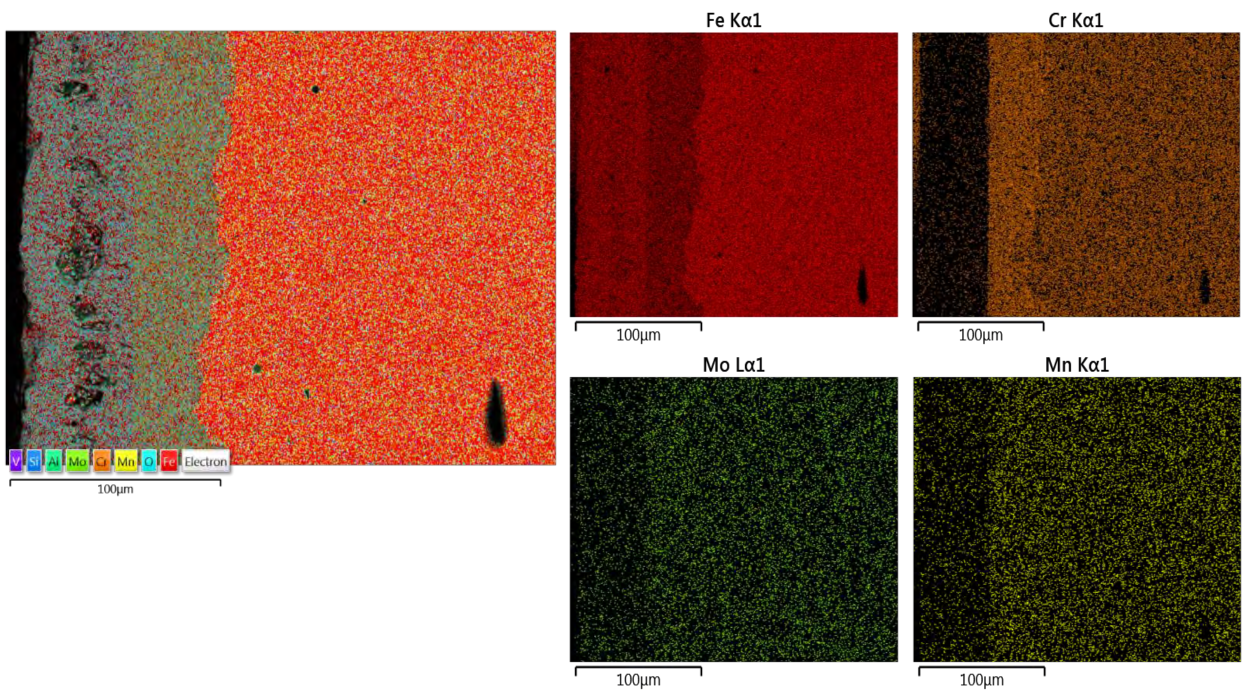


Figure 6 – Cross section elemental composition after 200 h of testing at 650 ºC in water vapor

As suggested by the corrosion mechanism proposed by Quadakkers *et al.* [20], and discussed in section 3.6, the inner layer was formed in the space initially occupied by the steel cations. The smooth line that separates the two layers is shown in Figure 6; whose guide, are the different morphologies, the abundance of Cr and the colour shades.

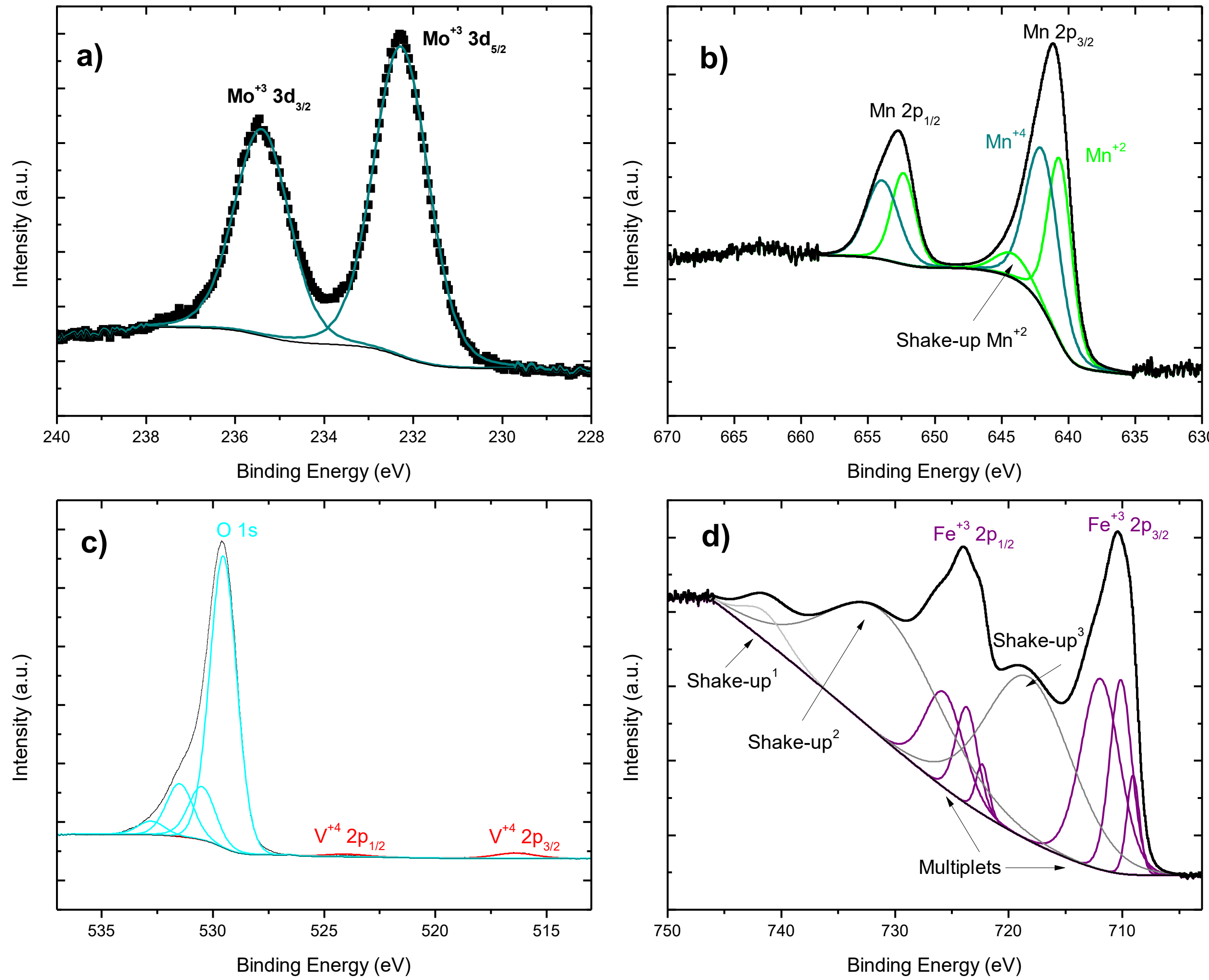


Figure 7 – Metallic regions identified by XPS at the water vapor side after 200 h at 650 ºC: a) Mo 3d, b) Mn 2p, c) V 2p and d) Fe 2p

The diffusion of metal cations was so important that it reached the layers' surface (Figure 7). Oxides that have received limited attention, such as those of Mo, Mn and V, were present at the binding energies ~232 eV, ~641 eV and ~516 eV (Figure 7a, 7b and 7c), respectively. Then, the oxidation states found were Mo^{+6}, Mn^{+2}, Mn^{+4} and V^{+4}, corresponding to the oxides MoO_3, MnO, MnO_2 and VO_2. Surprisingly, a vanadium oxide was present on the surface of the layers, despite its low content in the alloy, which gives a qualitatively high magnitude to the diffusive processes developed in water vapor at 650 °C.

At last, to finish defining the duplex layer structure, it was confirmed that among hematite and magnetite iron oxides, hematite is the one that is in thermodynamic equilibrium with the oxidizing environment, hence, it was superficially found while the magnetite was at the bulk of the layers (Figures 7d and 8).

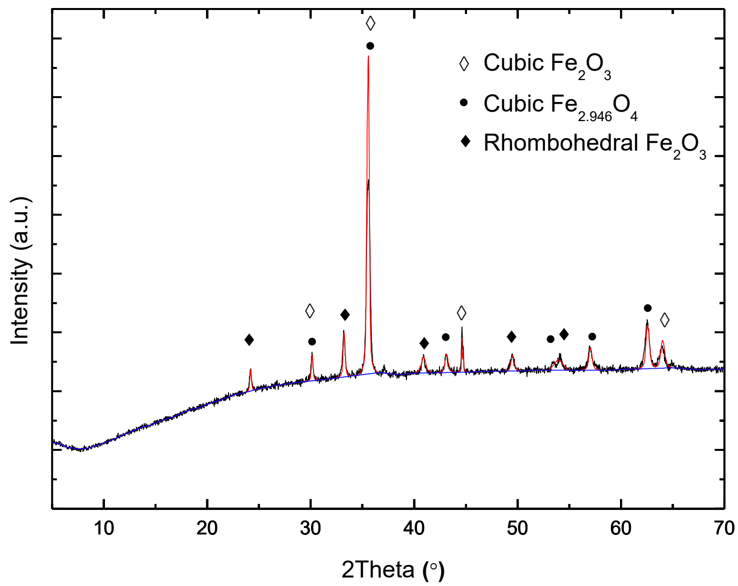


Figure 8 – Hematite and magnetite at the duplex oxide layer bulk after 200 h at 650 ºC

3.4 Scale Composition in Combustion Side

By adding CO_2, O_2 and N_2 species to water vapor, the simultaneous carburization, oxidation and nitridation effects are feasible [41]. Nonetheless, both nitriding and carburization are corrosive phenomena that require low oxidation potentials and long exposure times to penetrate considerably the steel bulk. Moreover, CO_2 and N_2 react with the free oxygen available to produce NO_x and CO_x at high temperatures; which use the fast access routes across the layers to feed the internal corrosion of the alloy.

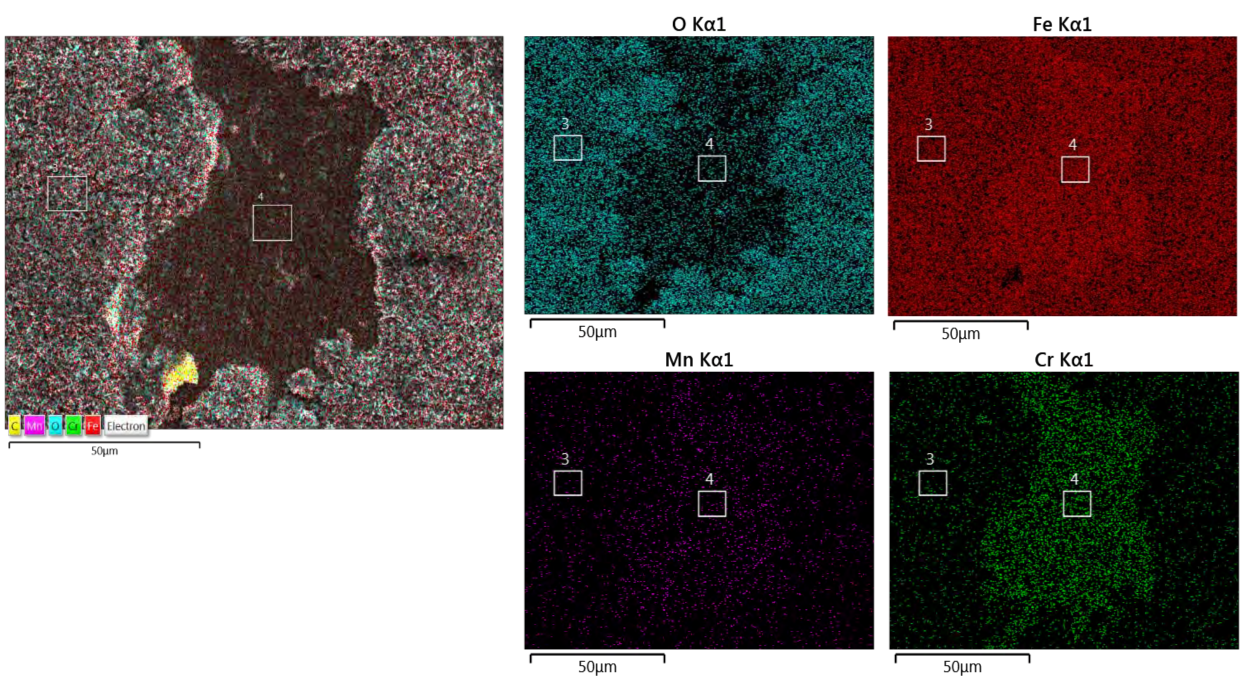


Figure 9 – Surface elemental composition after 1 h of testing at 650 ºC in combustion gases

After 1 h of testing at the combustion side (Figure 9) the nucleation process was not finished yet, such as happened with the water vapor face on the other side of the sample (Figure 5). The fast Cr depletion goes hand in hand with the rapid Fe diffusion; these cations take advantage from the chromium retention to be quickly oxidized, forming the initial spinel layer. Something similar could be reproduced by Mo and Mn cations but in less proportion, according to their mass amount in the steel.

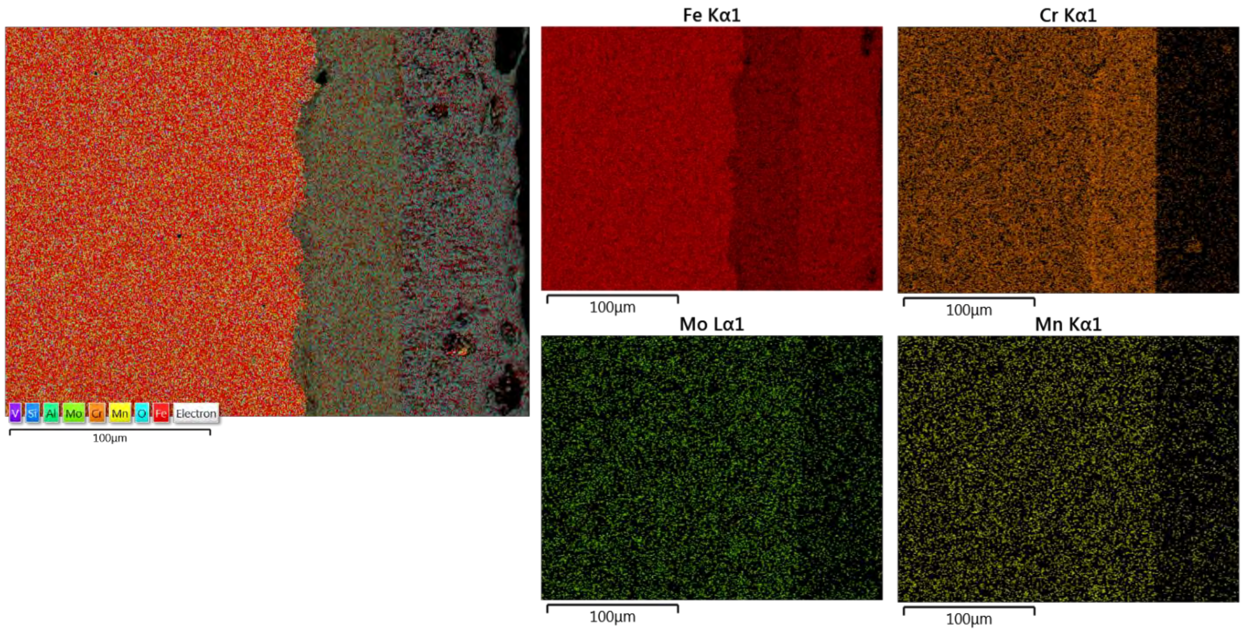


Figure 10 - Cross section elemental composition after 200 h of testing at 650 ºC in combustion gases

For its part, the ratio between the inner and outer layers was even closer to unity than in the atmosphere of pure vapor. This observation implies that oxidation was more severe, as well as happened with the diffusive processes and the transport of species along the layers, behaviour that could be explained by the greater participation of oxidant compounds in combustion environments. In fact, just with the free oxygen effect, the steel oxidation rate get highly stimulated, since the contribution of other oxidizing agents requires dissociation reactions. In addition, high oxidation potentials may be beneficial for alloys, insomuch as their generate significant reductions in the carburization and nitridation phenomena [26].

In other results, carbides and nitrides were found at the oxide layer surface (Figure 11a and 11b). Usually, the precipitation of these compounds is not viable at high oxidation potentials [41], [42], for which chemical and physical adsorption phenomena deserve to be considered in combustion environments. Namely, the molecules that would be involved in these processes would be the NO_x and CO_x, because of their continuous mass flow and feasible polarity. however, the re-oxidation and volatilization of these surface carbides and nitrides are thermodynamically probable. Even though, under this scenario, the penetration into the metal bulk of these simultaneous corrosive effects is only a matter of time to become visible, so 1000 h of laboratory testing are often used [26], [43].

Finally, the binding energies provided by the XPS analysis at ~283 eV and ~387 eV confirmed the superficially condensed metal carbides and nitrides (Figure 11).

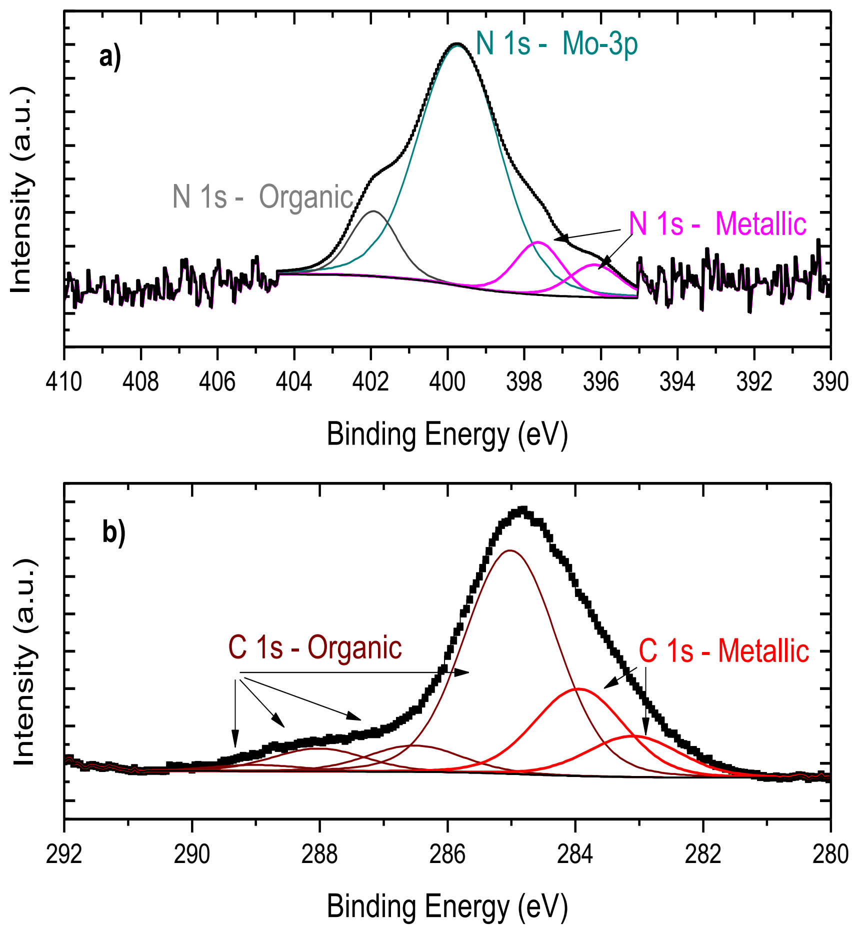


Figure 11 - Metallic regions identified by XPS at the combustion side: a) N 1s and b) C 1s after 200 h at 650 ºC

3.5 Corrosion Rates and Diffusion in Solid State

Through the kinetic study it was possible to confirm that the growth law that the oxide layers follow is related to diffusive processes (Figure 12). So that, as the oxidation time of the steel progresses, the metal cations find greater difficulties to reach the gas interface. However, this behavior is not typical of all alloys, since their require significant amounts of elements such as Al, Cr and Si, whose oxides have been found adherent and resistant to high temperatures conditions. Next, in Equation 1 the mathematical expression that responds to the parabolic layer growth law is presented.

Equation 1 – Parabolic growth law

$$X^2 = k_p t$$

Where, X represents the mass gain per unit area or the thickness of the layers, t the time and k_p the parabolic constant.

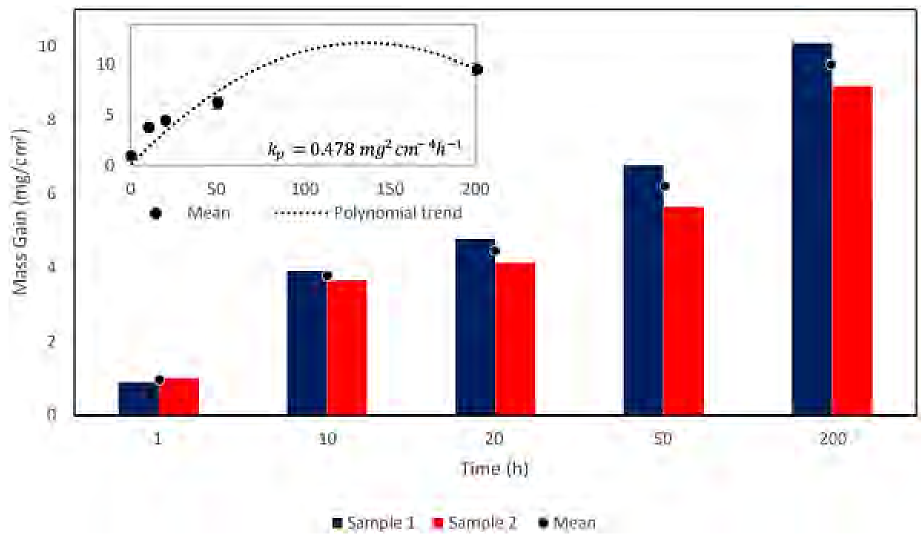


Figure 12 – Parabolic law followed by the P91 steel during its oxidation in the dual environment of water vapor/combustion gases

Apart from this, the corrosion rate was also calculated in both corrosion sides (Figure 13). These results were obtained based on the measurements of the internal layer thickness developed in each environment, and with the help of the NACE RP 0775 standard [44], which establishes the onset of severe corrosion from 0.25 mm/year.

Furthermore, and as expected, the corrosion rate was higher at the combustion products side than at the water vapor face, due to the direct contribution of free oxygen to the first one. Also, it is valid to point out that a limitation of these calculations were the short evaluation times implemented, which is why corrosion rates were found severe. In the long term, the trend would stabilize a relatively immutable value over time, yielding a more accurate measurement to properly assess P91 steel.

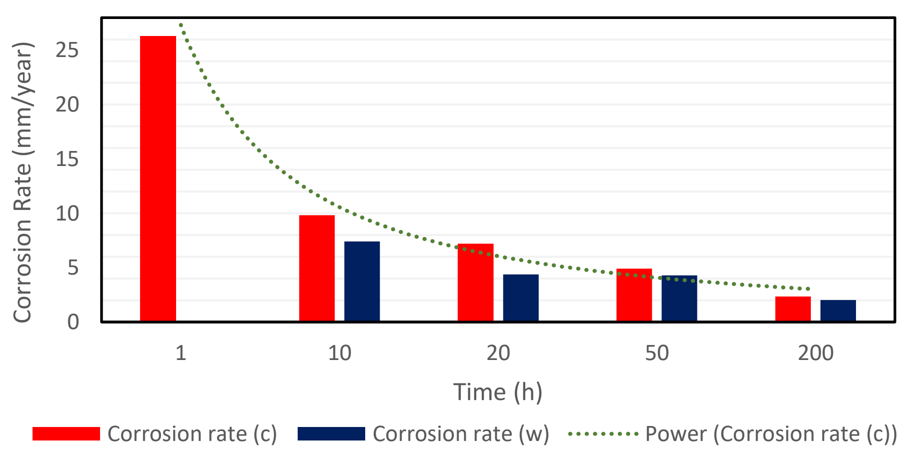


Figure 13 – Corrosion rate at combustion side (c) and water vapor side (w)

In short, when implementing P91 steel in different industrial processes in which the dual environment is composed by water vapor and flue gases, the side on which the failure would happens would be in the latter.

3.6 Corrosion Mechanism for Water Vapor

As was argued in sections 3.3 and 3.4, the mass transport in the duplex layers is conducted by the flow of cations towards the gas interface as much as by the flow of oxidizing species towards the metal matrix. Despite the fact that there is a slight domain of cations diffusion over the transport of oxidant species along the layers (Figures 14). This behavior is explained by the difficulties that the oxidizing species have to face through the duplex structure to finally get the metal interfase. Although, the non-uniformity of the layers and their detachment play in support to the gases mass flow (Figure 15). In this regard, authors such as Martinelli *et al.* [23] have proposed that the different gaseous compounds take advantage of the "available space" left by the multiple cations that leave the metal surface, leading to the nucleation of the new internal oxide, whereas the driven out cations constitute the external layer of iron oxides.

Further, Oleksak *et al.* [45] demonstrated the existence of these microchannels across the oxide layers, through the technique of atom probe tomography, as well as this work shows in the SEM picture of Figure 16. Besides, Ehlers *et al.* [17] confirmed the penetration of H_2O and O_2 compounds along the oxide layers by monitoring these molecules with O^{16} and O^{18} isotopes. In that sense, it was also summarized that water vapor can reach the metal matrix but is mainly concentrated in the outer layer, while O_2 is mostly in the inner layer.

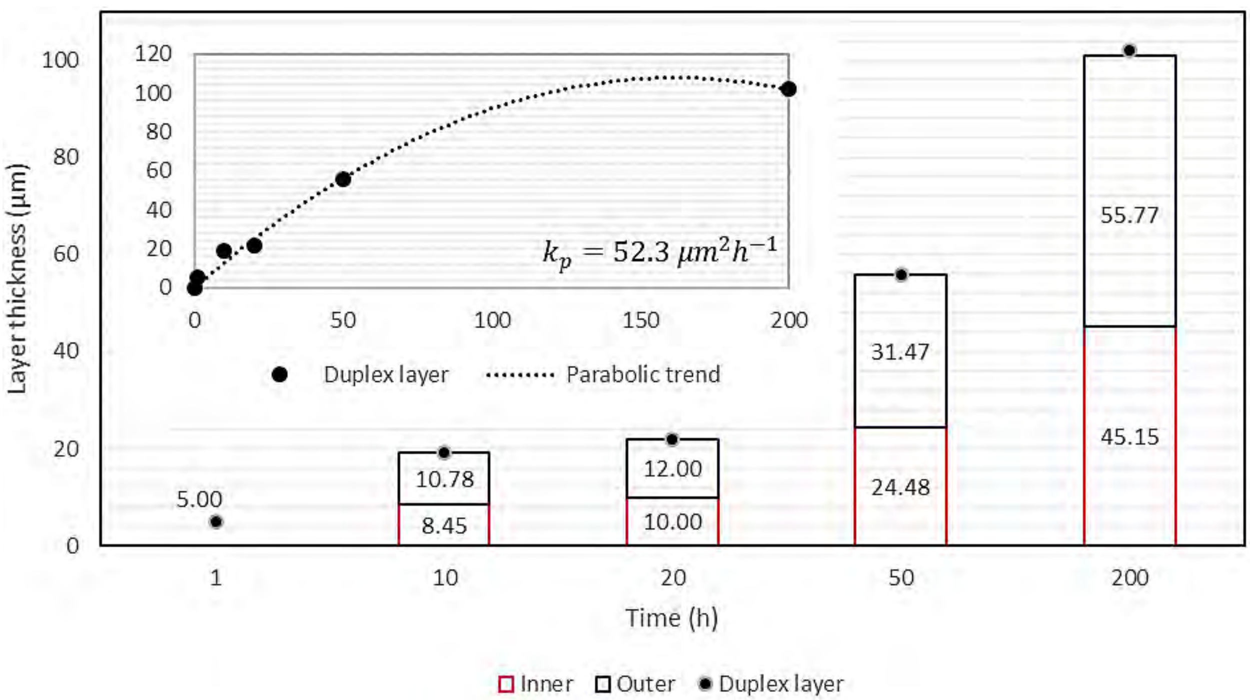
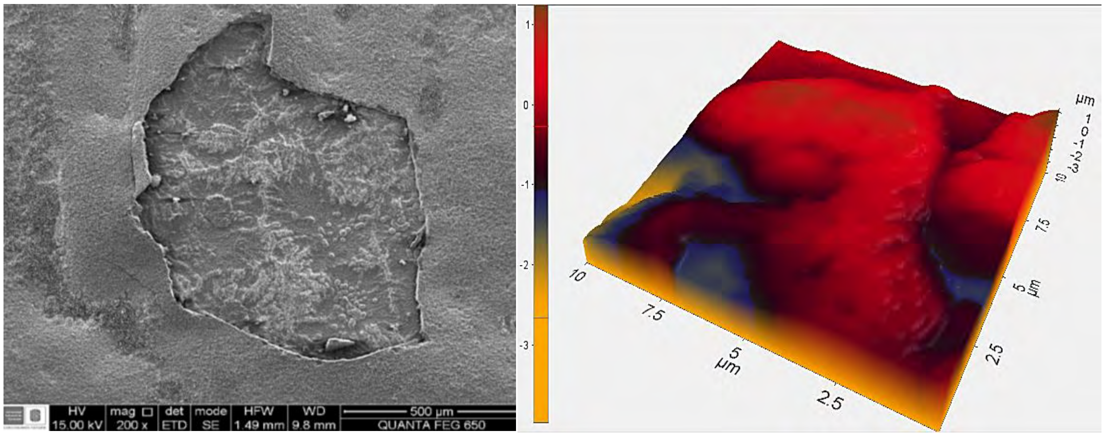


Figure 14 – Layers thicknesses in the water vapor side

To sum up, the duplex layer growth mechanism is based on the use of easily accessible microchannels by the oxidizing agents, which once created by the high diffusional processes of cations at high temperatures, try to match both mass transfer rates, reaching a ratio of one between the inner and outer layers.



. *Figure 15 – Duplex oxide layer surface at the water vapor side after 200 h at 650 ºC*

Element	Wt%	At%
CK	07.13	23.57
OK	05.51	13.68
SiK	00.63	00.89
MoL	01.05	00.43
CrK	08.82	06.74
MnK	00.74	00.53
FeK	76.13	54.15
Matrix	Correction	ZAF

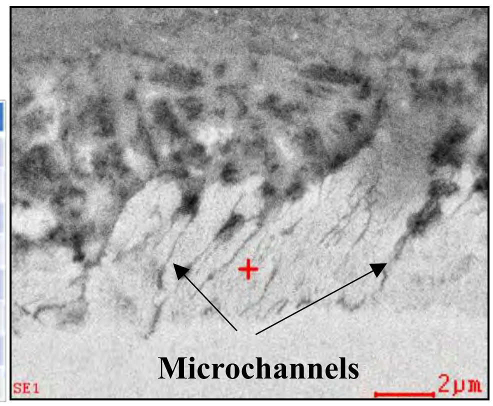


Figure 16. Internal oxidation zone for P91 steel at the water vapor side after 20 h at 650 ºC

3.7 Corrosion Mechanism for Combustion Gases

Taking as reference the oxidation mechanism previously proposed for P91 steel in water vapor, and with the intention of determining how it complements the effects of carburization in a combustion environment, the following theoretical calculations are presented. The reactions involved in the release of carbon from the gaseous environment are the following:

Equation 2 – CO_2 (g) dissociation reaction

$$CO_2\ (g) = CO(g) + 1/2\, O_2\ (g)$$

Equation 3 – Boudouard reaction

$$2CO\ (g) = CO_2(g) + C$$

It is then, through the Boudouard reaction that the carbon activity is obtained in the combustion environment studied, which has been reported more favourable at low temperatures [46]. In addition to Equations 2 and 3, Equations 4 and 5 are introduced as the thermodynamic support.

Equation 4 – Thermodinamic expresion for CO_2 (g) dissociation reaction

$$\Delta G^{\circ} = -RTln\left(P_{CO}P_{O_2}^{0,5} / P_{CO_2}\right), with\ \Delta G^{\circ} = 282420 - 86{,}8T\ (J/mol)$$

$$Equation\ 5 - Thermodinamic\ expresion\ for\ Boudouard\ reaction$$

$$\Delta G^{\circ} = -RTln\left({P_{CO_2} a_{c,gas}}\Big/{P^2{}_{CO}}\right), with\ \Delta G^{\circ} = -170700 + 174{,}5T\ (J/mol)$$

Additionally, the partial pressures of oxygen and carbon dioxide from the combustion environment were $P_{O_2} = 3.37 \times 10^{-2} atm$ and $P_{CO_2} = 8.30 \times 10^{-2} atm$. With these values and the mathematical expressions of Equations 2, 3, 4 and 5, the carbon activity in the carburization environment was determined as $a_{c,gas} = 1.10 \times 10^{-22}$.

$$Equation\ 6 - Cr_{23}C_6\ addition\ reaction$$

$$23/6\,Cr + C = \ 1/6\,Cr_{23}C_6$$

$$Equation\ 7 - Thermodinamic\ expresion\ for\ Cr_{23}C_6\ reaction$$

$$\Delta G^{\circ} = -RTln\left({a^{\frac{1}{6}}{}_{Cr_{23}C_6}}\Big/{a_{Cr}^{\frac{23}{6}} a_{c,P91}}\right), con\ \Delta G^{\circ} \ = -411200 - 38{,}7T\ (J/mol)$$

In like manner, to get the P91 carbon activity the carbide $Cr_{23}C_6$ was selected as the most stable for ferritic steels, with $a_{Cr_{23}C_6} = 1$ and $a_{Cr} = 0.08$. Then, the resulted carbon activity was calculated by Equations 6 and 7 as $a_{c,P91} = \ 1.10 \times 10^{-22}$. Consequently, the driving force that promotes carburization, in similar combustion atmospheres, is not the solid state diffusion, for which it was necessary satisfy the expression $a_{c,gas} > a_{c,P91}$.

The carburization mechanism is then based on the discussion previously raised around the oxidation of P91 steel in water vapor. For this purpose, Taylor *et al.* [47] demonstrated the entry of CO_2 to the alloy matrix by monitoring $C^{16}O_2$ and $C^{18}O_2$ isotopes, thus favoring the Boudouard reaction to stimulate the internal carburization and oxidation.

The same discussion proceeds for the nitridation mechanism, for which nitrogen atoms are transported by nitrates through the microchannels (Figure 17) until the metal interface, where the low oxidation potential allows the internal nitrides precipitation [10], [11].

Element	Wt%	At%
CK	04.95	16.71
OK	07.58	19.23
SiK	00.67	00.96
MoL	01.56	00.66
CrK	09.14	07.13
MnK	00.78	00.58
FeK	75.32	54.72
Matrix	Correction	ZAF

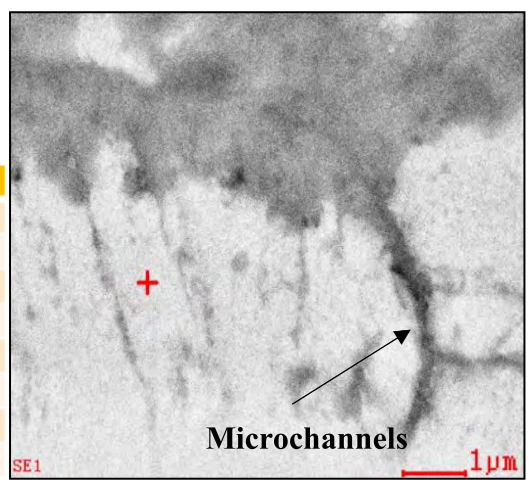


Figure 17 - . Internal oxidation zone for P91 steel at the combustion side after 20 h at 650 ºC

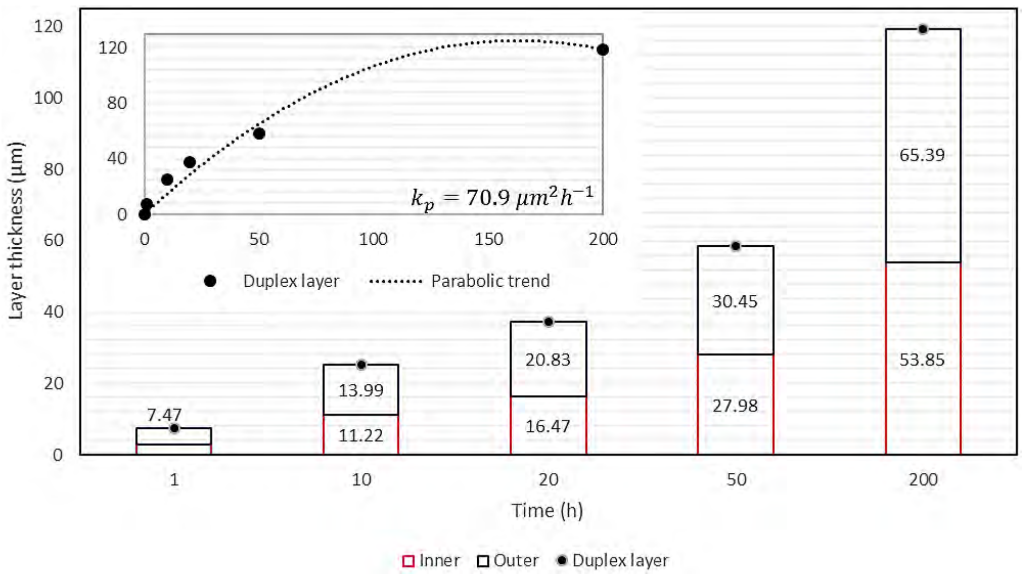


Figure 18 - Layers thicknesses in the combustion side

In other results, the layer thicknesses obtained in this atmosphere were in tune with the corrosion velocity results, as much as with the approaches made about the different corrosion mechanisms proposed. Further, by using Equations 1 and 8 a mathematical expression (Equation 9) was determined to relate the parabolic kinetic constants from the duplex layer structure.

Equation 8 - Relationship between the thicknesses of the outer and inner layers

$$X_T = X_e + X_i$$

Equation 9 – Mathematical expression among the parabolic kinetic constants of duplex layers

$$K_T = K_e + 2\sqrt{K_e K_i} + K_i$$

Finally, the kinetic constants obtained were: $K_i = 14.6\ \mu m^2 h^{-1}$ and $K_e = 21.2\ \mu m^2 h^{-1}$, confirming the higher growth rate of the outer layer.

4 Conclusions and Future Work

P91 ferritic steel is an alloy widely used in the petrochemical industry, which has earned its place thanks to its good mechanical properties and acceptable corrosion resistance. Nonetheless, its corrosion mechanism is not clearly established in the conditions in which it is normally implemented, which is why this research effort was developed. With this reference framework, study conditions similar to those used in boiler operation were selected; that is, a dual environment of combustion products and water vapor at 650 ° C.

The main results are summarized in a corrosion mechanism dominated by solid state diffusion processes and the use of available spaces left by metal cations. The high temperature, the long exposure times and the presence of water vapor, are the ideal allies for the multiple formation of micro routes, which serve as access to the gaseous oxidizing species on their way to the metal interface. Next, both mass transport mechanisms tend to equalize, making the flow of oxidizing carburizers and nitrurants agents easier through the duplex oxide layer structure. All of the above, without skipping the contribution of chemisorption or physisorption phenomena, which could also contribute to the precipitation of surface oxides, carbides and nitrides. Finally, the degradation rate of P91 steel resulted more severe in the combustion environment due to the presence of free oxygen, which is highly aggressive as oxidant since it does not depend on dissociation reactions.

As a recommendation, the implementation of longer exposure times, a greater revision of the internal corrosion zone, a detailed study of the surface adsorption phenomena, as well as the study of the influence of one environment on the other are left for future work.

5 References

[1] I. Le May, “Creep and fracture of engineering materials and structures,” *Mater. Charact.*, vol. 33, p. 79, 2003.

[2] F. Noble, B. Senior, and B. Eyre, “The effect of phosphorus on the ductility of 9Cr-1Mo steels,” *Acta Metall. Mater.*, vol. 38, no. 5, pp. 709–717, May 1990.

[3] A. Fabricius and P. S. Jackson, “Premature Grade 91 failures - worldwide plant operational experiences,” *Eng. Fail. Anal.*, vol. 66, pp. 398–406, 2016.

[4] ASTM International, “Standard Specification for Seamless Ferritic Alloy-Steel Pipe for High-Temperature: A335/A335M − 15a,” 2003.

[5] T. Sasaki, K. Kobayashi, T. Yamaura, T. Kasuya, and T. Masuda, “Production and properties of seamless modified 9Cr-1Mo steel boiler tubes,” *Kawasaki Steel Tech. Rep.*, vol. 25, pp. 78–87, 1991.

[6] G. Ju, W. Wu, and S. Dai, “Failure of 9Cr-1Mo tubes in a feed furnace of dehydrogenation unit,” *Int. J. Press. Vessel. Pip.*, vol. 74, no. 3, pp. 199–204, 1997.

[7] D. Peña, C. Vásquez, D. Laverde, and A. Serna, “Corrosión a temperatura alta del acero ferrítico 9Cr-1Mo modificado P91, en atmósferas simuladas oxidantes-carburantes,” *Rev. Metal.*, vol. 48, no. 2, pp. 97–106, 2012.

[8] A. Alviz, V. Kafarov, and L. Meriño, “Methodology for evaluation of corrosion damage during combustion process in refinery and petrochemical industry. Case study: AISI 304 and ASTM A335 P5 steels,” *Chem. Eng. Trans.*, vol. 61, pp. 1315–1320, 2017.

[9] J. Orozco, A. Alviz-Meza, V. Kafarov, D. Y. Peña-Ballesteros, C. Osses, and M. Pinto, “Evaluation of cyclic corrosion on ASTM A335 P92 steel exposed to a combustion atmosphere in a horizontal boiler,” *Chem. Eng. Trans.*, vol. 67, pp. 13–18, 2018.

[10] A. Alviz-Meza, V. Kafarov, and D. Y. Peña-ballesteros, “Evaluation of Corrosion Damage Obtained During the Combustion Process in a Boiler . Case Study : Ferritic ASTM A335 P91 Steel,” *Chem. Eng. Trans.*, vol. 70, pp. 1093–1098, 2018.

[11] A. Alviz-Meza, J. Sanabria-Cala, V. Kafarov, and D. Y. Peña-Ballesteros, “Study of Continuous Corrosion on ASTM A335 P91 Steel in an Environment of CO2-O2-N2-H2O Derived from the Theoretical Combustion Products of a Mixture of Refining Gases at High Temperatures,” *Chem. Eng. Trans.*, vol. 70, pp. 1069–1074, 2018.

[12] P. Alnegren, M. Sattari, J. Svensson, and J. Froitzheim, “Temperature dependence of corrosion of ferritic stainless steel in dual atmosphere at 600 – 800 ° C,” *J. Power Sources*, vol. 392, no. April, pp. 129–138, 2018.

[13] P. Alnegren, M. Sattari, J. Svensson, and J. Froitzheim, “Severe dual atmosphere effect at 600 C for stainless steel 441,” *J. Power Sources*, vol. 301, pp. 170–178, 2016.

[14] A. W. B. Skilbred and R. Haugsrud, “The effect of water vapour on the corrosion of Sandvik Sanergy HT under dual atmosphere conditions,” *Oxid. Met.*, vol. 79, no. 5–6, pp. 639–654, 2013.

[15] A. Alviz Meza, V. Kafarov, and D. Y. Pena Ballesteros, “Study of the continuous corrosion in an oxidation environment derived from the theoretical combustion products in a refinery.

Case study: Ferritic steel ASTM A335 P91," *J. Phys. Conf. Ser.*, vol. 935, no. 1, pp. 0–7, 2017.

[16] J. C. Orozco, V. Kafarov, D. Y. Pena, and A. Alviz, "Effects of oxidation-nitridation in the presence of water vapor on ASTM A335 P92 steel using SEM-EDS and XPS characterization techniques," *J. Phys. Conf. Ser.*, vol. 935, no. 1, pp. 0–7, 2017.

[17] J. Ehlers *et al.*, "Enhanced oxidation of the 9%Cr steel P91 in water vapour containing environments," *Corros. Sci.*, vol. 48, no. 11, pp. 3428–3454, 2006.

[18] S. Swaminathan, C. Mallika, N. Gopala, C. Thinaharan, T. Jayakumar, and K. Mudali, "Evolution of surface chemistry and morphology of oxide scale formed during initial stage oxidation of modified 9Cr – 1Mo steel," *Corros. Sci.*, vol. 79, pp. 59–68, 2014.

[19] S. Saunders, M. Monteiro, and F. Rizzo, "The oxidation behaviour of metals and alloys at high temperatures in atmospheres containing water vapour: A review," *Prog. Mater. Sci.*, vol. 53, no. 5, pp. 775–837, 2008.

[20] W. J. Quadakkers, P. J. Ennis, J. Zurek, and M. Michalik, "Steam oxidation of ferritic steels - Laboratory test kinetic data," *Mater. High Temp.*, vol. 22, no. 1–2, pp. 47–60, 2005.

[21] P. Ennis and W. Quadakkers, "Mechanisms of oxidation and the influence of steam oxidation on service life of steam power plant components," in *Creep Resistant Steels*, IV., F. Abe, Ed. Woodhead Publishing Limited, 2008, pp. 519–535.

[22] T. Jonsson *et al.*, "Oxidation of Fe–10Cr in O2 and in O2+H2O environment at 600°C: A microstructural investigation," *Corros. Sci.*, vol. 75, pp. 326–336, 2013.

[23] L. Martinelli, C. Desgranges, F. Rouillard, K. Ginestar, M. Tabarant, and K. Rousseau, "Comparative oxidation behaviour of Fe-9Crsteel in CO 2 and H 2 O at 550 ° C : detailed analysis of the inner oxide layer," *Corros. Sci.*, vol. 100, pp. 253–266, 2015.

[24] N. Otsuka, "Carburization of 9 %Cr steels in a simulated oxyfuel corrosion environment," *Oxid. Met.*, vol. 80, no. 5–6, pp. 565–575, 2013.

[25] T. Gheno *et al.*, "Carburisation of ferritic Fe-Cr alloys by low carbon activity gases," *Corros. Sci.*, vol. 53, no. 9, pp. 2767–2777, 2011.

[26] G. Meier *et al.*, "Effect of Alloy Composition and Exposure Conditions on the Selective Oxidation Behavior of Ferritic Fe-Cr and Fe-Cr -X Alloys," *Oxid. Met.*, vol. 74, no. 5–6, pp. 319–340, 2010.

[27] F. Rouillard and T. Furukawa, "Corrosion of 9-12Cr ferritic – martensitic steels in high-temperature," *Corros. Sci.*, vol. 105, pp. 120–132, 2016.

[28] K. Kaya, S. Hayashi, and S. Ukai, "High-temperature Oxidation Behavior of 9Cr Ferritic-steel in Carbon Dioxide," *ISIJ Int.*, vol. 54, no. 6, pp. 1379–1385, 2014.

[29] K. Chandra and A. Kranzmann, "High temperature oxidation of 9 – 12 % Cr ferritic / martensitic steels under dual-environment conditions," *Corros. Eng. Sci. Technol.*, vol. 53, no. S1, pp. 27–33, 2018.

[30] D. Huenert and A. Kranzmann, "Impact of oxyfuel atmospheres H2O / CO2 / O2 and H2O / CO2 on the oxidation of ferritic – martensitic and austenitic steels," *Corros. Sci.*, vol. 53, no. 6, pp. 2306–2317, 2011.

[31] ASTM Internacional, "Standard Test Methods for Determining Average Grain Size: E112 - 10," 2004.

[32] M. Dunder, I. Samardzic, and T. Vuherer, "Weldability investigation steel P91 by weld thermal cycle simulation," *Metalurgija*, vol. 54, no. 3, pp. 539–542, 2015.

[33] madeleine Durand-charre, "The basic phase diagrams," in *The Microestructure of Steels and Cast Irons*, Springer, Ed. pp. 51–73.

[34] N. E. Zavaleta, H. De Cicco, and C. Danón, "Influencia del tiempo de revenido a 780 o C sobre la resistencia al creep del acero ASTM A335 P91," *Materia*, vol. 23, no. 2, pp. 1–8, 2018.
[35] K. Delura, P. Bylina, M. Jele, and J. Kruczyk, "Mineralogy and magnetism of Fe – Cr spinel series minerals from podiform chromitites and dunites from T apadła (Sudetic ophiolite , SW Poland) and their relationship to palaeomagnetic results of the dunites," *Geophys. J. Int.*, vol. 175, pp. 885–900, 2008.
[36] J. Moulder, W. Stickle, P. Sobol, and K. Bomben, *Handbook of X-Ray Photoelectron Spectroscopy*. Eden Prairie, United States of America: Perkin- Elmer Corporation, 1992.
[37] NITS, "National Institute of Standards and Technology NIST X-ray Photoelectron Spectroscopy (XPS) Database," 2012. [Online]. Available: https://srdata.nist.gov/xps/main_search_menu.aspx. [Accessed: 06-Mar-2019].
[38] M. Bravo, J. Huerta, D. Cabrera, and A. Herrera, "Composition assessment of ferric oxide by accurate peak fitting of the Fe 2p photoemission spectrum," *Surf. Interface Anal.*, vol. 49, no. 4, pp. 253–260, 2016.
[39] F. Pérez and S. Castañeda, "Study of oxyhydroxides formation on P91 ferritic steel and CVD-FBR coated by Al in contact with Ar + 40% H 2O at 650 °C by by TG-mass spectrometry," *Surf. Coat. Technol.*, vol. 201, pp. 6239–6246, 2007.
[40] F. Pérez and S. Castañeda, "Study by means of the mass spectrometry of volatile species in the oxidation of Cr, Cr2O3, Al, Al2O3, Si, SiO2, Fe and ferritic/martensitic steel samples at 923 K in Ar+(10 to 80%)H2O vapor atmosphere for new-materials design," *Oxid. Met.*, vol. 66, no. 5–6, pp. 231–251, 2006.
[41] X. Zheng and D. Young, "High-Temperature Corrosion of Cr2O3-Forming Alloys in CO-CO2-N2 Atmospheres," *Oxid. Met.*, vol. 42, no. 3/4, 1994.
[42] X. G. Zheng and D. J. Young, "Corrosion of pure in CO-CO2-SO2-N2 atmospheres," *Corros. Sci.*, vol. 36, no. 12, pp. 1999–2015, 1994.
[43] J. Piro, T. Olszewski, H. Penkalla, G. Meier, L. Singheiser, and W. Quadakkers, "Scale formation mechanisms of martensitic steels in high CO2/H2O-containing gases simulating oxyfuel environments," *Mater. High Temp.*, vol. 26, no. 1, pp. 63–72, 2009.
[44] NACE International, "Standard Recommended Practice: Preparation, Installation, Analysis, and Interpretation of Corrosion Coupons in Oilfield Operation," Houston, RP 0775, 2005.
[45] R. P. Oleksak, M. Kapoor, D. Perea, G. Holcomb, and O. Dogan, "The role of metal vacancies during high-temperature oxidation of alloys," *npj Mater. Degrad.*, vol. 2, no. 1, p. 25, 2018.
[46] K. Sridharan and M. Anderson, "Corrosion of Structural Materials for Advanced Supercritical Carbon- Dioxide Brayton Cycle Final Report for Project : Corrosion of Structural Materials for Advanced Supercritical Carbon- Dioxide Brayton Cycle," Madison, 2017.
[47] M. R. Taylor, J. M. Calvert, D. G. Lees, and D. B. Meadowcroft, "The Mechanism of Corrosion of Fe-9 % Cr Alloys in Carbon Dioxide," *Oxid. Met.*, vol. 14, no. 6, pp. 499–516, 1980.

Poster Presentations

Process Safety and the Race for the Bomb: Process History Poster Presentation
Lindsey Bredemeyer, *Bredemeyer Engineering*

Analysis of the Low Perception of Risk: Causes, Consequences and Barriers
Salvador Ávila Filho, *Federal Universidad de Bahia*

Analysis of Reliability Mapping in Refining Industry: Identification of Critical Regions and Interventions in Complex Production Systems
Salvador Ávila Filho, *Federal Universidad de Bahia*

Relationship Between Human-Managerial and Social-Organizational Factors: For Industry Safeguards Project: Dynamic Bayesian Networks
Salvador Ávila Filho, *Universidad Federal de Bahia*

Machine Learning Prediction of Hydrocarbon Mixture Lower Flammability Limits Using Quantitative Structure-Property Relationship Models
Zeren Jiao, *MKOPSC*

Influence and Effects of the use of Flue Gas- Water Steam on the API N-80 Steel
Juan Orozco, *Universidad Industrial de Santander*

Effects of dust adhesion forces on cloud characteristics in minimum ignition energy (MIE) apparatus
Taylor Ritchie, *TAMU*

Thermal Hazard Assessment of Benzoyl Peroxide Mixed with Dry Fire-Extinguishing Chemicals
Yueqi Shen, *MKOPSC*

Reaction Hazard Study for H2O2 Oxidation of 2-Octanol in a Heterogeneous Batch Reactor
Yue Sun, *MKOPSC*

Speaker Bios

Day 1 Track 1

Management, Operational, and Offshore Assets Integrity

Abdul Aldeeb

Advancing Assets Integrity Management to Meet Safe, Reliable, and Sustainable Operations

Dr. Abdul Aldeeb is the Head of Technology and Consulting at Siemens Process & Safety Consulting based in Houston, Texas.
He has 20 years of extensive experience in process safety and risk management with focus on programs implementation, safety relief and disposal systems design and analysis, consequence modeling, assets integrity management, and runaway reactions hazards analysis, and process safety solutions digitalization. Dr. Aldeeb holds a BS in chemical engineering, MS in environmental engineering, and PhD in chemical engineering from Texas A&M University. He represents Siemens at API, CCPS, MKOPSC, and AIChE DIERS technical committees. Dr. Aldeeb is a member of the AIChE, IChemE, and ACS.

Justin Daarud

Life After A Risk-Based Inspection Implementation

Justin Daarud is the Asset Integrity Director at Cognascents Consulting Group. In this role, Justin provides valuable solutions to optimize integrity programs and enhance safety, increase knowledge, and reduce costs. Keenly interested in technology and building a better 'mouse trap', he is always looking for ways to improve existing processes. Justin is an inspirational motivator, leading and managing within the asset integrity management services market segment for energy, oil and gas, manufacturing, and petrochemicals for the last 12+ years. He is a mechanical engineer by training, people focused, and business leader by passion. Justin has five passions in life; family, work, running, drumming, and gaming.

Neil Prophet

Are you struggling with your Asset Integrity program?

Mr. Prophet is a Senior Partner at ioMosaic and brings over 20 years of experience in the field of process safety to his role as a leader of the Relief Systems group. His extensive experience includes providing project management and engineering expertise to large-scale pressure relief and flare systems design studies for chemical, pharmaceutical, and petrochemical companies worldwide. Mr. Prophet has also led numerous quantitative risk analyses, hazard identification studies, audits, and provided litigation support for safety and relief systems issues. Mr. Prophet has authored/co-authored many industry white papers on aspects of process safety in addition to presenting over fifty training courses and seminars covering consequence analysis and risk analysis to both operating and consulting companies.

Functional Safety

Luis Manuel Fernando Garcia

Choosing Functional Safety Field Instrumentation - Certified Vs Prior Use. Justification of VDI 2180 simplified equations

Luis Manuel Fernando Garcia Garcia
Siemens Process Safety Consultant for The Americas
Certified Functional Safety Expert (CFSE & TÜV SÜD)
Voting member – ISA 84 functional safety standards
ISA course instructor for SIS (Spanish and English)
Mechanical Eng. Rosario, Santa Fe, Argentina University
Metallurgy and Material Scientist, Liverpool, United Kingdom
Several publications Americas, Europe, Australia

Abhilash Menon

Leveraging the Power of Industry 4.0: ORM Digital Twin for Process Industry

Abhilash Menon is a Sphera business consultant focused on solving client operational excellence and digital transformation challenges. Abhilash has more than 14 years of experience working as a consultant and a project manager for top-tier Oil & Gas, engineering and manufacturing operators across Europe and Asia. Abhilash has an MBA from the University of Cambridge with a Project Management Professional (PMP) certification from the Project Management Institute. However, in his heart he is still a Mechanical Engineer, which is how he began his career

Dr. Diana Gallart Hamilton

On Model-Based Systems Engineering for Design, Management, and Governance of Protective Systems

Diana Gallart Hamilton has a Ph.D. in Interdisciplinary Engineering (Industrial & Systems Engineering) from Texas A&M University; a Master in Finance from the EGADE Business School of Tecnológico de Monterrey (with honors and best grade point average of her generation), and a Bachelor in Financial Management from Tecnológico de Monterrey Campus State of Mexico (with honors and award of excellence).

Her doctoral dissertation, titled “Model-Based Systems Engineering for Design, Management and Governance of Protective Systems” spans topics of industrial and systems engineering, chemical engineering, nuclear engineering, management and governance, from a systems engineering perspective.

Case Studies

Salvador Ávila Filho

Analysis of Reliability Mapping in Refining Industry: Identification of Critical Regions and Interventions in Complex Production Systems

Chemical Engineer, Certified Quality Engineer, Petrochemical Process Specialist, Clean Technology Specialist, Organizational Culture Specialist, Psychoanalist, Psychosomatic Specialist, Educational Process in the Community Specialist, Master in Clean Production, Doctor in Sociothecnical Reliability. Experience as Operation Engineering, Manager, Instructor, Nowadays Professor and

Researcher at University UFBA, Consultant in Human Factor, Reliability, Energy Loss and Risk.

Discussion of real-world cases where overfilling may not be an applicable scenario

Bob Siml

Bob Siml is a Fellow / SME with Siemens Process Safety Consulting. He has 40 years of hands-on experience in research, design, construction, startup and debottlenecking in specialty/commodity chemicals, petrochemicals, and refinery industries with 32 years of specialization in overpressure protection. He is currently serving as a technical advisor. His responsibilities also include leading the continuous improvement program, developing internal guidelines / training material, and assisting the quality assurance process. Notable achievements include an award from the Board of Directors of Dow Chemical for innovations in the relief system design and disposal systems and evaluation of several flares at BP Texas City after the Isom explosion.

Refrigerated Tanks Base Plate-Heating Hazards – A Case Study of Ethylene Tanks

Dr. Mahesh Murthy

Mr. Mahesh has over 20 years of experience working in the area of Process Safety in Australia, Kazakhstan, Russia, Canada, Saudi Arabia and India with strong working partnerships through professional engagements in countries like US, UK, Norway, Malaysia, Japan and Singapore. Mahesh Murthy has graduated from Harvard Business School, with a strong focus on Management. He also has a Chemical Engineering Bachelor's degree from India and Environmental Engineering Master's degree from Australia.

Mahesh has advised numerous educational institutes and mentored many young engineers in their career development.

Mahesh Murthy is passionate engineering manager and is very fond of Human Physiology, Organization Behavior and Advisory on educational matters.

Day 1 Track 2

Human Factors – People in Action
People and Equipment

A Practical Approach to Preventing Systematic Error in the Maintenance of Instrumented Safeguards

Angela Summers

Dr. Angela Summers started SIS-TECH (www.sis-tech.com) nearly 20 years ago with a passion to stop process safety incidents. Dr. Summers holds a PhD in chemical engineering and has over 30 years of experience in instrumentation and controls, process design, and environmental pollution controls. Dr. Summers is a fellow of AICHE, CCPS, and ISA and a distinguished engineering fellow of Mississippi State University and the University of Alabama. She has authored two books and published more than 50 papers on process safety and critical controls.

J. Gregory Hall

Managing an Instrumented Protective Systems Program for a Petrochemical Facility

Greg is a Principal Electrical Engineer with Eastman Chemical Company with 38 years of experience at Texas Operations in Longview, Texas. Greg is the IPS (Instrument Protective Systems) Design engineer, chairman of the Texas Operations IPS Committee, member of the Eastman Corporate IPS Governance Council, and received an Electrical Engineering degree from the University of Texas at Austin.

Principal Electrical Engineer * IPS Committee Chairman
Eastman Chemical Company * Texas Operation * July 16, 2019

Sean Dee

PPE – Can you have too much of a good thing?

Sean J. Dee, Ph.D., P.E., CFEI is a Managing Engineer at Exponent, Inc. At Exponent, Dr. Dee applies the fundamentals of chemical engineering in projects that help clients mitigate the risk of potential accidents, losses and injuries. His areas of expertise include incident investigation, process safety, green manufacturing, and clean energy. Over the course of his career, Dr. Dee has investigated incidents in residential, commercial, and industrial facilities. In many of these cases, Dr. Dee has helped his client understand the strengths and weaknesses of their process safety management programs. Dr. Dee has also published and presented on various topics related to process safety management, including Management of Change. He leverages his experiences in incident investigation and failure analysis to help facilities prevent large losses associated with their processes or products. Prior to joining Exponent, Sean completed his doctorate degree at Berkeley. His graduate thesis focused on the catalytic production of biofuels from biomass. He is a registered professional engineer in Illinois and Texas and a Certified Fire and Explosion Investigator.

Safety Culture, Leadership, and Training

Dr. Ramesh V.M.

Behaviour Based Safety

Dr. Ramesh V.M., is Senior Manager (Fire and Safety), Bharat Petroleum Corporation Limited-Kochi Refinery. He holds a doctoral degree in Management from Bharathiar University, Coimbatore apart from double master degrees in Business Administration (specialized in HR and Marketing) and Disaster Management from premier institutions of our country.With nearly 35 years of experience in various roles within the refining sector, he has gained immense experience as a Safety Trainer and Lead Safety Auditor. During this period, he has actively contributed to the refinery in its various expansion projects. He has also successfully completed programmes in Industrial Safety, Pollution Control and Project Management. He began his career after completing a graduate programme in Chemistry from University of Calicut.He has always been keen on industrial safety, safety management, disaster management and focused based safety and much of his research is focused on these themes. With over a dozen publications in international journals of repute apart from over 20 research presentations that won accolades in conferences/seminars and workshops, he has also participated/presented in several training programs across various parts of the country.

Nir Keren

Effective Remedies for Enhancing Safe Operations Through Analysis of Organizational Safety Climate

Nir Keren is an Associate Professor of Occupational Safety at Iowa State University. He is also Director for the NIOSH's Heartland Education and Research Center for Occupational Safety Program at ISU and the Director for the VirtuTrace Laboratory for Applied Decision-Making Research in Virtual Reality.

Engaging Your Safety Culture Appreciatively

Dana Cooper

Dana launched her consulting firm, Cooper Hayes LLC, in 2016. Cooper Hayes specializes in business performance improvements. Before her entrepreneurial start, she was the Director of Business Excellence and Resin Manufacturing & Product Development at Fairmount Santrol for seven years. Previously Dana worked for Ashland Chemical in various manufacturing, EH&S, and marketing positions. These roles included increasing responsibilities, progressing from process engineering to Global Business Development Manager. She also held responsibilities as plant manager, process safety management systems, and business management including Global Marketing Manager. Dana is a graduate of Michigan State University with a BS in Chemical Engineering and earned her MBA in 1998 from Cleveland State University. Dana currently serves as a board member for the Foundry Education Foundation. She is also the current president of the Cope & Drag Club, which is a technical group made up of foundry suppliers. She participates on the AFS Governmental Affairs Committee, Women in Metalcasting and Marketing Division. Previously she served on the Board of Directors for the American Foundry Society and as a Chairperson for the AFS Marketing Division & Sustainability. She completed the chairs of the Northeast Ohio AFS chapter. Dana was recognized with the Gold Award at a World Foundry Congress (WFO).

Learning from Incidents

Gabor Posta

Crude Oil by Rail Accidents: Cross-industry Learning for High Hazard Sectors

Gabor is a Senior Risk Consultant within Arup's Technical Risk team based in the United Kingdom, working across both established sectors (e.g. rail, infrastructure, oil and gas, and nuclear) as well as emerging ones (e.g. autonomous vehicles and hydrogen for domestic applications). With a background in safety case development for the international nuclear industry, one of Gabor's key interests lies in identifying and disseminating key learning opportunities outside of the original industry where they occurred, taking the view that often the best way to ensure history does not repeat itself is by sharing and collaborating across different sectors.

Karen Vilas

Are biases towards the recent past causing us to unintentionally expose personnel to increased levels of risk?

Karen Vilas works in the BakerRisk Houston office as part of the BakerRisk Process Safety Group. Karen has work experience in process safety, with focus on Facility Siting Studies and Quantitative Risk Analyses for petrochemical facilities in both the United States and abroad. Specifically, Karen has experience in modeling consequences and risk at oil refineries, natural gas facilities, storage facilities, and olefin units. Since completion of her MBA in 2018, Karen also works with the BakerRisk Business Development and Marketing team on establishing key BakerRisk service offerings for clients. In this role, Karen works closely with clients to ensure that their needs are met regarding risk prevention, risk management, and risk solutions.

Mark Galley

The Importance of Misalignment to Reduce Risk and Prevent Disasters

Mark Galley founded ThinkReliability, a training and consulting company specializing in root cause analysis and work process reliability. As a Cause Mapping® Root Cause Analysis Investigator and Instructor, Mark has been facilitating incident investigations and teaching workshops on root cause analysis for more than 20 years. His work spans several industries including manufacturing, power generation, aviation, refining, telecommunications, healthcare, information technology, aerospace, marine and transportation. Prior to starting ThinkReliability, he gained his practical experience in root cause analysis and work process reliability during his time at the Dow Chemical Company, where he worked for nearly nine years.

Mark has a Bachelor of Science in Mechanical Engineering from the University of Colorado in Boulder and obtained his certification as a Reliability Engineer in 1993 through the American Society for Quality. He is a regular presenter at national conferences and is a member of the National Speakers Association.

Day 1 Track 3

Design and Analysis
Probability and Confidence

Dave Grattan

Reverend Bayes, Meet Process Safety: Use Bayes' Theorem to establish site specific confidence in your LOPA calculation

Dave Grattan is an experienced 20+ years HAZOP and LOPA facilitator, specializing in Human Reliability and Human Performance analysis related to Barriers (e.g., Alarms, SOPs, Maintenance, and Operations).

Henrique Martini Paula

Confidence Level Assessment in Enterprise Risk Management: Case Study with Focus on Oil & Gas Production Incidents

With 40 years of engineering experience, Dr. Paula has extensive experience in enterprise risk management (ERM) and integrity, risk, and safety management, including quantitative risk assessment (QRA), consequence assessment, data analysis & analytics, root cause analysis/incident investigation, process safety management, reliability, mechanical integrity, and asset integrity programs (operations, maintenance, and inspection).

Jeff Marx

A New Look at Release Event Frequencies

Jeff is a Senior Engineer with Quest Consultants in Norman, Oklahoma, USA, and a registered professional engineer in the state of Oklahoma. He earned his Bachelor's degree in mechanical engineering from the University of Oklahoma and a Master's degree in Mechanical Engineering from Georgia Tech. In his 26 years at Quest, Jeff's primary responsibilities have been in consequence and risk analysis studies for the petrochemical industry. This work includes facility siting, building siting studies per API RP 752/753, and quantitative risk analysis (QRA) studies for various corporate and regulatory entities. Much of this work has been involved in the LNG industry, including siting studies for LNG plants (using 49 CFR 193, NFPA 59A, CSA Z276, EN 1473, and other standards), as an instructor for the DOT's 49 CFR 193 course that trains the federal and state inspectors of LNG plants, and as a member of the Canadian Standards Association's Z276 committee, the LNG standard for Canada. Jeff is also responsible for several portions of the CANARY by Quest consequence analysis software, and has helped to develop, maintain, and apply the CANARY+ risk analysis toolset used at Quest.

Risk Assessment I

Raymond "Randy" Freeman

Fault Tree Uncertainty Analysis

Randy Freeman has over 40 years professional experience in the process safety and process system design. He is a founder and president of S&PP Consulting of Houston, TX. He holds BS, MS and PhD degrees in Chemical Engineering from the University of Missouri – Rolla. He is an AIChE Fellow and is an Emeritus Member and Fellow of the Center for Chemical Process Safety (CCPS). He was the 2011 recipient of the AIChE Walton-Miller Award in process safety.

Christina Ng

Assessment of Hazard Analysis and Implementation of STPA in Process Industry

Christina Ng is a Fluor Control Systems/SIS Engineer with 18 years of experience in the Petrochemical Industry. Her job functions/area of expertise have been in Functional Safety Management and Automation Systems Specification/Procurement/Acceptance Testing. She develops and executes Functional Safety Management Plans including SRS and Test Procedures development, SIL Verification, PHA participation, Functional Safety Assessment. She is a Certified Functional Safety Expert (CFSE). She holds a B.S. Degree in Chemical Engineering from the University of Kansas and a MBA from University of Houston.

Phil Myers

Oil and Chemical Tank Hurricane Risks

Philip is director of PEMY Consulting, a company that specializes in petroleum storage risk assessment, advanced engineering, and help for piping, pressure vessels and tanks. Philip has been past chair of the American Petroleum Institute for tanks and has chaired numerous task groups and standards. Philip is on the NFPA committee that are associated with tanks, fuels, LNG and so forth. Philip has developed new methods of analysis of settlement as well as seismic and wind risks.

Consequence Analysis I

Mahesh Murthy

Analysis Oxygen Piping Layout to Eliminate High Consequences Risk

Mr. Mahesh has over 20 years of experience working in the area of Process Safety in Australia, Kazakhstan, Russia, Canada, Saudi Arabia and India with strong working partnerships through professional engagements in countries like US, UK, Norway, Malaysia, Japan and Singapore. Mahesh Murthy has graduated from Harvard Business School, with a strong focus on Management. He also has a Chemical Engineering Bachelor's degree from India and Environmental Engineering Master's degree from Australia. Mahesh has advised numerous educational institutes and mentored many young engineers in their career development. Mahesh Murthy is passionate engineering manager and is very fond of Human Physiology, Organization Behavior and Advisory on educational matters.

Priscilla George

Quantitative Assessment and Consequence Modeling of Deliberately Induced Domino Effects in Process Facilities

Priscilla Grace George joined the Division of safety and fire engineering, Cochin University of science and Technology, Kerala, India as a full time research scholar in September 2018. Her research focuses on the susceptibility of process plants to intentional attacks and their security risk analysis using Bayesian networks. She is also familiar with hazard identification techniques and consequence modelling using ALOHA software and PHAST software. She has co-authored papers published in reputed Elsevier journals such as Journal of Loss Prevention in Process Industries and International Journal of Disaster Risk Reduction. Before joining CUSAT, Priscilla worked as Lecturer at Muthoot Institute of Technology and Science- a reputed Engineering College in Kerala, India.

Zhuoran Zhang

Develop a Hazard Index for the Hazard Identification of Chemical Logistic Warehouses

Zhuoran Zhang is a master student in Safety Engineering from Mary Kay O'Connor Process Safety Center in the Department of Chemical Engineering, TAMU. His master thesis is focused on the hazard index development. Before joining TAMU, he got his Bachelor in chemical engineering from Tianjin University and Bachelor in chemistry from Nankai University in a joint program.

Day 1 Track 4

Research and Next Generation

Explosion Phenomena I

Russell Ogle

Dust Explosions and Collapsed Ductwork

Dr. Russell Ogle is a Principal Engineer and the Practice Director for Thermal Sciences at Exponent. He specializes in the scientific investigation and prevention of complex industrial accidents and catastrophic fires and explosions. He received his B.S in Chemical Engineering from Purdue University and a Ph.D. in Chemical Engineering from the University of Iowa. He has over 30 years of industrial experience working in fire, explosion, and chemical safety. Dr. Ogle is a licensed professional engineer, a certified safety professional, and a certified fire and explosion investigator. His book, "Dust Explosion Dynamics," is an introduction to the combustion science of dust explosions and fires.

Savio Vianna

The nature of flammable cloud volumes in semi-confined environment under the influence of flow of air

Sávio Vianna is an associate professor at the University of Campinas (Unicamp) in Brazil. His main research area concerns the investigation of computational modelling of reacting and non-reacting flows. By dealing with the latest numerical schemes and available open sources tools, as well as in house codes, Dr. Vianna has been trying to reinforce the bridge between basic science and the engineering of fluid flow. He is also interested in LES (Large Eddy Simulation) and DNS (Direct Numerical Simulation) for turbulent combustion.

Charline Fouchier

Image processing techniques for the characterization of explosively driven dispersions

Last year PhD Student - Project about Dispersion driven by an explosion in a complex environment.

Environmental Influences on Process Safety

Maria Papadaki

Storage vessels in the proximity of wild fires

Dr. Maria Papadaki is Professor of Environmental Chemistry and Environmental Processes of the Department of Environmental Engineering, University of Patras, Greece.

She is a Chemical Engineer and her PhD was in the field of Transport properties of fluids. She has over 20 year experience in the fields of thermophysical properties of fluids, reaction engineering and catalysis and reactive chemicals and process safety research. She is a Research Associate and a member of the Technical Advisory Committee of the Mary Kay O' Connor Process Safety Center.

Roland Moreau

SafeOCS Industry Safety Data - The Value Proposition for the Oil & Gas Industry

Roland retired from ExxonMobil in August 2014 with 34 years of service, where he held the position of Safety, Security, Health and Environment (SSH&E) Manager for ExxonMobil's Upstream Research, Gas & Power Marketing, and Upstream Ventures business units. He began his career with Exxon Company, U.S.A. as a Project Engineer at the Bayway Refinery in New Jersey in 1981. Since that time, he has held various technical, supervisory and managerial assignments for Exxon, and then ExxonMobil, in the Upstream production, development, and research organizations. Prior to ExxonMobil, Roland also worked for five years in the naval nuclear industry. In August 2018, Roland assumed the role of 2018 President of the Board of Trustees for the American Institute of Mining, Metallurgical, and Petroleum Engineers (AIME) and assumed the role of President in August 2018. In September 2019, he will start a four-year term on the Board of Trustees for the United Engineering Foundation (UEF). Prior to that, Roland served two terms on the Board of Directors for the Society of Petroleum Engineers (SPE) in the roles of Vice President of

Finance (2015-2018) and Health, Safety, Security, Environment & Social Responsibility (HSSE-SR) Technical Director (2011-2014). Roland received his BS degree in Mechanical Engineering from Worcester Polytechnic Institute in 1975, followed by an MBA in Finance from Fairleigh Dickinson University in 1984. He also completed the Certified Financial Planner program at Rice University in 2015. He remains active on various SPE and AIME initiatives, including co-chairing the April 2016 Summit with the U.S. Bureau of Safety and Environmental Engineering (BSEE) on "Assessing the Processes, Tools, and Value of Sharing & Learning from Offshore E&P Safety-Related Data." As a follow up to that Summit, Roland is currently consulting with the U.S. Bureau of Transportation Statistics (BTS) on development of an industry-wide safety data management framework. As part of his involvement with AIME, he also serves as program chair for a cross-industry sector safety event in June 2020.

Hongfei Xu

Modelling Ice and Wax Formation in a Pipeline in the Arctic Environment

Hongfei Xu is currently a PhD student in Chemical Engineering at the Texas A&M University. Before joining Texas A&M University, he worked as a research associated at the University of Tulsa. His research interests include flow assurance, process safety, thermodynamics, and computational fluid dynamics.

Structure Resistance to Fire & Explosion

Benjamin Ishii

External Fire Impacts on the Interior Temperature of a Building

Ben is a Project Engineer with Quest Consultants in Norman, Oklahoma. He earned his Bachelor's degree in chemical engineering from the University of Oklahoma and a Master's degree in chemical engineering from Kansas State University. In his 9 years at Quest, Ben's primary responsibilities have been in consequence and risk analysis studies for the petrochemical industry. This work includes facility siting, building siting studies per API RP 752/753, and quantitative risk analysis (QRA) studies for various Corporate and regulatory entities. Ben is also responsible for several portions of the CANARY by Quest consequence analysis software, and has helped to develop, maintain, and apply the risk analysis toolset used at Quest for performing QRAs.

Ruiqing Shen

Experimental Study of an Iron-Based Metal-Organic Framework as Flame Retardant for Poly (methyl methacrylate) (PMMA)

Ruiqing Shen is currently a Ph.D. student in Chemical Engineering at Texas A&M University, where he is working with Dr. Qingsheng Wang. He received his bachelor degree from Fire Protection & Safety Engineering Technology at Oklahoma State University and Southwest Jiaotong University (China). And he received his master degree from Chemical Engineering at Oklahoma State University. His research interests focus on flame retardant materials, cone calorimeter test, thermal analysis, polymer nanocomposites, and fire dynamics and modeling.

Development of a Blast-Resistant Roller Shutter Door

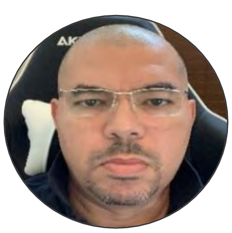
Darrell Barker

Darrell Barker is Vice President of Advanced Engineering for ABS Consulting. Prior to his current position, Darrell was Vice President of Extreme Loads and Structural Risk. He manages a unit of more than 50 engineers conducting advanced modeling and simulation to assess the effects of extreme wind, seismic, and blast loads as well as fatigue and fracture effects on a wide range of structures and equipment. Darrell has 35 of professional experience in blast resistant design and construction. He has conducted threat assessments of more than 200 facilities for government agencies across the country and internationally. Darrell has analyzed explosion hazards in petrochemical facilities and explosives processing operations. He has developed innovative solutions to protect buildings and personnel against these risks and conducted shock tube and high explosives test programs to validate analytical models. Darrell has conducted explosion accident investigations to determine proximate and root causes, working with clients to mitigate risks and provide safe operations. Mr. Barker is a recognized industry leader in the field of explosion hazards mitigation. He actively participates in industry technical committees developing guidelines and best practices for explosion hazard assessment and mitigation. He is a contributing author for publications produced by ASCE, ACI and ASME. He has more than 40 papers on explosion hazards, protective construction, dynamic analysis, and blast testing. Darrell received a BSCE degree from the University of Arkansas and was elected to the Arkansas Academy of Civil Engineering. He is a registered professional engineer in Texas, Arkansas and Louisiana.

Day 2 Track 1

Management, Operational, and Offshore
Offshore Case Studies

Lessons from Risk Assessment of 6th Generation Drill-ships and Sem-Submersibles



Wael Abouamin

Wael Abouamin is a professionally licensed engineer (TX) with 25 years of experience in the oil and gas industry. He is an experienced risk assessment facilitator and has managed over 200 risk assessment projects. He has served as an expert witness in a lawsuit between a major operator and drilling contractor, providing technical support, writing reports, and testimonies with regard to BOP shear calculations. He has published 5 papers in a variety of conferences and magazines including SPE, OTC, IADC Drilling Magazine, Mary Kay O'Connor Process Safety Center, and AspenWorld. He has been president of Energy Risk Consulting since 2011.

Chenxi Ji

Study of FSRU-LNGC System Based on a Quantitative Multi-cluster Risk Informed Model

Chenxi Ji joined MKOPSC in 2016 and worked for Ocean Energy Safety Institute since then. Before joining MKOPSC, Chenxi served as a senior lecturer at Dalian Maritime University, China, and a third mate deck officer on board. He has been seeking every opportunity to make the maritime industry safer, faster and greener. Currently, he is working to optimize LNG supply chain from the perspectives of operation research, process systems engineering and chemical process safety.

How to Improve the Trust in Safety Related Sensors

Wolter Last

Wout Last is the Founder and President of HINT (Human Interest in New Technology) a Consulting and Engineering Software system integrating firm located here in Houston TX, with offices in the Netherlands and Bahrain. Wout works closely with many of the Oil & Energy and Petrochemical Companies in the area of IT & Control and Automation. Besides his current business Wout is also involved in Merger & Acquisition with Hint Global Investment Inc. here in Houston, TX focusing on the integrating of IT companies to embrace digital transformation. Born and raised in Hattem the Netherlands an old Hanse city, established around 800.

Wout received his bachelor's degree in IT from the University of Windesheim in Zwolle, the Netherlands. Started his career at Shell in the Netherlands and graduated from them in Measurement & Control and specialized in Custody Transfer.

Just before he was moving to Houston, he went to Guthrie Castle in Scotland, the Business school in finance, Merge and Acquisition, Graduated in Quantum Leap Advantage (QLA) by Sir Dan Pena, a successful entrepreneur who also works in Houston.

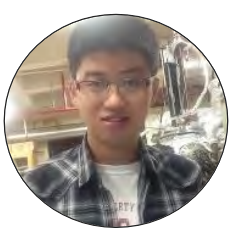
Wout 's wife Juanita also Dutch, she is a Councilor / Coach and have her own practice here in Houston, they are married, having 4 kids (3 boys and one girl) and currently living in Cinco Ranch Katy Texas.

Wout enjoys watching and playing sports like golf, tennis and soccer, was a fanatic Ice speed skater, has ran marathons, ice skates and has bicycled many long-distance tours (125 -220 miles a day).

He is a sponsor of the Netherlands-America Foundation (NAF) which is a 501 nonprofit organization maintaining and building friendships between the Dutch and the Americas.

Member/sponsor of the ISA – Instrumentation Society of Americas, SPE – Society of Petroleum Engineers and the Oil and Gas Reinvented Community

Biocompatible Herder for Rapid Oil Spill Treatment over a Wide Temperature Range



Dali Huang

Dali Huang is a Ph.D. student of Materials Science & Engineering at Texas A&M University. He joined Dr. Zhengdong Cheng's soft matter research group in Chemical Engineering at 2016. His research is focused on the development of oil spill mitigation, LNG high-expansion foam stabilizer and 2D magnetic nanoplatelets.

Incident Response and Project Planning

Kumar (Chris) Israni

When to Shut-down? How to Recover? Hurricanes Versus Tropical Storms Impacts

Chris has over 19 years' work experience in the areas of process safety and risk management offerings with an extensive process and environmental background. He has been the Process Safety Lead on offshore and onshore projects, which required managing the design safety requirements for oil operating companies. His O&G, Chemicals and Pharmaceuticals expertise includes various PSM, SEMS and RMP related areas such as process hazard analyses (PHAs) including HAZOPs, HAZIDs and What-If/checklists, Layer of protection analysis (LOPA), management of change (MOC), pre-startup safety reviews (PSSR), Safe work practices, HSE audits, gap analysis, applicability studies, and other process safety/regulatory requirements. In addition, Chris also is experienced in the areas FMEAs, JSAs and environmental engineering related tasks such as waste water designs, environmental statements, impact assessment and ENVIDs. One of Chris's strengths is his capability to work and interact with a wide variety of disciplines and functions—from Front level leadership to Senior Management. He currently provides these expertise to various safety & risk clients in the Gulf BU region, and is a recognized professional/presenter in various regional and national level safety conferences.

Alfonso Ibarreta

Exposure of Fabrics Used in Personal Protective Equipment to Combustible Dust Flash Fires

Dr. Ibarreta applies thermodynamics, fluid dynamics, and heat transfer principles to the study of combustion processes in fires, explosions, and a variety of combustion devices. He is a Certified Fire and Explosion Investigator and has investigated fires and explosions involving consumer products, residential and commercial buildings, and industrial facilities.

Dr. Ibarreta has evaluated the compliance of industrial facilities with NFPA standards, as well as state and federal codes for the prevention and mitigation of dust and gas explosions. He has performed Dust Hazard Analyses (DHAs) at facilities handling combustible dust. He has also participated in Process Hazard Analyses (PHAs) and performed consequence modeling of flammable liquid / gas releases during the permitting and planning stages of LNG terminals and other oil & gas facilities. Dr. Ibarreta has employed Computational Fluid Dynamic (CFD) models, including FLACS, to calculate the consequences of flammable liquid/vapor releases, vented deflagrations, and unconfined vapor cloud explosions.

Dr. Ibarreta is a principal member of the NFPA's Technical Committee on Explosion Protection Systems. This committee is responsible for NFPA documents related to explosion protection systems for buildings and equipment, including NFPA 67 Guide on Explosion Protection for

Gaseous Mixtures in Pipe Systems, NFPA 68 Standard on Explosion Protection by Deflagration Venting, and NFPA 69Standard on Explosion Prevention Systems. Dr. Ibarreta is also the mechanical engineering representative at the Massachusetts Board of Fire Prevention Regulations. This board is responsible for amending and promulgating the comprehensive fire safety code (527 CMR) for the Commonwealth of Massachusetts.

Integration of Process Safety into Engineering Design during Offshore Project Execution

Edward Liu

Edward Liu is a Technical Safety Professional in Wood. Edward has been working in Wood Technical Safety since 2015. His expertise in the field of Process Safety includes CFD gas dispersion, fire and blast risk assessment, QRA, helicopter risk assessment, engine exhaust study, etc. Before coming to the industry, Edward had been a process engineer in Sinopec for 2 years and an Assistant Research Scientist at the MKOPSC for 5 years. His role at the MKOPSC was mainly focused on the Process Safety researches for various LNG projects, gas flammability, dust explosion.

Operational Lessons

A Case Study From a Fire Incident in Naphtha Heater Caused by Sulfidation

Chao Pin Wen

Kevin C.P.Wen works as ESH advanced engineer in Nan Ya Plastics Corporation (NYPC), Taiwan, with expertise in process safety management (PSM) and more than 5-year-experience PSM in plastic processing, petrochemical, polyesters and electronic materials industry. He received his Master's degree in material engineering from National Cheng Kung University in 2005. He joined NYPC in 2007, and was responsible for expansion epoxy plant project in 2008, PHA facilitator in 2012. Then he has been transferred to be PSM coordinator of head office in 2015. He is currently responsible for the PSM business of the Nan Ya Plastics Corporation.

How to Treat Expert Judgement? With certainty it contains uncertainty!

Hans Pasman

Dr.Ir. Hans J. Pasman is TEES Research Professor at Mary Kay O'Connor Process Safety Center of the Department of Chemical Engineering of Texas A&M University and Emeritus Professor Chemical Risk Management of the Delft University of Technology in the Netherlands. Graduated in chemical technology at Delft University of Technology in 1961, with Ph.D. in 1964 while employed by Shell, joined the Dutch organisation for Applied Research, TNO, where he did many investigations into disastrous industrial accident, he initiated research in reactive materials, explosions of all types, and risk analysis. He was chairman of the International Group on Unstable Substances for 10 years, the European Study Group on Risk Analysis (1980-1985), a NATO Group on Explosives, and the Working Party on Loss Prevention and Safety Promotion in the Process Industries (1986-

2004) and in this latter capacity in 1992 co-founder of the European Process Safety Centre. He has been member of the Dutch Council of Hazardous Substances (2004-2012).

Lessons Learned - How to Make Them Stick

Jack Chosnek

Jack Chosnek has over forty years of experience in the petrochemical industry with involvement in process safety in the majority of them. He worked for Celanese Corporation for 25 years in R&D, Tolling, Pilot Plants, Operations, Process Engineering and Process Safety Management in management and staff positions.

He is President and Principal at KnowledgeOne LLC, where he has consulted for companies in the chemical, refining, oil and gas, offshore, and LNG industries, implementing process safety management systems, facilitating PHAs and LOPA/SIL studies, conducting incident investigations, and conducting process safety audits and gap analyses. He has developed commercial software for PHA facilitation, Management of Change (MOC) and a Hazards Register.

PSM Support Activities

Jack is the Chair of the Technical Advisory Committee of the Mary Kay O'Connor Process Safety Center (MKOPSC). He's also a member of the MKOPSC's Steering Committee.

Jack chaired PPSS at the 3rd Global Congress on Process Safety. He has been a PPSS session chair or co-chair every year (except for one year) since 2004.He has been the chair of the PSM session of AIChE's Southwest Process Technology Conference for the last 10 years (since its inception).He is a Certified Instructor for CCPS' Boot Camp (Process Safety Fundamentals) course. He has taught the course in the United States and Saudi Arabia. Jack has published over 15 PSM-related papers and is a listed contributor to the 4th edition of Lee's Loss Prevention in the Process Industries. He is a reviewer for the American Chemical Society Publications and for Elsevier's Journal of Loss Prevention.

Education and Certification

Jack has a BS and MS in Chemical Engineering from the Technion – Israel Institute of Technology, a PhD from the University of Missouri at Rolla (currently Missouri Science and Technology University), and an MBA from Texas A&M—Corpus Christi.

He is a Licensed Professional Engineer in the State of Texas.

Honors and Awards

AIChE Fellow. Recipient of the 2014 Harry West Memorial Service Award from the MKOPSC. Recipient of AIChE's South Texas Section 2005 Special Service Award and 2008 PSM Workshop Achievement Award. Member of the Academy of Sciences of Missouri S&T University. Holder of three patents related to chemical production.

Day 2 Track 2

Human Factors – People in Action
Human Performance

Changwon Son

Analyzing Procedure Performance using Abstraction Hierarchy: Implications of Designing Procedures for High-risk Process Operations

Changwon Son is a Ph.D. student in the Department of Industrial and Systems Engineering at Texas A&M University. His dissertation is focused on resilience in emergency management domain. He received his B.S. in Industrial Engineering from Hanyang University, Seoul, Korea, and M.S. in Safety Engineering from Mary Kay O'Connor Process Safety of Artie McFerrin Department of Chemical Engineering at Texas A&M University. Before coming to graduate schools, he worked for Hyundai Heavy Industries, the world's largest shipbuilding company, as health, safety, and environmental (HSE) manager for multiple projects. He also worked for Baker Engineering and Risk Consultants during his masters.

Salvador Avila Filho

Relationship Between Human-Managerial and Social-Organizational Factors: For Industry Safeguards Project: Dynamic Bayesian Networks

Chemical Engineer, Certified Quality Engineer, Petrochemical Process Specialist, Clean Technology Specialist, Organizational Culture Specialist, Psychoanalist, Psychosomatic Specialist, Educational Process in the Community Specialist, Master in Clean Production, Doctor in Sociothecnical Reliability. Experience as Operation Engineering, Manager, Instructor, Nowadays Professor and Researcher at University UFBA, Consultant in Human Factor, Reliability, Energy Loss and Risk.

Trent Parker

Exploration of relationships between safety performance and unsafe behavior in coal mining processes

Trent Parker is a second year PhD student advised by Dr. Wang and is part of the Multiscale Process Safety Research Lab in the chemical engineering department. His research primarily involves the use of RC1 calorimetry to investigate the production of 5-hydroxymethylfurfural, and his research interests include chemical reaction engineering, process safety, and human factors.

Reduce Human Error: Mistake-Proof Procedures and Create an Effective PPE Grid

Nicole Loontjens

Nicole Loontjens has been the Process Safety Manager for Americas Styrenics since 2012. In this role, she oversees process safety for AmSty's seven manufacturing facilities in the U.S. and Colombia. She is a co-inventor on a process patent for PolyRenew™, a plastic that contains up to 25% post-consumer recycled polystyrene. She has also volunteered on two book writing committees for the Center for Chemical Process Safety (Guidelines for Combustible Dust Hazard Analysis and Guidelines for Inherently Safer Design). After graduating from the University of Rhode Island in 2001 with degrees in chemical engineering and French, Nicole worked for The Dow Chemical Company in Midland, Michigan, and eventually transferred to the Dow plant in Gales Ferry, CT. Nicole lives with her family in Coventry, RI.

Safety Culture, Leadership, and Training

Beyond Participation—A Case Study for Driving Employee Engagement in Your Process Safety Program

Tony Bocek

Tony Bocek is a Senior Operations Technician at BP's Cherry Point Refinery located in Washington State. With over 12 years working in the oil refining industry, Tony has developed a passion for process safety with a specific penchant for identifying and implementing practical solutions to the real-world challenges faced by technicians. As a Process Operator, Tony believes that the only way to achieve process safety excellence in our industry is through a synergistic approach where site employees and managers, along with corporate leadership, work together to build and sustain a healthy safety culture at all levels within their organization. In addition to his duties as a Process Operator, Tony is a member of the Emergency Response Team as an Industrial Firefighter and Emergency Medical Responder. He has acted in several process safety capacities including as an Operations Process Safety Specialist and qualified PHA facilitator and also served on the Washington PSM rule review committee, working with State officials and stakeholders to review current PSM code and propose effective updates. In his personal life, Tony enjoys being active with his wife of 12 years and his three children

Options for teaching Operational Process Safety

Trish Kerin

Director, Institution of Chemical Engineers Safety Centre (ISC)
After graduating with honors in mechanical engineering, Trish spent several years working in project management, operational and safety roles for the oil, gas and chemical industries.
Trish has represented industry on many government committees related to process safety, and sits on the board of the Australian National Offshore Petroleum Safety and Environmental Management Authority and the Mary Kay O'Connor Process Safety Center steering committee. Trish is a Chartered Engineer, registered Professional

Process Safety Engineer, Fellow of IChemE and Fellow of Engineers Australia. Trish holds a diploma in OHS and is a Graduate of the Australian Institute of Company Directors.

Operator Error or Management Failure? Management's Role in Maintaining Operator Discipline

Marc Rothschild

Mr. Rothschild has a B.S. in Chemical Engineering (with honors) from the University of California at Davis, and is a registered Professional Engineer (Ohio). Marc has spent the last 33 of his 39 year professional career as a process safety engineer, working with the chemical, oil refining and other industries to manage their process risks. Marc is a highly experienced PHA facilitator, having led well over 100 studies. He is also a subject matter expert in quantitative risk analysis, LOPA facilitation, consequence analysis and dispersion modeling. Projects include: conducting facility siting analysis (PV burst, VCEE and toxic gas discharge dispersion analysis), evaluating vent discharge impact, developing PSM compliance programs and establishing and tracking process safety metrics. Marc is a TapRoot© certified incident investigator and has considerable experience investigating incidents and near misses, identifying their causal factors and root causes. Marc has developed and taught PSM and PHA training courses, and has published and presented several papers on process safety at technical conferences.

Learning from Incidents

The Future of the United States Chemical Investigation Board: Opportunities and Challenges

Rick Engler

Rick Engler U.S. Chemical Safety and Hazard Investigation Board (CSB) Rick Engler was nominated by President Barack Obama to the U.S. Chemical Safety and Hazard Investigation Board in January of 2014 and confirmed by the Senate in December 2014. Before his appointment, Mr. Engler spent more than four decades helping to prevent hazards, including to ensure that workers and the public had a "right to know" about chemical dangers. He also helped lead successful efforts to achieve landmark state and national policies on hazard communication, adoption of inherently safer processes, worker participation and whistleblower protection.

Mr. Engler was founder and Director of the New Jersey Work Environment Council and the Philadelphia Area Project on Occupational Safety and Health and was an elected Vice President of the NJ Industrial Union Council, AFL-CIO. Mr. Engler also served on the NJ Department of Health Occupational Health Surveillance Advisory Committee. As a CSB Board Member, his specific interests include modernization of process safety safeguards.

Robert Bellair

Unravelling Reactive Chemicals Mysteries: Experiences in Reactive Chemicals Incident Investigations

Robert Bellair is a Reactive Chemicals Subject Matter Expert and the Flammability Technical Leader at The Dow Chemical Company. In these roles, he provides expertise in reactivity and flammability hazards and properties to internal Dow clients for hazard evaluations, consequence analysis, emergency response, and root cause investigations. In his 10 years at Dow, he has been a key member of multiple high profile runaway reaction and explosion incident investigation teams. He is also an active member of the Mary K OConnor Process Safety Center Technical Advisory and ASTM E27 Technical Committees.

Monica Philippart

We Don't Learn Enough from Incidents: the Roots of Human Errors

Dr. Philippart owns a consultancy specialized in managing operational risks associated with human performance. Her career begun at NASA's Kennedy Space Center, where she applied her mechanical and industrial engineering degrees to develop and improve manned and unmanned spaceflight equipment and processes, including through the creation of a Human Factors Process Failure Modes & Effects Analysis (HF PFMEA) software tool for which she shares two U.S. patents. Since 2006, she has enhanced deepwater drilling process safety and risk management in the petroleum industry, most recently serving as the Human Factors and Industrial Engineering expert of the Process Safety Monitor team of four individuals formed following BP Exploration & Production's Plea Agreement with the U.S. Department of Justice as a result of the 2010 Deepwater Horizon incident. Mónica has also enjoyed working for The Walt Disney Company, and developed and imparted courses for NASA and Embry-Riddle Aeronautical University.

Day 2 Track 3

Design and Analysis
Consequence Analysis II

Dan Brooks

Managing Tanks as a Portfolio of Assets

Dan Brooks has 30 years of experience in consulting and teaching decision and risk management in both government and private sectors. He was a Senior Scientist at Applied Decision Analysis, a Menlo Park decision consultancy, for ten years and a Managing Director for PricewaterhouseCoopers' Financial Advisory Services group for several years. He is emeritus professor and now adjunct professor at Arizona State University where he teaches statistics and decision analysis. He was a founding faculty director of the Master of Science in Business Analytics at ASU. He worked with API, EPA, DOE, and U.S.DOT on prioritizing Superfund site and pipeline risk templates and guidelines. He has a bachelors and master's degree in mathematics from the Colorado School of Mines and a doctorate in decision sciences from Indiana University.

Building Siting Screening Criteria for Structural Failure Hazards to Occupants

Johnny Waclawczyk

Mr. Waclawczyk is Director of ABS Consulting's San Antonio Office. He has over twenty-five years of experience designing and analyzing structures subjected to blast loads produced from high explosives (HE), vapor cloud explosions, bursting pressure vessels, and venting dust explosions. He has designed and tested a variety of structures including blast resistant buildings, containment structures, and blast chambers. Mr. Waclawczyk is a graduate of Texas A&M University with a Civil/Structural Engineering Degree

Utilizing Turbulent Combustion Models to Better Quantify Far-Field VCE Blast Loads

Robert English

Robert English is an Associate at MMI Thornton Tomasetti, and works out of the Warrington office in the UK. Rob has more than ten years of experience in safety assessments for onshore and offshore oil and gas facilities. One of his main areas of expertise is CFD analysis to underpin fire and explosion risk assessments, QRA, ETRERA and other safety studies. In his work, Rob has performed ventilation, jet fire, spray fire, pool fire, gas dispersion and explosion analyses to assess the risk associated with accidental gas and spray releases. Through his work, Rob has gained experience working on studies for nuclear storage facilities and for oil and gas facilities including onshore sites, offshore platforms, FPSO and FLNG at multiple different stages of the asset lifecycle from FEED through to Brownfield projects.

Pressure Relief Valves Stability: Current Models Comparison and an Approach to Simplify Dynamic Modelling

Abdul Aldeeb

Dr. Abdul Aldeeb is the Head of Technology and Consulting at Siemens Process & Safety Consulting based in Houston, Texas.

He has 20 years of extensive experience in process safety and risk management with focus on programs implementation, safety relief and disposal systems design and analysis, consequence modeling, assets integrity management, and runaway reactions hazards analysis, and process safety solutions digitalization.

Dr. Aldeeb holds a BS in chemical engineering, MS in environmental engineering, and PhD in chemical engineering from Texas A&M University. He represents Siemens at API, CCPS, MKOPSC, and AIChE DIERS technical committees. Dr. Aldeeb is a member of the AIChE, IChemE, and ACS.

Risk Assessment II

Andrea Ortiz-Espinoza

Comparison of Safety Indexes for Chemical Processes Under Uncertainty

Andrea P. Ortiz-Espinoza is a chemical engineer by the Instituto Tecnológico de Aguascalientes. Currently, she is a Ph.D. student at Instituto Tecnológico de Celaya working under the supervision of Professor Arturo Jiménez. Her research focuses on the design of inherently safer chemical plants. She has been a visiting scholar at the TEES Fuels and Gas Research Center at Texas A&M University.

Thomas Mander

Consideration of Non-Structural Internal Debris in Siting of Blast Resistant Modules

Thomas Mander is a Senior Engineer at Baker Engineering and Risk Consultants, Inc. (BakerRisk), where he has worked for over ten years. His work includes the design, analysis, testing, and upgrade of buildings and infrastructure subjected to blast loads. His research interests of the blast performance of reinforced, precast, and prestressed concrete structures.

Jack Chosnek

Life Cycle Risk Management with The Help of a Hazard Registration

Jack Chosnek has over forty years of experience in the petrochemical industry with involvement in process safety in the majority of them. He worked for Celanese Corporation for 25 years in R&D, Tolling, Pilot Plants, Operations, Process Engineering and Process Safety Management in management and staff positions.

He is President and Principal at KnowledgeOne LLC, where he has consulted for companies in the chemical, refining, oil and gas, offshore, and LNG industries, implementing process safety management systems, facilitating PHAs and LOPA/SIL studies, conducting incident investigations, and conducting process safety audits and gap analyses. He has developed commercial software for PHA facilitation, Management of Change (MOC) and a Hazards Register.

PSM Support Activities

Jack is the Chair of the Technical Advisory Committee of the Mary Kay O'Connor Process Safety Center (MKOPSC). He's also a member of the MKOPSC's Steering Committee.

Jack chaired PPSS at the 3rd Global Congress on Process Safety. He has been a PPSS session chair or co-chair every year (except for one year) since 2004.He has been the chair of the PSM session of AIChE's Southwest Process Technology Conference for the last 10 years (since its inception).He is a Certified Instructor for CCPS' Boot Camp (Process Safety Fundamentals) course. He has taught the course in the United States and Saudi Arabia. Jack has published over 15 PSM-related papers and is a listed contributor to the 4th edition of Lee's Loss Prevention in the Process Industries. He is a reviewer for the

American Chemical Society Publications and for Elsevier's Journal of Loss Prevention.

Education and Certification

Jack has a BS and MS in Chemical Engineering from the Technion – Israel Institute of Technology, a PhD from the University of Missouri at Rolla (currently Missouri Science and Technology University), and an MBA from Texas A&M—Corpus Christi.

He is a Licensed Professional Engineer in the State of Texas.

Honors and Awards

AIChE Fellow. Recipient of the 2014 Harry West Memorial Service Award from the MKOPSC. Recipient of AIChE's South Texas Section 2005 Special Service Award and 2008 PSM Workshop Achievement Award. Member of the Academy of Sciences of Missouri S&T University. Holder of three patents related to chemical production.

Process Design and Mitigation Systems I

Drew Botwinick

How Effective Are Safety Gaps at Mitigating Explosions: Large Scale Testing of Safety Gaps to Prevent

*missing bio

Joshiba AriamuthuVenkidasalapathy

Safety-Centered Process Control Design Based on Dynamic Safe Sets

Joshiba is a PhD candidate at MKOPSC, Texas A&M University. She earned her B.Tech in Chemical Engineering from Indian Institute of Technology- Madras, India. Prior to pursuing a PhD, she worked as a manager in Reliance Industries Limited, Refinery Complex for a couple of years. Her research at Texas A&M focuses on safety-centered systems engineering with applications in alarm management and process control design. Her research implements concepts from optimization theory, data analytics and process control theory to design safer and more efficient systems. During her PhD program, she has also worked as an Engineering intern for GATE Consultancy in Texas.

Trish Kerin

Tamming the Wild River Rapids - How Process Safety Can Apply Outside

Director, Institution of Chemical Engineers Safety Centre (ISC)

After graduating with honors in mechanical engineering, Trish spent several years working in project management, operational and safety roles for the oil, gas and chemical industries.

Trish has represented industry on many government committees related to process safety, and sits on the board of the Australian National Offshore Petroleum Safety and Environmental Management

Authority and the Mary Kay O'Connor Process Safety Center steering committee. Trish is a Chartered Engineer, registered Professional Process Safety Engineer, Fellow of IChemE and Fellow of Engineers Australia. Trish holds a diploma in OHS and is a Graduate of the Australian Institute of Company Directors.

Day 2 Track 4

Research and Next Generation
Next Generation Process Safety

Finding Health & Safety Buried Treasure with AI

Tom Garvin

Mr. Thomas Garvin is a Senior Managing Consultant with IBM Services, in the global Chemicals & Petroleum Center of Competence. He has over 30 years of experience in process industries and operational technology, acting in multiple roles within Health/Safety/Environmental operations, operations management, knowledge management, laboratory information and real-time data architectures. Over his career, Mr. Garvin has held multi-year engagements with several international majors in the oil, petrochemical and mining industries, including Chevron, ExxonMobil, BP, ConocoPhillips, and Alcoa

Smart machine learning analytic tools for alarm rationalization

Sirish Shah

Sirish L. Shah is Emeritus Professor with the Department of Chemical and Materials Engineering at the University of Alberta, where he held the NSERC-Matrikon-Suncor-iCORE Senior Industrial Research Chair in Computer Process Control from 2000 to 2012. He has held visiting appointments at Oxford University and Balliol College as a SERC fellow, Kumamoto University (Japan) as a Senior Research Fellow of the Japan Society for the Promotion of Science, the University of Newcastle, Australia, IIT-Madras India, and the National University of Singapore. He was the recipient of the Albright & Wilson Americas Award of the Canadian Society for Chemical Engineering (CSChE) in recognition of distinguished contributions to chemical engineering in 1989; the Killam Professor in 2003; the D.G. Fisher Award of the CSChE for significant contributions in the field of systems and control; the ASTECH "Innovations Prize in Oil Sands Research" in 2011; the 2014 IEEE Transition to Practice award of the control systems society and the RS Jane award of the CSChE in 2017. He is a fellow of the Canadian Academy of Engineering (FCAE) and holds a honorary doctorate from Kumamoto University, Japan. He has supervised more than 80 graduate students and published more than 200 referred journal papers.The main areas of his current research are process and performance monitoring, system identification and design, analysis and rationalization of alarm systems. He has co-authored three books: "Performance Assessment of Control Loops: Theory and Applications", "Diagnosis of Process Nonlinearities and Valve Stiction: Data Driven Approaches", and a more recent brief monograph on "Capturing Connectivity and Causality in Complex Industrial Processes". Results from Shah’s research group have been translated into commercial software for process and performance monitoring and advanced alarm tools. He has consulted widely for the process industry and control software vendors.

Nir Keren

Opportunities and challenges of high-level visualization technology in process operations and safety

Nir Keren is an Associate Professor of Occupational Safety at Iowa State University, He is also Director for the NIOSH's Heartland Education and Research Center for Occupational Safety Program at ISU and the Director for the VirtuTrace Laboratory for Applied Decision-Making Research in Virtual Reality.

Edward Marszal

Unified Hazard Assessment - Bringing Together HAZOP, LOPA, Hazard Registers, and Bowtie in a Unified Structure

Ed Marszal is President and CEO of Kenexis and Member of the Scientific Advisory Board for the Purdue University Process Safety and Assurzhuoance Center. He has over 25 years of experience in risk analysis and technical safety engineering of process industry plants, including design of Safety Instrumented Systems and Fire and Gas Systems. Ed is an ISA Fellow and former Director of the ISA Safety Division and 20 year veteran of the ISA 84 standards committee for safety instrumented systems. He is also the author of the “Safety Integrity Level Selection” and “Security PHA Review” textbooks from ISA.

Reactive Chemicals/Flammibility

Ji Yun Han

Measurement for decomposition of lithium ion battery electrolytes with STA-MS and risk assessment of toxic gases

I am a student of doctoral course in Ajou university of republic korea. I am interested in research of the risk caused from battery and that can give the idea to control the battery's risk.

Harold Escobar

Quantitative Structure-Property Relationships Methods to expedite Reactive Chemicals Hazards Assessment Processes

Harold Escobar is a third year Doctorate Student of Chemical Engineering at Texas A&M. He has extensive experience in process safety after working for more than 5 years at the Mary Kay O'Connor Process Safety Center.

Aristides Morillo

Mitigation of a Reactive Relief Case by Instrumentation in Lieu of a Relief Device: A Case Study

Aristides Morillo From the past 15+years I have been working on the Technical Safety arena for different companies, including BASF SE headquartered in Ludwigshafen (Germany), Bayer in Baytown (Texas) and Shell Global Solutions (Houston). My areas of expertise are related with pressure safety/safeguarding, flare and relief disposal, and reactive hazards assessment. During my Ph.D. at the University of Stuttgart, I focused on the rigorous design and modeling of chemical reactors. I am originally from Venezuela, where I first completed my career as a Chemical Engineer.

Explosion Modling

Cassio Brunoro Ahumada

Comparison of Explosion Methods for Large-Scale Unconfined Elongated Explosions with Propane and Methane mixtures

Cassio Ahumada is a Ph.D. candidate at the Chemical Engineering Department at Texas A&M under supervision of Dr. Qinsheng Wang. His research focuses on vapor cloud explosions and investigating conditions that enhance flame acceleration and transition to detonation (DDT). He expertise combines both experimental analyses as well as numerical simulation. During his time as a graduate research assistant at MKOPSC, Cassio participated in several projects related to consequence modeling and process safety management. He recently finished a summer internship at Tesla in Fremont, California, supporting the EHS department on process safety related activities. Before that, he worked as a Technical Safety intern at Wood Group in Houston, during the design of an offshore installation.

Alfonso Ibarreta

Modeling of Vented Deflagration Fireball Hazard

Dr. Ibarreta applies thermodynamics, fluid dynamics, and heat transfer principles to the study of combustion processes in fires, explosions, and a variety of combustion devices. He is a Certified Fire and Explosion Investigator and has investigated fires and explosions involving consumer products, residential and commercial buildings, and industrial facilities.

Dr. Ibarreta has evaluated the compliance of industrial facilities with NFPA standards, as well as state and federal codes for the prevention and mitigation of dust and gas explosions. He has performed Dust Hazard Analyses (DHAs) at facilities handling combustible dust. He has also participated in Process Hazard Analyses (PHAs) and performed consequence modeling of flammable liquid / gas releases during the permitting and planning stages of LNG terminals and other oil & gas facilities. Dr. Ibarreta has employed Computational Fluid Dynamic (CFD) models, including FLACS, to calculate the consequences of flammable liquid/vapor releases, vented deflagrations, and unconfined vapor cloud explosions.

Dr. Ibarreta is a principal member of the NFPA's Technical Committee on Explosion Protection Systems. This committee is responsible for NFPA documents related to explosion protection systems for buildings and equipment, including NFPA 67 Guide on Explosion Protection for Gaseous Mixtures in Pipe Systems, NFPA 68 Standard on Explosion Protection by Deflagration Venting, and NFPA 69Standard on Explosion Prevention Systems. Dr. Ibarreta is also the mechanical engineering representative at the Massachusetts Board of Fire Prevention Regulations. This board is responsible for amending and promulgating the comprehensive fire safety code (527 CMR) for the Commonwealth of Massachusetts.

Jiayong Zhu

Heavy gas concentration prediction on complex terrain using CFD with Monin-Obukhov similarity theory

Jiayong Zhu got his bachelor's degree in Chemical Engineering from University of Florida. Now he is a fifth year PhD student in Mary Kay O'Connor Process Safety Center at Texas A&M University. His doctoral research is to develop a reliable and robust Computational Fluid Dynamics (CFD) model and to generate a correlation chart, which is used to predict the hazardous zone and obstacle sizes. He has experiences on process safety, data analysis and incident investigation. He will continue to devote his passion and efforts on the field of process safety.

Engineering Ethics

Lindsey Bredemeyer

Engineering Ethics

27 Years of Valve Engineering
18 Years of Engineering Consulting
22 Year PE

Day 3 Track 1

Management, Operational, and Offshore Assurance

Dana Cooper

PSM Alarm Management – "It's Alarming"

Dana R Cooper, Founder, and President of Cooper Hayes LLC., brings over 25 years of experience in the fields of global industrial manufacturing, marketing and management. She has earned a reputation for creating value and transforming functions by being creative in finding new and innovative ways to increase Best Practice Alignment, Business Integration, Strategy Formulation, and Delivering Results. Dana launched her consulting firm, Cooper Hayes LLC, in 2016. Cooper Hayes specializes in business performance improvements. Before her entrepreneurial start, she was the Director of Business Excellence and Resin Manufacturing & Product Development at Fairmount Santrol for seven years. Previously Dana worked for Ashland Chemical in various manufacturing, EH&S, and marketing positions. These roles included increasing responsibilities, progressing from process engineering to Global Business

Development Manager. She also held responsibilities as plant manager, process safety management systems, and business management including Global Marketing Manager. Dana is a graduate of Michigan State University with a BS in Chemical Engineering and earned her MBA in 1998 from Cleveland State University. Dana currently serves as a board member for the Foundry Education Foundation. She is also the current president of the Cope & Drag Club, which is a technical group made up of foundry suppliers. She participates on the AFS Governmental Affairs Committee, Women in Metalcasting and Marketing Division. Previously she served on the Board of Directors for the American Foundry Society and as a Chairperson for the AFS Marketing Division & Sustainability. She completed the chairs of the Northeast Ohio AFS chapter. Dana was recognized with the Gold Award at a World Foundry Congress (WFO).

Abdullah AlMulla

Safeguards Verification

Abdullah AlMulla Joined SABIC Scholarship Program 2007 (3rd cohort)
B.S. Degree in Chemical Engineering & Minor in Chemistry.
Graduated from Widener University, Chester, PA, USA 2014.
Joined SADAF "SABIC" as fresh graduate in July 2014. Worked as Process Engineer supporting Utilities & Distributions Plant then moved in as Production Engineer supporting Utilities & Distributions Plant. Joined Process Engineering Department as Process Safety Engineer Since March 2018.Attended and graduated from Process Safety Competency Development Program - Batch 2 in 2017 provided by Mary Kay O'Connor Process Safety Center.
Certified in LOPA and PHA studies.

Christopher Gordon

Data-Driven Prescriptive Maintenance Scheduling and Process Optimization

*missing bio

Gregg Kiihne

More effective use of Leading Indicators

Gregg received his BS in Chemical Engineering 27 years ago from UT-Austin and immediately started work at BASF. After several different traditional Chemical Engineering roles over 6 years, Gregg transitioned into a Process Safety expertise role.
He has served in EHS and Process Safety roles for about 20 years, working in Texas, Michigan, Mexico and Germany, and currently heads Process Safety for BASF in North America.
When not at work, Gregg enjoys spending time with his family, traveling and cooking.

Day 3 Track 2

Human Factors – People in Action

Human Performance

S Camille Peres

Procedural Systems as Independent Layers of Protection: Are We Giving More Credit Than is Due?

Dr. S. Camille Peres is an Associate Professor with Environmental and Occupational Health at Texas A&M University as well as the assistant director of Human Systems Engineering with the Mary Kay O'Connor Process Safety Center. Her expertise is Human Factors and she does research regarding: procedures; Human Robotic Interaction in disasters; and team performance in Emergency Operations.

Salvador Avila Filho

Analysis of the Low Perception of Risk: Causes, Consequences and Barriers

Chemical Engineer, Certified Quality Engineer, Petrochemical Process Specialist, Clean Technology Specialist, Organizational Culture Specialist, Psychoanalist, Psychosomatic Specialist, Educational Process in the Community Specialist, Master in Clean Production, Doctor in Sociothecnical Reliability. Experience as Operation Engineering, Manager, Instructor, Nowadays Professor and Researcher at University UFBA, Consultant in Human Factor, Reliability, Energy Loss and Risk.

Sridhar Ketavarapu

Enhancing Safety Through strengthening Human Barrier

Sridhar Ketavarapu has a Bachelor's degree in Mechanical Engineering, Master's degree in Energy Systems and an MBA in Insurance and risk management. Having started his career as a Claims Risk Engineer with an Indian Insurance company, where he analyzed a variety of accidents and its possible causes. Following the stint, the author started as a Consultant within the Oil and Gas Industry and worked with many National and International Oil Companies.
The experience culminated from working with both financial and technical worlds with respective experts in his career, the author developed a deep understanding of barriers and its significance. Also the author suggests the importance of integration - Personnel with Process safety is the key to ensure overall safety in all critical industrial activities. Currently the author works as a HSE professional with Kuwait Oil Company.

Tina Miyake

Crosswalk of Human Reliability Methods of Offshore Oil Incidents

My background is in cognitive psychology specifically working memory and interference. I earned my Ph.D. from North Carolina at Greensboro. I taught at Idaho State University for 8 years. I was first an adjunct instructor and then a visiting assistant professor. I recently transitioned to Human Factors at the Idaho National Laboratory. Additionally, I still teach a class at ISU.

Day 3 Track 3

Design and Analysis

Process Design and Mitigation Systems II

Kartik Maniar

Omi Soni

How Dynamic Simulation Helped Mitigate Vapor Disposal System

Kartik Maniar, has worked more than 10 years in the field of relief system design. Has been involved as a lead in multiple refinery wide pressure relief and flare analysis projects. Currently working as Principal Process Engineer with Siemens. He has also worked previously with various EPC during his career.

Omi Soni- Process Safety Consultant/Lead, Siemens Energy.
Mr. Omi Soni has over 10 years of Industrial experience with process engineering fundamentals and leads projects related to PRA (pressure relief analysis), flare mitigation, dynamic simulation and flare QRA. He holds a Master's degree in Chemical Engineering with a Lean Green belt certification. Mr. Soni's most recent experience includes mitigation of vapor disposal system by performing detailed quantitative risk analysis (QRA), hydraulic analysis and dynamic simulation.

William Pittman

Fire and Gas Hazard Mapping Continues to Require Engineering Judgment

Dr. Pittman holds a Ph.D. in Chemical Engineering from Texas A&M University and received the university's Safety Engineering Certificate in August 2015. His doctoral research investigated the potential for micro-emulsion formation and phase inversion within semi-batch mixed-acid nitration of Toluene. He has 10 years of experience with process safety research working mostly with Texas A&M's Mary Kay O'Connor Process Safety Center (MKOPSC). He has worked in process safety consulting and incident investigation for 5 years. After receiving his doctorate, he briefly served as a post-doctoral research scientist with MKOPSC before joining Smith and Burgess to work as a safety relief engineer. He now works with Micropack Detection (Americas) as a Fire and Gas Detection Consultant and Risk Analyst.
Dr. Pittman has authored or co-authored over 10 papers on topics including the West Fertilizer explosion, risk communication, and confirmation of process de-energization.

Hari Attal

Inherent Safety as a driver for business success in the Oil & Gas Industry

Hari's experience includes 4 years with Chevron in ETC – FE-Design Technical Safety Engineering as a Sr. Process Safety and Risk Engineer. He has prior Professional Experience of 30 years at HP Mumbai (Esso), Technip & PetroMin (Saudi Arabia), Bechtel USA, Foster Wheeler USA, and BP USA (Houston and Basra Iraq). His experience includes Process Safety, Process Systems, and Relief Systems. Hari's Process Safety and Risk Engineering Education and Professional License include MS

ChemE from Institute of Chemical Technology, Mumbai, India and P. E. (Texas). Hari continues industry representation on API Subcommittee on Overpressure Protection (API- 520 – 521 – 526 and 2000).

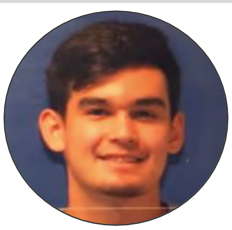
Fadwa Eljack

Studying the Inherent Safety of Flare Utilization Alternatives during Abnormal Operations

Dr. Fadwa Eljack is an Associate Professor in the Department of Chemical Engineering at Qatar University and an adjunct faculty at Texas A&M University in College Station, USA. Fadwa obtained her bachelor (1999) and PhD (2007) degrees from Auburn University, USA. She has served as the Director of the Gas Processing Center (GPC) at Qatar University from 2008 – 2010. Her research areas of expertise focus in the area of Process System Engineering (PSE) that includes process design and multi-objective optimization, sustainable management of gas processing facilities through the development of integrated designs, flare reduction, and product design. She has over 60 refereed papers, several book chapters and co-edited three books. She has led a number of research projects in collaboration with academic institutions and Qatari Industry, with over $4 million in funding.

Day 3 Track 4

Research and Next Generation Explosion Phenomena II



Christian Schweizer

Impact of particle density on dust cloud characteristics in the minimum ignition energy testing apparatus using high-speed digital in-line holography

Christian Schweizer is a graduate research assistant at the J. Mike Walker '66 Department of Mechanical Engineering of Texas A&M University. Christian works in the Optical Diagnostics and Imaging Laboratory to develop and apply cutting-edge laser techniques to study reacting and non-reacting flows.

Sonia Ruiz-Perez

Modelling of the plume rise phenomenon due to warehouse fires considering penetration of the mixing layer

Sonia Ruiz Pérez is a Research Scientist at Gexcon Netherlands BV, which is a joint venture between TNO and Gexcon AS. Her main responsibilities are to develop and implement new consequence models in the software package EFFECTS, as well as to perform QRAs and safety studies for the (petro)chemical industry using software modelling tools such as: EFFECTS, RISKCURVES, PHAST and SAFETI. Prior to her experience as a Research Scientist, Sonia worked as an Environment, Health and Safety (EHS) Coordinator at International Paper where her main role was to investigate incidents, conduct safety observations, raise awareness of safety and give training related to occupational risks, preventive measures and hazard recognition. Sonia holds a Master and Bachelor degree from the IQS School of Engineering in Barcelona, Spain.

Collision of Convex Objects for Calculation of Porous Mesh in Gas Explosion Simulation

Savio Vianna

Sávio Vianna is an associate professor at the University of Campinas (Unicamp) in Brazil. His main research area concerns the investigation of computational modelling of reacting and non-reacting flows. By dealing with the latest numerical schemes and available open sources tools, as well as in house codes, Dr. Vianna has been trying to reinforce the bridge between basic science and the engineering of fluid flow. He is also interested in LES (Large Eddy Simulation) and DNS (Direct Numerical Simulation) for turbulent combustion.

Effects of non-uniform blockage ratio and obstacle spacing on flame propagation in premixed H2/O2 mixtures

Cassio Brunoro Ahumada

Cassio Ahumada is a Ph.D. candidate at the Chemical Engineering Department at Texas A&M under supervision of Dr. Qinsheng Wang. His research focuses on vapor cloud explosions and investigating conditions that enhance flame acceleration and transition to detonation (DDT). He expertise combines both experimental analyses as well as numerical simulation. During his time as a graduate research assistant at MKOPSC, Cassio participated in several projects related to consequence modeling and process safety management. He recently finished a summer internship at Tesla in Fremont, California, supporting the EHS department on process safety related activities. Before that, he worked as a Technical Safety intern at Wood Group in Houston, during the design of an offshore installation.

Poster Presentations

Lindsey Bredemeyer

Process Safety and the Race for the Bomb: Process History Poster Presentation

27 Years of Valve Engineering
18 Years of Engineering Consulting
22 Year PE

Salvador Ávila Filho

1. ***Analysis of the Low Perception of Risk: Causes, Consequences and Barriers***
2. ***Analysis of Reliability Mapping in Refining Industry: Identification of Critical Regions and Interventions in Complex Production Systems***
3. ***Relationship Between Human-Managerial and Social-Organizational Factors: For Industry Safeguards Project: Dynamic Bayesian Networks***

Chemical Engineer, Certified Quality Engineer, Petrochemical Process Specialist, Clean Technology Specialist, Organizational Culture Specialist, Psychoanalist, Psychosomatic Specialist, Educational Process in the Community Specialist, Master in Clean Production, Doctor in Sociothecnical Reliability. Experience as Operation Engineering, Manager, Instructor, Nowadays Professor and Researcher at University UFBA, Consultant in Human Factor, Reliability, Energy Loss and Risk.

Zeren Jiao

Machine Learning Prediction of Hydrocarbon Mixture Lower Flammability Limits Using Quantitative Structure-Property Relationship Models

Zeren Jiao is a chemical engineering Ph.D. student from Mary Kay O'Connor Process Safety Center. His research field is developing quantitative structure-property relationship models for fire and explosion related properties.

Juan Orozco

Influence and Effects of the use of Flue Gas- Water Steam on the API N-80 Steel

*Missing bio.

Taylor Ritchie

Effects of dust adhesion forces on cloud characteristics in minimum ignition energy (MIE) apparatus

I am a mechanical engineering undergraduate student. I have worked alongside Dr. Chad Mashuga as part of the MKOSC chemical and safety engineering internship over the summer of 2019.

Yueqi Shen

Thermal Hazard Assessment of Benzoyl Peroxide Mixed with Dry Fire-Extinguishing Chemicals

Yueqi is a PhD candidate in Chemical Engineering at Texas A&M University and also a graduate research assistant at Mary Kay O'Connor Process Safety Center. Her background includes biochemical engineering, chemical engineering, and process safety engineering. Her current research area is reactive chemical in process safety, employing calorimetry techniques to characterize reaction kinetics, analyze decomposition mechanism, and evaluate the risk of thermal runaway reactions. The topic of her thesis is Thermal Stability Analysis of Benzoyl Peroxide Systems.

Yue Sun

Reaction Hazard Study for H2O2 Oxidation of 2-Octanol in a Heterogeneous Batch Reactor

Yue Sun is a PhD candidate in Chemical Engineering. She is the graduate assistant for Mary Kay O'Connor Process Safety Center and the Artie McFerrin Department of Chemical Engineering at Texas A&M University. She holds a Bachelor's degree in Chemical Engineering from Tsinghua University, China.