TEXAS A&M ENGINEERING EXPERIMENT STATION

MARY KAY O'CONNOR PROCESS SAFETY CENTER

21st Annual International Symposium

XXI

2018 Proceedings

Beyond Regulatory Compliance Making Safety Second Nature

In Association with IChemE

October 23–25, 2018

Hilton Conference Center, College Station

Table of Contents

Welcome

Sponsors
Shell and Gexcon

Symposium Media Sponsors
Chemical Processing and Chemical Engineering

Process Safety in the 21st Century

In Association with IChemE

Consortium Members

Steering Committee

Technical Advisory Committee

Frank P. Lees Memorial Lecture

Keynote Speakers
Laurie Muse Shelby, Prof. Genserik Reniers, Prof. Jenq-Renn Chen

Remembering Dr. Sam Mannan

Day 1 Track 1
First Line Supervisors - A Safety Critical Layer
Hesham K. Al-Subait

Evaluating Learning of Process Safety Among Engineering Students
Nina Fatma Ali

On Telling the Whole Story: Operator Task Performances and Physiological Costs during Complex and Critical Offshore Drilling
Ranjana K. Mehta

Biocompatible Herders for Offshore Oil Spill Mitigation
Dr. Zhengdong Cheng

Measuring Expertise Acquisition with Virtual Industrial Tasks - Implications for Procedure Design and Use
Timothy Neville

A Practical Approach to Human Error
Kyle Wingate

Representing 'Work-As-Done (WAD)' of Communication and Information Flow in an Incident Management Team
Jurkin Moon, Timothy Neville, S. Camille Peres, Farzan Sasangohar, Changwon Son

Day 1 Track 2

What to Do if PSM/HSE Performance Flattens Out? How to Resume Your Drive to ZERO
Steve Arendt

Hazard Analysis Study on Vehicle Impact Inside a Chemical Plant
Jaime Tseng

Achieving Operational Excellence by a Robust Sustainable Safety (Process and People) Program
Chris Israni

Acting on Information from Small Incidents and Near Misses
Mike Munsil

Assessing Operational Excellence
Ian Sutton

Cybersecurity Consideration in Process Hazard Analysis
Addie Cormier

Addressing the Security Requirements in Functional Safety Standard IEC 61511-1:2016
Marco Ayala, John Cusimano

Facility Security - Are You Ready
Bill Efaw

Day 1 Track 3

HAZID to SIL - Challenges in Hazard Identification Impacting SIL of SIF
Amit K. Aglave, Fluor Daniel

Integration of Control Systems: A focus on Safety
Mark Buchman

Changes in IEC 61511 2nd Edition
Paul Gruhn

The Importance of Properly Evaluating Consequence in a Process Hazard Analysis
Rhonda Schmidt

PHA Guidance for Correlating H2S Concentrations in Process Streams to Severity of Adverse Health Outcomes in the Event of a Leak
Anee Bertelsmann

Evaluating the Transient Radiant Heat Flux Impacts to Occupied Buildings
Jeffrey D. Marx

CAROL - Robotic Catalyst Removal
Christopher Jansen

Connecting Process Safety and the Dynamic Frontline
Simon Jones

Using Process Historian Data to Understand and Assure Barriers
A.M. Tony Downes

Day 1 Track 4

Fire Incidents at Ethylene Oxide Reactors in Ethylene Glycol Plant
Kevin S. H. Hsueh

After the HAZOP: A Practical View of Process Hazards
Gregg M. Kiihne

Assessment and Analysis of Fuel Storage Terminal Explosion: Consequences and Challenges Ahead
Ravi Kumar Sharma

System-focused Risk and Process Safety Education
Ian Cameron

Improving the Quality of Undergraduate and Company Interactions in Process Safety
Trish Kerin

High Surface Area Oxidation - Calorimetric Determination and Modeling of Solids Oxidation of Organics on High Surface Area Substrates
Brenton L. Drake

Thermal Analysis and Characterization of Polystyrene Initiated by Benzoyl Peroxide
Xin-Miao Liang

Potential for Hydrogen DDT with Ambient Vaporizers
J. Kelly Thomas

Day 2 Track 1

Quantitative Risk Calculations for a U.S. DOT Natural Gas Pipeline Using Population Classifications
John B. Cornwell

Managing the Risk of Organizational Incidents
Brian Dickson

Common Bow Tie Errors and How the CCPS Concept Book Rectifies

Tatiana Norman

Considering Multiple Initiating Events in a LOPA
Denise Chastain-Knight, Loren Stewart

Evolutionary Themes from ISA 84 to ISA 61511
Eloise Roche

Process Safety Time Analysis for Upstream Facilities
Anupa Baharrysingh

Successful Implementation of Hazards and Effects Management System in Capital Project
Divya Narayanan

Sizing Rupture Disk Vent Line Systems for High-velocity Gas Flows
Mondie K. Mutegi

Development of a Company-Specific Consequences Severity Model to Improve Efficiency and Consistency in PHAs
Sam Aigen, Rich Santo

Day 2 Track 2

Team Cognition for Coordinated Decision-making during Hurricane Harvey: A Case Study from Interviews with Responding Commanders
Jurkin Moon

Assesment and Mitigation of NaTech Events Caused by Floods
Valerio Cozzani, Alessio Misuri, Simone Vivarelli

Designing Effective Emergency Response Plans: Lessons Learned from Investigating Two Major Incidents
Scott Davis

Computational Fluid Dynamics Study of Heat Flux from Large LPG Pool Fires
Qingsheng Wang, Hang Yi

Does a HAZOP Reveal to Us All the Hazards We Need to Know, or Are We Overlooking Serious Threats?
Sunhwa Park

Distinguishing Offshore Drilling Safety Improvement Through Engineered New Technologies versus Mandates & BAST - MPD Example
Robert M. Pilko

Dropped Object Risk Assessment for Fixed Offshore Platforms
Ali Sari

Day 2 Track 3

Experimental Research on the Decontamination Effect of Aqueous Solutions Containing Organic Acids on the Relsease of Ammonia within Confined Space
Xuhai Pan

Numerical Modelling for Effect of Water Curtain in Mitigating Toxic Gas Relsease
Seungho Jung, Dong Seok Min, Eui-young Oh

Risk Based Process Safety for Semiconductor Fabrication Operations
Steve Hawkins, Chris Israni

Transient Large-Scale Chlorine Releases in the Jack Rabbit II Field Tests: Estimates of the Airborne Mass Rate for Atmospheric Dispersion Modeling
Tom Spicer

Integrating Human Factors Concepts into Improving Risk Management and Safety Performance
Philip Grossweiler

Procedural Performance: Possible Costs of Time Pressure, Shift Change, and Task Complexity
S. Camille Peres

Multi-level Failure, Causality and Hazard Insights Via Knowledge Based Systems
Ian Cameron

An Intelligent Video Fire Detection Approach Based on Object Detection Technology
Hao Wu

A Refreshing Take: Analysing Accident Scenarios Through Casual Network Topology Metrics
Hans J. Pasman

Day 2 Track 4

Heat Transfer Modeling of High Expansion Foam Application for Vapor Risk Mitigation of Liquefied Natural Gas
Salma Akhter, Pratik Krishnan, M. Sam Mannan, Bin Zhang

Experimental and Computational Study of the Dispersion and Combustion of Wheat Starch and Carbon-Black Particles during the Standard 20L Sphere Test
Paula Pico and Jose Serrano

A Risk-Based Dust Hazard Analysis (DHA)
Fuman Zhao

Advanced Fire Integrity Analysis and PFP Optimization Method for Petrochemical Facilities
Necip Onder Akinci

Developing Safety Culture in an Undergraduate Chemical Process Safety Course
David W. Murhammer

Process Safety Academy (PSA) for First Line Supervisors
Hesham K. Al-Subait

Flipping the Assessment Model: Teaching and Assessing Things That Matter
Christopher Lilburne

Inherent Safer Design for Chemical Process of 1,4-dioldiacetate-2-butene Oxidized by Ozone
Min Hua

Deficiencies Frequently Encountered in the Promotion of Process Safety Information
Horng-Jang Liaw

Day 3 Track 1

Process Safety Fundamentals - Making Process Safety 'Real' in the Field
Graham McVinnie

Evergreening - Managing Risk in the Face of Constant Change
Alysson Ferriera

Lifecycle Management of Risks with a Hazards Register
Jack Chosnek

The Application of Bowties for a Robust PSM Program
Tatiana Norman, Marisa Pierce

Day 3 Track 2

Hazard Mapping Case Study on a Compressor House
William Pittman

Enclosed Process Bay Vented Blast Loads and Impacts on Near-by Occupied Buildings
Mark Whitney

Development of Empirical Method to Calculate Natural Gas Pipelines Rupture Exposure Radius
Arafat Aloqaily

Stream Drum Level Measurement Compensation through the use of Constant Head Chamber with Dynamic Compensation
Lianwei Zhong

Day 3 Track 3

Analytics and Artificial Intelligence: Deep Learning for Anomaly Detection - A case study from the financial sector with application to process safety
Franz Hiebert, Arul Livingstone, Nnamdi Orakwue

Multi-objective Stochastic Optimization for Preventive Maintenance Planning
Christopher K. Gordon

A Framework of Hazard Identification of Complex Systems
Mengxi Yu

Day 3 Track 4

The Gulf Research Program's Initiative for Safer Offshore Operations
Kelly Oskvig

How a Small E&P Company Manages SEMS(Safety and Environmental Management Systems) On Large Deepwater Drilling Operations
Charlie Culver

WellSafe Initiative
Mike French, Robert Hinojosa, Marcel Robichaux, and Jeff Smith

Ocean Energy Safety Institute, The First Five Years
M. Sam Mannan, Hans Pasman, James C. Pettigrew

WELCOME TO THE
2018 ANNUAL INTERNATIONAL SYMPOSIUM

Ladies and Gentlemen:

I am delighted to welcome you to the 2018 Annual Symposium of the Mary Kay O'Connor Process Safety Center. This Symposium is missing something – something that we all are feeling. We are missing Dr. Sam Mannan. I miss Sam. I miss the 6' 3''-man from Bangladesh. He was a giant of a man in the land of short people, but he surely was a Giant – a Titan among the Process Safety Community and much more.

When I joined Texas A& M University in 2012, he told me, "Naz, I have a vision – a vision of NO ACCIDENTS. Help me realize this vision by education young people so that they carry the message of NO ACCIDENT." Ladies and gentlemen, let's promise to ourselves and to our future generations that we will not stop until we achieve Sam's vision.

Sam was a hardworking man. Sam was a kind man. He helped countless people with his generous help (financially) and by giving his golden wisdom. Sam was also a very humorous man. He liked a good joke or two; I am sure many of you have heard his jokes. If it was after 6:00 PM, and if you would go by his office in Jack E Brown Building, the door would be cracked open and you would hear (occasionally) strange voice saying something in a foreign language and there would be laughter. Sam was listening to Bhanu Bandyopadhyay (a Bengali actor and comedian) jokes. On some other evenings, you would probably listen to some interesting songs – songs called Kawali, sung by Nusrat Fateh Ali Khan. What I want to convey to you is that Sam worked all day and all night (possibly) but he knew what was important in life. Richness of one's mind and richness of one's heritage. He loved the Aggies, he loved Dallas Cowboys, and he definitely loved the Sooners, but if you needed to see him in his own "hood" in Dhaka; he would be like a child, trying to do everything he did when he was a student at BUET and before. He never missed a chance to eat at "Kasturi" restaurant in Dhaka. It is very well-known for traditional Bangladeshi food (Anthony Bourdain should have gone there!). More than once, he had gone directly there, and the owner knew what to cook for their favorite customer from America! I could go on and on about how my friend lived his life, but we need to move on to the Symposium. I am going to give you the same message Sam gave you in his welcome addresses in the past.

This is the 21th in the series, "an important annual event that focuses on research, education, training and service issues that impact safety. Your participation is essential in making the symposium a success, and ultimately advancing the process safety technologies and concepts to make industry safer. We also believe that proactive safety programs are good business and have a positive impact on the bottom line." Your participation is very special this year to make it a success, as we are hell-bent on realizing Sam Mannan's dream.

"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 tremendous 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 complete papers presented at the symposium, 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."

M Nazmul Karim, PhD, Fellow of AIChE
Holder of the Michael O'Connor Chair II
Professor and Head,
Artie McFerrin Department of Chemical Engineering
Texas A&M University
255 Jack E. Brown Building

Distinguished Sponsor

Shell is a leading global enterprise in today's oil and gas exploration and production business, and one of America's leading oil and natural gas producers, gasoline and natural gas marketers and petrochemical manufacturers. Shell operates in 50 states and employs more than 22,000 people delivering energy in technically innovative ways.

Shell strategy is to generate profitable growth, to drive forward with investment programs, to deliver sustainable growth, and provide competitive returns to shareholders, while helping to meet global energy demand in a responsible way.

Shell supports the sustainability and development of the MKOPSC's unique process safety curriculum, opportunities to develop process safety training available globally through universities, and a neutral forum to advance process safety practices and cultures through engagement of academia, industry and regulators.

Symposium Select Sponsors

GexCon is an engineering and scientific consulting firm that specializes in process safety hazard analyses and accident investigations. GexCon combines unparalleled technical expertise with the ability to respond rapidly and to focus this knowledge in extremely short time frames. GexCon offers a range of services—from in-depth research and analysis to rapid-response evaluations—providing our clients with the critical information required to make day-to-day or long-term strategic decisions.

4833 Rugby Ave.
Suite 100
Bethesda, MD 20814
www.gexconus.com
Phone: +1 (301) 915-9940
Fax: +1 (301) 656-2953
Email: gexconus@gexcon.com

Symposium Media Sponsors

Chemical Processing, ChemicalProcessing.com and Chemical Processing E-Newsletters reach a monthly worldwide audience of over 140,000 chemical industry professionals responsible for designing, operating and managing more than 40,000 chemical, petrochemical, refining, plastics and pharmaceutical facilities in North America and across the globe. These professionals are responsible for developing cost effective processes, optimizing the efficiency and reliability of plant assets and implementing product and production strategies.

Chemical Processing
1501 E. Woodfield Road, Suite 400N
Schaumburg, IL 60173
Phone: 708-404-3334
http://www.chemicalprocessing.com
bmarz@putman.net

Chemical Engineering is published monthly by Access Intelligence, primarily for chemical engineers and related technical people in the chemical process industries (CPI), as well as at engineering, design and construction companies that serve the CPI. The magazine is edited for the "technical decision-maker," an individual who applies engineering training to the making of technical and business decisions. This person most often is a chemical engineer, chemist or mechanical engineer, working in research and development, design, construction, production or technical management. Whether a recent technical graduate or someone with years of experience, this individual is applying technology for profit in the CPI. Such a person looks to *Chemical Engineering* for practical information that can be used directly on the job, plus the latest about what's happening in, or will be affecting, the CPI. Serving these needs is the primary function of our magazine.

11000 Richmond Avenue, Suite 690
Houston, Texas 77042
Phone: (832) 242-1969
Fax: (832) 242-1971
http://www.chemengonline.com/

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. This 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 the 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 professional 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 obliges to improve process safety because engineering and science are essential to us all and it must be sustainable in all senses of the world, 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, this 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 the 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

Consortium Members, Mary Kay O'Connor Process Safety Center

Partners

Albemarle
BHP Billiton
BP America, Inc
Cheniere
Chevron
ConocoPhillips
Dow Chemical Company
Eastman Chemical
Evonik
ExxonMobil
Formosa
Huntsman Corporation
Occidental Petroleum Corporation
P66
Patricia C. Hamlin
Reliance Industries
Saudi Aramco
Shell E&P
Total Petrochemicals & Refining

Sponsors

ABS Consulting
AcuTech Consulting
aeSolutions
Atkins
Bayer
DNV GL
FM Global
GexCon
HIMA Americas
Honeywell
INEOS
KBR
Lloyd's Register
MMI Engineering
Petrotechnics
Siemens
SIS-TECH Solutions

Associates

Environmental Intellect
Kestrel Management Services

Steering Committee, Mary Kay O'Connor Process Safety Center

Arafat Aloqaily
Saudi Aramco

Steve Arendt
ABS Consulting

Jehova Arenas
Pemex

A.W. Armstrong
Kestrel Management

Stewart Behie
Occidental Petroleum

Vivek Bichave
Reliance Industries

Carl Brown
KBR

Steve Burton
Total Petrochemicals

Ron Chittim
API

Jack Chosnek
Knowledge One

Bill Clark
Phillips 66

Joey Cranston
Albemarle

Buddy Creef
HIMA-Americas

Scott Davis
GexCon

William Efaw, *Co-Chair*
Dow Chemical

Leonard Gomes
Cheniere

David Greganti
Dow
Subin Hada
Evonik

Patricia C. Hamlin

Anil Hegde
Reliance Industries

Erwin Icayan
Atkins

Shakeel Kadri
AIChE-CCPS

Kelly Keim

Trish Kerin
IChemE Safety Centre

Paul Klein
BHP Billiton

Patrick Mahan
FM Global

Margarita Malaspina
BHP Billiton

Liz McDaniel, *Chair*
Huntsman

Mike McGuire
WinSim

David Moore
AcuTech Consulting

Derek Nelson
Occidental Petroleum

T. Michael O'Connor
MKOPSC

Scott Ostrowski
ExxonMobil

Dennis Parker

Gijs-Jan Peek
Honeywell

Marisa Pierce
DNV GL

Cathy Pincus
ExxonMobil

Norberto Pineda
Lloyd's Register

Robin Pitblado
DNV GL
Ben Pratt
Siemens

Neha Rajan
Bayer

William Ralph
BP America

CV Ramaswamy
Shell

James Reisz
ExxonMobil

Hector Rivero
Texas Chemical Council

Carlos Robles-Sanchez
INEOS

Ellen Ross
Chevron

Kathy Shell
aeSolutions

David Stacy
Eastman Chemical

Andrew Staszak
MMI Engineering

Eric Steinhauser
Albemarle

Kris Terpening
BHP Billiton

Jaime Tseng
Formosa

Tracy Whipple
BP

Mark Whitney
ABS Consulting

Steven Tyler
Bayer

Tracey Whipple
BP

Simon Wragg
Conoco Phill

Technical Advisory Committee, Mary Kay O'Connor Process Safety Center

Stewart Behie
Occidental Oil & Gas

Rob Bellair
Dow Chemical

Joe Berg Huntsman

Mark Briggs
OSHA

Carl A. Brown
KBR

Jack Chosnek, *Chair*
KnowledgeOne

Lizbeth Cisneros

Scott Davis
GexCon

Victor Edwards

Steven D. Emerson
Emerson Technical Analysis

Dave Greganti
Dow

Phillip Hodge
BakerRisk

Colin S. Howat
CS Howat & Associates

Seungho Jung
Ajou University

Daryl Kenefake
ExxonMobil

Marc E. Levin
Washington State University

Yen-Shan Amy Liu
Provenance Consulting

Jeff Marx
Quest Consultants Inc.

Hager Mhekeba
Department of Labor

David Moore
AcuTech Consulting

Derek Nelson
Occidental Oil & Gas

Giang Nguyen
aeSolutions

T. Michael O'Connor
MKOPSC

Irvin Osborne-Lee
Prairie View A&M University

Scott W. Ostrowski
ExxonMobil

Maria Papadaki
University of Patras

Ray Qi
Huntsman

CV Ramaswamy
Shell

Maxxine Roopchand
Atkins

Srini Sambasivam
Shell

Roy Sanders
MKOPSC

Karen Study
Dow

Angela E. Summers
SIS-TECH Solutions

Jeff Thomas, *Co-Chair*
ExxonMobil

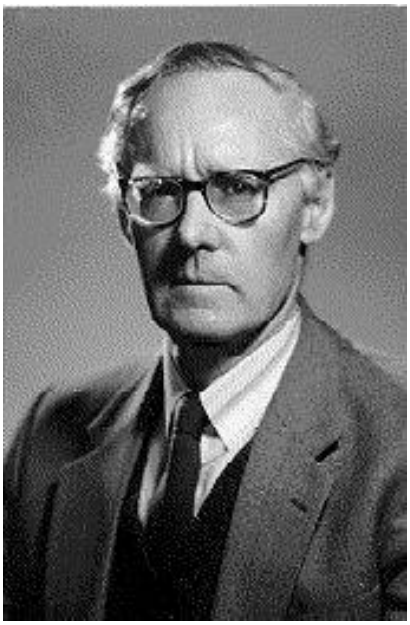
Jaime Tseng
Formosa

Qingsheng Wang
Oklahoma State University

Kevin Watson
Chevron

Cindy Wei
Genesis Oil and Gas

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.

Keynote Speakers

LAURIE MUSE SHELBY, CIH, CSP, M.S.

Vice President - Environmental, Health and Safety
Tesla, Inc.

Laurie Shelby joined Tesla Inc. as the EHS Vice President in October 2017. She leads worldwide EHS for approximately 50,000 employees in the automotive, energy, and sales, service, delivery operations.

Previously, she was the EHS Vice President for Alcoa Inc. where she led the global EHS process for approximately 15,000 employees in the mining, refining, smelting, and rolling operations. Prior roles at Alcoa included EHS Director for United States primary aluminum operations and EHS global audit Manager.

Laurie is active in the American Society of Safety Engineers (ASSE) and is a sub-committee lead for the Health and Safety Management System (Z10) fatal and serious injury reduction team. Laurie is a human and organizational performance expert known for her new view thinking to improve safety.

Laurie completed her bachelor's degree in chemistry from Radford University. She earned her master's in Industrial Hygiene/Biomedical Engineering from Virginia Commonwealth University/Medical College of Virginia. Laurie is also a Certified Safety Professional (CSP) and Certified Industrial Hygienist (CIH).

Prior to joining Alcoa and Tesla, Laurie worked as an EHS consultant in the Washington DC area where she led numerous federal environmental projects and Superfund site cleanups. She also worked for Dominion Energy as an industrial hygienist.

Laurie and her husband, Joe, live in Alameda, California, but they are both native Virginians. She has 2 daughters, one who is working on her Environmental Science Masters at University of Virginia and the other is in law school at Dickinson - Penn State.

Prof. Genserik Reniers

Safety and Security Science Group
Delft University of Technology

Genserik Reniers, a Master of Science in chemical engineering, is Full Professor at the Safety and Security Science Group of the Delft University of Technology, in the Netherlands, where he teaches Risk Analysis and Risk Management. At the University of Antwerp in Belgium, he is a Full professor lecturing amongst others in chemistry, organic chemistry, and Technological Risk Management. At the Brussels campus of the KU Leuven, Belgium, he lectures as a Professor, amongst others, in Engineering Risk Management. His main research interests concern the collaboration surrounding safety and security topics and socio-economic optimization within the chemical industry. Amongst many other academic achievements and output, he has published 150+ scientific papers in high-quality academic journals, and has (co-)authored and (co-)edited some 35 books. He serves as an Editor of the Journal of Loss Prevention in the Process Industries and as an Associate Editor of the Journal 'Safety Science'.

Prof. Jenq-Renn Chen

National Kaohsiung University of Science and Technology, Taiwan

Jenq-Renn Chen is a Distinguished Professor in the Department of Safety, Health and Environmental Engineering, National Kaohsiung University of Science and Technology, Taiwan. Previously, he has held the position as Chairman of the Department, Dean of College of Engineering and Vice President in the same university. He is also in charge of the Taiwan EPA Southern Environmental Incident Specialist Team, which provided emergency response services to southern Taiwan. He received MSc and PhD from Imperial College, London, UK, both in Chemical Engineering. He has 4 patents and authored more than 50 referred papers in international journals, all in the broad range of chemical process safety. He also participated in more than 100 chemical and gas emergency responses and incident investigations in Taiwan, including the catastrophic Kaohsiung pipeline explosion in 2014. His current research interests are gas safety, explosion suppression, ignition mechanism, and fundamental aspects of chemical safety.

Remembering Dr. Sam Mannan

Dr. Mannan was an outstanding ambassador for the Aggie Core Values, and went above and beyond with his outstanding scholarship, mentorship and leadership of both the Mary Kay O'Connor Process Safety Center and the field of process safety. His passion to make safety second nature and the dedication to make a difference will be sorely missed, but his legacy will continue to serve as a North Star for us and the future of process safety.
Pranav Kannan, Ph.D., MKPOSC Alumni

I was so shocked and sad to hear about the news that the respectful Dr. Mannan passed away. He was my postdoctoral advisor who brought me into the field of process safety and risk assessment. I was fortunate to have a chance to work with him for two years and receive guidance from him both career wise and life wise. He is a pioneer and made significant contributions for protecting people, environment and assets by making industrial processes safer. He is a big name, proven by his tons of publications, testimonies to the government, countless of received awards and titles, and being key-note speakers for many international and national companies and conferences, but he never just sat on his fame. I cannot remember how many times I saw him working in the late night and during the weekends. His schedule is always so full that a normal person wouldn't want to bear. Wish he enjoys the rest in peace after this "retirement". He left but his spirit and attitude towards work and life will drive us to create safer industrial places, cleaner environment, and less incidents and losses for everyone.
Hao Chen, MKOPSC Alumni

As an advisor, Optimistic and strong are the characteristics that I learn from him.
Even though Dr. Mannan have very busy schedules, he always spends time for his students. When I have difficulties to continue on my research, I will go and see Dr. M. Sam Mannan for advices. Dr. Mannan is very patient and listening to me. He always tries to find me a solution. As a leader, Dr. Mannan always teaches us to be prepared and confident. I remembered I had a chance to contribute in a project led by Dr. Mannan. I can see how he communicates with clients and I learn the values of hard working. I really enjoy working with Dr. Mannan.
Thank you so much to my advisor, Dr. M. Sam Mannan.
Jiayong (Chris) Zhu, MKOPSC PhD Student
"Dr. Mannan found me rather than the other way around. He was the first professor to return my undergraduate email - little did I know but that would change the direction of my career. He showed, modeled, and led process safety for me. As I've grown from undergraduate researcher to PhD student to alumni, he's been a constant example and leader. I had big shoes to fill in following his example in my industry process safety role, but I know I am capable because he prepared me."
Susan Losavio, MKOPSC Alumni

I was always impressed with Dr Sam Mannan's network, and he used that network to get results that benefitted the safety for everybody. He was very approachable and personable. Since he was that way people listened to him; he was able to deliver results, and became a pioneer in process safety. He definitely was a role model on why your network with others, listening to others, etc is important to get results. It is something I think about in my own career. I will definitely miss him.
Christina Sposato, MKOPSC Alumni

Sam was a great friend and colleague. I am forever in his debt for building the MKOPSC beyond anything either of us had envisioned. It is a tremendous memorial to Mary Kay and a lasting legacy of Dr Mannan's. While we face many challenges in continuing without his leadership I am confident that the process safety community will work together to build on what he started.
Mike O'Connor

I was, am, and will be grateful for him to provide everyone in the center a fabulous platform to build our identity and to establish effective connections with people who may bring significant influence in our career and life.
Thanks to him, we are lucky to benefit from him to seek our career goal in the right track. I cannot image who else can do more for his students than him.
As life is going on, he is always here to see how we make safety second nature.
Chenxi Ji, MKOPSC Alumni

Dr. Mannan was a one of a kind professor whose presence will leave an impact on you even when you have a trivial conversation with him. I still remember the day when I first met him in the advisor selection meeting in the first year of my PhD. He started his presentation with LNG which immediately fascinated me. Soon after that presentation, I had discussions with him and decided to join the Mary Kay O' Connor Process Safety center as his student. During my early years of PhD, he

encouraged me and other students to actively participate in the steering committee meeting and process safety conferences. The initial steering committee, technical committee meeting and safety conference led to slow growth of my professional career. He made me learn professionalism, public speaking and stressed a lot on communication time to time. He also encouraged me to learn driving and drive all students to the consortium meeting from College station to Houston. Within few months, I took his course on process safety which provided a remarkable foundation for my research. He is an excellent teacher. I particularly use to like process safety class as all the problems had metric units in it. Given that I was an international student who is used to metric units, the course was breezy. He used to teach in a way that every student can understand. His classes used to be filled with case studies and anecdotes which will never fail to impress anybody. I still remember the day when told a sentence about problem solving in the class where he mentioned "You should eat an elephant piece by piece". This small sentence had a heavy impact on my research. Whenever I got stuck with my research elephant, I used to cut it piece by piece and solve it. As my own career developed, I still use this sentence as a guidance when I work in large projects. During my course of my PhD, I learnt that Dr. Mannan was an excellent manager. He efficiently managed multiple stakeholders effectively. Outside MKOPSC, he always put his students in perspective, be it in department meetings, TAMU Qatar or CCPS. Dr. Mannan's commitment to process safety is unmatchable. There have been times, when he used to be tired from travelling. He still used to show up to the meeting and come to the department to work. Once during my PhD, I asked him about his retirements plans. He jokingly mentioned that work is his retirement plan. He mentioned that he wanted to work till his last breath, which he did. Time to time, we also discussed life in general while submitting my papers to the journal. Submission would take some time and during that time, we discussed my experiences and the issues that I was having during my PhD. He was kind and always had a listening ear. He used to lend me some good advice based on his experience. During my final year of my PhD, I was exploring my career path as a professor. He explained me the various requirements to become a professor which I still remember. He also shared his experience as professor in University of Oklahoma and lessons that he learnt there. I met him last during the alumni meeting this year and never did I imagine that it would be the last conversation with him. He is always inspiring. I deeply miss Dr. Mannan and it will be difficult to fill this void. While I will miss him as my mentor and advisor, I am sure that his accomplishments in the process safety field will continue to exemplify for years to come. *Nirupama Gopalaswami, MKOPSC Alumni*

Dr. Mannan, thank you for everything: As my advisor, mentor and guide you always had an unflagging confidence in me. Thank you for helping me with difficult decisions and sticking your neck out for me, and many others, when we most needed it. Thank you for your commitment to process safety and passion for engineering research. Above all, thank you for always being a father figure, a trusted advisor and a true inspiration to me.
Kiran Krishna, MKOPSC Alumni

Dr. Mannan was not only my advisor; he was my mentor, my role model and a real friend. He taught me how I can contribute to my self-confidence and excel at any level, just by believing in myself. He is the reason I choose to become a Process Safety Engineer. His advice, guidance, speech and actions will always motivate me to become a better-quality professional engineer and above all to be a good human.
Morshed Rana, PhD., MKOPSC Alumni

Thank you for being such a great advisor, a mentor, a leader, and a father. You showed tremendous care and support to my research as well as my family. The "can do" attitude will always stay with me. Your legendary life and legacy will forever be remembered.
Zhe (Zhe Han), MKOPSC Alumni

I appreciated Dr. Mannan's mentorship and took inspiration from his tremendous work ethic and breadth of knowledge. He was warmth, kindness, and strength.
Christopher Gordon, MKOPSC PhD Student

Through we did not realize it before, Dr. Mannan had influenced in a manner that instilled in us a general love for humanity and a passion for process safety which inspires us to ensure safer operation for the well-being of individuals, communities and nations.
Syeda Zohra Halim, MKOPSC PhD Student

Dr. M. Sam Mannan shaped us in different ways; he made us passionate about process safety, teaching us how to use science as the basis to lead safer initiatives in any sphere of our lives, from everyday tasks to industrial activities. We will make him proud and maintain his legacy, while being brave to make process safety the priority, just the way he did.
Tatiana Flechas, MKOPSC PhD Student

Dr. Mannan made an impact on me in many ways. For my career, my dream is to exactly follow in his footsteps

in the center. He influenced me a lot for the enthusiastic attitude on process safety.
Seungho, MKOPSC Alumni

Dr. Mannan is the reason I am where I am today in my career. He accepted me into the Master's program at the Mary Kay O'Conner Process Safety Center and gave me the guidance I needed to successfully complete it and get a great job. Dr. Mannan was fully invested in each one of his students' success and always available to listen to our concerns and give us advice. I was always amazed by how someone as busy as Dr. Mannan was able to find the time to spend with each one of us, check on the progress of our research, and help us get to where we want.
Sally Nicola, MKOPSC Alumni

Dr. Mannan was like a father figure to me. He has had a great impact on my life. I have learned so much from him, in particular, his wisdom, hardworking nature, and most of all, grit. I will always remember him for his guidance during my PhD and many other times in my career. Qingsheng Wang, MKOPSC Alumni

The first time I met Dr. Mannan, he motivated me to pursue Ph.D. focusing in Process Safety without directly mentioning it for once. He just told me, "see you in Texas"; I realized the rest. He has changed my plan of higher education towards something more challenging and rewarding in our first meeting, just with a subtle hint. Throughout my Ph.D. education and Post-Doctoral Fellowship, he has rescued me, stand-by my side, challenged, encouraged and praised. I had trouble in my research, he listened and let me do what I wanted. He helped me overcoming depression. He had believed in me, more than I believed myself. During our last meeting, Dr. Mannan told me how to plan and progress in industrial career. To me, he just showed me the path that I need follow. I am forever indebted to this amazing person, for the education I received, the leadership quality I learned, teamwork, communication skills I possess, critical thinking and challenges I dare face and having courage to standby the "right-thing".
Monir Ahammad, MKOPSC Alumni

Dr. Mannan once told me – 'Make a decision and go at it at 100 mph, although it's illegal to drive so fast'. He was the wisest person I knew and he inspired me to look at the 'big picture' while making important decisions in life. I cannot thank you enough for your positive impact on me. Dushyant Chaudhari, MKOPSC Alumni
In 2007 I attended the conference for the first time, in fact on invitation. While driving his SUV with Michael O'Connor sitting next to him and me on the back seat, Sam Mannan asked me rather unexpectedly and bluntly whether I would like to get over to the Center twice a year for a month to teach and coach students, while he spelled out the conditions. Knowing him already 10 years, initially from European Loss Prevention symposiums as he was towering above all other attendants, I hesitated only two seconds, although I was still at the Delft University. Since, then I made a lot of jumps over the Atlantic and learned to fill out the stream of web forms that make existence at Texas A&M possible. Although not really visible, process safety life has been a growing burden to him. The knowledge field expands so fast. My wife and I met him last in Trondheim at the 2018 European Safety and Reliability symposium. Ina had good contact with him there, serving her fruit when I was following another lecture.
Hans Hasman

I cannot exaggerate how much Dr. Mannan has changed my life and how much I miss him. He knows everybody in my family and my extended family. I am still remembering the days that I was so shy and try to avoid him in the hall way and he "forced" me to present every week in our team meeting for half year.
Yanjun Wang, MKOPSC Alumni

Dr. Mannan taught me the principles of leadership. His word was important to Him and he also had a gentle, humorous side. He showed me that there is no substitute to hard work. He genuinely cared about all of us like his own family and helped carve out a good career for me and many others. I will always be grateful to Dr. Mannan and his family Mrs. Mannan, Joya and Rumki for sacrifices they made as Dr. Mannan spent time with us students and for the vision of the center, striving to make safety second nature in the process industry around the world!
Katherine Prem, MKOPSC Alumni

As Dr. Mannan's first Ph.D. student, I was fortunate to spend a great deal of one on one time with him and witness his ability to better every life he touched. Back then, nobody knew him as a Professor, so I based my decision to join his group on his passion, his amazing personality, and his ability to motivate people. Many specific pieces of advice come to mind; some work related like "networking" and "what matters is what you communicate, not what you know", but the one I cherish the most is the advice he gave me when my father died: "We all spend a limited time in this earth. What matters is how we lived our lives and the memories we leave behind in the people we knew". Dr. Mannan is an example of a life well-lived that will be remembered by many. Lizbeth Cisneros, MKOPSC Alumni

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

First Line Supervisors (FLS): A Safety Critical Layer

Hesham K. Al-Subait
SABIC

E-mail: subaithk@sabic.com

Abstract

First line supervisors (FLS) are key players in the success of any operation plant being a versatile layer leveraging between management and field crew. Based on our experience gained during commissioning, start up and bringing into operation of a plant, this paper highlight the experience of empowering this critical layer for safety success. The critical role of first line supervisor in industries and road map of empowering him and making him competent as process safety field risk discoverer are outlined. The cultural transformation will happen the moment FLS is empowered, because he will lead his team operators/ technicians for empowerment. This practice will create numerous initiatives and systematic KPI's of which empowerment of FLS will be the foremost leading KPI. The proposal plan on how to convert the FLS and his team to a field risk discovery and empowerment tool from both Technical and leadership aspect are discussed. Industries can benefit by focusing more on FLS for sustainable safety excellence and that practice will lead to other organizational achievements as well.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Evaluating Learning of Process Safety among Engineering Students

Nina Fatma Ali, Juliana Kaya Prpic, David C Shallcross*
Department of Chemical Engineering, Melbourne School of Engineering
The University of Melbourne, Victoria 3010 Australia
*Corresponding Author Email: dcshal@unimelb.edu.au

Keywords: Process safety, concept mapping, assessment

Abstract

The understanding of process safety and its principles is crucial to any chemical engineering program. Students need to understand why process safety is critical and how it is applied in industry. The aims of this study are to identify whether the use of concept maps is a suitable method of evaluating cohort learning on process safety and then to explore the student learning and understanding of process safety. An analysis of 103 students' concept maps by three independent reviewers was undertaken. It was completed by classifying every concept contained in the student-generated maps into one of ten proposed concept categories. The analysis has sharpened the definition of each category and provides an insight into how well the key concepts associated with the process safety were captured by students. The results show that at second year, students appreciate of process safety is still maturing, but by later years they have developed deeper appreciation of the concepts.

Introduction

Knowledge and awareness of safety are critical elements of any undergraduate engineering program. Lacking elements of these could result in young engineers leaving university with an inadequate understanding of their roles and responsibilities in ensuring safety in their workplaces. Therefore, it is crucial to equip undergraduate students who are taking engineering courses with essential understanding of process safety. They are also need to be kept up to date with the dynamic nature of industrial practices.

At the University of Melbourne, full-time undergraduate students enrolled in a 3-year Master of Engineering (Chemical) program learn about process safety in three core subjects that is being conducted in Semester 4 and Semester 5. Process safety is first being introduced to students in the subject of Safety and Sustainability Case Studies, in which they are expected to which among others include performing HAZOP and QRA safety analysis and constructing an

environmental impact assessment. Following that, their understanding of issues relating to safety will be deepened in subsequent subjects particularly in Process Equipment Design and Process Engineering in later year.

Apart from providing engineering students with adequate knowledge focusing specifically on process safety domain, the other important criteria is how to properly assess their learning in this domain. The reason being said that, a proper assessment method would be able to show the amount of knowledge students had captured in class. Generally, in the University of Melbourne, students' learning was assessed from several in-class or/and take home written reports and assignments either conducted individually or group, oral presentations as well as end-of-semester examination. This study, however is proposing the use of concept maps to evaluating individual student and cohort learning and understanding around process safety.

Concept Mapping

Human memory is an interrelated system in which learning involves the adjustment of the system to integrate newly learned knowledge (Strautmane, 2012). Learning in this context is crucially reliant upon the learner's existing awareness of concepts and their interconnections (Ausubel, 1968). This indicates that learning emerges from the interaction between newly learned knowledge and the learner's existing knowledge. Such processes involve the ability to differentiate between alternative meanings and to negotiate a solution to any disagreement that might exist between a new and existing notion. Hence, this learning interaction results in more definite classifications of concept and connections, as well as the decision for ambiguous or incorrect ones.

The National Research Council (2004) in their study "*How People Learn: Brain, Mind, Experience, and School*", posit that human brains organise information into hierarchies and network structures, much like those represented by concept maps. So, what are concept maps? According to Novak and Gowin (1984) based on Ausubel's assimilation theory of learning, concept maps are graphical method use to organise and represent knowledge that outline relationships between concepts. They also defined it as a method to facilitate the process of meaningful learning. Ju (1989) suggested that concept maps represent the subject's unique internalisation or understanding of a domain. Zeilik, cited in Besterfield-Sacre *et al*., (2004) in his study determined that the purpose of concept maps is to investigate understanding of concepts, to capture development of ideas over time, and to document the nature and frequency of misconceptions among students. As such, for Ausubel's theory, Zeilik projected that interrelatedness is important in knowledge; as meaningful learning occurs when new knowledge relates to existing knowledge.

Concept maps consist of three important components; concepts, connecting links and connecting phrases. Two concepts in a map may be joined by a connecting link labelled with connecting phrase which together form a proposition, in which specifies the relationship between concepts. Students link their existing knowledge to new information and create maps which show interrelated ideas. Mathes *et al*., (2001) have shown in their study that concept maps provide motivation for languages' students to identify the relationships among different sets of information. Since the development of concept maps, they have successfully been used in the

education sector for over 30 years (Daley and Torre, 2010), and their use in the engineering field is increasing with the passage of time. For instance, Segalàs *et al*., (2008) introduced the use of concept maps as a tool to assess the knowledge acquired by students in the sustainability domain. Besterfield-Sacre *et al*., (2004) have also used concept maps to assess knowledge integration in industrial engineering.

Methods for Concept Maps Analysis

Concept maps may be assessed by several different techniques that aim to assess different elements depending on researchers' intentions.

- The weighted component scoring system. This method was used by Novak and Gowin (1984), where they scored concept maps based on number of concepts, links, cross-links and hierarchies.
- The holistic scoring system. This approach was utilized by Besterfield-Sacre *et al*., (2004), as they analysed comprehensiveness, organisation and correctness of a map based on three-point scale dimension.
- The map comparison system. Acton *et al*., (1994) used this technique to compare students' concept maps in terms of likeness of concepts, their adjacent concepts, and links to a criterion map.
- The categorical scoring system. This method was used by Shallcross (2013) to analyse concept maps by grouping each concept to its relevant categories to present students' appreciation around a study domain.
- The qualitative approach. Kinchin and Hay (2000) proposed to extract three types of structure from concept maps; spokes, chains and nets to indicate whether students demonstrated rote learning or meaningful learning. Another alternative to that was developed by Liu *et al*., (2005), who used algorithms to perform link analysis in order to identify misconceptions shown by students.

The work reported here aimed at adapting categorical scoring system to assess students' concept maps. It was noticed that one of the challenges associated with such an approach was the identification of concept map categories. Our approach began with the process safety categories that we defined in (Ali *et al*., 2018). The same approach was used for the assessment presented in this paper.

Our work in Context

It is difficult to evaluate what students perceive in a broad subject field like process safety. Furthermore, since human minds are highly unique, especially in terms of interpretation, different students would have different concept maps despite answering the same focus question and level of expertise (Calafate *et al*., 2009). Due to such uniqueness, our previous study was dedicated to validating concept map categories in a more elaborate and precise process ensuring that all possible concepts constructed by students were included.

We realised that in categorical scoring method, there will be some level of subjectivity in allocating each concept to their relevant categories. To decrease the level of the subjectivity, the

process was initiated with the idea of having three independent assessors to analyse each concept map and then evaluate the extent to which the assessors agree or disagree with one another. The assessors were (1) a chemical engineering professor who has expertise in process safety and the industry; (2) a PhD student who has degrees in chemical engineering and process safety; and (3) a non-engineering scientist, who has extensive experience in using concept maps.

In our previous study, we explained the process of developing the categories' taxonomy for process safety domain. Briefly, the validation study involved two phases. The first phase started with the establishment of ten categories' taxonomy. This was followed by the assessors assessing 51 concept maps using the proposed categories. It is in phase one that all assessors' responses were evaluated to identify all agreement and disagreement. Following that, discussions were carried out between all assessors to revise the proposed categories' taxonomy. In phase two, another assessment was conducted to validate the outcomes obtained from the first phase. However, in the second phase, assessors used the revised categories' taxonomy on another 52 concept maps, followed by analysis and discussions of assessors' responses.

By having all three assessors analysing each concept maps independently in two elaborate phases, we were able to locate several categories and concepts that were prone to individual subjectivity that leads to different responses and complete disagreement between assessors. As a result, we were able to develop not only a novel validation method for defining categories' taxonomy, but also for validating categories for process safety domain (Table 1).

Table 1: Categories' taxonomy for process safety domain

Category		**Example of concepts**
0	Irrelevant/ Unrelated	chronology, non-often, form
1	Potential Hazards	extreme temperature, human error, unguarded equipment
2	Preventative – physical	alarm, barrier, personal protective equipment
3	Preventative – non-physical, procedural	standard operating procedure, maintenance, design
4	Consequences and Outcomes	fire, blemished reputation, profit, safe operation
5	Incident response	medical treatment, emergency shut down, containment/dikes
6	Education and Training	worksite demonstrations, evacuation drill, awareness training
7	Actors and Objects	society, management, equipment
8	Ideal and Values	ethics, commitment, safety culture
9	Others	location

These categories cover the entire range of concepts relating to process safety that might be encountered in maps developed by students. The eight important categories are listed from 1 to 8. Category 0 was designed to capture concepts that are unclear or largely unrelated to process

safety, while category 9 was used to capture concepts that are relevant and significant but do not really fit into any of the other categories.

Concepts that display a situation or a source with potential for harm and adverse effects to people, property or environment will be classified in the 'Potential Hazards' category. The 'Physical Preventative' category is designed for concepts that include physical equipment that protects people or process from hazards to avoid any potential incidents. If the concepts involve policies, procedures, practices or actions to protect people, property or environment, then it should be classified into the 'Non-physical and Procedural Preventative' category. The category of 'Consequences and Outcomes' is not only for concepts relating to the effects of an unplanned event but also for concepts that show results of action or materials occurring earlier. The 'Incident Responses' category comprises concepts that demonstrate any action and/or involve the usage of equipment or procedure as a response after an imminent event to mitigate the impact. The 'Education and Training' category is for concepts that illustrate process to equip or maintain personnel with knowledge and skills, awareness, understanding and know-how required to work safely, identify hazards, report, respond, and mitigate the impact of incidents. While concepts that involve people, institutions, stakeholders as well as general description of equipment, machineries, materials belong to the category titled 'Actors and Objects'. Finally, the 'Ideal and Values' category is established for concepts related to the principle or standards of behaviour or attributes that are important to process safety.

Second year undergraduate chemical engineering students from the University of Melbourne were given up to 30 minutes to prepare and complete a concept map based around the process safety. Prior to the activity, the students were trained and instructed on how to construct concept maps. In the activity, the students were given the domain of 'process safety' in the middle of a standard A4 page without any concepts or linking phrases.

Study Results

The 103 concept maps that were analysed contained an average of 22.1 concepts other than the central domain of 'Process Safety'. Two students had maps with ten and fewer concepts and one student constructed a map with 50 concepts. Figure 1, 2 and 3 are examples of typical concept maps drawn by second year chemical engineering students. Students X, Y and Z have included adequate linking phrases in their concept maps, ensuring that the assessment process of categorising each concept into its relevant categories, by all three assessors was done consistenly.

Figure 1 shows a map of Student X that has only 10 concepts other than the central domain in which emphasise heavily on consequences and outcomes as well as ideal and values, but very minimal on education and potential hazards. It is also observed that student X has not acquired concepts relating to physical and non-physical preventative measures, incident response, and actors and objects in his map based on what he had learned in the class. Although Student X has 50% less concepts than the average cohort, his map features more sophisticated concepts.

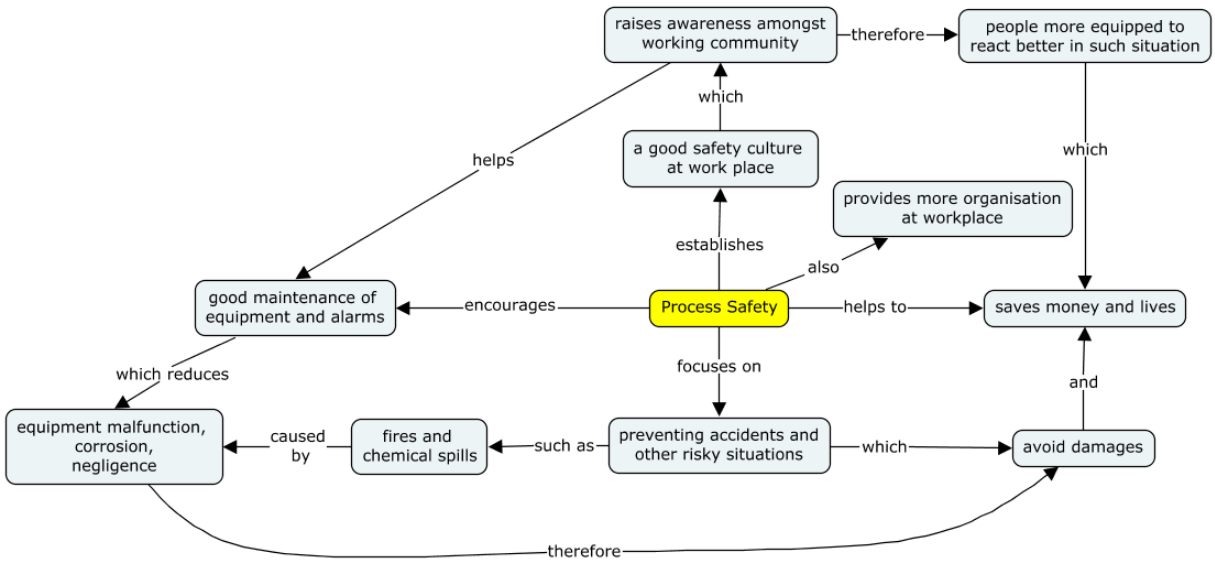


Figure 1: Concept maps of 10 concepts and 15 propositions by Student X.

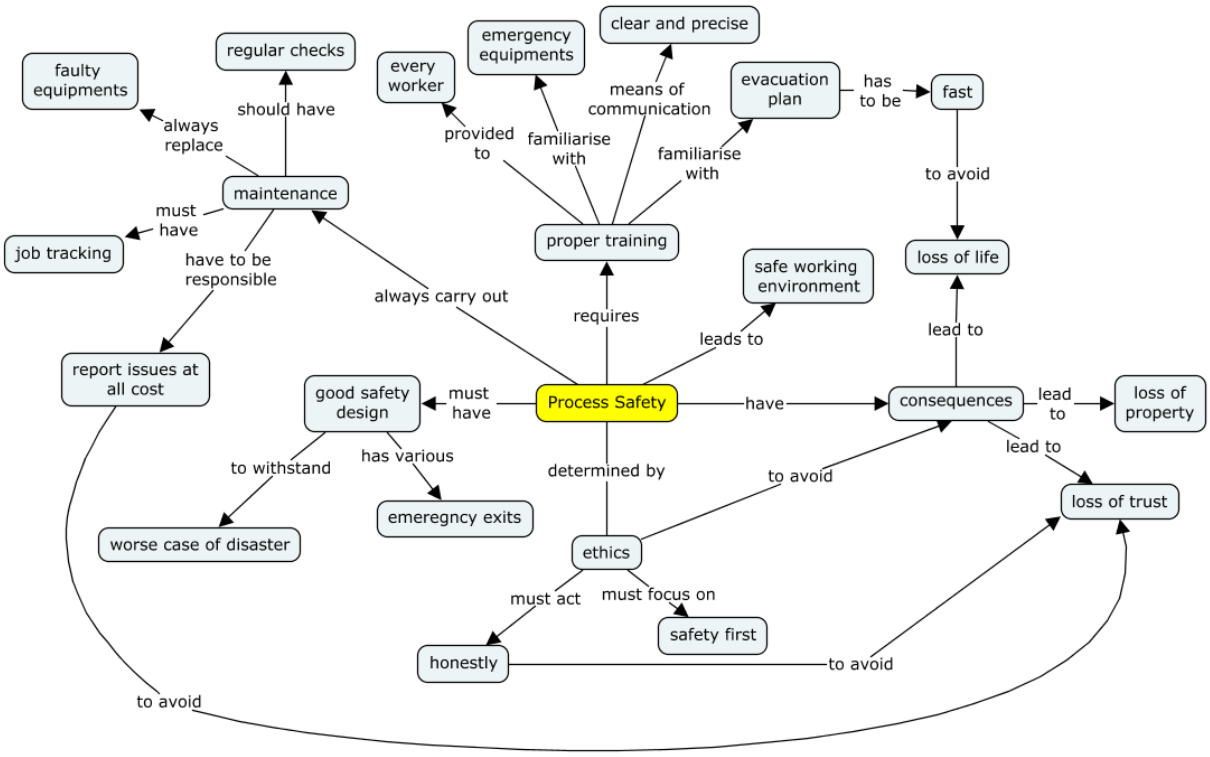


Figure 2: Concept maps of 22 concepts and 26 propositions by Student Y.

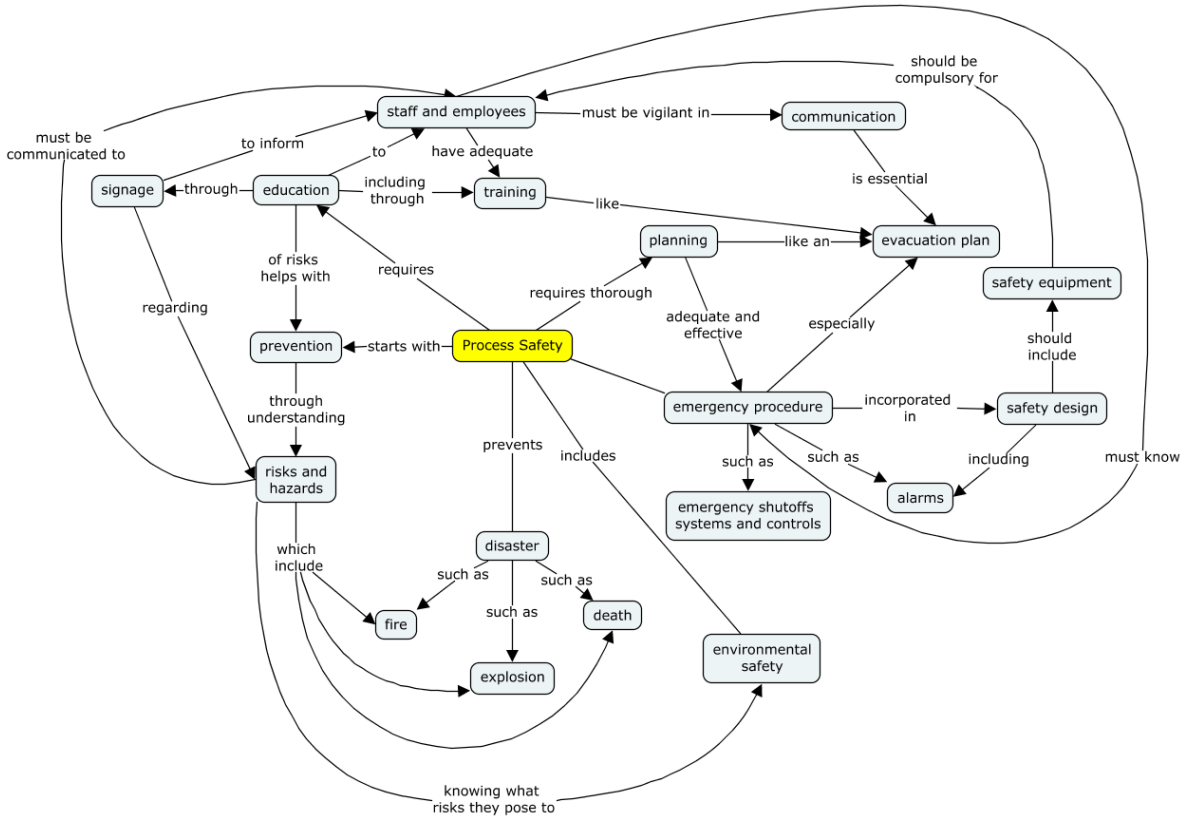


Figure 3: Concept maps of 19 concepts and 35 propositions by Student Z.

By contrast, the concept map produced by Student Y and Student Z contain more components in terms of concepts, propositions and cross-links between different segments of their maps. Student Y illustrates his understanding by constructing 22 concepts that cover all eight critical categories except the importance of physical preventative measure. Although Student Z has fewer concepts than Student Y, his map recognises all eight important categories of process safety in the map.

In terms of comprehensiveness, despite missing the element of physical preventative measure, Student Y has shown a great appreciation on the non-physical preventative category. Student Y's map has emphasised deeply on practices or actions that should be taken by personnel to protect people and process from workplace hazards. This can be noted from the the use of the following concepts; 'maintenance', 'good safety design', 'job tracking', 'report issues at all cost', 'regular checks' and 'clear and precise'. Student Y has also considered deeply the consequences and outcomes category, as the student showed different types of incidents that might happen in chemical industries.

For the purpose and limited scope of this paper, we were unable to provide a detailed analysis of all the concept maps considered. We did note that, in the case of the concept map with more that 50 concepts, more than 70% of the concepts were related only to categories 1 to 4. The map also contains significant numbers of concepts that were completely irrelevant to the domain.

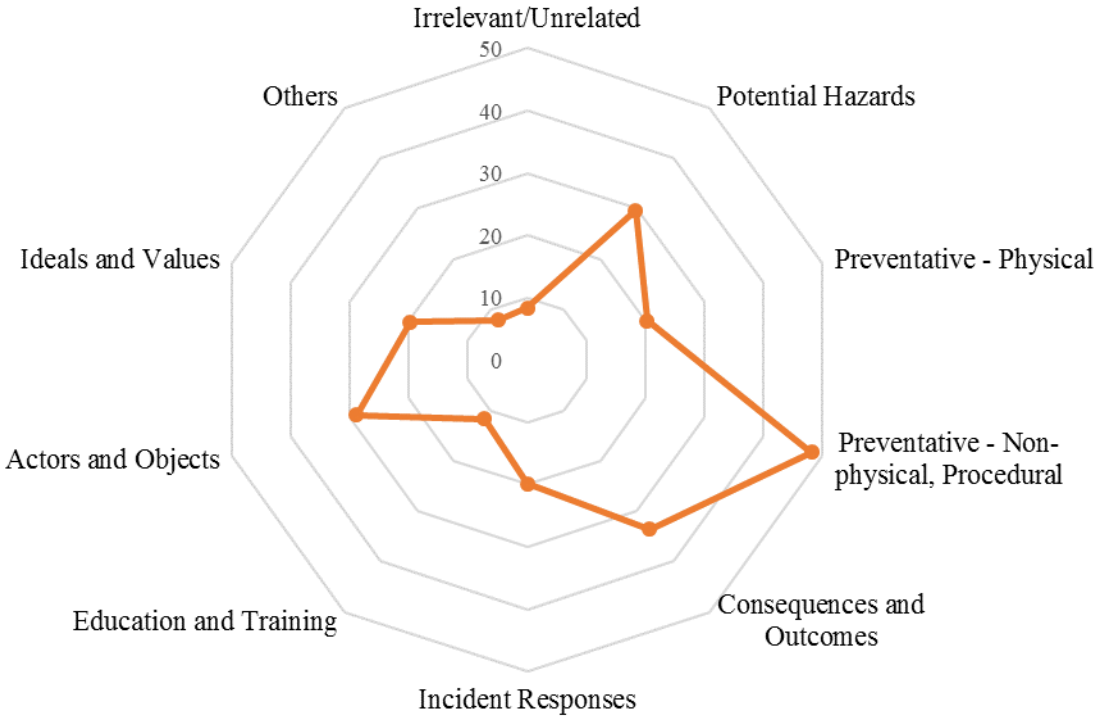


Figure 4: Distribution of number of concepts in each of ten categories for the 103 concept maps generated by the students.

All 103 students' concept maps that were independently analysed by all three assessors are presented in Figure 4, which shows the distribution of the number of concepts across ten categories. This figure indicates that the cohort had grasped well on the elements of non-physical preventative measure, consequences and outcomes, potential hazards as well as actors and objects. While the elements of physical preventative and incident responses categories were covered just adequately. If both irrelevant/unrelated and other categories were omitted, it is found that the education and training category have the lowest number of concepts in students' concept maps, of which only 5% of student's concept were classified in Category 6. Another noteworthy observation is the fact that the second last category that have limited number of concepts, was the category ideals and values. The category was considered critical and should be mastered by chemical engineering students. We hypothesised that those less well covered concepts might be overlooked as subtopics by the students when attending lectures.

The remaining part of our study was directed at investigating the correlation between each category to underpin student learning on process safety. This part of analysis will possibly lay down the basis of whether students joint the concepts randomly or whether they had given a thought to any important relationship within and between categories. Once again, we decided not to report correlation between categories that involves Category 0 and 9 as we see the concepts under those categories were irrelevant and less crucial to the study analysis.

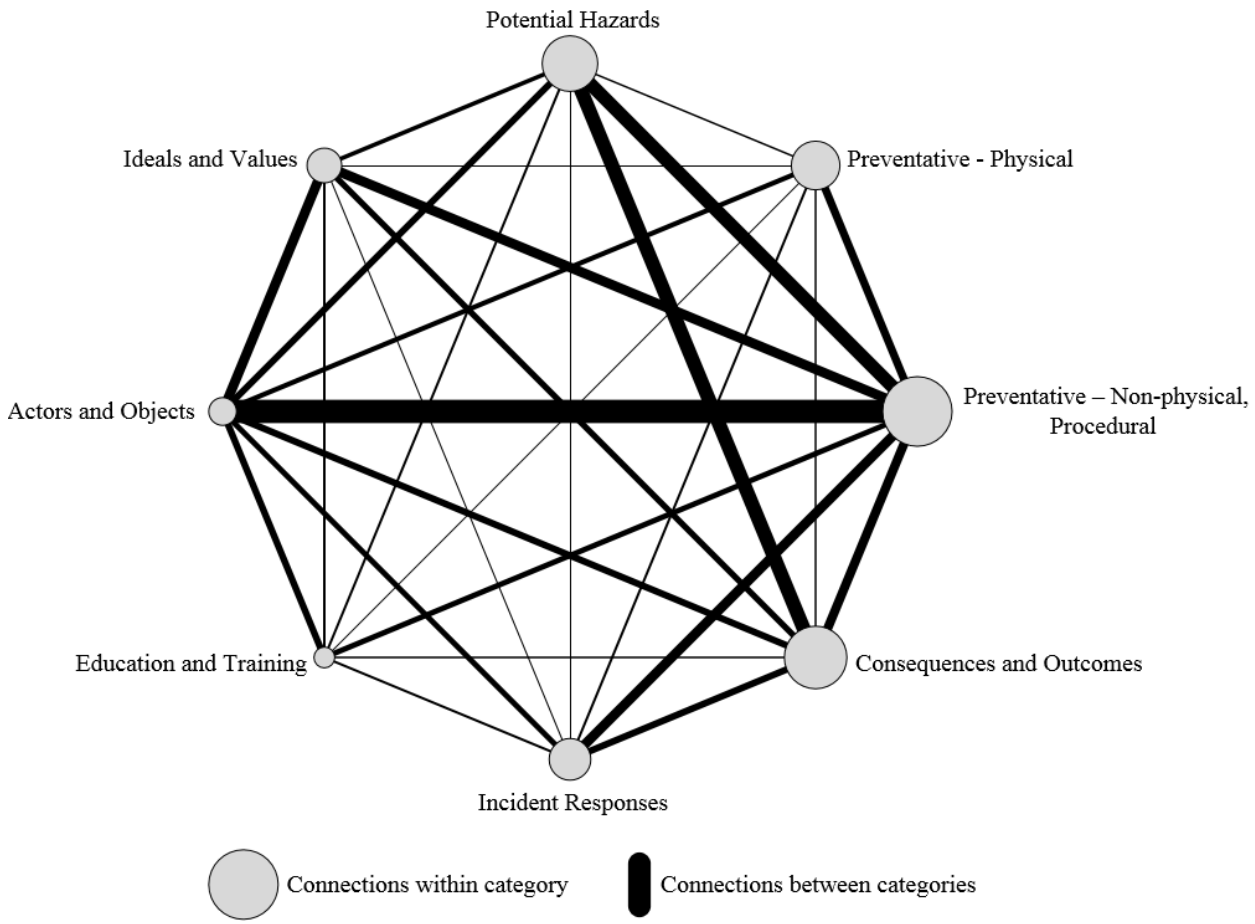


Figure 5: Octagon network diagram displaying the connections within and between the eight important categories.

The network diagram was produced at part of this study (Figure 5). It shows connections within and between categories made by study cohort. The thickness of the lines and the size of the circles indicate number of connections found on student's concept maps. It is clearly observed that most students are able to make many connections within categories of non-physical preventative measure, followed by connections within categories on consequences and outcomes element. This was expected as Figure 4 showed that students have large number of concepts on each of those categories.

It was hypothesised that if concepts were randomly joined, connection line between category preventative-non-physical and category consequences and outcomes was expected to be the thickest. In comparison with the actual cohort performances, the trend shows a different outcome, in which the more connection were found to be between non-physical, procedural preventative category and actors and objects category. Students were also able to show natural correlation between potential hazards and its consequences and between potential hazards and non-physical preventative category. Therefore, these findings suggest two conditions, Firstly, the students understand very well the relationship between every category and the lines were not connected randomly. Secondly, it may be occurred because of the position or place between the

two concepts. For example, in Figure 3 the concept ‘signage’ is located at the top left of the figure, which was far from the concept ‘safety design’, which was located in the middle right, hence students were not able to see the interaction between those two.

Conclusion

In this study, we used concept maps to assess individual student and cohort learning around process safety domain. The result indicates that across all 103 students, students generally have great understanding on the non-physical preventative measure in the process industries and as well as the consequences and potential outcomes. The overall outcome also suggests that many students are missing the importance of having education and training element in maintaining safety as well as the critical element of ideals and values.

The results of this analysis show that concept maps are valuable tools in assessing process safety learning on individual student as well as cohort in class. We also believe that knowing exactly what the students have learnt in class, is important in further evaluating the appropriateness of teaching and learning objectives. Hence, this study would be beneficial not only to guide instructors in teaching process safety, but also on deciding some curriculum improvement pertaining to process safety.

References

Acton, W. H., Johnson, P. J., and Goldsmith, T. E. (1994). Structural knowledge assessment: Comparison of referent structures. *Journal of Educational Psychology*, **86(2)**, 303 – 311.

Ali, N. F., Prpic, J. K. and Shallcross, D. C. (2018). A new validation method for defining concept map categories. *Proceedings of the Eight International Conference on Concept Mapping*, Medellin, Colombia, 2018.

Ausubel, D. P. (1968). Facilitating meaningful verbal learning in the classroom. *The Arithmetic Teacher*, **15(2)**, 126-132.

Besterfield-Sacre, M., Gerchak, J., Lyons, M. R., Shuman, L. J., and Wolfe, H. (2004). Scoring concept maps: An integrated rubric for assessing engineering education. *Journal of Engineering Education*, **93(2)**, 105-115.

Calafate, C. T., Cano, J. C., and Manzoni, P., (2009). A comprehensive methodology for concept map assessment. *Advanced Learning Technologies. Ninth IEEE International Conference*. 15-17.

Cortes, J. M., Pellicer A, E., and Catalá, A. J. (2012). Integration of occupational risk prevention courses in engineering degrees: Delphi study. *Journal of Professional Issues in Engineering Education and Practice*. **138(1)**, 31-36.

Daley, B. J., and Torre, D. M. (2010). Concept maps in medical education: an analytical literature review. *Medical Education*, **44(5)**, 440-448.

Ju, T. P., (1989). The development of a microcomputer-assisted measurement tool to display a person's knowledge structure," Dissertation, University of Pittsburgh.

Kinchin, I. M., Hay, D. B., and Adams, A. (2000). How a qualitative approach to concept map analysis can be used to aid learning by illustrating patterns of conceptual development. *Educational Research*, **42(1)**, 43-57.

Liu, C. C., Don, P. H., and Tsai, C. M. (2005). Assessment based on linkage patterns in concept maps. *Journal of Information Science and Engineering*, **21(5)**, 873-890.

Mathes, P. G., Torgesen, J. K., and Allor, J. H. (2001). The effects of peer-assisted literacy strategies for first-grade readers with and without additional computer-assisted instruction in phonological awareness. *American Educational Research Journal*, **38**, 371–410.

National Research Council. (2000). How people learn: Brain, mind, experience, and school: Expanded edition. *National Academy Press*. Washington D.C.

Novak J. D. and Gowin D.B. (1984). Learning how to learn. *Cambridge University Press.* New York.

Segalàs, J., Ferrer-Balas, D., and Mulder, K. F. (2008). Conceptual maps: measuring learning processes of engineering students concerning sustainable development. *European Journal of Engineering Education*, **33(3)**, 297–306.

Shallcross, D. C. (2013). Using concept maps to assess learning of safety case studies–The Piper Alpha disaster. *Education for Chemical Engineers*, **8(1)**, e1-e11.

Strautmane, M. (2012). Concept map-based knowledge assessment tasks and their scoring criteria: an overview. *Concept Maps: Theory, Methodology, Technology: Proceedings of the Fifth International Conference on Concept Mapping*, Valletta, Malta, 80-89.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

On Telling the Whole Story: Operator Task Performances and Physiological Costs during Complex and Critical Offshore Drilling

Ranjana K. Mehta, S. Camille Peres, Ashley Shortz, Wimberley Hoyle
Dept. of Environmental and Occupational Health
Texas A&M University
College Station, Texas, 77843-3131
Emails: rmehta@tamu.edu, peres@sph.tamhsc.edu, aeshortz@sph.tamhsc.edu, whoyle@sph.tamhsc.edu

Abstract

In offshore drilling operations, shiftwork has been implicated as a major risk factor of adverse performance and safety outcomes. In addition, offshore drillers continually perform intense vigilance and monitoring tasks during their 12-hour shifts, ensuring that the drill plan is properly followed to avoid any well control incidents. The aim of this study was to 1) develop offshore drilling simulations that presented complex (monitoring load) and critical (occurrences of kicks and loss of circulation) drilling scenarios in a high-fidelity NOV drilling simulator, and 2) to examine how drillers respond, covertly and overtly, to these events during a typical day and a night shift. Eleven male drillers, who had a minimum of 2 years drilling experience, underwent a 12-hour shift during a day (7am-7pm) and night shift (7pm-7am) and their performance (accuracy and time) during the different scenarios and physiological responses (heart rate and heart rate variability) were recorded. While accuracy on the scenarios did not differ between shifts, time taken to complete the tasks were observed to be longer during the night than during the day shift. The performances remained comparable between the different critical conditions i.e., the scenarios that presented kicks or loss of circulation events). Interestingly, the critical scenarios were associated with increased physiological burden on the drillers, particularly during the night shift, irrespective of the monitoring demand placed on the drillers (i.e., level of complexity). These results indicate that collecting task performance information alone does not provide a complete understanding of operator behavior during events that are of high-risk and high-consequence. To identify critical scenarios and to develop effective error-mitigation strategies in offshore operations, it is critical to understand the physiological "cost" of maintaining task performance.

Keywords: Shiftwork, Fatigue, Hazards, Risk Assessment, Human Factors

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Biocompatible Herders for Offshore Oil Spill Mitigation

Dali Huang, Lecheng (Eric) Zhang, Roshan Sebastian, Dr. M. Sam Mannan, Dr. Zhengdong Cheng
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University System
College Station, Texas 77843-3122, USA
Emails: zcheng@mail.che.tamu.edu, dhuang@tamu.edu

Abstract

Crude oil spilled offshore is a major threat to ecological cycle and human activities. When oil starts to spill on the water, it is very challenging to make quick response, especially in remote offshore areas and under severe low temperatures. The amphiphilic oil-collecting agent, also termed as herder, is designed to spray in oil spill areas and is able to retract oil slick from a thin layer to a thick mass. The oil aggregation will be then easier to harvest or for in-situ burning.

There are brands of industry herders in the market, however, two major concerns restricted their applications to some extent. One is that herders better be nontoxic and biocompatible to the ocean. The other, herders should perform well even near 0 Celsius degree to adjust various marine environment including the Arctic Ocean, which has now aroused great interest for the energy sector.

Herein, we develop a konjac-based biocompatible herder for offshore oil spill mitigation. Compared to existing industry products, our konjac oil herder is ecofriendly to the sea and could have high herding effect under ultralow temperature maritime space like the Arctic Ocean.

Keywords: Crude Oil Spill, Herders, Oil-collecting agents, Accidental Offshore, Low Temperature

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Measuring Expertise Acquisition with Virtual Industrial Tasks – Implications for Procedure Design and Use

Timothy J. Neville [1,2,*], S. Camille Peres[1,2], Joseph W. Hendricks[1], Cara A. Armstrong[1], M. Sam Mannan[2]
[1] *Department of Environmental and Occupational Health, Texas A&M University*
[2] *Mary Kay O'Connor Process Safety Center, Texas A&M University*
[*]Presenter Email: timothy.neville@tamu.edu

Abstract

Expertise plays an important role in how workers use procedures and conduct tasks in high risk industries. In particular, as workers gain expertise and conduct tasks more frequently, their use and adherence to written procedures changes. The RIHM Lab (Research on the Interaction between Humans and Machines) conducted an exploratory study in a virtual manufacturing warehouse developed in the SecondLife® environment to examine how a novice develops expertise over time, how their use of procedures changes as a function of their expertise development, and how their mental model of the task/procedure system develops over the same period. Ten undergraduate students completed 8 separate sessions in the warehouse over the course of two weeks. The number of products produced as well as a participant's behavior as a function of task frequency, procedure use and procedure adherence were measured within each session. Results indicated that participants demonstrated improvement in their productivity over the course of 8 sessions up to asymptote. Furthermore, participants developed their own pattern and routines of conducting the tasks and following procedures. The results suggest that expertise acquisition can be demonstrated within a virtual, lab environment, making it a viable setting in which to study procedure use as expertise develops. Indeed, as expertise develops the reliance on procedural tools to complete a task decreases, especially for frequent tasks. The decrease, however, also results in a reduced adherence to specific steps in the procedure. The findings from the study have implications on procedure design and use for workers as they acquire expertise in the field.

Keywords: Procedures, expertise, experience, training

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

A Practical Approach to Human Error

Kyle Wingate
Risktec Solutions Inc.
Email: Kyle.Wingate@Risktec.tuv.com

Abstract

Human error is something every organization has to deal with, but the potential consequences in a high-risk process safety industry requires even more awareness and strategy for dealing with it. Since no one is perfect, human error is inevitable; however, the key is to understand what mistakes may occur (and their potential impact) as well as when they are most likely to materialize.

This presentation will focus on the various tools and techniques to predict, assess, measure, and mitigate the negative consequences of human error that may lead to high-impact process safety incidents. At the core of this lies a field of science called Human Factors, in which the human and their work environment must be fully understood and integrated into the wider safety and operational systems across the organization. Human factors engineering (HFE), competency management, fatigue, and many other human element barriers and controls will be discussed along with how a comprehensive approach can lead to a robust safety culture.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Representing 'Work-As-Done (WAD)' of Communication and Information Flow in an Incident Management Team

Changwon Son[1], Jukrin Moon[1], Farzan Sasangohar[1,2], S. Camille Peres[1,2], Timothy Neville[2]
1 Industrial and Systems Engineering Department, TAMU, College Station, TX
2 Environmental and Occupational Health Department, TAMU, College Station, TX
Emails: coralx@tamu.edu, peres@tamu.edu

Abstract

Resilience is considered an essential capability of an incident management team (IMT) to cope with increasing complexity of disasters and catastrophes, as it represents the IMT's ability to adapt its performance to emerging challenges as the incident evolves. Among many aspects of the performance of the IMT, communication and information management are crucial components that facilitate incident action planning and operational activities. To investigate such components and to understand the patterns of resilient performance that manifests itself in operation, a naturalistic observational study was conducted in a high-fidelity emergency management training environment. The study aimed at identifying the communication and information flow following injects of scenario information into the training environment. An episode analysis was conducted to traces communication, information flow and resilient performance following the inject of scenario-based information. The analysis also facilitated the identification of complex and dynamic interactions among human and technological agents to satisfy work demands, representing work-as-done (WAD) vs. work-as-planned (WAP) in large-scale emergency response operations. Overall, this analysis method has shown promise and is expected to provide a measure of resilience in other safety-critical, complex team environments.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Quantitative Risk Calculations for a U.S. DOT Natural Gas Pipeline Using Population Classifications

John B. Cornwell, Benjamin R. Ishii
Quest Consultants Inc. ®
Emails: jbc@questconsult.com, bri@questconsult.com

Keywords: QRA, natural gas pipeline, risk analysis

Abstract

Over the past several years, Quest Consultants Inc. has conducted quantitative risk analysis (QRA) and risk assessment studies for a range of pipelines in the United States and abroad. In most instances, the risk acceptance or tolerability criteria are defined by the individual risk (IR) to a person; often this risk is presented as location specific individual risk (LSIR). The LSIR is a measure of the risk to a person who is continuously at a specific location.

In recent years, there has been increasing dependence on the use of societal risk acceptance or tolerability criteria, including the risk associated with pipelines. Pipelines are often described as linear sources of risk, like highways and rail lines. The risk analysis methodology used to calculate the risk associated with fixed facilities (e.g., refineries and chemical plants) cannot be directly applied to linear risk sources.

This paper presents a risk calculation methodology that can be applied to linear risk sources, like natural gas pipelines, and compares the societal risk indices for U.S. DOT pipeline classes.

INTRODUCTION

Natural gas pipelines that service public populations fall into three main groups: transmission, distribution, and home service. In general, these three pipelines are defined by the pressure of the natural gas transported in the pipeline. From the guidance provided by the United State Department of Transportation (USDOT) the pressures in these three pipeline classes can be defined as follows.

- Transmission pipelines operate at pressures above 500 psig (pounds per square inch gauge)
- Distribution pipelines operate between 200 psig and 10 psig
- Home service lines operate at pressures below 10 psig

There is a current interest in describing the risk associated with the transport of natural gas by pipeline as part of the evaluation of its potential impacts. The natural gas that is to be transported in the pipelines does not have significant amounts of toxic components. Thus, the primary hazards that have the potential to extend more than a few feet from these pipelines are:

- Jet fire radiant hazard
- Flash fire radiant hazard
- Vapor cloud explosion overpressure hazard

For natural gas pipelines, the flash fire hazard zone is often smaller than the jet fire hazard zone. In addition, the potential to develop significant overpressure (high enough to injure or kill members of the public) requires a degree of congestion and/or confinement that might not exist along portions of the pipeline route or even an entire pipeline. Thus, the jet fire is the dominant hazard along the pipeline route. Any release of natural gas from a pipeline, once ignited, will form a momentum-based jet fire. The radiant impact from the jet fire will dominate the risk along the pipeline route.

The USDOT collects data on natural gas pipeline failures that result in one or more fatalities (public and worker combined). The data collected by the USDOT produce backward-looking statistics and do not provide an accurate view of what could happen in the future since *where* a release occurs along a pipeline route can have a significant impact on the number of fatalities and injuries. Quantitative Risk Analysis (QRA) studies are forward-looking studies that are designed to show potential future impacts. Since the designer of the QRA cannot determine exactly where a release might occur along a pipeline route, the designer of the QRA must use a pipeline failure rate (number of pipeline failures per year per length [e.g., mile]) in a predictive mode. In this manner, a release along the pipeline route may be thought of as the same anywhere along the route. The failure rate can be modified by the inclusion of ancillary pipeline equipment such as regulator stations, etc.

POPULATION

The most difficult and site-specific aspect of calculating the risk associated with natural gas pipelines has to do with the population distribution along the pipeline route. Unlike fixed facilities such as a refinery where the population around the facility fence line is assumed to be constant and has to be evaluated and used as an input to the overall risk analysis, the population along a pipeline route can vary along the route. Thus, while the potential for a release and the sizes of the hazard zones might not change significantly along the pipeline route, the risk to the public might vary due to the variation in population (density and/or distance from the pipeline).

The USDOT uses the density of buildings in order to define the pipeline class location[1]. The USDOT class location is dependent on the density of buildings along a one-mile segment of the pipeline out to 220 yards perpendicular the pipeline. This area is equivalent to one-quarter of a square mile (1.0 mile * 440 yards [1/4 of a square mile]). The USDOT provides the following definitions for the pipeline classes.

USDOT Class	Definition
Class 1	Fewer than 10 buildings in the one-quarter square mile area.
Class 2	From 10 to 46 buildings in the one-quarter square mile area.
Class 3	More than 46 buildings in the one-quarter square mile area or if the pipeline lies with 100 yards (90 meters) of a building or area that is occupied by 20 or more persons at least 5 days a week for 10 weeks in any 12-month period. (e.g., playground, golf course, etc.)
Class 4	Any Class (1, 2, or 3) where buildings with four or more stories are prevalent.

Natural Gas Transmission Pipeline Failure Data

The USDOT onshore natural gas transmission pipeline data by class from 2010 to 2016 is listed in Table 1. As would be expected, Class 1 which occurs primarily in rural areas, dominates the total mileage. However, as both Table 1 and Figure 1 show, the failure rate for the natural gas transmission pipeline is fairly constant for the different USDOT pipeline class definitions. When viewing Table 1 and Figure 1, it should be noted that the total amount of onshore Class 4 natural gas transmission pipelines in service is less than 0.4 % of the total mileage.

Table 1. Accidental Release Rate for Onshore Natural Gas Pipelines by Class

Transmission Mileage by Class	Failures	Onshore [miles]	Accidental Release Rate [per mile per year]
Class 1	228	1,633,139	1.396E-04
Class 2	21	212,017	9.905E-05
Class 3	40	235,646	1.697E-04
Class4	1	7,432	1.346E-04
Total	290	2,088,234	1.389E-04

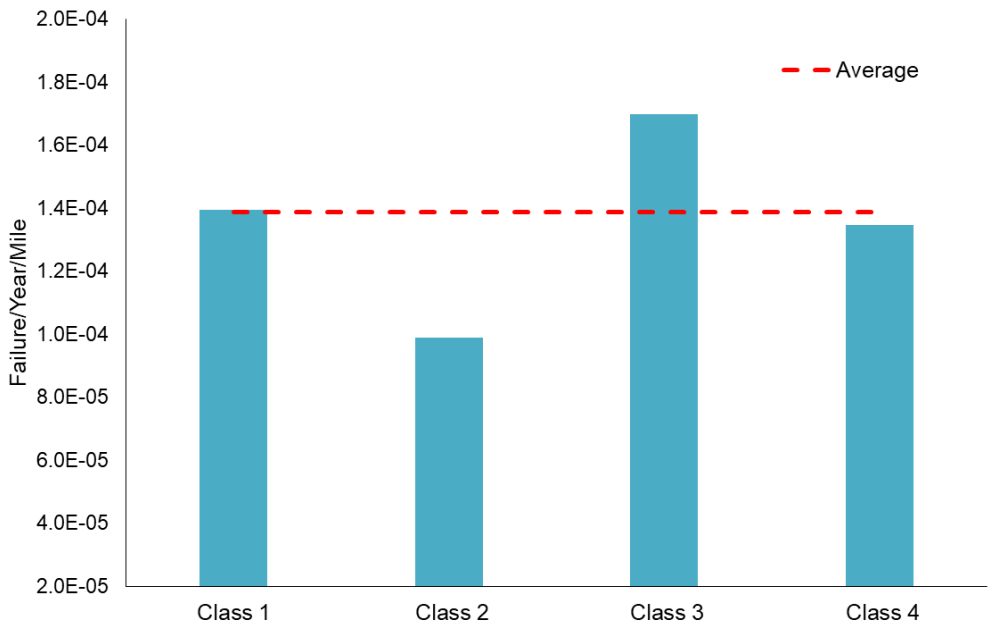


Figure 1. Natural Gas Transmission Pipeline Failure Rates by Class Definition

Using the USDOT natural gas transmission data for the 2010 to 2016 time period results in an average (over all Class types) natural gas release frequency of 1.39 $(10)^{-4}$ releases of natural gas transmission pipeline per mile per year.

Risk Acceptability Criteria

There are several measures of risk and the project proponent and the regulator must make decisions about the acceptability of risk in order to determine the acceptability of a pipeline project or pipeline route. There are different risk acceptability criteria for individual (a single person) and societal (multiple persons) risk measures.

The most common risk calculation made is for what is often called individual risk (IR). In all of the risk criteria to be discussed, it is the risk of fatality, not risk of exposure or risk of injury, which is defined. The risk of fatality is universal, while the definition of injury is not.

While the IR calculation may be made correctly, it is often interpreted incorrectly. Most IR calculations are actually the predicted risk to a location and not to a person. In order for the risk to a person to be equal to the risk at a location, the following would have to be true.

- The hazard endpoints (i.e., limits) would have to be defined for people not property.
- The person would have to stay at the specific location 24 hours a day and 365 days a year, in other words continuously for a full year.

Since most people do not stay in the same location continuously for a full year, the IR calculated is really the location specific individual risk (LSIR). The IR value for a person is never greater than the LSIR, and often can be quite a bit lower.

The LSIR for a pipeline is often presented in what is referred to as a risk transect. A risk transect presents the LSIR as it extends perpendicularly away from a pipeline. An example of an LSIR transect is presented in Figure 2.

A second risk measure is one that calculates the risk of <u>one or more</u> persons being killed due to an individual event. This is called societal risk since it measures the impact on more than one exposed person. Societal risk may be presented in the form of an F-N curve, where the y-axis is defined as F, where F is the cumulative frequency of N or more fatalities. The x-axis is N. An example of F-N curves (solid lines) is presented in Figure 3.

A project whose F-N curve lies above or extends into the area above the red line (for example, the dashed blue line in Figure 3) is deemed as unacceptable. This project will be rejected on the grounds that the risk to the public is too high, thus unacceptable.

A project whose F-N curve lies entirely below the below the green line (for example, the dashed orange line in Figure 3) is deemed as acceptable. This project should be accepted on the grounds that the risk to the public is low, thus acceptable. A project with an F-N curve entirely in the acceptable region would not require any additional risk reduction measures.

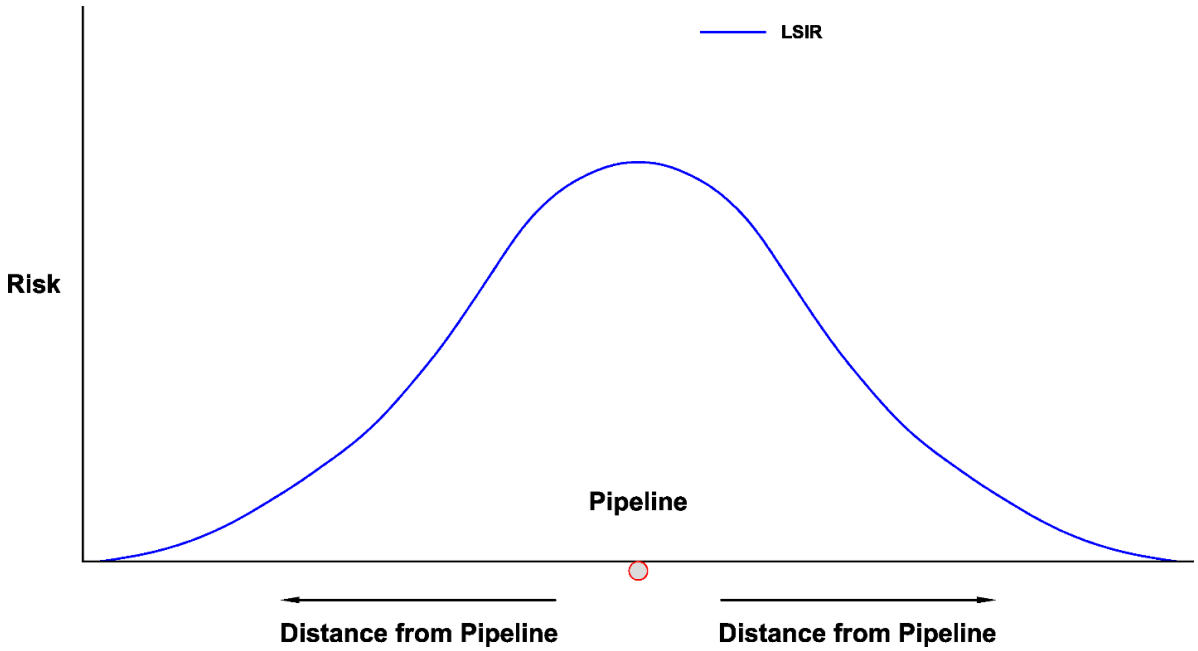


Figure 2. LSIR Transect for a Pipeline

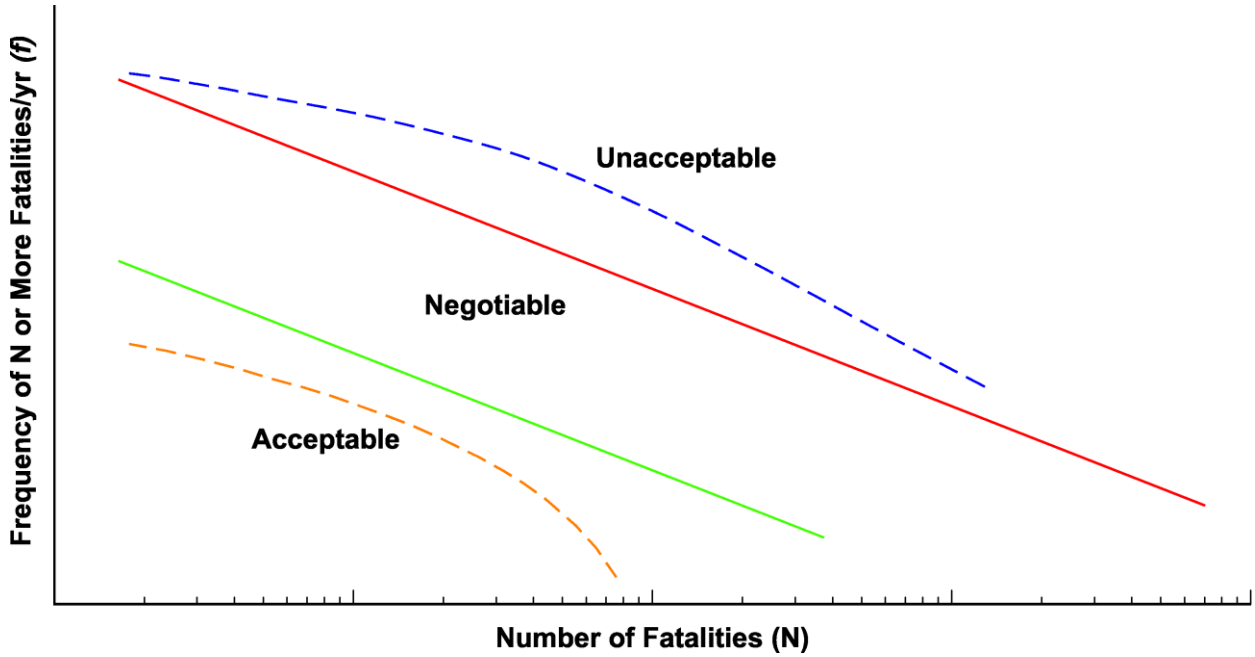


Figure 3. Form of an F-N Curve

Notice the area in Figure 3 between the two solid diagonal lines. The area between the lines is defined as negotiable. In some risk criteria, this area is called As Low As Reasonably Practicable (ALARP). The definition of reasonably practicable is described by the United Kingdom's Health and Safety Executive (HSE)[2] as

> "Reasonably practicable involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled."

In other words, an F-N curve that lies within or partially within the two solid diagonal lines would require the project to lower the F-N risk curve to below the lower (green) diagonal line if reasonably practicable. The decision of whether enough risk reduction has been made such that further risk reduction is not reasonable practicable, is up to the regulator(s), thus the use of the term "negotiable."

For fixed or point facilities, the societal risk measure (F-N curve) works well since the assumption is that the population near the facility is clearly defined and constant. For pipelines, this type of measure can cause some degree of confusion as a pipeline may pass through an area without any resident population (risk = 0), but also pass through or by a populated residential area (risk > 0).

EXAMPLE RISK CRITERIA FOR NATURAL GAS TRANSMISSION PIPELINES

Individual Risk

As an example consider an onshore natural gas transmission pipeline. This pipeline is a 24-inch diameter pipeline that operates at 1,000 psig. The pipeline is buried by traditional trenching. A hole develops in a segment of the pipeline that is approximately 2 miles downstream of a compressor. The area where the release occurs has moderate humidity and 10-year average wind pattern as described in Figure 4.

The risk transect for the example onshore natural gas transmission pipeline is presented in Figure 5. As shown in Figure 5, the risk to persons in the area near the pipeline decreases as the distance from the pipeline increases.

If the one in a million ($1.0\ (10)^{-6}$) risk level is a value that is deemed an acceptable IR level for the public then the natural gas transmission pipeline would be deemed acceptable. Different countries (e.g., Australia, Mexico, Hong Kong, Brazil) use this risk criteria for IR. It should be kept in mind that the IR is defined to be risk of a fatality. Keeping in mind that the calculated risk is location-specific, the true risk to an individual at a distance from the pipeline is less than that shown.

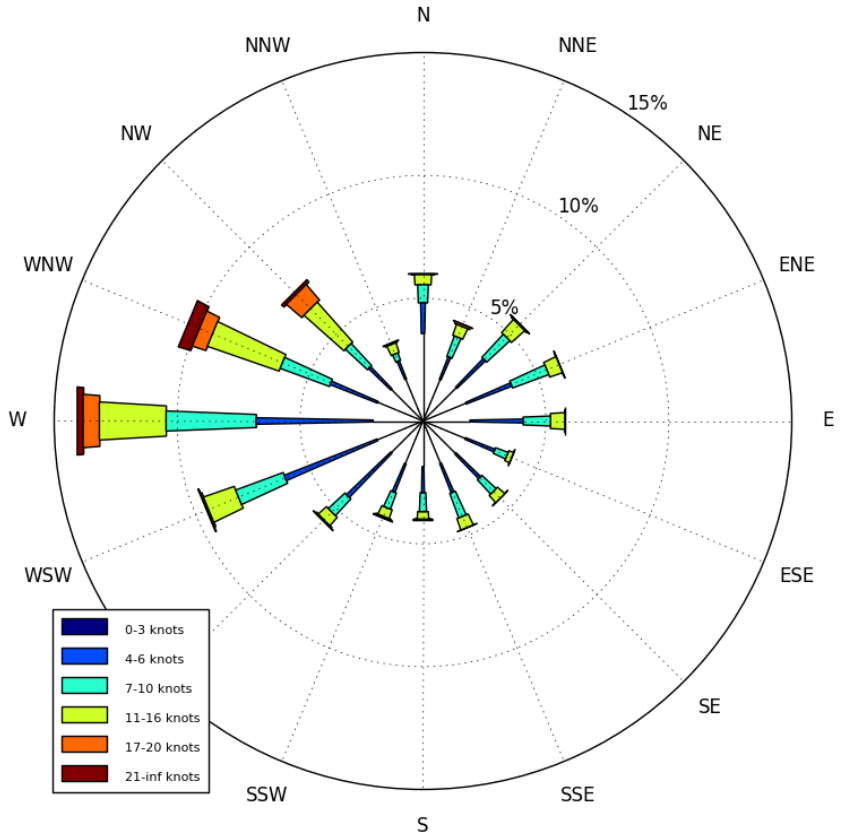


Figure 4. Wind Rose for Example Pipeline QRAs

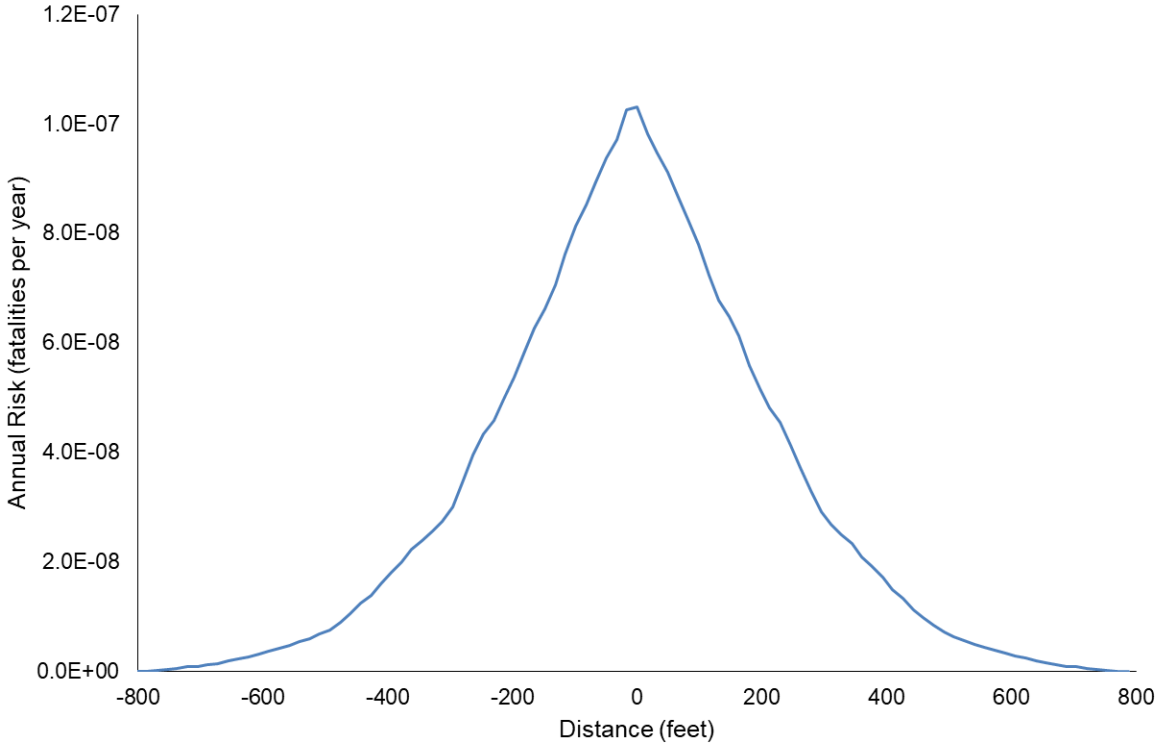


Figure 5. Risk Transect for Example Onshore Natural Gas Transmission Pipeline

Societal Risk

As described above, the population along a pipeline route may change and this causes the risk to the public along the pipeline to change as well. Using the USDOT pipeline classifications as a way to define the population provides a consistent, reproducible method to develop the risk along the pipeline. Using the maximum number of buildings in the one-quarter square mile area and the following assumptions

Each building is a residence
Each residence has 2.5 people[3]

Class 1	Maximum of nine buildings in the one-quarter square mile area.
Class 2	Maximum of 46 buildings in the one-quarter square mile area.
Class 3	More than 46 buildings in the one-quarter square mile area. Class 3 is evaluated by two population layouts for demonstration, Class 3a and Class 3b.
Class 3a	46 buildings per mile of pipeline
Class 3b	92 buildings per mile of pipeline
Class 4	Any Class 4 pipeline has to be analyzed on a site-specific basis

These population distributions are shown graphically in Figure 6. It should be noted that the buildings (i.e., houses) are located a minimum of 33 feet from the natural gas transmission pipeline. The 33 feet is designed to represent the right-of-way for the pipeline.

One method to evaluate the pipeline route allows each subject pipeline to be divided into segments (constant lengths of pipeline) and each segment evaluated and compared against established societal risk criteria. One-mile pipeline segments are selected because the USDOT pipeline classification system is based on the population along one mile of pipeline. Since the natural gas transmission pipelines that are the subject of this paper do not have any significant toxic components, a one-mile length of pipeline will not exclude the impact of any potential hazard (e.g., flash fire, jet fire, or explosion overpressure).

The societal risk F-N curve would be constructed for each one-mile section of pipe. The F-N curves for each one-mile section would be plotted against established societal risk criteria and each pipeline section's risk acceptability will be evaluated. In this example the British F-N criteria[4] are presented as the established societal risk criteria. The example natural gas transmission pipelines, by DOT Class designations, are plotted in Figure 7. As can be seen in Figure 7, as the number of buildings (and thus the number of persons) increases, the overall F-N curves move to the right (greater N). The low historical frequency of natural gas transmission pipeline failure keeps the F-N curves below the risk acceptability criteria.

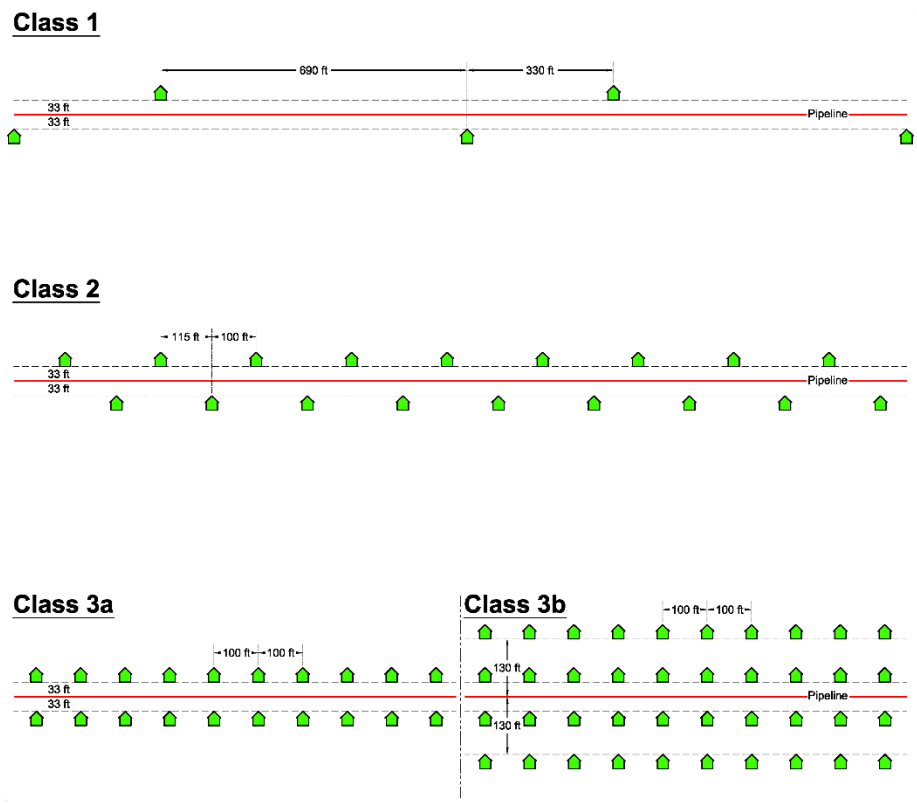


Figure 6. Example Building Distributions According to DOT Class Designations

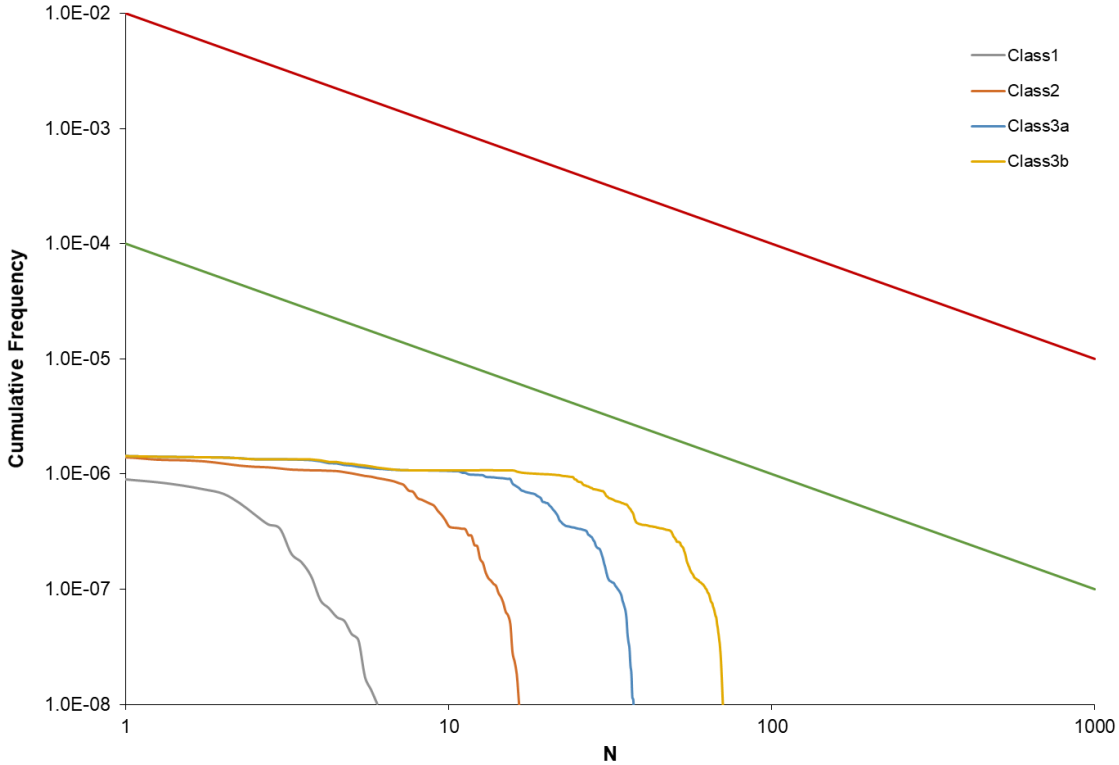


Figure 7. F-N Curves for Example Natural Gas Transmission Pipeline by DOT Class

As described above, what makes the risk calculations for a pipeline unique it the variability of the population along the route. In an effort to determine how sensitive the risk calculations (i.e., the F-N curves) are to the layout of the buildings along the pipeline route, several different Class 2 layouts were evaluated. These variations, using a constant population of 15, are identified on Figures 8 and 9 and can be summarized as follows:

- 15 persons parallel to the East-West (E-W) pipeline
- 15 persons perpendicular to the E-W pipeline
- 15 persons spread out near the right-of-way of the E-W pipeline
- 15 persons spread out far from the right-of-way of the E-W pipeline
- 15 persons parallel to the same pipeline when the pipeline is oriented North to South (this shows the impact of the wind rose relative to the pipeline orientation)

As can be seen by the F-N results presented in Figure 9, there are small differences in the calculated risk to the exposed public. When the people are located away from the pipeline (the yellow line), the risk is lower than when the people are located near the pipeline. In addition, the shape of the wind rose or the orientation of the pipeline relative to the wind rose makes little difference in the resulting F-N curve. The reason for this is that the dominate hazard from a natural gas transmission pipeline release is a torch fire and torch fires are not significantly influenced by the prevailing wind patterns.

Some analysts use a population density instead of discrete population maps. This can lead to significant errors in the risk calculations. Using a Class 2 building (population) designation as the basis, three population maps were evaluated. These three population distributions are presented in Figure 10. Each distribution has the same total number of persons (115) within the DOT Class definition area. The constant density methodology yields a population density of 115 people per mile of pipeline or 0.0000165 persons/ft^2 or one person every 60,605 ft^2.

When risk calculations are performed on the three DOT Class 2 population distributions shown in Figure 10, the F-N curves in Figure 11 result. When the population density distribution is employed, as shown in “Class 2 Density” portion of Figure 10, the people are separated by such large distances that it is mathematically impossible to kill a single person. Thus, the F-N curve for the constant density population does not reach the N=1 number of fatalities. Similar to Figure 9, varying the specific locations of the population within the Class 2 area does not make much difference in the calculated risk.

Historically, there have been failures of natural gas transmission pipelines that resulted in multiple fatalities. As shown above, the potential number of fatalities is affected by the people’s locations relative to the pipeline. Figure 12 presents the natural gas transmission pipeline fatality data collected over a 47-year period. As can be seen from Figure 12, most of the fatalities recorded over the 47-year period are either single fatalities (N=1), or small groups of fatalities.

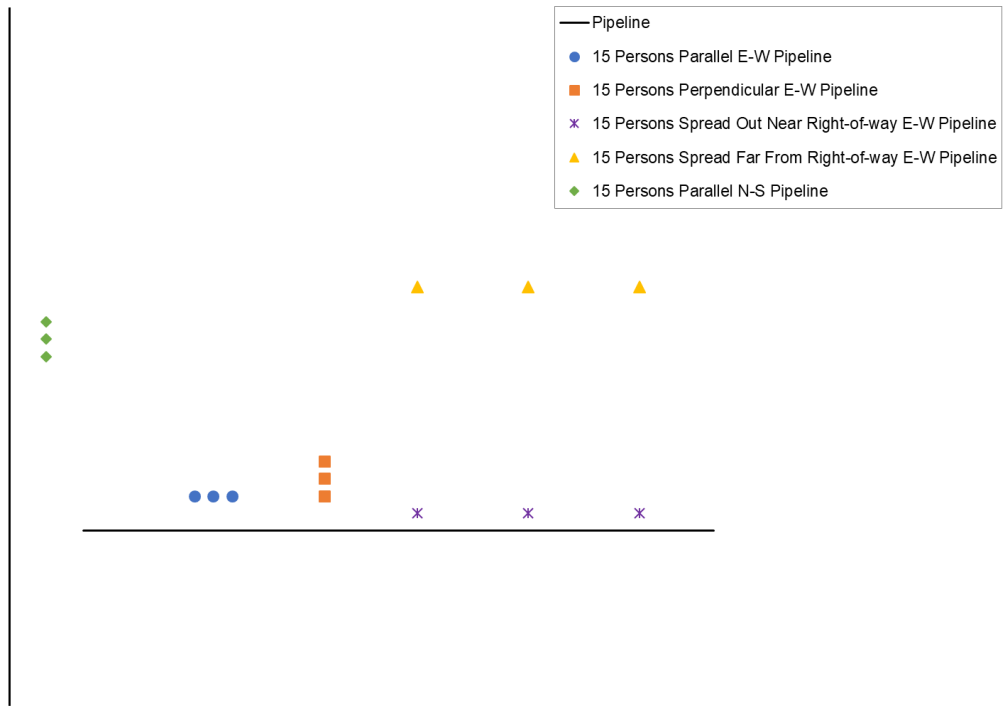


Figure 8. Population Distributions along Example Transmission Pipelines

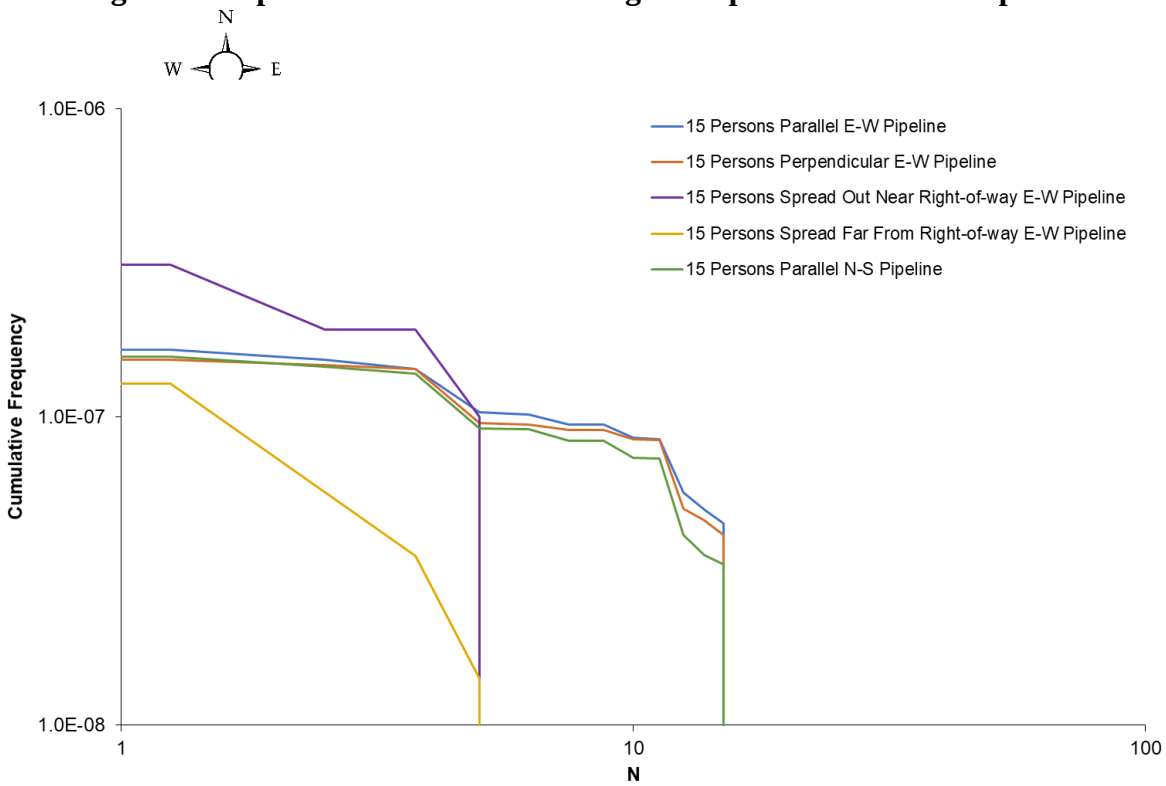


Figure 9. F-N Curves for Various Population Distributions

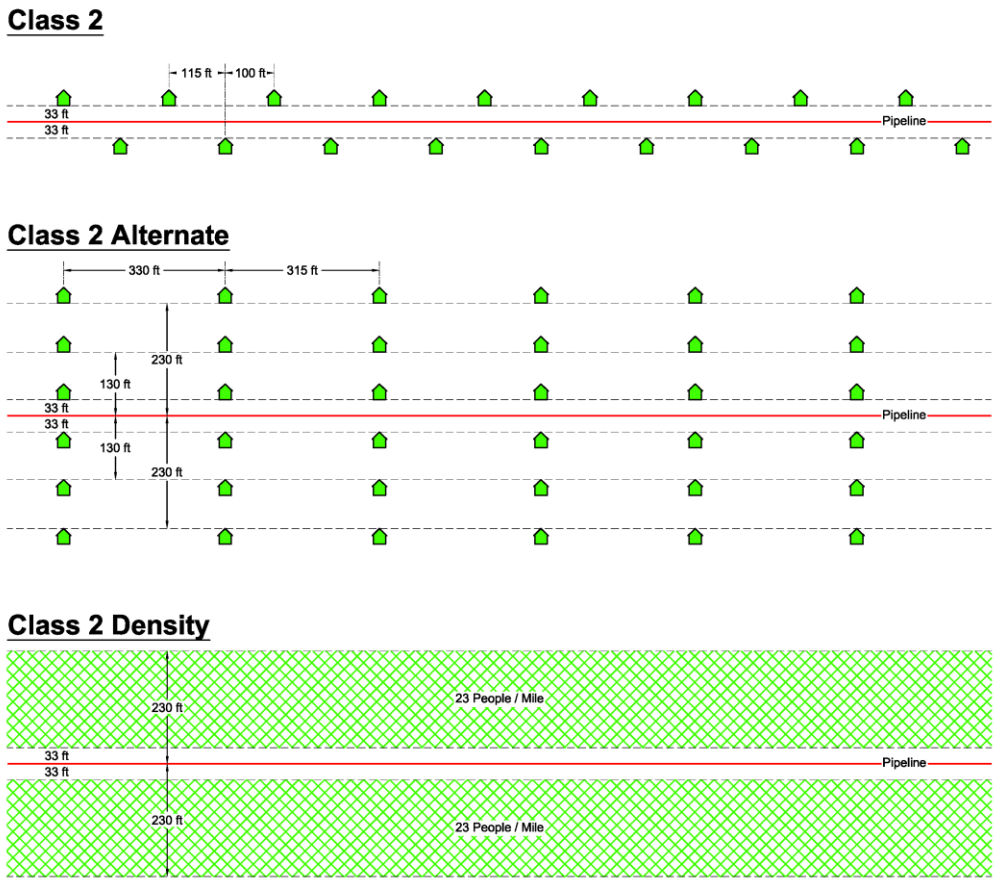


Figure 10. DOT Class 2 Population Distributions along the Example Natural Gas Transmission Pipeline (drawing not to scale)

There have been three natural gas transmission pipeline accidents that resulted in eight or more fatalities during this 47-year period. These are shown on the right-hand side of Figure 12 and described in Table 2.

The specific accidents listed in Table 2 could be modeled with the approach described above by locating a group or groups of people by the natural gas transmission pipeline. However, the frequency at which the specific event occurs (e.g., rupture of pipeline near bridge where people are camping for the night) would be so low that the single event may be acceptable according to the risk criteria.

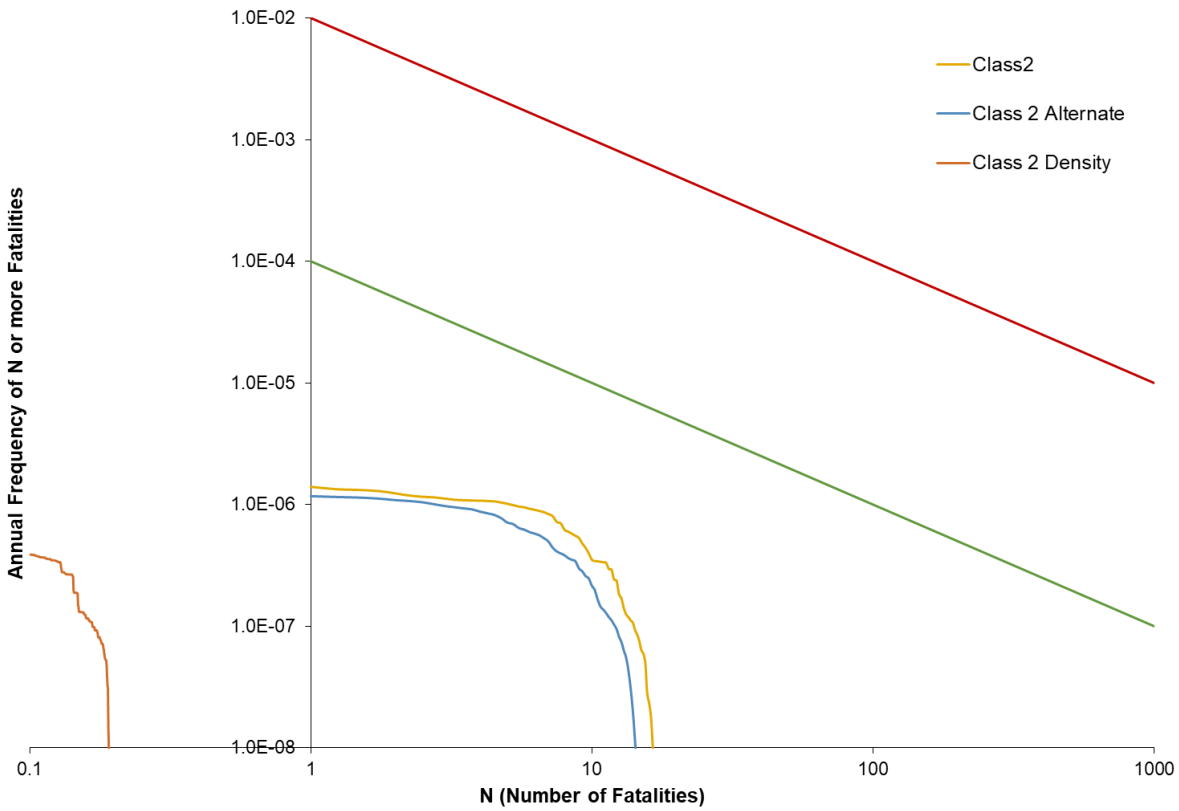


Figure 11. F-N Curves for Three DOT Class 2 Population Distributions

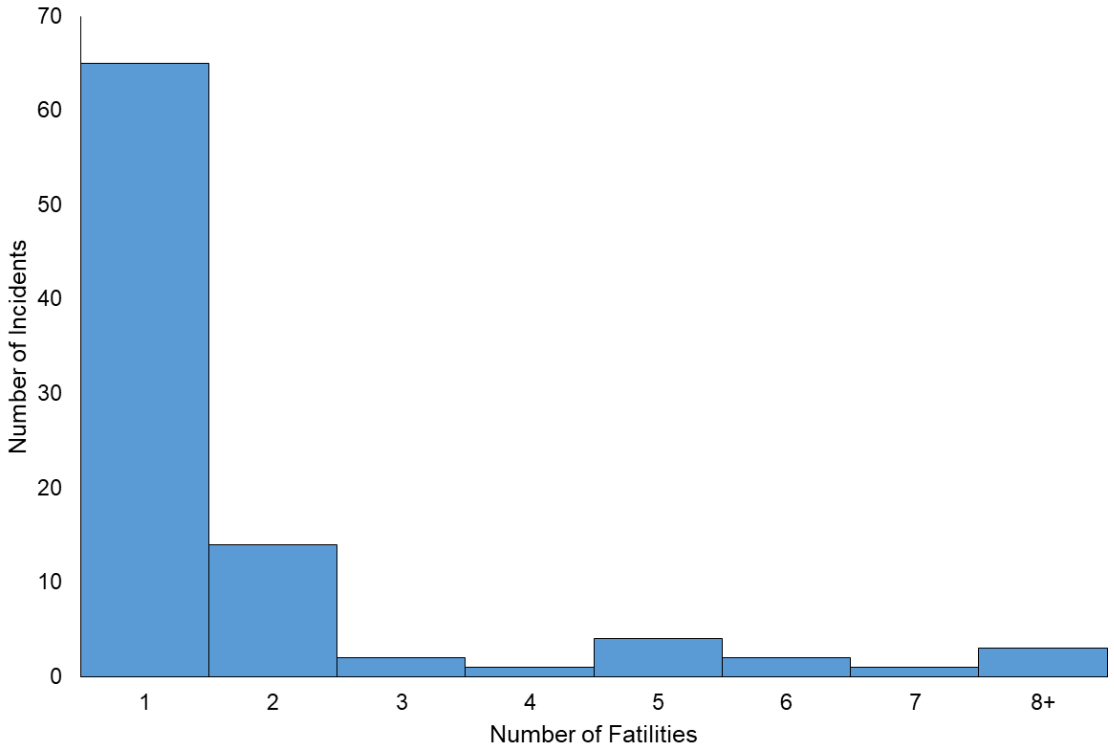


Figure 12. Historical Natural Gas Transmission Fatality Data from 1970 – 2016

Table 2. Historical Fatality Data for Eight or More Fatalities over a 47-Year Period

Date	Fatalities	Accident Description
10/3/1989	11	On October 3, 1989, the United States fishing vessel NORTHUMBERLAND struck and ruptured a 16-inch diameter natural gas transmission pipeline about ½ nautical mile offshore in the Gulf of Mexico, and about 5 1/3 natural miles west of the jetties and the entrance to Sabine Pass, Texas. Natural gas under a pressure of 835 psig was released. An undetermined source on board the vessel ignited the gas, and within seconds, the entire vessel was engulfed in flames. The fire on the vessel burned itself out on October 4. Leaking gas from the pipeline also continued to burn until October 4. Of the 14 crewmembers, 11 died as a result of the accident[5].
8/9/2000	12	At 5:26 a.m., mountain daylight time, on Saturday, August 19, 2000, a 30-inch-diameter natural gas transmission pipeline operated by El Paso Natural Gas Company ruptured adjacent to the Pecos River near Carlsbad, New Mexico. The released gas ignited and burned for 55 minutes. Twelve persons who were camping under a concrete-decked steel bridge that supported the pipeline across the river were killed and their three vehicles destroyed. Two nearby steel suspension bridges for gas pipelines crossing the river were extensively damaged[6].
9/9/2010	8	On September 9, 2010, about 6:11 p.m. Pacific daylight time, a 30-inch-diameter segment of an intrastate natural gas transmission pipeline known as Line 132, owned and operated by the Pacific Gas and Electric Company (PG&E), ruptured in a residential area in San Bruno, California. The rupture occurred at mile point 39.28 of Line 132, at the intersection of Earl Avenue and Glenview Drive. The rupture produced a crater about 72 feet long by 26 feet wide. The section of pipe that ruptured, which was about 28 feet long and weighed about 3,000 pounds, was found 100 feet south of the crater. PG&E estimated that 47.6 million standard cubic feet of natural gas was released. The released natural gas ignited, resulting in a fire that destroyed 38 homes and damaged 70. Eight people were killed, many were injured, and many more were evacuated from the area[7].

SUMMARY

The quantitative risk analysis methodology presented in this paper allows the user of the methodology to evaluate the individual and societal risk associated with natural gas pipelines. The individual risk associated with pipelines has been the traditional method used to evaluate the risk associated with natural gas pipelines. The individual risk approach does not take population into account. As project proponents and regulators struggle to assess the risk associated with natural gas pipelines that are routed though populated areas, another risk measure is needed.

By the use of DOT Class definitions, converted to people instead of buildings, the risk associated with each pipeline section (this paper uses one-mile pipeline sections) can be evaluated. If a pipeline section is shown to extend into an unacceptable or negotiable region of the societal risk criteria (F-N curves) measures can be taken to lower the risk. These measures could include, but are not limited to, depth of burial, change of operating conditions, and rerouting part of the pipeline. With this approach the risk associated with any natural gas pipeline can be assessed.

REFERENCES

[1] DOT (2011), Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards U.S. Department of Transportation, (49 CFR 192.5). U.S. Department of Transportation, Washington, D.C., October, 2011.

[2] HSE (2018), http://www.hse.gov.uk/comah/alarp.htm, accessed August 2018.

[3] U.S. Census Bureau (2017), Table HH-4, https://www.census.gov/data/tables/time-series/demo/families/households.html, accessed January 2018.

[4] HSE (2001), *Reducing Risks, Protecting People; HSE's Decision-making Process*. Health and Safety Executive, United Kingdom, 2001 (ISBN 0 7176 2151 0).

[5] NTSB (1990), "Fire on Board the F/V Northumberland and Rupture of a Natural Gas Transmission Pipeline in the Gulf of Mexico Near Sabine Pass, Texas, October 3, 1989." *National Transportation Safety Board Pipeline Accident Report,* No. NTSB-PAR-90-02, September 11, 1990 (PB90-916502).

[6] NTSB (2003), "Natural Gas Pipeline Rupture and Fire Near Carlsbad, New Mexico, August 19, 2000." *National Transportation Safety Board Pipeline Accident Report,* No. NTSB-PAR-03-01, February 11, 2003 (PB2003-916501).

[7] NTSB (2011), "Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California, September 9, 2010." *National Transportation Safety Board Pipeline Accident Report,* No. NTSB-PAR-11-01, August 30, 2011, (PB2011-916501).

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Managing the Risk of Organizational Incidents

Brian R. Dickson
Dept. Chemical & Process Engineering
University of Strathclyde, Glasgow, G1 1XJ, UK.
Email: brian.dickson@strath.ac.uk

Key Words: Process Safety Management, Risk, Human factors

Abstract

In Reason's, *Managing the Risk of Organizational Incidents*, `Reason draws on the work of other authors, and how awareness of the operating consequences of action is more important that causes of error.
It is the intention of this paper to review some of this work, in particular in the light of current trends that promote Risk Management, Incident Recording and Lead/Lagging Indicators as the "new direction in safety management". It will then go on to suggest why we need to encompass more of general management principles in the way that we think about safety in the work place and perhaps create new tools that move away from the Engineering model and its linear solutions, to an Organizational Model, where responsibility lies with the Individual rather than the System.

It will draw on case studies to demonstrate a sample of how the approach may have validity.

Introduction

In 2016, I asked a Masters Chemical Engineering student to consider major process safety events over the past 25 years, to consider whether there were common patterns across 20+ incidents by applying principles from good audit practice set. We hoped to then factorise these against frequency and build a model of a predictive nature.

What we discover was that the influencing factors could be set out into design, safety processes, management practice, legislator demands, Safety models, current development or trends.

As part of this work, we set out Stages in Safety Practice (SP) as follows:

1. F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

2. HAZOP (H_z), LOPA (L_{pa})

3. Safety Case/COMAH (S_c), QRA(Q_{ra}),

4. Management of Change (M_{ch}), Swiss Cheese Model (S_{cm}) and Safety Management Systems (SMS)

5. Leading/Lagging Indicators (L_{li}), Stress Cracking (S_{cr}), Management of Safety Competence (M_{sc})

This could be written in a <u>quasi-Equation of State</u> as;

$SP= F [M_c, P_m, R_k, E_{fe}, H_z, L_{pa}, S_c, Q_{ra}, M_{ch}, S_{cm}, Lli, S_{cr}, M_{sc}]$

and my source of reference: Perry, Lees, CCPS (Eng. Design for Process Safety) Kletz (What went wrong), IChemE (Hazop), Reason (Human Factors), CCPS (Implementing Process Safety Management System), CCPS (Integrating Management Systems & Metrics to improve Process Safety Performance) and 30 other books on my shelf **but lastly Dekker [2] (Drift into Failure)**

It was perhaps now impossible to codify as we had thought because of the many factors involved, and had to rethink out linear simple engineering tool approach.

Yet on re-reading Dekker and Reason, we arrived at a tentative link between **Management of Safety Competence (M_{sc}), Safety Space and Drift into Failure.**

Discussion

To understand why there is perhaps a theory with considering, it's worth considering some of the writings on the causes of what is often referred to as an Atrophy of Progress and the lessons that need to be drawn.

Charles Perrow [3], an organizational theorist, suggests a bleak proposition that “accidents are inevitable in complex, tightly-coupled systems ……...regardless of the skills of their operators and managers.”

Hence the title: accidents in such systems are 'normal'" According to Perrow the redundancies that go to make up defences-in-depth have three dangerous features.

1. Redundant defensive back-ups increase the interactive complexity of high-technology organizations and thus increase the likelihood of unforeseeable common-mode failures. While the assumption of independence may be appropriate for purely technical breakdowns, human errors at the 'sharp end', in the maintenance sector and in the managerial domains are uniquely capable of creating failures that can affect a number of defensive layers simultaneously"
2. Adding redundancy makes the system more opaque to the people who nominally control and manage it. Undiscovered errors and other latent problems accumulate over time and increase the likelihood of the 'holes' in the defensive lining up to permit the passage of an accident trajectory. This alignment of the gaps can be created either by interactive common-mode failures or by the simultaneous disabling of supposedly independent defences, as at Chernobyl.
3. As a consequence of this dangerous concealment, and because their obvious engineering sophistication, redundant defences can cause systems operators and managers to forget to be afraid. This false sense of security prompts them to strive even higher levels of production. Fixes including safety devices, often merely allow those in charge to run the system faster, or… with bigger explosives”

Karl Weick reinforces this view of unstable systems in control and tells us that “We know that single causes are rare, but we don't know how small events can become chained together so that they result in a disastrous outcome. In the absence of this understanding, people must wait until some crisis actually occurs before they can diagnose a problem, rather than be in a position to detect a potential problem before it emerges.

To anticipate and forestall disasters is to understand regularities in the ways small events can combine to have disproportionately large effects.” [4]

In taking forward this view, we appear to set ourselves a challenge of inevitable failure and if one were to take a pessimistic view of the safety history of the process industries then this may well be the case. Although this is where Reason[5] brings us and this papers challenge in “Making Sense of Reason”. His “Safety Space” is a natural extension of the resistance-vulnerability continuum introduced in the previous section. It is a boundary within which the current resistance or vulnerability of an individual or an organization is represented. As shown in Figure 1, it is cigar-shaped, with extreme resistance located at the left-hand end and extreme vulnerability at the right-hand end. The shape acknowledges that most people or organizations will occupy some intermediate point within this space.

An organization's position within the safety space is determined by the quality of the processes used to combat its operational hazards. In other words, its location on the resistance-vulnerability dimension will be a function of the extent and integrity of its defences at anyone point in time.

However, here is no such thing as absolute safety, human fallibility, latent conditions and the possibility of chance conjunctions of these accident-producing factors continue to exist, even the most intrinsically resistant organizations-those at the extreme left-hand end- can still have accidents. By the same token, 'lucky' but unsafe organizations at the extreme right-hand end of the space can still escape accidents for quite long periods of time.

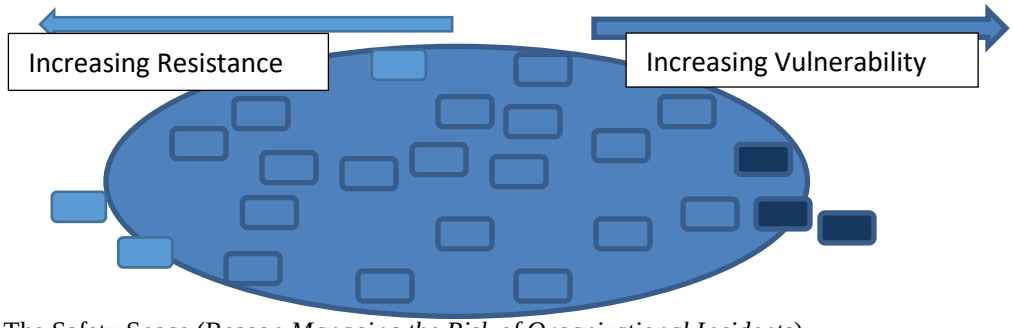


Fig 1: The Safety Space (Reason *Managing the Risk of Organizational Incidents*)

"The key to navigating the safety space lies in appreciating what is manageable and what is not. Many organizations treat safety management as a negative production process, they set reduced negative outcome targets for the coming accounting period (e.g., 'Next year we'll reduce our lost-time accidents by half'), yet accidents by their nature, are not directly controllable, so much of their causal variance lies outside the organization's sphere of influence. The organisation can only defend against hazards; it cannot remove or avoid them and still stay in business. Similarly, an organization can only strive to minimize unsafe acts, it cannot eliminate them altogether, and figure 2 demonstrates some of the high level factors that need to be in place."

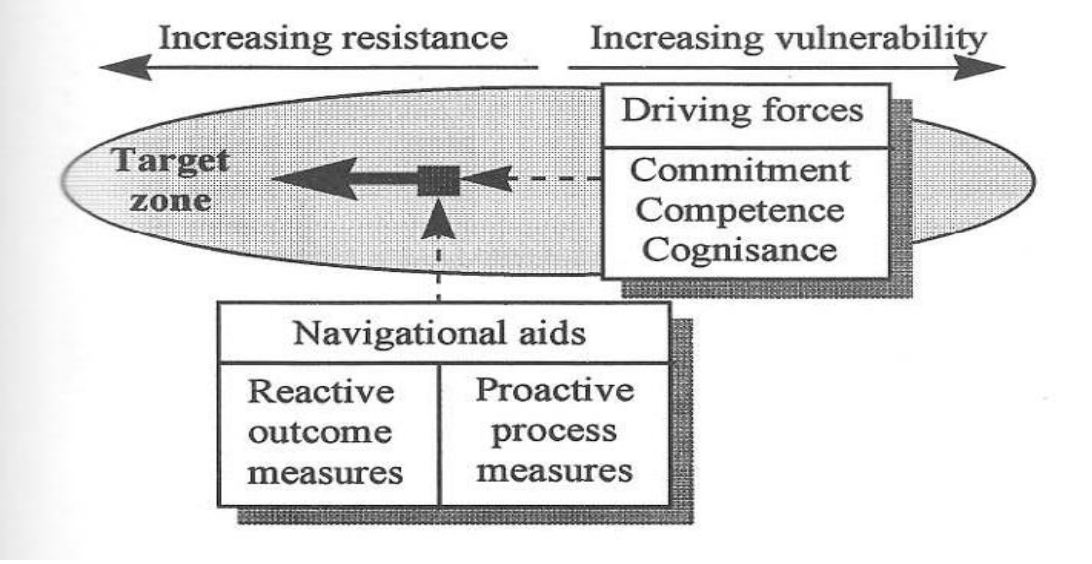


Fig 2: A summary of the principal factors involved in navigating the "Safety Space" with The Driving Forces and the Navigational Aids that together comprise the safety information system (Reason *Managing the Risk of Organizational Incidents*)

This is where the sense of matching our studies and the link to Safety Competency where reports spanning 40 years highlight this common factor amongst many others from our Equation of State:

Date	Event Name
1974	Flixborough
1979	3 Mile Island
1984	Bhopal,
1986	Chernobyl
1998	Piper Alpha
	Longford, Australia
2005	Texas City Buncefield
2010	Deep Water Horizon/Mocondo Dupont Belle Tesoro Refinery
2015	ExxonMobil Torrance, CA
	Tianjin, China

This analysis is supported by Baybutt's "Insights into process safety incidents from an analysis of CSB Investigations" of 64 incidents [8].where he too sees lack of competence arising with regular frequency.

Conclusion

Effective safety management is more like a long-term fitness programme than negative production. Rather than struggling vainly to exercise direct control over incidents and accidents, managers should regularly measure and improve those processes--design, hardware, training, procedures, maintenance, planning, budgeting, communication, goal conflicts, and the like-that are known to be implicated in the occurrence of organizational accidents. These are the manageable processes determining a system's safety health. They are, in any case, the processes that managers are hired to manage; safety management is not an add-on, but an essential part of the system's core business.

Perhaps safety indictors need brought into the management world, where there is no room for "loss time statistics", "leading/lagging indicators", or current position on the "Heinrich's Safety Triangle/Dashboard" and more about:

- Did the work force feel safe at work today?
- What did we do safely today to make the business more secure?
- What marginal gains have we developed today to make us all safer?

These are perhaps 3 from many indicators to be used by managers who normally show concern about the viability of their business by asking about Quality (throughput) & Financial (Cash at bank) indicators.

However, there is a challenge in this view and in addressing "why", it is suggested here that the concept of competence or the lack of it is the problem.

In his review of "Texas City Refinery Explosion: Lessons Learned", Mogford [6] mentions five underlying causes, all management responsibilities and two in particular are linked to the theme of this paper:

> "Secondly, process safety, operations performance and systematic risk reduction priorities had not been set nor consistently reinforced by management. Safety lessons from other parts of BP were not acted on.
>
> And finally, poor performance management and vertical communication in the refinery meant there was no adequate early warning system of problems and no independent means of understanding the deteriorating standards in the plant through thorough audit of the organisation."

This is reinforced in the Baker [7] commission report for BP,

> **"Recommendation #3**
> **– process safety knowledge and expertise**
> BP should develop and implement a system to ensure that its executive management, its refining line management above the refinery level, and all U.S. refining personnel, including managers, supervisors, workers, and contractors, possess an appropriate level of process safety knowledge and expertise."

BP and many other companies have done much in progressing this idea, yet CCPS's *Guidelines for Auditing Process Safety Management Systems* (2nd edition 2011) places "Training and Performance Assurance" at p547 out of 835, and this really returns to the start of this paper, if the senior management don't understand

The Process Safety First Equation of State;

Safety Practice (SP) =
F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

Just understanding Cash Flow, Six Sigma, Coaching & Leadership and all the other chapters of *"How to be an Even Better Manager: A Complete A-Z of Proven Techniques and Essential Skills"* or some other book of that ilk, is not being a manager and the anthology of Process safety events presented in this paper will continue.

References

[1] Dickson B.R: Making Sense of Reason: A review of the message James Reason put forward for a re-think of Safety Management Principles, AIChE,11th Global Congress on Process Safety Proceedings, 2015

[2] Dekker Sidney: Drift into Failure Ashgate Publishing 2011

[3] Perrow Charles: Normal Accidents: Living with High risk Technologies, Basic Books, 1984

[4] Weick Karl quoted in P.J. Frost et al.: Reframing Organizations Sage 1991

[5] Reason James: Managing the Risk of Organizational Incidents, Ashgate Publishing, 1997

[6] Mogford J: The Texas City Refinery Explosion: The Lessons Learned**,** AIChE,2nd Global Congress on Process Safety Proceedings, 2006

[7] Baker J: BP US Refineries Independent Safety Review Panel Report, 2007

[8] Baybutt P: Insights into process safety incidents from an analysis of CSB Investigations, *Journal Of Loss Prevention In The Process Industries*, JLPP 3258, 2016

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Common Bow Tie Errors and How the CCPS Concept Book Rectifies

Tatiana Norman
DNV GL USA, Inc.
1400 Ravello Drive
Katy, Texas 77449, USA
Email: tatiana.norman@dnvgl.com

Keywords: Bow tie; Hazard Identification; Risk Analysis; Human Factors

Abstract

The bow tie risk analysis method is growing in its application as it is a powerful tool for visually communicating major accident risks and the barriers deployed to prevent or mitigate these. The ease of communication can mislead users to think that bow tie creation is also easy. A new CCPS Concept Book, Bow Ties in Risk Management, thoroughly reviews how to create bow ties and provides detailed guidance on how to avoid errors.

This paper provides several examples of common errors seen in the current bow ties. These cover structural errors, such as degradation factors and controls are misplaced onto main pathways, barriers that do not comply with guidance on required barrier core attributes, and incorrect hazards, top events, and consequences. The paper also covers a better means to treat human error.

A final part of the paper presents a novel multi-level approach to bow ties that can be helpful for human error and mechanical integrity applications where deeper degradation controls are important to display.

Abbreviations

CCPS	Center for Chemical Process Safety
EI	Energy Institute
HAZOP	Hazard and Operability Study
HOF	Human and Organizational Factors
LOTO	Lock Out Tag Out

Introduction

Bow tie analysis has been used for many years and is growing in its application as it is a powerful tool for visually communicating major accident risks and the barriers deployed to prevent or mitigate these. The ease of communication can mislead users to think that bow tie creation is also easy, and this is not the case. The method is qualitative and uses a diagrammatic representation of major accident threat and consequence pathways showing the hazard, top event, threats and consequences, with intervening barriers and degradation factor pathways linked to the main pathway barriers. A unique feature of the bow tie is its ability to communicate complex major hazard events in a simple format that is easily communicated to all members of staff, contractors, regulators and other stakeholders. Bow ties require a significant effort to create and update as necessary. A new CCPS Concept Book (CCPS & EI, 2018) thoroughly reviews creation of bow ties and provides detailed guidance on avoiding errors.

One of the primary goals of the book is to ensure consistent application of the bow tie technique by defining structural elements together with good and poor examples for clarification. An issue with bow ties is that there is no widely accepted methodology or definitions and this has resulted in many inconsistencies, poor structures, and poor treatment of human and organizational factors. CCPS along with the Energy Institute, collaborated to provide a book that compiles current practices and provided a set of suggested approaches.

The basic bow tie is shown in Figure 1. The figure shows the 8 main bow ties elements: 1) hazard, 2) top event, 3) consequence, 4) threat, 5) prevention barrier, 6) mitigation barrier, 7) degradation factor, and 8) degradation control.

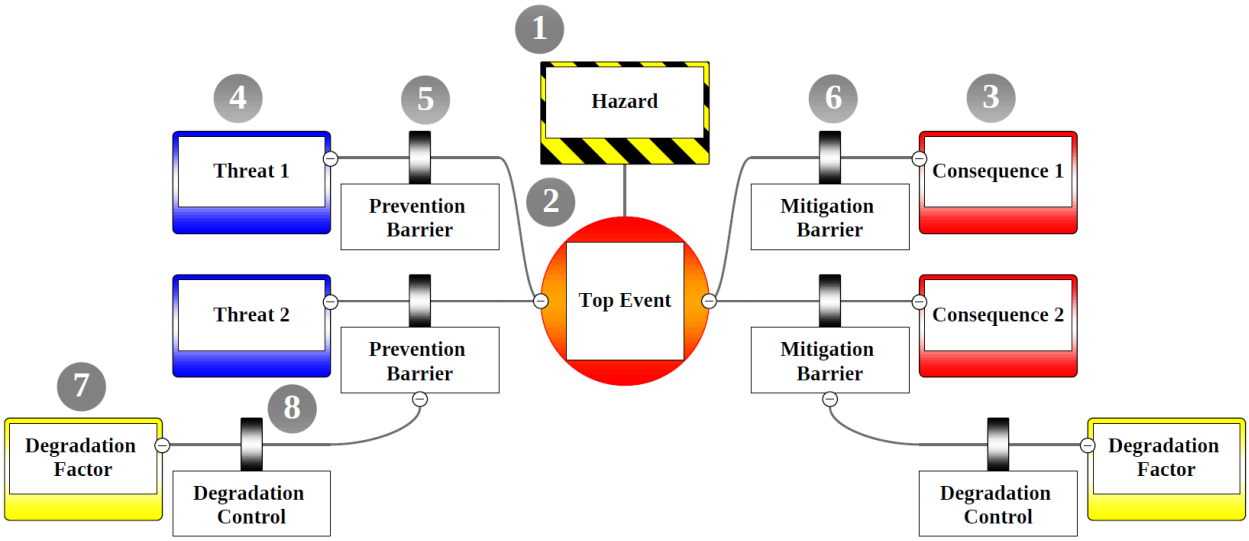


Figure 1. Basic Bow Tie

Common Errors: Hazard and Top Event

<u>Hazard</u>

Hazard is defined in the book as an operation, activity or material with the potential to cause harm. It appears at the top of the bow tie diagram and is the source of the risk. It is important

that the hazard is defined properly as this is the basis for the entire bow tie diagram. Generic hazards can lead to generic bow ties and lack the necessary detail.

A common error of bow tie is a hazard that is too vague. For example, specifying 'Chlorine' alone as the hazard would be too generic of a description. A better example would be 'Chlorine stored in a tank' as in Figure 2. Hazards should be formulated in a controlled state and not the loss of control of the hazard (this is the top event) or the actual harm (the consequences). CCPS/EI suggest the reader ask "Is the hazard as described part of our normal business?"

Figure 2. Example Hazard

Another common error is a hazard that does not link to the consequences listed. It is important to include enough detail in the hazard box to ensure the correct consequences are listed. The hazard box on the bow tie diagram cannot show all the details of the hazard but the specifics should be documented. The common theme from the CCPS/EI book is that the hazard should be defined as specific as possible and ensure that it links to the Top Event.

The book provides a table of well-defined and poorly defined hazards. A few examples are given in Table 1 below.

Table 1. Well-defined and Poorly-defined Hazards (CCPS/EI 2018)

Hazard	**Commentary**
Working at height (>2m) on formwork	Working at height is a common hazard and specifying the height provides additional detail.
Pressurized propane storage in sphere	The normal operational state is defined and some context of the volume is indicated.
H_2S	The hazard does not properly set the scope nor identify the scenario that will be analyzed. The bow tie will be different depending on the controlled state of the H_2S (e.g. drilling into formation containing H_2S, smelting iron with H_2S as by-product, or working in sewers where H_2S is present).
Control System Failure	This can be a top event, threat or a barrier failure depending on the context. It does not specify the actual hazard – perhaps 'hydrocarbons in formation'.

Top Event

The top event is the moment when control over the hazard or its containment is lost. Common generic top events include loss of containment, loss of separation, loss of stability or loss of control. The top event should be linked to the hazard. If the hazard is gasoline stored in tank and good example for top event could be tank overflow.

The top event should not be a consequence (e.g. explosion). A common error in defining a top event is to choose a consequence with damage or harm rather than a loss of control event. CCPS & EI (2018) recommend asking the question, "Is this loss of control or is this a consequence?" Another common error is choosing a top event that is part of an event sequence (e.g. ignition).

Good practice is to define a top event where multiple threats and consequences can be identified. If the top event is too narrow you run the risk of needing several diagrams to cover the risks surrounding your asset or operations. On the contrast, the top event should not be too broad. Building more than ten threats and consequences for a single top event could be too broad. The balance between detail and economy should be influenced by the intended audience, the objective of the study or historical incidents.

Common Errors: Consequence and Threat

Consequence

After defining the top event, the next step is to determine the consequences. A common mistake is defining treats before consequences since this would be the natural progression given the way the bow tie is drawn. The book suggests defining consequences before threats as this will help the team later define only the threats that acting on the hazard can lead to significant consequences. Consequences are unwanted outcomes that could result from the top event and lead to damage or harm.

CCPS & EI (2018) suggest describing the consequence as '[Damage] due to [Event]'. By describing the consequence this way, different barriers can be required to stop or mitigate damage depending on the event leading to the damage. For example, 'fatalities due to fire' might call for different mitigation barriers than 'fatalities due to toxic gas'. Consequences can be chosen which are good or poor, but generally selecting consequences is less prone to error than some other bow tie elements. Table 2 provides a few examples of poorly worded consequences.

Table 2. Common Consequence Errors

Top event	One Consequence	Comment – why this is poorly worded
Gasoline tank overflow	Environmental damage or Pollution	The consequence links directly to the top event but it is vague, and not specific as to the nature or severity of the environmental damage. Is the damage to land or water (small stream or large river?) or to specific species? Consequences should name the receptor affected. Inclusion of the scale is useful to design an adequate response from the mitigation barriers.
Loss of control over the vehicle	Crash barrier damage	This is a possible consequence, but it is likely to be unimportant compared to other consequences and might be better grouped (e.g. 'asset damage to car and road infrastructure').

Threat

Threats are possible initiating events that can result in a loss of control or containment of a hazard. The threat must lead to the top event if the pathway is not prevented. Three categories are helpful to initiate discussion in identifying threats:

1. primary equipment not performing within normal operating limits (mechanical fault),
2. environmental influence (overpressure due to solar heating of blocked in pipeline),
3. operational issues (insufficient personnel present to support all required human barriers during start-up).

Using 'human error' as a threat is not recommended by CCPS/EI as this commonly leads to structural errors in the bow tie. A structural error in a bow tie means that some important rule for bow tie construction has been violated. This is topic is elaborated more in a later section of the paper.

A frequent mistake is to exclude threats that will rarely lead to the top event because of the argument that there are already many prevention barriers in place to control this threat. Every credible threat should be added to facilitate decisions as to whether there are enough prevention barriers in place to control the particular threat and visualizing the credible threats enables a more complete overview. Threats should have a direct causation and be specific. Identifying direct threats will often result in inclusion of more specific barriers compared to indirect threats. They should also be sufficient and not barrier failures. If a threat can only cause the tope event in combination with another threat, it is not sufficient and therefore incorrect. Table 3 provides a few examples of poorly worded threats.

Table 3. Common Threat Errors

Threat	Top event	Comment – why this is poorly worded
Level gauge out of preventive maintenance cycle	Tank overflow	The threat is not a direct cause of tank overflow just because it is late on a preventive maintenance cycle. The threat is excess flow into the tank and the barrier is associated with operator vigilance using the level gauge.
Failure of anti-lock braking system (ABS)	Loss of control over the car	This is a safety system which has failed. It does not cause the top event on its own. A better threat would be a sudden burst tire.

Common Errors: Barriers

The most common error often found on a bow tie diagram is with barriers. CCPS & EI define barrier as a control measure or grouping of control elements that on its own can prevent a threat developing into a top event (prevention barrier) or can mitigate the consequences of a top event once it has occurred (mitigation barrier). A barrier must be effective, independent, and auditable. This provides confidence that it will be able to act when required and as intended, without any action or intervention external to the barrier, and that its degradation will be prevented. The book differentiates between barriers and degradation controls. Barriers appear on the main pathway (threat to top event or top event to consequence) and degradation controls only appear on degradation pathways and serve to support main pathway barriers against degradation. The biggest mistake found on bow tie diagrams is mistaking degradation controls as barriers. For example, training and competence are not barriers but are however degradation controls. Training competence may support a particular barrier but are not capable of preventing a top event or mitigating the consequences. Effective, independent and auditable are explored furthered in the next sections.

Effective

A barrier is effective is it performs the intended function when demanded and to the standard intended. A common mistake when representing effective barriers on a bow tie include identifying incomplete barriers, like fire and gas detection. While these are important barriers they rely on other elements to completely stop the scenario from developing further. The book suggests a complete barrier could be fire and gas detection, automatic logic controller (or human response to alarm) and ESD.

Independent

Barriers should be independent of the threat and or other barriers on that pathway. For example, if the threat is loss of power a barrier requiring power to operate would not be permissible. The barrier is not independent of the threat. Also, it is important that there is as little common mode failure between barriers as possible. It is often difficult to find barriers that have no common mode and for this reason it is not necessary to remove barriers with some minor aspect of common mode. The book suggests managing the risk of a plausible common mode failure by the adding other

barriers that do not have that common mode. Adding different types of barriers is advisable and usually can help avoid some general common mode failures.

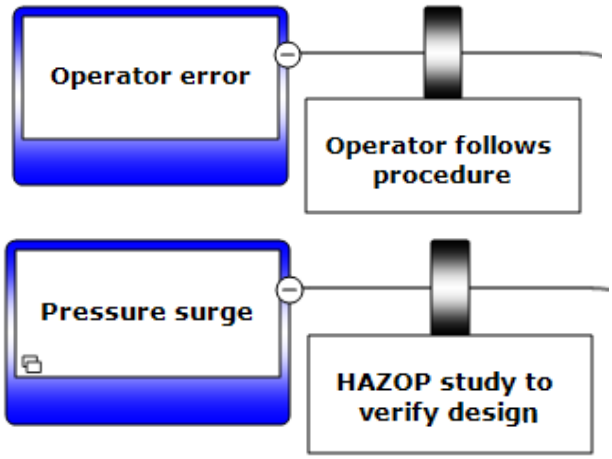
Auditable

Barriers should be capable of being audited to check that they work when called upon.

The most common mistakes regarding barriers are:

- displaying multiple barriers that are actually elements of a single barrier;
- barrier titles that are not informative;
- placing barriers on the wrong side of the top event; and
- indicating measures which are not barriers.

The figures below are further examples of common errors and remedies.



Threat and barrier are not independent

HAZOP study is not a barrier

Figure 3. Incorrect Barrier Examples

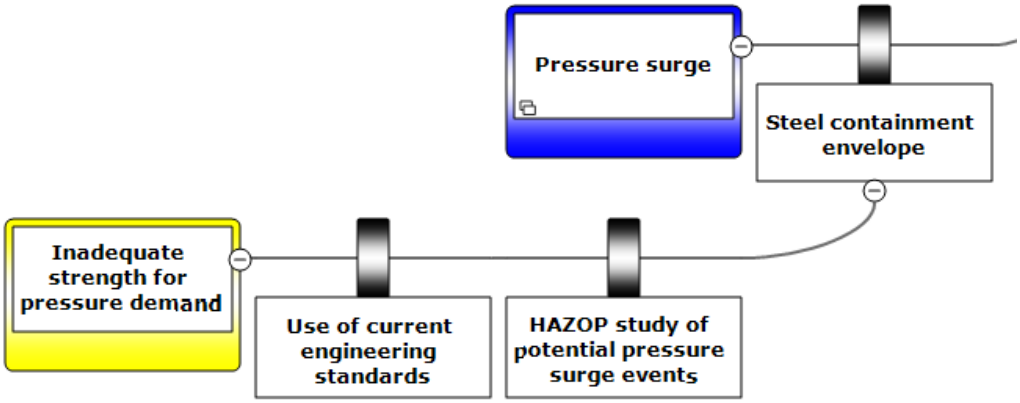


Figure 4. Better Barrier Examples

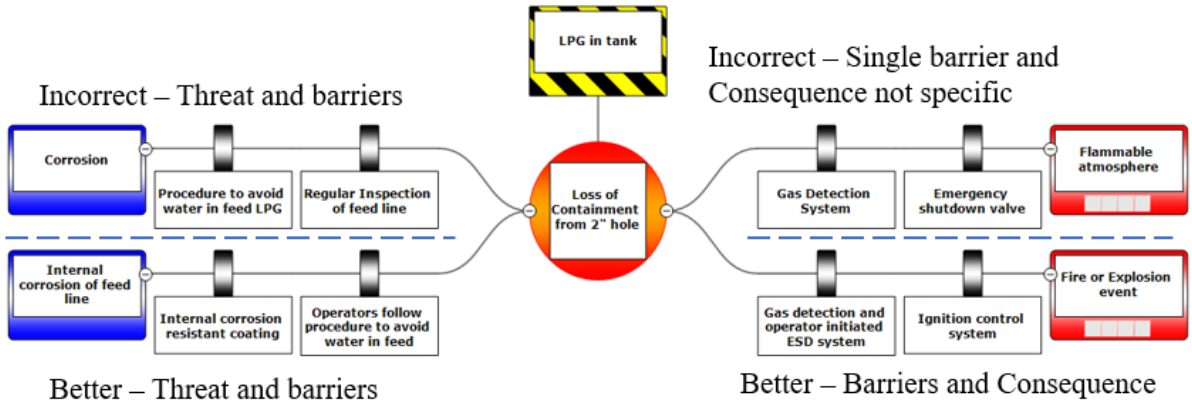


Figure 5. Incorrect and Better Barrier Examples

In summary, the list below provides some dos and don'ts regarding barriers on the bow tie diagram:

- Effective / Independent / Auditable
- If active – must display all elements of Detect – Decide – Act
- Should not be degradation controls
- If prevention side – must be able to stop Top Event
- If Mitigation side – must significantly mitigate consequence
- A procedure is NOT a barrier, but an operator executing a procedure is
- Similarly, a warning sign is not a barrier
- Systems are usually not barriers
- Inspection and Maintenance are usually not barriers
- Lock out tag out (LOTO) and Work Permit are usually not barriers
- HAZOP review is not a barrier
- A trivial control is not a barrier

Treatment of Human Error in Bow Ties

The CCPS and the Energy Institute recognized the need to address the current inconsistencies in the treatment of Human and Organizational Factors (HOF) in bow ties as this could significantly improve process safety. In bow ties, HOF issues can appear in several places. Humans (including human failure – error or inaction) can be modeled a threat, but more often appear either i) as part(s) of a prevention or mitigation barrier, ii) as a degradation factor, or iii) as part(s) of a degradation factor control. Therefore, humans can form a barrier or a barrier element. Since a human barrier is always active, it must have all elements of 'detect-decide-act' present (CCPS & EI, 2018).

The term 'human error' has sometimes been used as a main pathway threat. However, the required barriers can be very different based on the type of human error and the context in which it might occur. Degradation controls against a slip (e.g., fatigue management) would be different to a mistake (e.g., refresher training). The term 'human error' is usually too imprecise to be a good main pathway threat - it should appear as a specific degradation factor linking through the degradation pathway to a main pathway barrier. The book recommends that human failure should not be used as a main pathway threat. Making human error a threat almost always results in structural errors to bow ties; mainly barriers that do not meet the validity criteria.

CCPS & EI (2018) found many organizations developed bow ties where HOFs were represented as a threat for a main pathway. For example, part a of Figure 6 shows adding catalyst to an exothermic reactor before proper mixing is established can lead to a runaway reaction and an explosion. Treating human error as a threat results in an incorrect analysis because:

1. The HOF fails to meet the definition of a threat as it lacks the ability to combine with the hazard to lead to a top event.
2. The resulting barriers "Training" and "Supervision" on the main pathway fail to meet the definition of barriers as they lack the ability on their own to prevent a threat developing into a top event and cannot detect-decide-act.
3. The resulting four barriers on the main pathway lead to overconfidence in control over the threat.

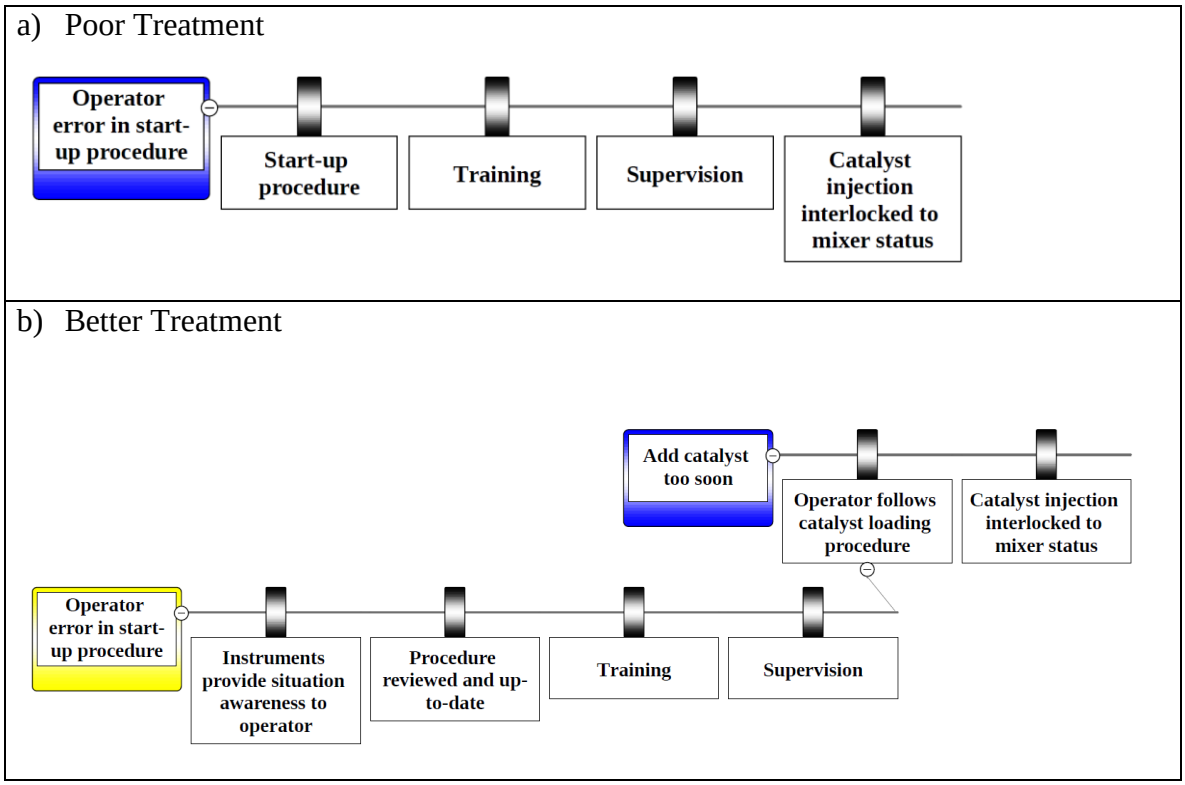


Figure 6. Example 1 Poor and Better Treatment of Human Error in Bow Tie

Treating human error as a degradation factor for a main pathway barrier is shown in part b of Figure 6 which results in a correct analysis because:

1. The HOF "Operator error startup procedure" as a degradation factor for the barrier "Operator follows catalyst loading procedure" meets the definition of being a situation, condition, defect, or error that compromises the function of a main pathway barrier, either through degrading it or reducing its effectiveness.
2. The resulting barriers "Training" and "Supervision" on the degradation factor pathway meet the definition of safeguards as they support the main pathway barrier and lie along degradation pathways into that barrier where they help defeat the degradation factor.
3. The resulting barrier "catalyst injection interlocked to mixer status" on the main pathway more correctly represent the control over the threat and the resulting four safeguards on the

degradation pathway more correctly represent the level of attention paid to maintaining the barrier "Operator follows catalyst loading procedure".

Figure 7 provides another example of poor and better treatment of human error on bow ties.

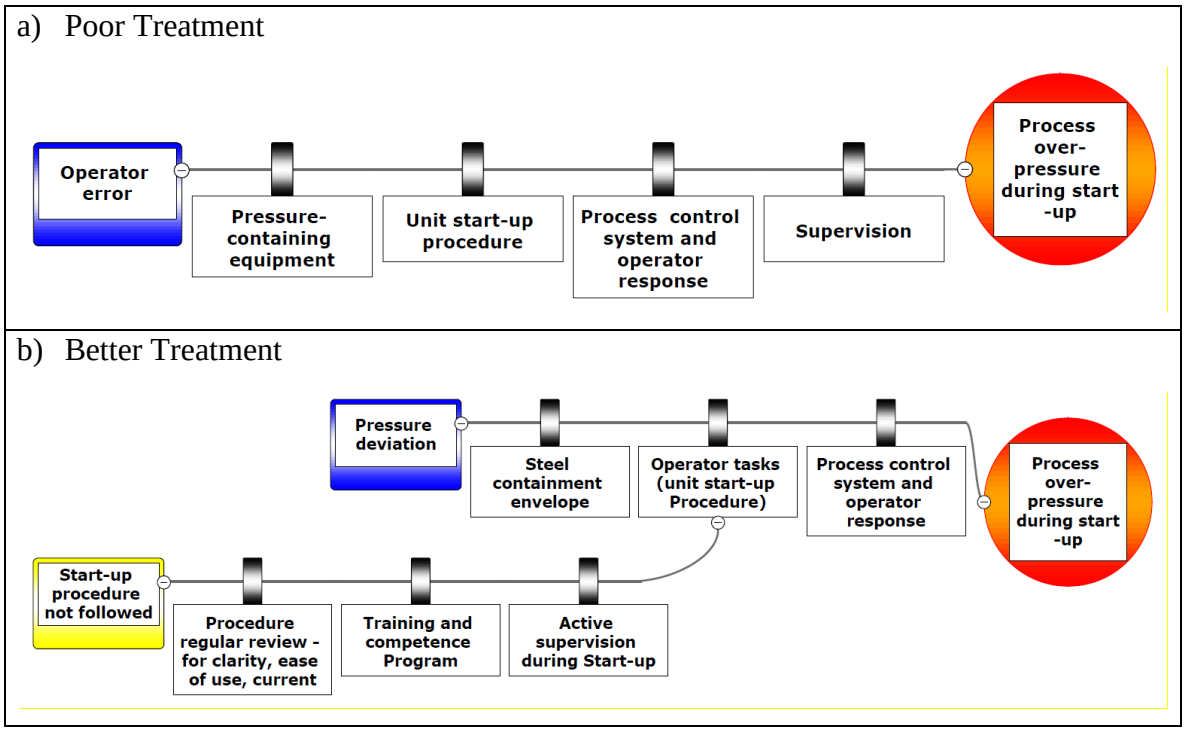


Figure 7. Example 2 Poor and Better Treatment of Human Error in Bow Tie

Defining Human and Organizational Factors in Bow ties

In Bow Ties in Risk Management two approaches to bow ties are presented: a conventional approach (standard bow tie) and a more advanced multi-level approach (multi-level bow tie). The multi-level approach is a new approach and offers potential benefits in addressing additional analysis of HOF. Multi-level bow ties can be a better approach to exploring human failure aspects in bow ties and can display a range of degradation controls. These would be deeper level controls supporting standard bow tie degradation controls against their own degradation.

In the multi-level approach, the standard bow ties main pathways and degradation factor pathways remain unchanged. The extension shows how degradation controls in the standard bow tie can be degraded and the additional controls that might be needed. This is shown in Figure 8. This extra level is defined as extension level 1. Degradation control examples at the standard bow tie level might include: procedures reviewed and up-to-date, training, and supervision; while extension level degradation controls might include: drug and alcohol testing, stop work authority, and senior management tours.

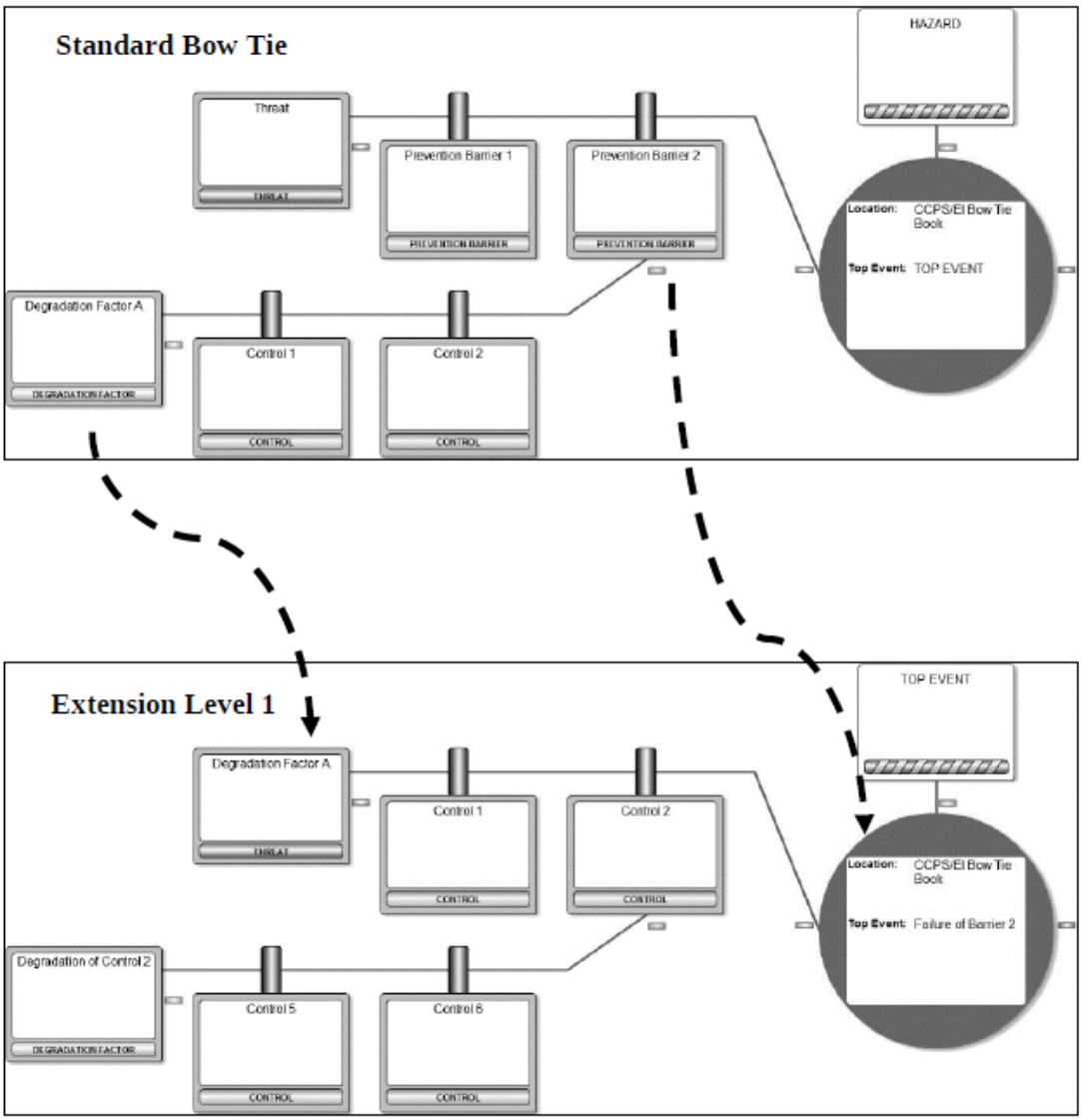


Figure 8. Concept of Multi-Level Bow Tie Approach (CCPS & EI, 2018)

Quality Checks

CCPS/EI identifies many matters to check, post workshop, in order that the final bow ties are useful and structurally correct. The list includes overall checks for items including consistent terminology, the right mix of people in the workshop and consistency with the agreed study terms of reference. There are several other quality checks for items pertaining to the bow elements themselves; for example, is the hazard clearly expressed with sufficient data or do all the main pathway barriers meet the validity criteria.

Conclusion

The bow tie method is a qualitative risk analysis method addressing major accident events and the key barriers and safeguards used to manage these. The method is growing in use in the process industries, for both upstream and downstream petro-chemical industries, as well as other major

hazard industries such as aviation, railways, and shipping. A bow tie can be a very powerful communication tool. The ease of communication can mislead users to think that bow tie creation is also easy. CCPS along with the Energy Institute, collaborated to provide a book that compiles current practices and provides a set of suggested approaches.

One of the primary goals of the book is to ensure consistent application of the bow tie technique by defining structural elements together with good and poor examples for clarification. This paper set out to highlight some of the common errors for the eight bow tie elements. The hazard should be specific and link to the top event. Typical top events include loss of containment or loss of control. Consequences should be described as '[Damage] due to [Event]'. Threats should have a direct causation and be specific. A majority of the mistakes are realized when defining barriers. A barrier must be effective, independent and auditable. Each individual barrier must have the capability to completely stop the threat from leading to the top event, or if a mitigation barrier, significantly reduce or eliminate the consequence. HOF has often been poorly treated in current bow ties. The book recommends that human failure should not be used as a main pathway threat. Multi-level bow ties were introduced as a method to better approach to exploring human failure aspects in bow ties and can display a range of degradation controls.

References

CCPS & EI (2018) *Bow Ties in Risk Management: A Concept Book for Process Safety*. American Institute of Chemical Engineers, John Wiley & Sons, New Jersey.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Considering Multiple Initiating Events in a LOPA

Denise Chastain-Knight, PE, CFSE, CCPSC
Loren Stewart, CFSE
exida
80 North Main Street
Sellersville, PA, 18960, USA
Emails: dchastainknight@exida.com, lstewart@exida.com

Keywords: Semiquantitative Risk Assessment, Layer of Protection Analysis (LOPA), Interlocks & Safety, Safety Instrumented Systems (SIS), Residual Risk Management, Alarm and Instrument Management, Automatic SIS System

Abstract

Layer of Protection Analysis (LOPA) is a risk reduction evaluation methodology well suited to consider hazard scenarios with multiple initiating events. The presence of multiple initiators increases the likelihood that a hazard scenario could occur placing additional demands on the Independent Protection Layers (IPLs) that prevent and mitigate the hazard. This paper will discuss the impact of multiple initiating events on demand frequency, discuss methods to evaluate the effectiveness of IPLs, and determine which may be considered to reduce the demand on a Safety Instrumented Function (SIF) and Safety Integrity Level (SIL) targeting. Finally, the impact of demand frequency and proof test interval on SIF demand mode will be illustrated.

Introduction

The Layer of Protection Analysis (LOPA) was developed nearly twenty years ago to fill the gap between qualitative process hazard analysis (PHA) and detailed quantitative risk analysis (QRA). The objective of a LOPA is to determine what PHA safeguards serve as Independent Protection Layers (IPL) and confirm risk is reduced to as low as reasonably practicable (ALARP)[1] levels. When a Safety Instrumented Function (SIF) is one of the IPLs, the LOPA is also used to determine Safety Integrity Level (SIL) and SIF demand frequency. When used thoughtfully, much more information can be captured by the LOPA that is required for specification and design of a SIF. LOPA will also document key information later needed for Safety Requirements Specification (SRS) including:

- Demand source
- Demand frequency
- Additional mitigation
- Risk receptors
- Related interlock

LOPA Presentation

LOPA may be presented in many different formats. Figure 1 illustrates some common formats including portrait format summary (A), event tree (B), and landscape format summary (C).

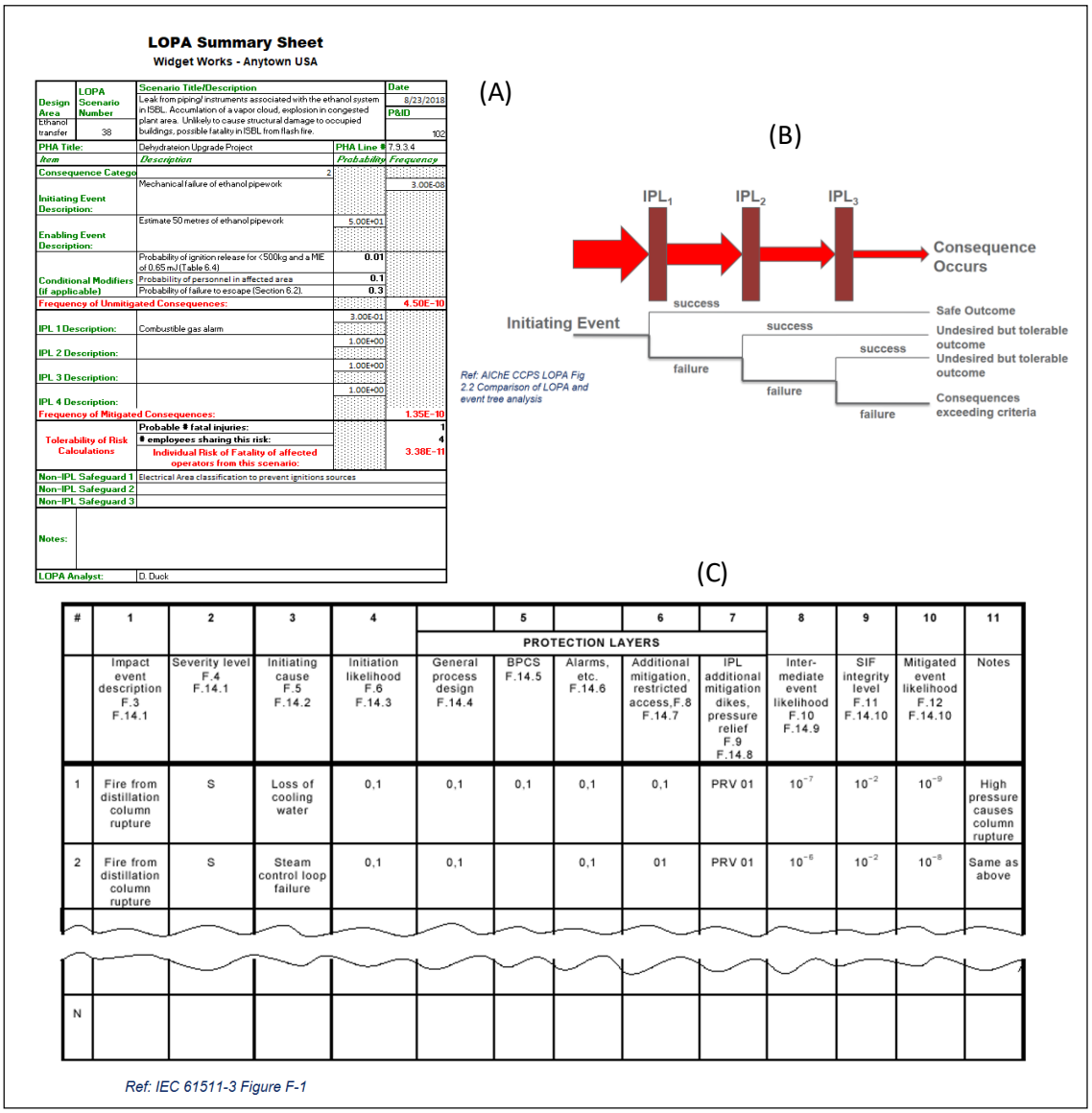


Figure 1 – Common LOPA Presentations

Figure 1A is consequence based and captures a lot of information including identification of multiple initiating events and IPLs, but it does not provide a framework to assess the effectiveness of IPLs against individual initiators or risk receptors. Figure 1B is initiating event focused, provides a detailed analysis of the effectiveness of IPLs against the initiator, identifies multiple potential outcomes for an event and delivers some risk receptor information. Figure 1C is cause/consequence pair based focusing analysis on one branch of the event tree. All of these methods consider a worst case tolerable frequency regardless of risk receptor (e.g. safety, environment, business) for the analysis.

This paper will utilize a LOPA format that considers multiple initiators in a single view and provides a framework to analyze the effectiveness of IPLs against individual initiators, separately for each risk receptor (Figure 2)[2].

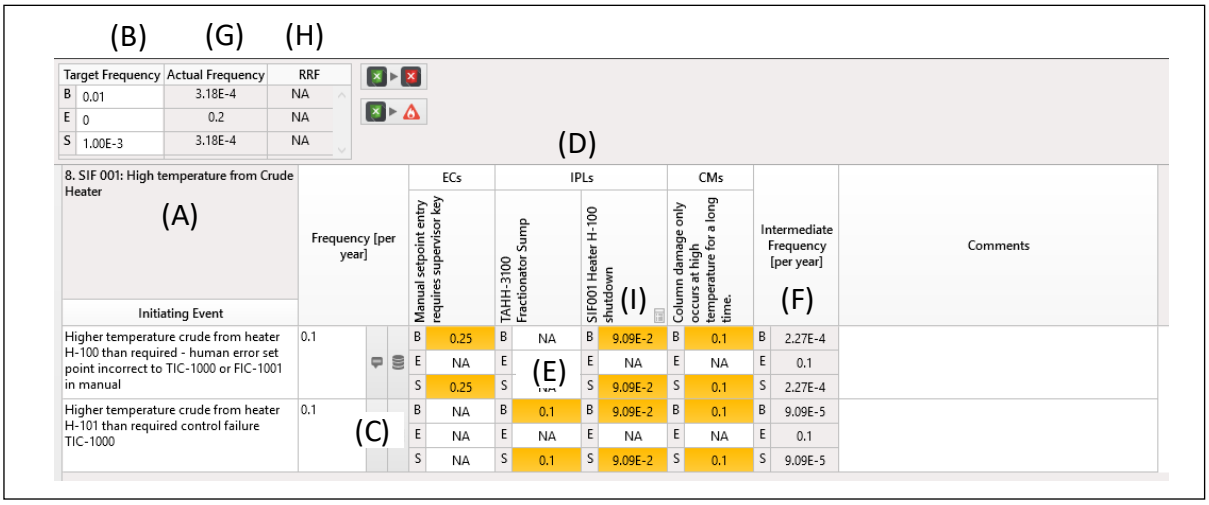


Figure 2 – exSILentia Framework

The LOPA is named (A) to represent the undesired consequence and may contain identifiers for the SIF intended to protect against the consequence. The tolerable target frequency of consequence for each risk receptor is defined in the summary table (B) at the top of Figure 2. Initiating events are presented in rows of the analysis table (C) with sub-rows for each risk receptor. Columns are grouped (left to right) by enabling conditions (EC), IPLs and Conditional Modifiers (CM) (D). Within the IPL subgroup, the IPLs are positioned in the sequence in which they are effective. For example, if the intended protection layer sequence is operator response to a process alarm, SIF action, then relief device actuation, IPLs would be placed in this order. The software interprets the sequencing to indicate which IPLs act to reduce demand (alarm) on the SIF and those that do not (relief). Probability of failure on demand (PFD) for the EC, IPL and CM layers are recorded in a background database and are applied where the user indicates effectiveness against initiating events (E). Intermediate frequency is calculated for each IE by risk receptor (F), and cumulative frequency is tallied by risk receptor in the summary table (G). The RRF column of the summary table indicates a gap between tolerable risk and scenario risk (H). Once PFD data is entered for all non-SIF IPLS, and protection has been assigned, target SIL may be calculated for the SIF (I). From this arrangement the information which may be extracted for the SRS includes:

- Demand source – Description of initiating events with individual frequencies.
- SIF Demand frequency – Calculated from individual demand frequencies considering EC and IPLs that reduce demand.
- Additional mitigation – Complete list of IPLs that provides mitigation, ECs and CM that could be managed through other means.
- Risk receptors – Summary by receptor provide information that could impact design decisions.
- Related interlock – Processes may have interlocks in DCS, package equipment and SIS. Each is indicated by a separate IPL.

- SIL Target – Directly calculated including residual risk.

LOPA Evaluation as Individual Records

When a LOPA does not consider multiple initiating events in a combined analysis, the SIL target and demand frequency can be underestimated, thus resulting demand mode may be misjudged. The following example considers three records extracted from a HAZOP for scenarios where the consequence of concern is a loss of pilots to a fired heater, with the potential for fire/explosion. The event consequence was determined to have a tolerable frequency of 1E-4 for business interruption, 1E-2 for environmental consequence and 1E-3 for safety. Figure 3 illustrates a cause/consequence pair for a human error initiating event (cause 1). The valve is remotely located, so an enabling condition regarding accessibility of the valve is included to reduce the likelihood of this initiating event. Potential IPLs identified from the HAZOP safeguards are listed as a group. The PFD for the IPLs is entered in a database and assigned individually to each risk receptor, where they are effective. After all information is entered, the SIF PFD is calculated to close the gap between intermediate frequency and tolerable frequency. This analysis suggests the SIF should be a SIL 1 target RRF of 10 (RRF = 1/PFD = 1/0.1) with a demand frequency of 0.01/year (f_{IE} * f_{EC}).

	Target Frequency	Actual Frequency	RRF
B	1.00E-4	1.00E-4	NA
E	1.00E-2	1.00E-4	NA
S	1.00E-3	1.00E-4	NA

3. Loss of Pilots Heater Trip - Cause 1	Frequency [per year]	ECs		IPLs								Intermediate Frequency [per year]	
Initiating Event			Liklihood of personnel working in area where valve is located		Cause 1 SIF		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure				
Battery Limit Natural Gas Ball Valve inadvertently closed.	0.1	B	0.1	B	1.00E-1	B	0.1	B	NA	B	1.00E-4
		E	0.1	E	1.00E-1	E	0.1	E	NA	E	1.00E-4
		S	0.1	S	1.00E-1	S	0.1	S	NA	S	1.00E-4

Figure 3 - Cause 1

Figures 4 and 5 illustrate analysis for two additional cause/consequence pairs from the HAZOP record. Figures 3 and 4 both credit the pilot gas low pressure alarm for the operator response, but in Figure 5, the firebox high pressure is considered the more effective alarm. Only one alarm may be considered per IE because they reside in the same DCS, and are managed by the same operator (not independent).

Target Frequency		Actual Frequency	RRF
B	1.00E-4	1.00E-4	NA
E	1.00E-2	1.00E-4	NA
S	1.00E-3	1.00E-4	NA

4. Loss of Pilots Heater Trip - Cause 2	Frequency [per year]	IPLs								Intermediate Frequency [per year]	
Initiating Event		Cause 2 SIF		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure					
PCV-033 Natural Gas to Heater pilots fails.	0.1	B	1.00E-2	B	0.1	B	NA	B	1.00E-4
		E	1.00E-2	E	0.1	E	NA	E	1.00E-4
		S	1.00E-2	S	0.1	S	NA	S	1.00E-4

Figure 4 - Cause 2

Target Frequency		Actual Frequency	RRF
B	1.00E-4	1.00E-4	NA
E	1.00E-2	1.00E-4	NA
S	1.00E-3	1.00E-4	NA

5. Loss of Pilots Heater Trip - Cause 3	Frequency [per year]	IPLs								Intermediate Frequency [per year]	
Initiating Event		Cause 3 SIF		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure					
Combustion chamber steam inadvertently opened	0.01	B	1.00E-1	B	NA	B	0.1	B	1.00E-4
		E	1.00E-1	E	NA	E	0.1	E	1.00E-4
		S	1.00E-1	S	NA	S	0.1	S	1.00E-4

Figure 5 - Cause 3

Each of the three LOPAs are anticipated to set the SIL target for the SIF. That will identify the loss of the pilot flame and bring the process to a safe state by tripping the fuel valves. Results of the analysis are summarized in below in Table 1.

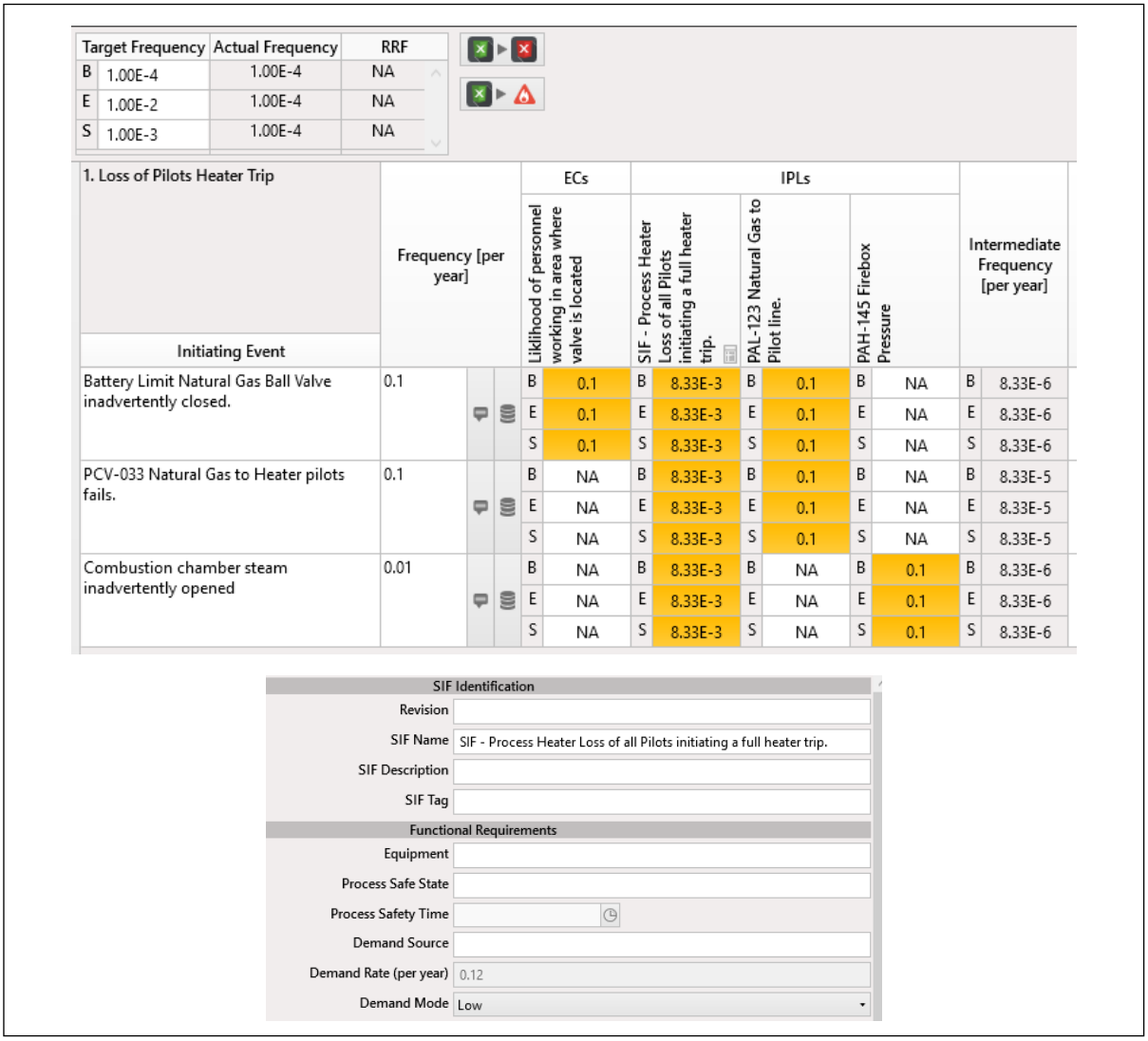
Table 1 – Cause/Consequence Pair Analysis Summary

	SIL Target	SIF RRF target	Demand Frequency / year
Cause 1	1	10	0.01
Cause 2	2	100	0.1
Cause 3	1	10	0.01

So what is the design basis for the SIF? Frequently, causes are considered separately so the SIF design basis may be selected on the 'worst case' scenario without consideration for the cumulative impact of multiple causes. Cause 2 has the highest SIL target and the highest demand frequency so users might select this as the 'worst case' design basis. Simply selecting the case that delivers the highest target, ignores residual risk and multiple demands as illustrated by a combined LOPA evaluation.

Combined LOPA Evaluation

In SIF design, the user must consider the combined impact of multiple initiating events, the effectiveness of IPLs against each cause, and the cumulative effect on both demand and RRF requirements. Figure 6 is a combined LOPA which includes all three initiating events in a single analysis. The inset below the LOPA is a view of the SRS, where the demand rate is automatically populated by exSILentia based on the LOPA. Target frequency, initiating event frequency, EC and non-SIF IPLs are the same as given in the individual analysis. The EC/IPL effectiveness is noted the same as in Figures 3-5, then the SIL target for the SIF is calculated.



	Target Frequency	Actual Frequency	RRF
B	1.00E-4	1.00E-4	NA
E	1.00E-2	1.00E-4	NA
S	1.00E-3	1.00E-4	NA

1. Loss of Pilots Heater Trip	Frequency [per year]			ECs		IPLs						Intermediate Frequency [per year]	
Initiating Event					Liklihood of personnel working in area where valve is located		SIF - Process Heater Loss of all Pilots initiating a full heater trip.		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure		
Battery Limit Natural Gas Ball Valve inadvertently closed.	0.1			B	0.1	B	8.33E-3	B	0.1	B	NA	B	8.33E-6
				E	0.1	E	8.33E-3	E	0.1	E	NA	E	8.33E-6
				S	0.1	S	8.33E-3	S	0.1	S	NA	S	8.33E-6
PCV-033 Natural Gas to Heater pilots fails.	0.1			B	NA	B	8.33E-3	B	0.1	B	NA	B	8.33E-5
				E	NA	E	8.33E-3	E	0.1	E	NA	E	8.33E-5
				S	NA	S	8.33E-3	S	0.1	S	NA	S	8.33E-5
Combustion chamber steam inadvertently opened	0.01			B	NA	B	8.33E-3	B	NA	B	0.1	B	8.33E-6
				E	NA	E	8.33E-3	E	NA	E	0.1	E	8.33E-6
				S	NA	S	8.33E-3	S	NA	S	0.1	S	8.33E-6

SIF Identification	
Revision	
SIF Name	SIF - Process Heater Loss of all Pilots initiating a full heater trip.
SIF Description	
SIF Tag	
Functional Requirements	
Equipment	
Process Safe State	
Process Safety Time	
Demand Source	
Demand Rate (per year)	0.12
Demand Mode	Low

Figure 6 – Combined Evaluation

The analysis yields a combined initiating event frequency of 0.12 demands per year and a SIL 2 target with minimum RRF of 120. Table 2 is a summary comparing the results of the combined analysis to the results of the 'worst case' individual analysis from above.

Table 2 – Design Basis Comparison

	SIL Target	SIF PFD target	Demand Frequency / year
Cause 2 design basis ('worst case')	2	100	0.1
Combined analysis design basis	2	120	0.12

The comparison in Table 2 demonstrates that the composite LOPA is effective in identifying the impact of multiple initiating events on the overall demand frequency and takes into account the

residual risk, when establishing the SIL target. Considering cause/consequence scenarios separately results in an underestimation of both demand and the required RRF. It is important to note that summing the results of the individual analysis, shown in Table 1, will produce the same result as the combined analysis, unfortunately this step is often overlooked.

Benefit of IPLs that Reduce Demand Frequency

ECs, IPLs and CMs are arranged in the LOPA to consider the impact on initiating event and consequence frequency. This is similar to the approach of the event tree method shown in Figure 1B. The columns should be placed left to right to reflect the expected sequence of events. Figure 3 illustrates the adjustment of initiating event frequency based on the application of an enabling condition. In this example, the valve is located remotely from the process in an area where valves are seldom operated. The use of an EC clearly indicates a reduced likelihood of this initiator (human error) to those reviewing the LOPA at a later date. In this LOPA format, ECs are conditions that impact the initiating event frequency so they always reduce demand and are placed left of the IPLs. Conditional modifiers are conditions that impact the likelihood of a particular outcome once the scenario is initiated. CMs will always appear to the right of the IPLs because they do not impact SIF demand but do impact the potential for worst case consequence.

Within the IPL group, columns are shifted left or right of the SIF based on both scenario development sequence and confidence in the IPL effectiveness to reduce demand. For example, a pressure safety valve (PSV) IPL would be placed to the right of the SIF because the SIF set point is below the relief threshold and the SIF should act before the PSV where a loss of containment consequence is realized. In a scenario where the initiating event is not DCS related (e.g. a human error), response of a DCS control loop may be credited as an IPL and would be placed left of the SIF because it is effective in reducing demand on the SIF.

Operator response to an alarm is an IPL that may be considered to reduce SIF demand, or discounted due to potential ineffectiveness. The efficacy of operator response to an alarm is largely dependent on a facility's alarm management program. A large quantity of alarms, confusing priority (e.g. critical alarm on a situation the operator knows to be minimal risk) and known nuisance alarms (e.g. sensor out of service) can work together to desensitize an operator and increase the likelihood that an operator would fail to respond appropriately to an alarm. Standards like ISA 18.2[3] have established a lifecycle framework for alarm management. Figure 7[4] illustrates experience of one oil and gas producer for two operator consoles before, during and after implementation of ISA 18.2.

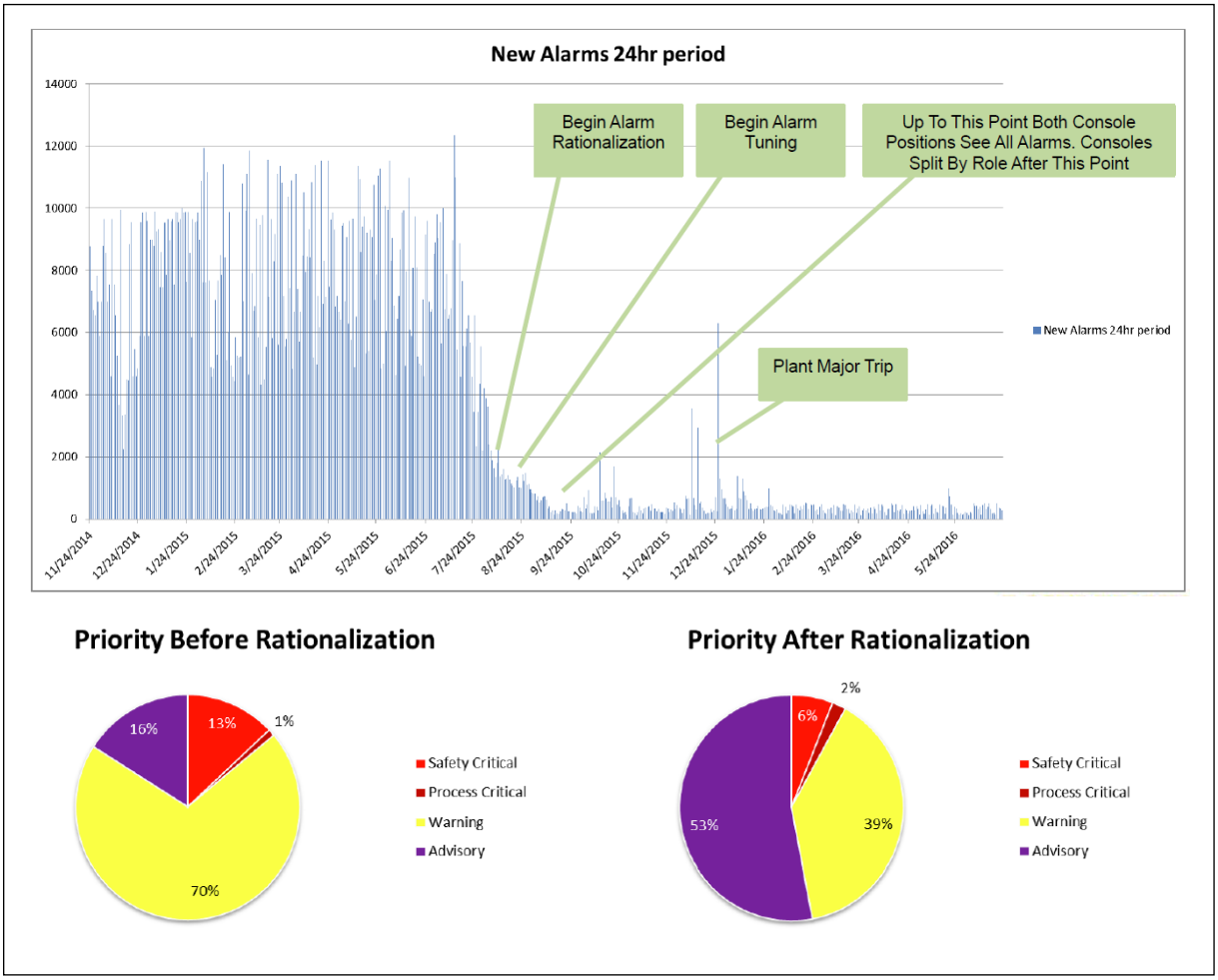


Figure 7 – Impact of ISA 18.2 on Alarm Load and Priority

Before ISA 18.2 implementation, the operators routinely received large numbers of alarms and 70% of the alarms were the same priority. After implementation the operators received significantly fewer alarms, and priority distribution was adjusted to improve visibility of more important alarms. A facility that has implemented an alarm management program, has completed alarm rationalization, utilizes advance alarm groups (flood suppression) and has a routine monitoring program to identify and correct issues, may have more confidence in the effectiveness of the alarm IPL[5]. Such an organization may elect to take credit for this and reduce the design demand rate on SIFs. In the exSILentia tool the alarm IPL columns are shifted left of the SIF and the demand rate calculated for the SRS is adjusted accordingly (Figure 8).

	Target Frequency	Actual Frequency	RRF
B	1.00E-4	1.00E-4	NA
E	1.00E-2	1.00E-4	NA
S	1.00E-3	1.00E-4	NA

6. Loss of Pilots Heater Trip - With Alarm to reduce demand	Frequency [per year]			ECs		IPLs						Intermediate Frequency [per year]	
Initiating Event				Likilihood of personnel working in area where valve is located		PAL-123 Natural Gas to Pilot line.		PAH-145 Firebox Pressure		SIF - with alarm to reduce demand			
Battery Limit Natural Gas Ball Valve inadvertently closed.	0.1			B	0.1	B	0.1	B	NA	B	8.33E-3	B	8.33E-6
				E	0.1	E	0.1	E	NA	E	8.33E-3	E	8.33E-6
				S	0.1	S	0.1	S	NA	S	8.33E-3	S	8.33E-6
PCV-033 Natural Gas to Heater pilots fails.	0.1			B	NA	B	0.1	B	NA	B	8.33E-3	B	8.33E-5
				E	NA	E	0.1	E	NA	E	8.33E-3	E	8.33E-5
				S	NA	S	0.1	S	NA	S	8.33E-3	S	8.33E-5
Combustion chamber steam inadvertently opened	0.01			B	NA	B	NA	B	0.1	B	8.33E-3	B	8.33E-6
				E	NA	E	NA	E	0.1	E	8.33E-3	E	8.33E-6
				S	NA	S	NA	S	0.1	S	8.33E-3	S	8.33E-6

SIF Identification	
Revision	
SIF Name	SIF - with alarm to reduce demand
SIF Description	
SIF Tag	
Functional Requirements	
Equipment	
Process Safe State	
Process Safety Time	
Demand Source	
Demand Rate (per year)	0.012
Demand Mode	Low

Figure 8 – Alarm Credit to Reduce Demand Frequency

Demand Mode

It is a common expectation in the process industry that SIFs operate in low demand mode; however, this is not always the case. IEC 61511 2nd edition explicitly states that a SIF is in high demand mode if the demand frequency is greater than once per year, and it suggests that a SIF should be considered high demand if "the failure [of the SIF] is undetected and a demand occurs before the next proof test interval" [6]. It is important for facilities to document every SIF trip and perform periodic analysis to confirm the demand frequency is consistent with design basis.

Demand frequency on a SIF is derived directly from the LOPA; however, additional information is required to determine SIF demand mode. Both demand frequency and proof test interval (PTI)

must be considered when determining SIF demand mode. If a SIF is tested annually, the potential for an undetected SIF component failure is low, and the one-per-year threshold from low to high demand holds. As PTI is increased, the potential for a demand to occur between proof tests is increased. For a SIF to be low demand mode, the initiating event frequency must be less than 1/(2*PTI)[7]. Figure 9 illustrates how demand mode threshold changes as PTI is increased.

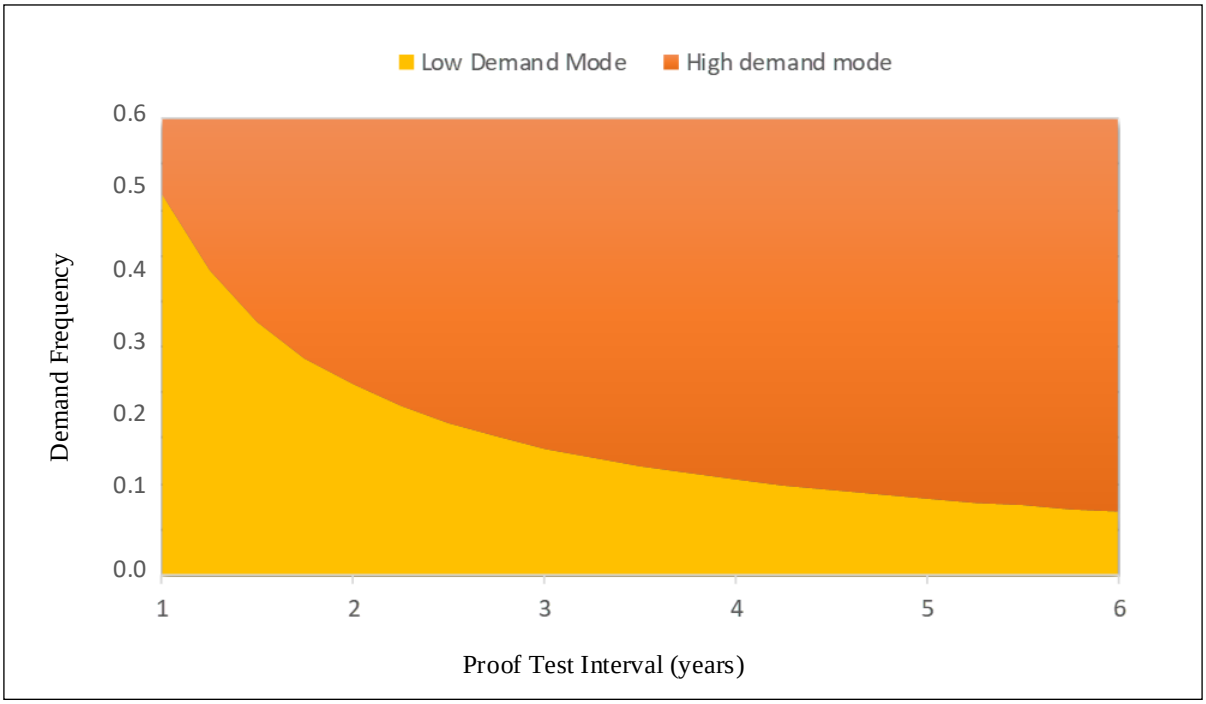


Figure 9 – SIF Demand Mode Threshold

Frequently, processes are designed so they must be shut down to complete proof testing, therefore, often PTI's will correspond to turnaround schedules. As time between turnarounds is increased, the SIFs' PTI is also increased and the SIF can unexpectedly move from low demand mode of operation to high demand mode. If the demand frequency identified in the SRS does not consider all initiating events, a SIF may be believed to operate in low demand mode when it is actually in high demand mode. In high demand mode the effectiveness of proof testing is not achieved, thus the risk reduction provided by the SIF may fall short of requirements and expectations.

Early identification of SIFs that operate in high demand mode provides the most options to resolve back to low demand mode. A SIF may be moved from high to low demand by reducing the frequency of demand or decreasing the proof test interval. Table 3 provides some options:

Table 3 – Demand Reduction Options

Action	Example
Implement administrative program to reduce likelihood of single initiating event	Implement valve locking (carseal) program for manual valves
Reduce failure potential of initiating event through engineering solution	Install two regulators in series rather than one
Install additional instrumentation upstream that will address IEs closer to the source	BPCS or hardwire interlock

Implement programs that improve IPL confidence and reduce demands on SIF	Alarm Management program per ISA 18.2
Reduce proof test interval	Install isolation and bypass capability to permit on line testing

If proof testing can't be implemented for the entire SIF on-line testing, such as partial stroke testing of a valve, can be helpful. Automatic diagnostics with appropriate diagnostics frequency and coverage are required to provide proof testing of high demand mode SIFs.

Conclusion

LOPA is a valuable tool to analyze the risk associated with an event scenario and document the expected effectiveness of protective layers. Many tools are available for conducting the analysis, but few are designed to consider multiple initiating events in a single view as illustrated by the figures above. When using a tool that performs analysis on single cause/consequence pairs, it is necessary to perform an additional step to determine the combined demand frequency and RRF requirement for the SIF. Failure to do so will result in an underestimation of both the initiating event frequency and the RRF target.

When a LOPA is used to determine the design basis for a Safety Instrumented Function (SIF) it is critical that the cumulative effects of multiple initiating events be considered together when assessing IPL effectiveness, and determining the SIF demand frequency and the SIL target. IPLs should be applied only against the initiating events where they are effective thus reducing the residual risk for that scenario. Some IPLs, such as operator response to an alarm, may be considered to reduce the demand rate on a SIF when well managed and monitored by a process such as the ISA 18.2 lifecycle. IPLs should only be considered to reduce SIF demand frequency when they are well managed and monitored to assure effectiveness.

Finally, the proof test interval must be considered to convert demand frequency to demand mode. As intervals between PTI are increased, the potential for hidden failures is increased, thus high demand mode design criteria, including use of diagnostics, is more appropriate. A SIF designed for low demand mode, that is operating in a high demand mode condition is likely to deliver less risk reduction than targeted and may not be effective when called upon to bring the process to a safe state.

---

[1] Health and Safety Executive, ALARP "at a glance", http://www.hse.gov.uk/risk/theory/alarpglance.htm

[2] exSILentia 4 Integrated Lifecycle Tool, exida.com LLC.

[3] Instrument Society of America (ISA), *ANSI/ISA-18.2-2016 Part 1 Management of Alarm Systems for the Process Industries*.

[4] Benji Kidmose and Jamie Errington, *Austin We Have a Problem*, Emerson Exchange Session 1-9829, 2016

[5] Todd Stauffer, Nicholas Sands, and David Strobhar, *"Closing the Holes in the Swiss Cheese Model"- Maximizing the Reliability of Operator response to Alarms*, Global Congress on Process Safety, March 2017.

[6] IEC 61511-1 Ed 2.0, *Functional Safety: Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements,* IEC, Geneva, Switzerland 2016

[7] Iwan van Buerden, William M. Goble, *Safety instrumented System Design, Techniques and Design Verification*, Instrument Society of America (ISA), Research Triangle Park, NC, 2018

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Evolutionary Themes from ISA 84 to ISA 61511

Eloise Roche*, Angela Summers
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
*Presenter E-mail: eroche@sis-tech.com

Keywords: Safety Management System, Standards

Abstract

ANSI/ISA 84.00.01 was the second edition of ISA standard to address safety instrumented systems for the process industry sector and was recognized by OSHA as a good engineering practice within process safety management. Nevertheless, standards must evolve over time based on application experience. After a decade of international process sector experience in applying these requirements for safety instrumented systems (SIS), a new edition of the IEC 61511 international standard was published. Recently published, ANSI/ISA 61511-1 brings the ISA standard into complete alignment with IEC 61511-1. This paper will review ten major themes of change between ANSI/ISA 84.00.01 and ANSI/ISA 61511-1.

1 Introduction

The American National Standard ANSI/ISA-S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries" [1] was published just a few years after the issuance of the OSHA regulation on process safety management (PSM) [2]. Within this context, this first edition of the safety instrumented system (SIS) standard focused predominately on the design, installation and change management of the system hardware and said little about other aspects of functional safety management already addressed in the PSM regulation. This original standard also said little about application programming for programmable electronic systems, which were a relatively new logic solver technology compared to the simpler safety relays and trip amplifiers that were in common use at the time for emergency shutdown systems and other safety applications.

Of course, the need for a standard on safety instrumented systems was not limited to the United States of America. The first edition of the U.S. standard on SIS was an input to the newly formed IEC 61511 committee. Not all of the nations involved in the IEC committee had laws similar to the U.S. regulation on process safety management. Therefore, many of the changes made in the

development of IEC 61511-1:2003 [3] focused on adding the functional safety management requirements that would otherwise have been absent in the international context. Since the programmable electronic logic solver was by this time a much more established technology, IEC 61511-1:2003 also included requirements for the application programming for SIS using this technology. For the most part, the resulting set of requirements would have been very familiar to facilities subject to both OSHA PSM regulations and the ANSI/ISA-S84.01 standard. IEC 61511-1:2003 was adopted the following year as the second edition of the ISA SIS standard, retitled ANSI/ISA 84.00.01 [4], with only the addition of one clause in the scope to address existing systems that had been designed and implemented using the 1996 standard.

During the first handful of years after the publication of ANSI/ISA 84.00.01, members of the ISA 84 committee, the MT61511 team, and the broader industrial community began to note sections of the standard where systematic misunderstanding in application still seemed to be occurring relatively often. The fundamental safety instrumented system hardware and functional safety management requirements in the standard were by this time well-established process safety practice across the globe. Therefore, the major change themes for the second edition of IEC 61511-1 [5] focused on clarifying existing concepts in the requirements to improve the systematic use of the standard in these sections. Adopted by ISA without change in late 2017, the standard now known as ANSI/ISA 61511-1 [6] (retiring the ISA 84.00.01 nomenclature) can be more consistently applied around the world.

These major change themes can be grouped together into the following categories:

- Hazards and Risk Analysis (H&RA) and Specification
- Detailed Design and Engineering
- Operations and Maintenance

2 H&RA and Specification

The failure frequency claimed for initiating sources related to the basic process control system (BPCS) and the risk reduction allocated to BPCS protection layers directly impact the risk reduction target for an associated safety instrumented function (SIF). Likewise, any common causes or dependencies between functions involved in a hazardous event initiation or the responding protection strategy can affect the residual frequency of the hazardous outcome. Finally, once a SIF is required by the H&RA, the specification of performance requirements for the SIS performing the SIF must be sufficiently clear that the system is designed and implemented correctly, resulting in a demonstrated performance consistent with the safety integrity level (SIL) the H&RA assumed.

All three of these concepts were addressed in ANSI/ISA 84.00.01. However, a few years after this standard was published, comments submitted by experienced personnel revealed that further clarification would be needed in the new edition.

2.1 Limits on BPCS failure frequency and target risk reduction

Submitted comments on IEC 61511-1:2003 and ANSI/ISA 84.00.01 revealed that the previously existing two clauses (9.4.2 and 9.4.3) were not sufficiently clear in expressing the limitations that had been intended by the committee:

a) Minimum assumed frequency of a BPCS failure (whether referring to the system as a whole or to just one part thereof) that could initiate a hazardous event
b) Maximum risk reduction that could be claimed for a protection layer within the BPCS
c) Maximum number of protection layers that could be executed within the BPCS for a given hazardous events
d) Requirements for independence for protective layers executed within the BPCS

These limitations reflect the overall performance impact associated to the less rigorous design, implementation, and management practices typically applied to the BPCS (as compared to those used to manage the SIS). The recognition that the BPCS had a limited capability to provide risk reduction for process safety incidents had been documented in the first edition of CCPS *Guidelines for Safe Automation of Chemical Processes* [7], published just after the OSHA PSM standard was issued. Further guidance was provided a few years later in CCPS *Layer of Protection Analysis: Simplified Process Risk Assessment* [8]. Reinforcing and building upon these original positions, additional technical guidance was provided in CCPS *Guidelines for Safe and Reliable Instrumented Protective Systems* [9] and *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis* [10]. The values provided in ANSI/ISA 61511 for each of limitations listed above reflect the long-standing experience of overall BPCS performance that is documented in these industry consensus publications.

2.2 Requirements for claiming RRF>10,000 in total for instrumented safeguards

The verification, validation, and change management practices documented in ANSI/ISA 84.00.01 were designed to keep the probability of systematic error relatively low for a given safeguard. However, once the overall risk reduction for the BPCS protection layer(s) and SIS(s) exceeded 10,000 (i.e., equivalent to 4 orders of magnitude in LOPA), the impact of systematic error could no longer be considered negligible in the evaluation of risk reduction achieved. ANSI/ISA 84.00.01 addressed these issues for a single function in a clause on the requirements for a SIL 4 SIF.

However, even when the risk reduction allocation is spread over multiple protection layers with independent primary safety system devices (sensors, logic solvers, final elements), common personnel are often used to program, operate and maintain the instrumented safeguards. Likewise, internal process and external environmental impacts on the reliable operation of instrumentation can impact multiple instrumented functions. ANSI/ISA 84.00.01 included requirements to address common cause and dependent cause failure between all protection layers, as well as with the BPCS that could initiate a demand on those protections. Where multiple instrumented safeguards provided an overall risk reduction of 10,000, all the issues noted in the clause on SIL 4 SIFs would

be applicable to the required common cause analysis. Making it easier to recognize the technical interaction of the ANSI/ISA 84.00.01 clauses, the SIL-4 clause in ANSI/ISA 61511-1 explicitly addresses the case where the risk reduction of 10,000 is spread across multiple instrumented safeguards.

2.3 SRS clarity and traceability

Experienced users of ANSI/ISA 84.00.01 reflected that the safety requirements specification (SRS) and the instrument selection justification for SIS are sometimes written in highly technical language that may not be maintainable, verifiable, or even understandable by operations and maintenance, but which nevertheless were considered compliant with the standard. For example, it could not always be determined that the information used in the instrument selection and system design was even relevant to the operating environment for that installation. As is the case with any other engineering document, clarity and applicability of this information is essential to achieving and maintaining the expected performance of the resulting system, including supporting nearly inevitable management of change. ANSI/ISA 61511-1 requires clarity and traceability of all the assumed parameters back to the SRS, H&RA, and operating environment, not just the application programming as was already required in ANSI/ISA 84.00.01. The requirement for clarity and traceability reflects the automation systems engineering reality described above and supports the OSHA PSM expectation that the compilation of process safety information enables "the employer and the employees involved in operating the process to identify and understand the hazards".

3 Detailed Design and Engineering

Most of the current SIS hardware requirements have origins in the original standard from over two decades ago. However, some of the design and engineering clauses in ANSI/ISA 84.00.01 were unnecessarily complex. Design and engineering change themes implemented in ANSI/ISA 61511-1 sought to relocate or reword these more complex provisions to make them easier to understand and simpler to incorporate into a design. Being a standard addressing instrumented safety systems, design and engineering provision changes also needed to be made to reflect the ongoing evolution in industrial automation and control system technology.

3.1 Application programming provision relocation

When they were added to IEC 61511-1:2003, the set of new provisions related to SIS application programming were gathered together in clause 12. For simplicity of adoption into ISA, this structure was unchanged in ANSI/ISA 84.00.01. With the rest of the document being structured in the order of the safety lifecycle, however, this separation let to confusion regarding when the application programming activities were to take place during the execution of a project. In addition, some of these activities would typically impact both the hardware and application program design or implementation, requiring careful coordination. In ANSI/ISA 61511-1, a significant number of application programming provisions were relocated from clause 12 to provide clearer guidance on when the activity should be executed. For example, application program safety requirements have been incorporated into the main SRS requirements to emphasize

the need for a close relationship between the SIS SRS and the application program safety requirement development.

3.2 Hardware fault tolerance

Prescriptive hardware fault tolerance (HFT) limits were added in the previous edition of the standard to mitigate some of the more common design and implementation systematic failures:

a) Using overly optimistic reliability parameter assumptions
b) Maintenance error such as leaving a root valve closed or a bypass jumper in place

However, the complex rules, which had been derived from the original edition of IEC 61508-2 [11], were themselves subject to systematic error and differences of interpretation. The basic HFT requirements in ANSI/ISA 61511-1 are simplified, adapting one of the second edition IEC 61508-2 [12] approaches in a manner that better supports implementation using prior use justification of SIS field devices within the process sector.

3.3 Fault detection, bypassing, and compensating measures

One common underlying SIS design assumption is that a SIS device will be out of service due to bypass or detected failure for a limited time and that compensating measures will be used to manage any gap in risk reduction during that time. This expectation is closely aligned to the OSHA PSM requirement that the employer "correct deficiencies in equipment that are outside acceptable limits…before further use or in a safe and timely manner when necessary means are taken to assure safe operation." ANSI/ISA 84.00.01 addressed this concept in a series of provisions that stated the requirement in a different way depending on the architecture of the subsystem that was degraded. User observations from a decade of application of this standard exposed a lack of clarity regarding the requirement of managing known periods of SIS unavailability or degraded performance while the equipment the SIS was designed to protect remained in operation. The two clauses in ANSI/ISA 61511-1 that require compensating measures to maintain safe operation when a dangerous fault in the SIS is detected or when the SIS is bypassed are stated in a simpler manner than in the prior edition.

3.4 Cybersecurity for SIS

With continued occurrences of successful cyber security attacks against industrial control systems and more frequent installations of SIS with digital communication to other devices, cybersecurity needed to be incorporated into the updated SIS standard. To avoid unnecessary overlap with the ANSI/ISA 62443 [13] series of standards on network and system security for industrial communication networks, ANSI/ISA 61511 contains only two new clauses on this topic. The first requires a security risk assessment to be performed that included the SIS. The second clause requires the SIS be designed to provide the necessary resilience against the identified security risks. Located in the risk analysis and detailed design sections of ANSI/ISA 61511-1, these two clauses are "anchors" that can help the user understand how the ANSI/ISA 62443 activities should fit into the functional safety lifecycle.

4 Operations and Maintenance

As noted above, a primary change theme behind the new content in ANSI/ISA 84.00.01 was the incorporation of functional safety management requirements. Most of these have very clear relationships to OSHA PSM requirements, with technical details added appropriate to the nature of instrumented safety systems. However, over time it became evident that the topics of existing systems, change management, and periodic performance assessment were still systematically confusing to some users of the standard.

4.1 Existing systems

Addressing systems that predated the standard has been incorporated into all editions of the SIS standard. This concept is sometimes referred to as "grandfathering". In ANSI/ISA 84.00.01, the provision on existing systems had been located in the scope section of the document. This led to a misunderstanding that none of the functional safety management requirements would apply to such systems. Such a misunderstanding would have also been inconsistent with the expectations of OSHA PSM as well. In ANSI/ISA 61511-1, the clause on existing systems is relocated into clause 5, to clarify that the ongoing management of systems that predated the standard is part of functional safety management and that only the hardware and application programming (i.e., the SIS) were intended to be "grandfathered".

4.2 Change management

As part of the process safety information defined in OSHA PSM, the SIS and other safeguard systems and all documentation related to it were already subject to change management in the U.S, inclusive of the H&RA itself. Since existing SIS tend to be changed piece by piece, however, further clarity was needed in clauses 5 and 17 on how to handle such changes using the functional safety management activities, such as system verification and validation. This includes changes that affect the requirements on an existing SIS.

4.3 Performance metrics and quality assurance

A common concern in SIS design is the use of overly optimistic data or data that is not applicable to the operating environment the SIS will be used in. However, even if data and assumptions appropriate to a given operating environment are used in the initial SIS design, variations in the performance of the process, operations, maintenance, and automation management systems over time can result in poor system performance and inadequate risk reduction. The only way to correct for these systematic errors and restore the necessary performance is to collect performance data on an ongoing basis, periodically assess for conformance to the H&RA and SRS requirements, and correct deviations as needed. The expectations of performance monitoring and quality assurance are consistent with basic process safety management practices (e.g., USA CFR 1910.119(j), COMAH, DSEAR).

5 Conclusion

The SIS standard began alongside the origination of process safety management regulation. ISA S84.01 evolved from a document focused primarily on hardware management to the well-rounded ANSI/ISA 84.00.01 standard addressing both the hardware and human side of functional safety management. ANSI/ISA 61511-1, the third stage of evolution of the SIS standard, strives for continuous improvement in the global use of its long-established requirements. The changes between ANSI/ISA 61511-1 and the previous edition contains updates primarily intended to create more consistent understanding and application of previously existing provisions. The major themes of change address topics such as risk reduction allocation between instrumented safeguards, prescriptive design requirements for HFT, managing risk during bypass or failure of safety system devices, and the need to "close the loop" on functional safety performance to ensure the overall control and safety systems are delivering the performance assumed in the H&RA and SIS design. Finally, in keeping with the technological advances in automation systems, ANSI/ISA 61511-1 includes crucial cross-ties to cybersecurity requirements that make the SIS more resilient to malicious attack.

6 References

[1] ISA. 1996. Application of Safety Instrumented Systems (SIS) for the Process Industry. ANSI/ISA S84.01-1996. Research Triangle Park, NC: ISA.

[2] U.S. OSHA. 1992-2018. Occupational Safety and Health Standards: Process safety management of highly hazardous chemicals, 29 CFR 1910.119. Washington D.C.: OSHA.

[3] IEC. 2003. Functional safety: Safety instrumented systems for the process industry sector - Part 1. IEC 61511. Geneva: IEC.

[4] ISA. 2004. Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1. ANSI/ ISA-84.00.01-2004. Research Triangle Park, NC: ISA.

[5] IEC. 2016 + AMD1:2017. Functional safety: Safety instrumented systems for the process industry sector - Part 1. IEC 61511. Geneva: IEC.

[6] ISA. 2018. Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1. ANSI/ISA-61511-1-2018. Research Triangle Park, NC: ISA.

[7] CCPS. 1993. Guidelines for Safe Automation of Chemical Processes. New York: AIChE.

[8] CCPS. 2001. Layer of Protection Analysis: Simplified Process Risk Assessment, Concept Series. New York: AIChE.

[9] CCPS. 2007. Guidelines for Safe and Reliable Instrumented Protective Systems. New York: AIChE.

[10] CCPS. 2014. Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis. New York: AIChE.

[11] IEC. 2000. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - Part 2. IEC 61508. Geneva: IEC.

[12] IEC. 2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - Part 2. IEC 61508. Geneva: IEC.

[13] ISA. 2009. Security for Industrial Automation and Control Systems. ANSI/ISA-62443. Research Triangle Park, NC: ISA.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Process Safety Time Analysis for Upstream Facilities

Anupa Beharrysingh, M. Hernandez, C. Ng, C. Maher
Fluor Cooperation,
Sugar Land, TX, 77478.
Emails: anupa.beharrysingh@fluor.com, manuel.hernandez@fluor.com

Keywords: Process Safety Time, Upstream, Safety Instrumented Function

Abstract

Per IEC 61511-1 Process Safety Time is defined as, "the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed".

This paper will discuss how Process Safety Times were categorized, evaluated, and verified in order to comply with the standard and on a upstream mega project containing over 580 Safety Instrumented Functions, 350 of which were rated SIL 1 or higher.

In the past, the practice has been to assign general overall values to Process Safety Times, many times for an entire project or possibly for individual units in a process facility. On our recent mega project, our client challenged the engineering team to develop more customized values based on individual processes. Our expectation is that in the future this expectation will grow more stringent and focused. Our control systems and process engineering teams will have to work together to develop the necessary work processes and methods to generate, justify, and report these critical time values.

Definitions

Per IEC 61511 Part 1 Section 3.2.52.1, Process Safety Time is defined as, "the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed".

Per IEC 61508-4, Section 3.6.20, Process Safety Time is the period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring.

Therefore, Process Safety Time is essentially; the time from an initiating event to the occurrence of an incident.

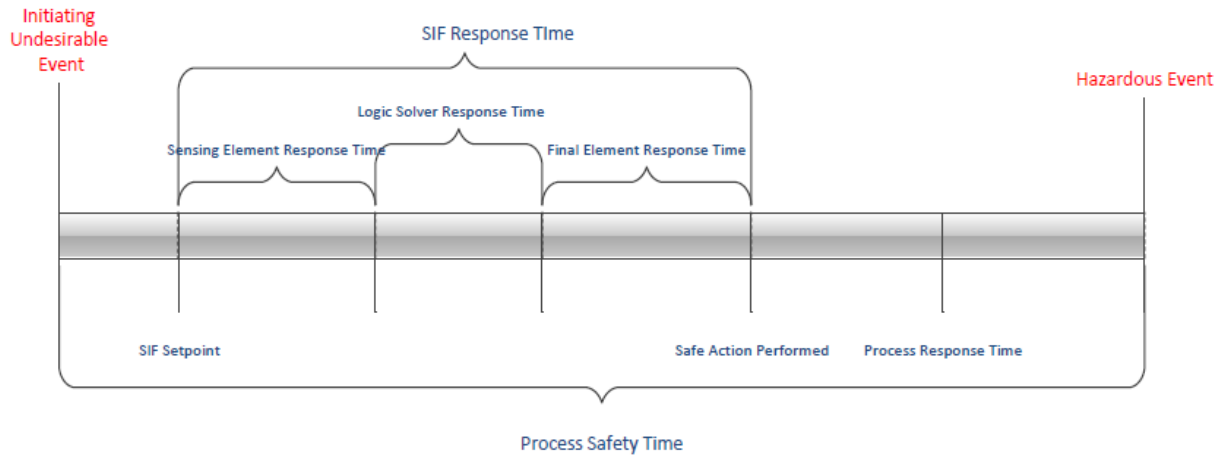


Figure 1.0: Process Safety Time Timeline

IEC 61511-1 Section 3.2.57 defines a protection layer as, "any independent mechanism that reduces risk by control, prevention or mitigation." The intent of Process Safety Time, PST analysis is to ensure that the SIS protection layer is successful at preventing the imminent hazard.

IEC 61511-1 Section 10.3.2 states the following as a SIS safety requirement: "response time requirements for each SIF to bring the process to a safe state within the Process Safety Time."

The response time for a SIF will be from detection at the sensor to completion of the final element action. After the final elements have completed their actions, there is a time for the process to respond to the actions before reaching a safe state. This is referred to as the Process Response Time.

The project was committed to demonstrate compliance with IEC 61511-1, Section 10.3.2.

For the assurance of a safe design as well as for compliance with the IEC standard, SIF-RT and PRT as well as safety margins are all considered and summed to ensure that the SIF reacts within the PST.

Process Safety Times are required to be considered for all independent protection layers, not only for safety instrumented functions. When considering the implementation of an alarm, for example, there must be an associated expected time frame in which an operator response or intervention to the alarm is required in order for it to be effective. Similarly with PSVs, these devices are sized and set at a pressure to allow mitigation of system over-pressure / rupture.

The analysis this paper will discuss focuses on Process Safety Times applicable for safety instrumented functions.

PST for a SIF is required to be defined / provided in the project's Safety Requirements Specification, but little direction is provided on how it should be assessed.

Roles and Responsibilities

On a project, PST analysis is a joint effort among a number of responsible parties. These include the client, who will assume ownership and ultimate responsibility for the safe operation of the facility; the General Contractor, who has responsibility for the safe design of systems for the facility; the Main Automation Contractor, who has responsibility for implementation of control and safety related items; and, on occasion, third party vendors who supply packaged systems for the project.

The Client will supply or approve project specifications to be used by the General Contractor, and others, in the development and design of the facility. The Client may have a core group that directs and coordinates project activities on a wide range of projects and may participate in development of and/or approve Process Safety Times developed by an individual project. The client may also supply discipline engineers to oversee specific projects on an ongoing basis. The assigned client engineers may include a control systems engineer and a process/facility engineer. Additionally, client operations personnel from a specific facility may participate in the review and approval of Process Safety Times based on actual facility operating experience.

The General Contractor will bear the overall responsibility for development of a Safety Requirements Specification and for the establishment of Process Safety Times on a project working with an inter-discipline team of process, control systems, and mechanical engineers.

The MAC is tasked with implementation of the Process Safety Times in the MAC supplied hardware, configuration, and programming based on project supplied design documents. Software Acceptance Testing will demonstrate that the required Process Safety Times in the configuration and programming align the provided design documents.

Third party vendor documents will be consulted and evaluated as required to ensure that any Process Safety Time associated with a third party vendor package is capable of meeting the required Process Safety Time.

Project Methodology

After HAZOP, LOPA and SIL assignments for the project were completed, the resulting number of SIFs were 580, 350 of which were rated SIL 1 or higher. Given the number of SIFs which required PST evaluation and the schedule for confirming / finalizing process limits and set-points, the project was tasked with developing a method of PST evaluation to identify and

mitigate any deficiency finding within the project timeframe while still complying with the IEC 61511 standard.

The general practice in the past regarding evaluation or Process Safety Time has been based on generally assigning a maximum operating time for shutdown valves. A project might set a value to cover all shutdown valves regardless of size or process, or there may be varying values established on valve size, with larger valves being assigned a longer operating time than smaller valves. Once these times were established it was up to control systems engineering personnel to specify the correct shutdown valves and auxiliary equipment necessary to meet the established operating times. This might mean having to procure a quick exhaust solenoid valve to allow the valve to move to its safe position in the specified time frame.

As the Process Safety Time practice evolved, process engineers based the times on a system response to process pressure, temperature or level disturbances or upsets.

The project developed a document "Process Safety Time Analysis – Charter" which dictated how the Process Safety Times were to be categorized and evaluated with their associated SIF response time in order to demonstrate compliance.

The document first set the scope boundaries for assessment. All SIFs with a SIL rating of SIL 1 or higher would require PST evaluation. This prioritized the PST assessment and reduced / avoided overloading with non-critical items. Also, no mitigative SIFs would be evaluated (Fire & Gas).

SIFs which were part of a standard vendor supplied package would not be evaluated, as these SIFs would be regarded as 'proven-in-use', provided that the vendor(s) supplied these standard packages for many years and had done their own process safety evaluations.

The document identified the responsible engineering disciplines: Process and Control Systems, where Process engineers were responsible for calculating the Process Safety Times and Control Systems would be responsible for calculating the SIF Response Times.

The document defined the methodology for Process Safety Time evaluation. All SIFs were initially screened and identified as either time critical (PST<60s) or non-time critical (PST>60s). SIFs with a PST>60s underwent a qualitative analysis with a descriptive assessment only. The time critical SIFs (PST<60s) were classified as requiring additional quantitative analysis. This was done based on system configuration and a steady state model.

In each case the hazard cause would be aligned with the cause documented in the HAZOP and SIL assignment reports.

To meet the demands of project schedule and finalize the design, areas of the process were segregated and prioritized for analysis. Process Safety Time analysis would then be performed in order of priority as SIL assignments were completed.

Typical SIF-RTs for each type of sensor, logic solver, and final element were determined and tabulated. These times were then utilized to calculate the overall SIF-RT for each SIF with a SIL assignment greater than or equal to SIL 1.

The end result was a deliverable listing each SIF (with a SIL assignment greater than or equal to SIL 1) along with its associated hazard cause, PST, and SIF-RT.

Process Safety Time Analysis Evaluations

PST calculations took into consideration design tolerances (short term temperature or pressure excursions) allowed by ASME / API codes. Pressure excursions were modeled / analyzed to the PSV set-point. This served to validate the SIS and the physical pressure relief as an independent protection layer.

Of note, low pressure trips are typically used to mitigate against line ruptures or leaks (loss of containment scenarios). In these cases, as the hazardous event has already occurred, no Process Safety Time analysis was done on low pressure safety instrumented functions.

Process Safety Time calculations involving level measurement took into account overflow at full flow rates for HiHi trips and underflow at zero flow rates for LoLo trips.

For pump and compressor trips, rundown times may need to be considered if they allow for hazard escalation.

Project Considerations

What if the PST is less than the SIF-RT? The project considered the following options in order of cost and timing in effort to mitigate the deficiency.

- Review the PST calculation and the assumptions which contributed to the PST calculation.
- Consider altering the trip set-point of the input sensor; for example, raising the LoLo level set-point can give more liquid volume. Lowering a HiHi pressure set-point will provide more of a pressure cushion before reaching overpressure.
- Consider the addition of a quick exhaust solenoid valve to the actuator. In some instances the main contributing factor to the SIF response time is the closure of a safety shutdown valve. In one instance the project was able to reduce the SIF response time by adding a quick exhaust solenoid to an 8” safety shutdown valve. This addition reduced the final element response time from 8s to 2s.
- Consider the possibility of an additional or alternative IPL to the SIF.
- Re-validate / evaluate LOPA scenario.
- Another alternative and last resort was to consider the addition of logic to prevent or mitigate the cause of the scenario. For example, the PST for overpressure on the production header was calculated to be 1.8s. As commitments for a production rate were already made, altering the HiHi pressure trip set-point was not an option. Per the HAZOP report the initiating cause of the potential overpressure scenario was documented to be the failure of a 30” safety shutdown valve.

An advanced warning for the failure of the 30" safety shutdown valve was considered using the safety shutdown valve limit switches which were wired to the SIS. If the limit switches for the valve read that is was travelling un-commanded by the SIS, then the final elements which were required to go to the safe state as part of the overpressure SIF would actuate. By doing this an advanced warning of the failure of the SDV was essentially created and the SIS was programmed to act in the same manner as if the HiHi pressure on the production header was realized.

Summary

There is a general rule of thumb which suggests that the SIF-RT be less than or equal to half of the Process Safety Time; however, as the PST calculations were done to the PSV set-point and not to the time of occurrence of the unwanted event, this rule of thumb was not applied.

At the end of the exercise, despite PST's as low as 1.8s, the project was able to demonstrate compliance with the IEC 61511 requirement for each SIF with a SIL rating of SIL 1 or more.

The development of this integrity critical document required collaboration from multiple groups: Process and Control Systems engineers, Clients, Mechanical package engineers / vendors, Safety engineers, and Subject Matter Experts.

Safety consideration in the process industry must progress continually to ensure safety of people and the environment. The evolution of the evaluation and implementation of Process Safety Time is an indication of how the industry engages in the process of taking standards and guidelines and developing them into the engineering process and final construction. Putting safety first profits everyone involved from the client, the engineering and construction contractors, the public, and the environment. Operating experience will help refine the process of developing the Process Safety Times for future projects.

Abbreviations

Abbreviation	Description
HAZOP	Hazard and Operability Analysis
EUC	Equipment under control
HiHi	High High
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LoLo	Low Low
LOPA	Layer of Protection Analysis
MAC	Main Automation Contractor

Abbreviation	Description
PRT	Process Response Time
PST	Process Safety Time
PSV	Pressure Safety Valve
SDV	Safety Shutdown Valve
SIF	Safety Instrumented Function
SIF-RT	Safety Instrumented Function Response Time
SIL	Safety Integrity Level
SIS	Safety Instrumented System

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Successful Implementation of Hazards and Effects Management System in Capital Project

Divya Narayanan, Jiaqi Zhang, Alok Khandelwal
Shell International Exploration & Production, Inc.
Shell Technology Center
3333 Highway 6 South, Houston, TX 77082
Emails: D.Narayanan@shell.com, Alok.Khandelwal@shell.com

Keywords: HEMP, ALARP, Capital Project, Safety Case Asset Integrity

Abstract

Tiger AO4 Project delivers a competitive Linear Alpha Olefins (LAO) project at Geismar in 2018, recovering 100 kta of "stranded" LAO capacity in the Geismar Chemical Plan and contributes an additional 716 MMlbs/year of LAO to the Shell LAO Capacity. This paper elaborates the successful implementation of Hazards and Effects Management Process (HEMP) in Tiger AO4 project through design, procurement, construction, commissioning, startup, and operation. During the design process, the key processes include hazard identification, risk assessment, risk management to ALARP (as low as reasonably possible). It also covers the technical integrity verification process during the procurement, construction, commissioning, and startup., this paper explains the processes of incorporating HSSE critical activities (*e.g.* inspection, maintenance, surveillance, operator response, operating procedure steps, *etc.*) with current Geismar management system. At last, this paper also describes the development and operationalization of the Safety Case.

INTRODUCTION

Project Tiger AO4 will add a new Linear Alpha Olefins (LAO) at the Geismar Chemical Plant using Shell Technology. When completed, it will make the Shell Geismar site the largest alpha olefins producer in the world. Alpha olefins are used to produce household detergents, plastics, synthetic lubricants, and drilling fluids, among other useful products. The AO4 Unit will use ethylene as feed stock and produce full range of Linear Alpha Olefins.

The paper documents the effective application of the Hazards and Effects Management Process (HEMP) during the design, fabrication, and construction of the facilities under the scope of the AO4 Project (referred to as Project hereafter).

HEMP OVERVIEW

The Hazards & Effects Management Process (HEMP) is the process by which the Project identifies and assesses hazards, implements measures to manage them, and demonstrates that their risks are reduced to a level that is As Low As Reasonably Practicable (ALARP). This paper gives an overview of how the Hazards and Effects Management Process (HEMP) has been implemented on the Project to identify, assess and manage risks to ALARP.

The HEMP included the following:

- A robust Hazard Identification Process to identify the full range of hazards applicable to the operation of the facilities designed and constructed by the Project
- Appropriate risk assessment tools to assess the risks associated with the identified hazards
- Implementation of effective and valid controls to reduce the risk to ALARP.
- Defining operation and maintenance activities for effective management of Major HSSE Hazards to ALARP risk levels.

See Figure 1 for an overview of the HEMP process.

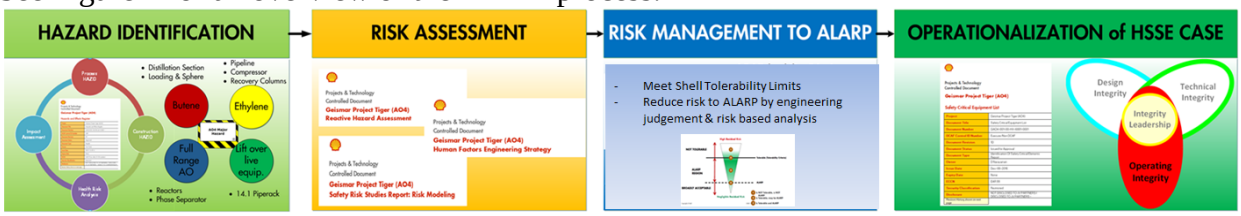


Figure 1. HEMP Overview

HEMP in Project

Hazard Identification and Risk Assessment

Hazard identification and risk assessment were done through a series of studies such as the HAZID (Hazards Identification), HAZOP (Hazards and Operability study), RHA (reactive hazards analysis), Consequence Modelling, layout assessment, health risk assessment and HFE (Human Factor Engineering) Screening. Also, Health, Security, Environmental Hazards and social aspects were identified through an Impact Assessment. The risk ranking is based on the established Shell Risk Assessment Matrix (RAM), which accounts for the likelihood and severity of consequences associated with the hazards.

A Hazards and Effects Register was developed which is a compilation of all AO4 process and construction hazards, along with the source of the hazard, credible worst-case consequence, risk ranking and methodology for demonstrating ALARP.

Risk Management and ALARP Determination

AO4 Project selected the risk management methodology based on the severity and likelihood of the hazards. The risks were managed to tolerability criteria defined by the Project HSSE Premise. The tolerability criteria were in line with current industry practices. In addition, the Project drove the risks to ALARP, which was not a specific numerical quantity but was defined as the level of

risk reduction beyond which the cost of further risk reduction is grossly disproportionate to its benefit.

Figure 2 provides an overview of the Risk Management Methodology.

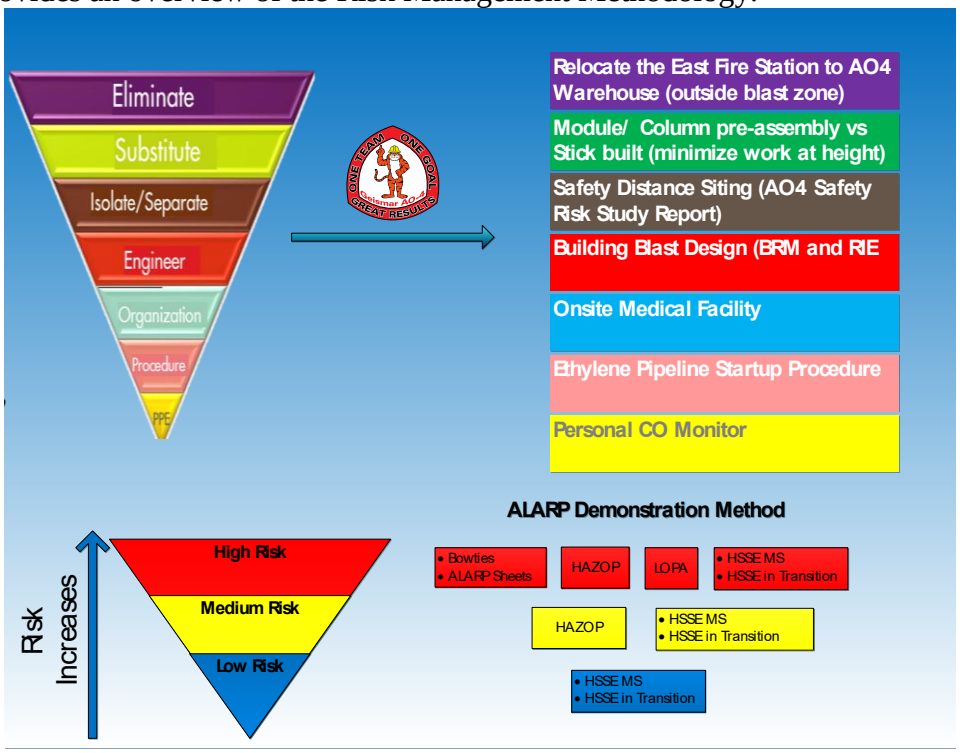


Figure 2. Risk Management to ALARP

- Low Risk Hazards: The Project managed hazards having low risks through the effective implementation of the Shell Project HSSE Management System
- Medium Risk Hazards: The Project managed hazards having medium risks through compliance to International codes and standards (i.e. ISO, API, ASME, IEC, etc.); and Shell DEPs (Design Engineering Practices). In addition, the Project identified and documented control and recovery measures for all scenarios associated with medium risks through the HAZOP study.
- High Risk Hazards: For each of the high-risk hazards identified in the Hazards and Effects Register, the Project demonstrated that the risk is tolerable through the LOPA exercise. The LOPA exercises focused on verifying whether previously identified Control and Recovery Measures (during the HAZOP) were sufficient to meet the Tolerability and ALARP criteria set for the project. Additional barriers were provided if the previously identified barriers did not meet the tolerability or ALARP criteria. Demonstration of ALARP involved an assessment of residual risk compared to project premises to determine whether sufficient controls are in place to manage the residual risk to an acceptable level and whether additional risk reduction options are reasonably practicable. Residual Risk is considered ALARP if further action is grossly disproportionate to the reduction in risk achieved. Hazard control sheets and bowties were developed to

summarize the risks associated with these major process hazards and provide an indication of how these risks have been managed to ALARP.

Implementation of HEMP in Design Phase

Results of various risk management studies were incorporated into the design of the AO4 unit. Here are a few examples:

- The results of consequence modelling were used in the development of the unit layout.
- The HFE requirements were included into the design and verified through 3D model reviews
- Design requirements were developed for barriers identified through HAZOP and LOPA studies to ensure their validity.

The control and recover measures for high risk hazards identified through LOPA, Safety Risk Studies and Application of Design Standards were considered safety critical barriers. The barriers were categorized into safety critical equipment, safety critical activities and other design features. For each of these categories, design performance standards were developed by the responsible disciplines to define the design performance criteria, and the assurance activities.

Implementation of HEMP in Construction Phase

Focused risk assessments were conducted to evaluate the risks and develop risk mitigation measures for the construction hazards identified in the project Hazards and Effects Register. These risk mitigation measures were incorporated into construction plans.

The integrity of safety critical equipment identified in the design phase was managed through various quality inspection test plans developed by the responsible disciplines to meet the performance criteria. Implementation of these inspection test plans were assured by field engineers.

Implementation of HEMP in Commissioning/Start-up (CSU) Phase

HEMP during commissioning and start-up focused on the simultaneous operation (SIMOPs) between construction and CSU activities. Focused risk assessments were conducted to evaluate the risks associated with the SIMOPs. The risk mitigation measures identified in these studies, such as demarcation, energy isolation, communication, were developed into SIMOPs checklists. Implementation of these SIMOPs checklists were assured by field engineers.

The integrity of safety critical equipment identified in the design phase was managed through commissioning procedures developed by the responsible disciplines to meet the performance criteria.

Operationalization of HEMP

The various AO4 Project HEMP deliverables were operationalized and integrated into the existing Geismar HEMP studies, such as the existing Geismar Hazards and Effects Register, facility siting study, consequence model, and HAZOP report. .

In addition, the integrity of safety critical hardware barriers identified in the design phase (HAZOP/LOPA studies) was managed through various Reliability Centered Maintenance

Process. The resulting inspection and maintenance activities and frequencies were incorporated into the existing Geismar management systems.

Operator actions/activities that were used as valid barriers in the HAZOP/LOPA Study for major hazard scenarios were considered as safety critical activity barriers. These activities/actions were incorporated into

- Operating procedures
- Operator response to alarms
- Surveillance/ Operator Rounds
- Emergency Response plans

Figure 3 shows the detailed process of operationalization of the safety critical barriers.

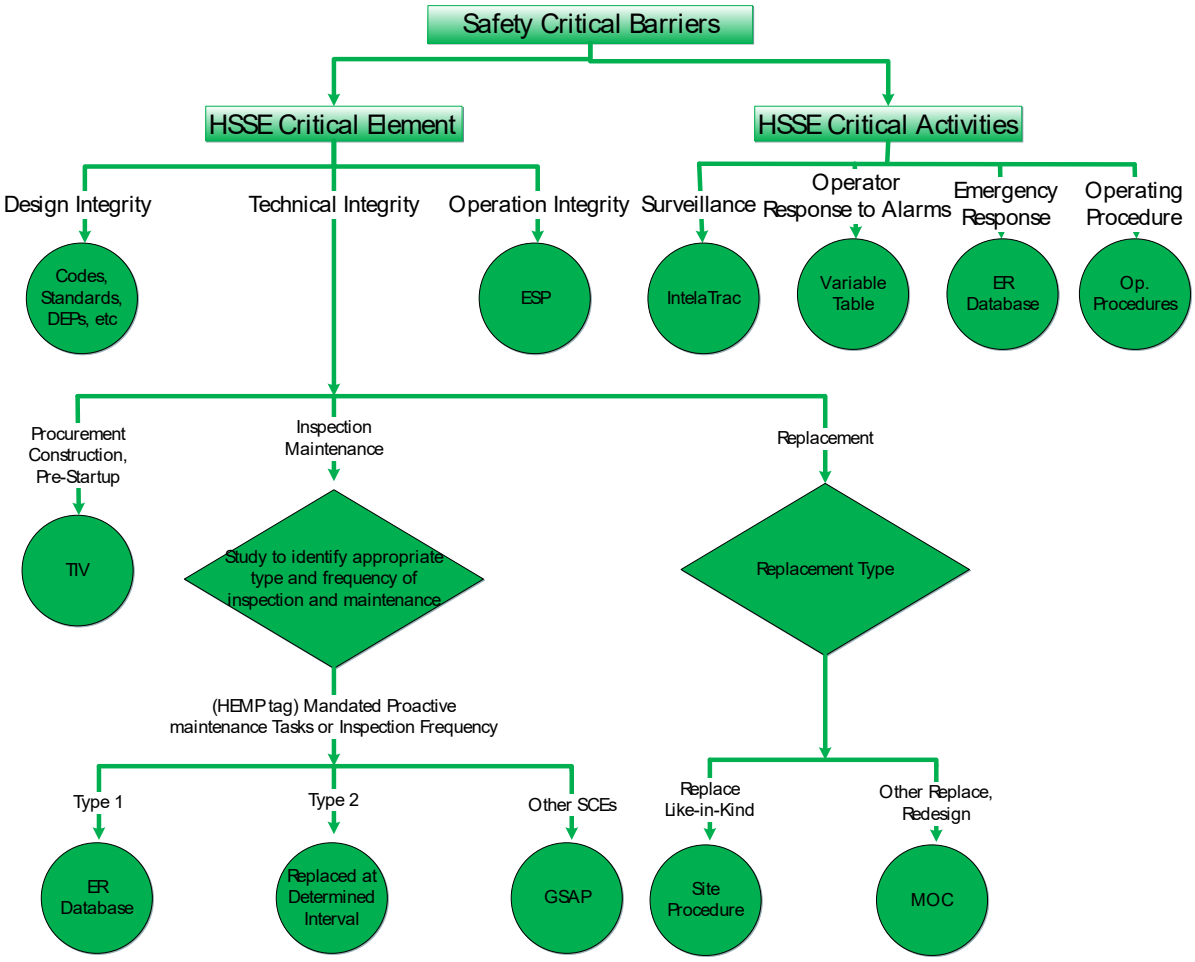


Figure 3. Operationalization of Safety Critical Barriers

Bow-tie diagrams showing threats and barriers associated with the major hazards were developed using the results of the HAZOP/LOPA Studies. These Bow-tie diagrams were used to train operators and to communicate to stakeholders:

- Major hazards and their location in the Unit
- Associated barriers installed

- Operator activities that are required to mitigate risks
- A link to processes that was used to maintain the integrity of the barriers during the operate phase

CONCLUSION

This paper elaborates the successful implementation of Hazards and Effects Management Process (HEMP) in Tiger AO4 project. The project recognizes that HEMP implementation is not effective if it ends with completion of risk management studies. The effectiveness can only be guaranteed if the integrity of the barriers identified through the studies is managed through the life-cycle of the project and the asset. The Project accomplished this by establishing work process to ensure the integrity of the barriers through design, procurement, construction, CSU, and operation. In addition, the Project did not considered HEMP as a standalone or single discipline work process; instead, made it an integral element of multiple discipline work process.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Sizing Rupture Disk Vent Line Systems for High-velocity Gas Flows

Dipl.-Ing. Mondie K. Mutegi*
Research Associate
[a]*CSE Center of Safety Excellence (CSE-Institut)*
Joseph-von-Fraunhofer-Str. 9, 76327 Pfinztal, Deutschland

Prof. Dr. Jürgen Schmidt[a], Prof. Dr. Jens Denecke[a], Dr. Stefan Rüsenberg[b]
[b]*REMBE® GmbH Safety + Control*
*Presenter Email: mondie.mutegi@cse-institut.de

Abstract

In the chemical and petrochemical industry, vessels and pipes are protected against overpressure using safety relief devices, usually rupture disks (also called a bursting disc) or safety valves installed in a vent-line. Proper sizing of rupture disk vent-line system involves fluid dynamic coupling of the rupture disk device and the entire vent-line with all its fittings. Sizing requires correct consideration of the fitting's and piping's minor loss coefficients to determine of the pressure drop and dischargeable mass flow rate. A fitting's minor loss coefficient is typically determined under low-velocity and incompressible flow. It is however not precisely applicable for all plausible flow cases that occur in practice especially for high-velocity compressible gas flow, two-phase flow, flashing liquids or multiphase service without proper consideration of compressibility. Experiments show that rupture disk irreversible pressure drop, determined assuming a constant minor loss coefficient, with current methods is underestimated by at least 30% for high-velocity compressible gas flow. This is because the compressibility is not accurately considered there and the pressure profile calculated this way is faulty.
This work presents a scientific method to calculate the pressure profile and dischargeable mass flow rate in a vent-line system with a rupture disk installed seamlessly. The pipe and rupture disk loss coefficients are enhanced to factor compressibility fully. Experiments show that this method predicts the pressure profile along a vent-line with a rupture disk installed and the dischargeable mass flow rate better as compared to current methods. The method is applicable for both low-velocity and high-velocity compressible gas flow as is typically the case during pressure relief.

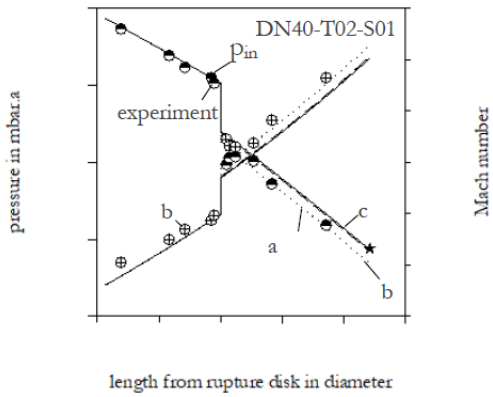


Figure 1 Predicted pressure profile a rupture disk (low-velocity flow)

a: New-theory b: (Levenspiel, 1998) c: (ASME, 2014)

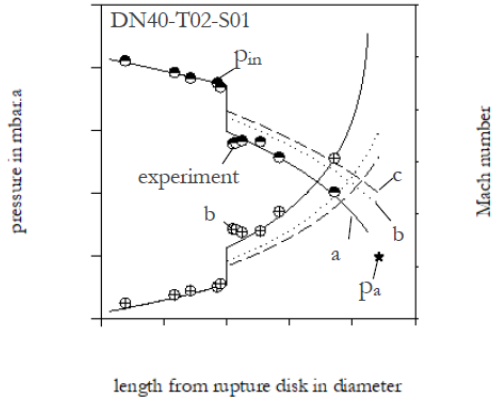


Figure 2 Predicted pressure profile a rupture disk (high-velocity flow)

Keywords: Rupture disk, Flow area, Minor loss coefficient, Pressure drop, Dischargeable Mass Flow Rate

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Development of a Company-Specific Consequence Severity Model to Improve Efficiency and Consistency in PHAs

Sam Aigen, Rich Santo
AcuTech Consulting Group
Emails: SAigen@acutech-consulting.com, RSanto@AcuTech-Consulting.com

Abstract

The consequence severity of hypothetical release scenarios developed during a Process Hazard Analysis (PHA) can be difficult to evaluate consistently. Even though most companies now have clear and concise consequence category descriptions for impacts to people, environment, assets, and business, PHA teams continue to struggle with determining the worst-credible consequence level(s). Such reasons include:

- Scenario has not occurred at the site, and is being ranked too low or too high.
- Scenario has occurred at the site, but with variable outcomes each time
- PHA team leader or team members influencing the ranking based on their experience/ judgment.

In the AIChE Center for Chemical Process Safety (CCPS) publication *Layer of Protection Analysis – Simplified Process Risk Assessment* (2001), a hypothetical model is presented in Chapter 3, as the "Category Approach without Direct Reference to Human Harm", and is presented as an example only. Developing and applying this model in a practical PHA team setting requires defining, refining and adjusting each consequence category to the facility's hazardous chemicals and risk matrix.
This paper describes adapting the hypothetical model from the CCPS LOPA book for a facility's use. This includes defining the consequence categories, working with/ modifying existing risk matrices, consequence modeling, interpreting the results, developing/ implementing the finished Consequence Severity tool, and the benefit to future PHAs.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Process Safety Fundamentals – Making Process Safety 'Real' in the Field

Graham McVinnie
Process Safety & Engineering Manager
Shell's Deepwater Gulf of Mexico operations.
Email: Graham.mcvinnie@shell.com

Abstract

Process safety management aims to ensure that all physical assets are well designed, safely operated and properly maintained. Process safety management is central to achieving Shell's Goal Zero ambition of no harm and no leaks across our operations. Shell's approach to achieving this combines our asset integrity principles with our risk management approach, which is based on the "bow-tie" model.

Continuous improvement in the management of hardware barriers and the robustness of human barriers is important to our overall risk management approach. Within the overall improvement trend, the number of technical integrity related events has significantly reduced. This suggests that operating integrity incidents make up an increasing fraction of process safety incidents, and, deeper process safety leadership and a different approach to behavioural change at the front line may be required to maintain improvement.

Analysis of operational integrity events in Shell identified that a small set of human barriers contribute to half of the releases and it is likely that the potential for these occurrences could have been reduced by people adhering to known good operating practices. From this analysis, a set of "Process Safety Fundamentals" were derived. The Process Safety Fundamentals were first rolled out across our Downstream Manufacturing Business. Building on the Manufacturing experience, and further incident analysis, an updated set of ten Process Safety Fundamentals are being rolled out across our businesses.

The ten Process Safety Fundamentals and the roll-out uses Hearts and Minds principles to engage the workforce and unlock process safety leadership at all levels. The Fundamentals aim to leverage the knowledge of a capable workforce, supporting them to apply known safe operating techniques.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Evergreening - Managing risk in the face of constant change

Allyson Ferriera
Process Safety Consultant
Siemens Oil & Gas Consulting
E-mail: alysson.takara@siemens.com

Abstract

Change is constant in processing facilities such as refineries and petrochemical plants. The drivers for change may vary from investment decisions, operational productivity initiatives, regulatory and compliance requirements, inspection and maintenance activities amongst other drivers. Every time a change is introduced to an operating facility, there is likelihood that risk is introduced to the facility if a strong management of change process is not in place or diligently adhered to. Over several changes, these risks compound which imperils the facility, its personnel and the community as a whole.

Evergreening is a structured program to manage a facility's process risk exposure in the face of incessant change. The program involves distinct steps defining, assessing, aligning, developing and executing change in a structured approach, leveraging well defined processes, facilitated by proper tools and executed by appropriate resources. Evergreening looks to frontload expert engagement in the change management process to ensure better outcomes while also giving the owner's opportunities for cost savings. This paper will review the practice of evergreening applied to pressure relief and flare systems with relevant examples and cases studies that validate the program.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Lifecycle Management of Risks with a Hazards Register

Jack Chosnek,
PhD PE

E-mail: jc@knowledge1.net

Abstract

From project inception to continuous plant operation a stream of safety studies will be conducted on the process, and the identified hazards will have to be either eliminated or reduced to an acceptable risk level. This risk level needs to be maintained at an acceptable level throughout the lifecycle of the plant. As changes occur and time passes the safeguards and protection layers start getting disconnected from the intent of the safety studies. This happens for many reasons but mainly because on proposing and implementing the layers of protection, the assumptions and intent made during the study are not explicitly attached to the specification of the equipment, instrumentation, or procedures. This is aggravated when the recommendations coming out of a study are implemented in a different manner as the recommended one or a totally different solution is adopted. Furthermore, the same equipment may be part of different safeguards in different studies.

A Hazards Register would contain all the pertinent information related to the risks assessed during all the safety studies performed by the company, whether a PHA, or a MOC review, or an incident investigation. The resolution of each hazard should be available in the Register, and not only the latest resolution but also its evolution (history) starting from the original study. In order to be effective, the Hazards Register should be easily accessible, be capable of simultaneous use by all plant personnel, have appropriate security, and be fully and effortlessly searchable. It should also automatically provide metrics that allow to manage outstanding recommendations and automatic recalculate relevant risk information (e.g., cumulative probability of failure on demand, pfd, from a LOPA study). It should be able to import data from any type of safety study and to export all or part of the data for other uses (e.g., instrument specifications). Such a system was successfully used in a very large project in which over 9,000 safeguards and their justifications were managed. At the end of the project the Hazards Register was transferred to the operating company for continued management of the process risks.

Introduction

Managing the risks of a process is a task that starts at the conceptual stage and continues throughout the design, startup, operation of the process, and decommissioning of the plant. Thus, we have to continuously manage the risks through the life cycle of the process. But the risks keep changing as we define in more detail the equipment and instrumentation of the process during the design, or introduce changes as a result of a desire for process improvement, or a change in operation. The nature and severity of the risks will also change when we analyze them and implement measures for either avoiding them, or minimizing or mitigating them. Whichever method we use for safety studies, we will start with identifying the hazards, defining a potential cause for a process deviation that will make the hazard become an event, determining the consequence of that event, and then we will identify what safeguards exist to prevent or mitigate the consequence. If we use risk-based process safety we will also want to describe the risk by assessing the severity of the consequence and the probability of that occurring given the identified safeguards. During the analysis we will make assumptions and develop some logic that supports the description of the found risk. We may want to reduce the risk and therefore we will recommend and implement additional safeguards. So, there is a lot of information that lets us understand the risk which then allows us to control it.
As time passes this information evolves and the basis for its creation becomes faint. This may lead to adding, modifying or removing necessary safeguards adopted from safety studies, as the reason for these safeguards being there is hidden or forgotten. Thus, a tool is needed for the long-term maintenance of the assumptions and logic for all the control schemes, instrumentation loops and equipment specs that make up the safety infrastructure of the plant.

The Evolution of Risk Assessment in the Life Cycle of the Plant or a Project

Any process design will undergo safety studies to determine the hazards of the process and the means to control them. Most of the time this is done through PHAs using many different methodologies. If the company practices risk-based process safety, this may be followed by a LOPA and/or a QRA, if the consequence level demands it. When performing the PHA oft times recommendations are made to mitigate the risk resulting from a given cause that leads to a specific consequence (we will call it a cause-consequence pair or c-c pair for short). The recommendation will generally propose adding or modifying safeguards (or even changing equipment to make that part of the process inherently safer). If a LOPA is performed in order to evaluate the risk in more detail, the same c-c pair may produce a more detailed safeguard, which can be an independent layer of protection (IPL) with its own rules [1, 2, 3]. Those rules will dictate, depending on the desired risk reduction and independence from other instrumented protections, a Safety Integrity Level (SIL) for the IPL. We then specify instrumentation that is part of a Safety Instrumented System (SIS) and which gets documented in the SIS archives of the plant. The same applies to a non-SIS layer of protection or safeguard, except that the documentation is in another place. This applies as well as to procedural (administrative) safeguards, where only the required actions will become a part of an SOP and their basis may not be documented in any place except for a PHA report. Unless we document very well the reason behind a layer of protection (and are able to find it at any time), we are destined to defeat it at some point in time.

A change in risk also occurs when a change in the plant occurs. The change will go through the MOC process and obviously an MOC safety study will be performed. In order to be successful, the safety study will need to review the hazards identified during the process' PHA, and the protections that were identified at the time, plus the mitigations recommended by the PHA team. In addition, the safety study will have to review any previous modifications of the equipment and instrumentation, that is, search the MOC database to see if any of the existing layers of protection are not impacted.

An additional challenge is that recommendations made by any of the teams, be it a PHA or an MOC (or an incident investigation), sometimes doesn't get executed as the team proposed, as a better solution may be implemented once there's more time to think and come up with a potentially better design. When this happens, chances are that the implementation will only refer to the PHA report, or MOC number, and there will be a disconnect between the cause of the event and the implemented solution. It is very common to create a new document in order to track implementation of the recommendations and this document will increase the gap between the implementation and the understanding of why the recommendation was needed.

The effect of all this is that, as time goes by, the process safety reason for a certain process configuration gets lost. A new safety analysis may totally miss the underlying safety need for that configuration as the need may have been identified a couple of iterations before and it may not be obvious at the present time. This gets complicated even more when there are interlocks that activate various valves (for example a plant shutdown) but one of the valves is also part of a control loop that has a different safety function (SIF) from that of the shutdown. The plant shutdown may be obvious after some analysis, but the other SIF may not be that obvious. At some point in time a decision could be made to reduce the SIL rating of the loop because it is unnecessary for the shutdown, but by doing this the risk reduction for the other safety function may be compromised.

It all depends how the safety documentation and the process documentation are interrelated. The following documents would need to be consulted for a proper risk estimation in case of a change in the process:

1. PHA report
2. MOC database
3. Safety study of the MOC (if not integrated into the MOC database)
4. Cause and Effect Table
5. Instrument list containing instrument specifications.
6. Incident investigation reports if there had been any incidents in the plant.
7. Action-tracking table to see if there are unimplemented safety recommendations.

And, of course, up-to-date P&IDs that reflect all the actual control schemes and other protections, be it SIS, DCS, or other.

All this information can be easily integrated in a Hazards Register, which is a dynamic database that can also serve as a tracking device for all safety recommendations. The Hazards Register ought to also include a historical record of all the resolutions that were ever made with respect to

safety studies or changes affecting safety systems. Such a database was created and its capabilities are described below.

The Hazards Register

The Hazards Register is a database with all the causes and consequences that were ever identified in a plant, including its grass-roots design project. These c-c pairs will have unique identifiers that will allow them to be tracked throughout the life cycle of the plant. In order to avoid errors created by compilation of data, all the data is imported directly from most commonly used PHA/LOPA software, or from any spreadsheets used in safety studies. The only required manual entries are the name, date and type of the source safety study (PHA, LOPA, MOC, etc.). If desired, additional information can also be entered, such as study team composition, remarks, etc., without limitations.

The data elements that the Hazards Register includes for each c-c pair are:

- C-c unique identifier (created automatically on entering the data by importing or otherwise)
- Source study name, type and date
- System (e.g. Operating Unit, plant area)
- Subsystem (e.g. Compressor system, Cold Box, Final Purification, etc.)
- Process deviation/keyword used in PHA for the c-c pair
- Consequence (Hazard)
- Cause
- Consequence severity level
- Type of consequence severity (e.g. economic, safety, environmental, etc.)
- Safeguards or IPLs
- Frequency of initiating event (LOPA)
- Frequency and type of enabling event (LOPA)
- Frequency and type of modification event (LOPA)
- PFD (Probability of Failure on Demand) for each IPL
- Probability (calculated from PFDs or entered from Risk Matrix)
- Risk (from risk matrix)
- Mitigated risk
- Reference (e.g. P&ID or other)
- PFD gap
- Recommendation or Action Plan
- Owner (for tracking purposes)
- Target date of implementation (for tracking purposes)
- Resolution (the latest resolution for the item will show, but all the resolutions from the beginning can be seen by clicking a button)
- New safeguards/IPLs resulting from recommendation(s)
- SILs of each of the new IPLs
- Final cumulative PFD (calculated automatically)
- Documentation description

- Status (open, closed, deferred, in progress, etc.). Milestones are defined by the user. Past due items, that is items not closed by target date, will show in red.
- Comments

That is, all the information contained in a PHA and LOPA plus some. A main table (see Fig. 1) is a list of the c-c pairs with all the data above and is fully searchable. If a c-c pair from a HAZOP, for example, which was imported into the program, was taken further into a LOPA which was then also imported into the program, the database will create a link between the two identical c-c pairs. At the click of a button you can switch between one and the other. All the data can be easily searched, filtered, sorted and exported. Excel spreadsheets and Adobe Acrobat reports can be created at the click of a button.
The main table will also automatically show statistics of all the table contents, both of those shown (after filtering) and of the total number of items. The statistics will reflect the milestones previously selected by the company (e.g., open, closed, in progress, deferred, etc.).

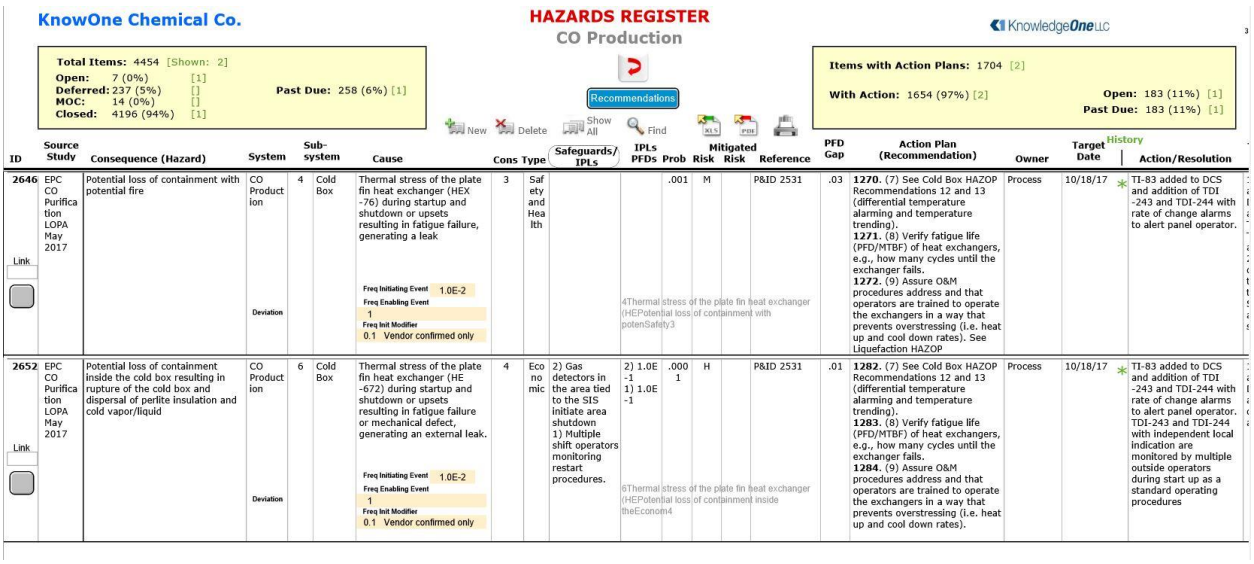


Figure 1. Hazards Register Main Table

Each c-c pair can be closely examined by clicking on the item ID which will take you to a detailed view as shown in Figure 2.

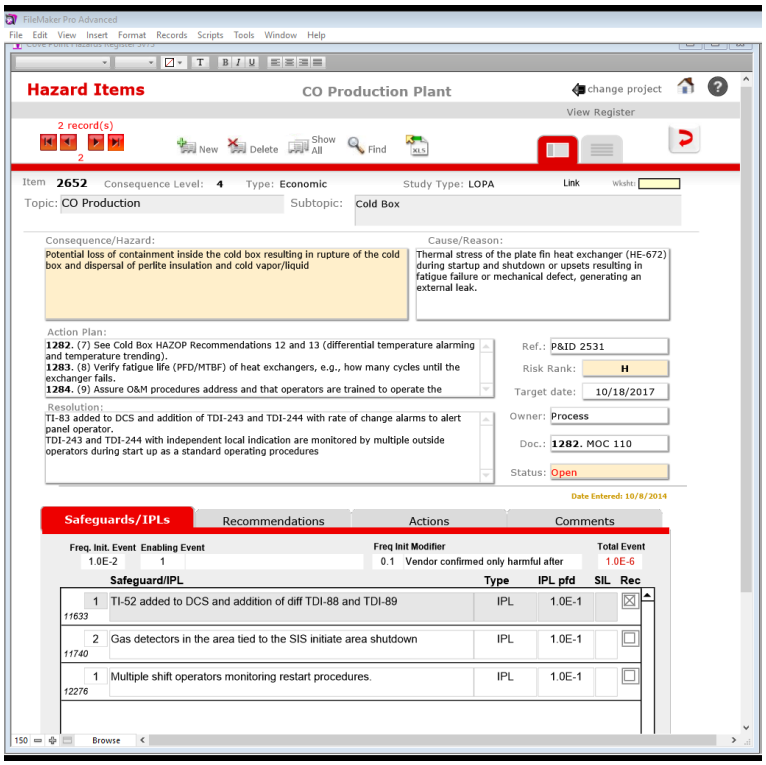


Figure 2. Item's Detailed View Showing Safeguards/IPLs

In this view, all the safeguards/IPLs can be seen and SIL values assigned. If a PFD has been entered, the program will calculate the cumulative (total event) PFD. If an IPL's PFD is changed, the cumulative PFD will be recalculated. If a safeguard or IPL came from a recommendation, it will be marked so, and it's possible to see the contribution of the recommendation to the total item's risk.

There are other views, of all the recommendations and actions taken for each recommendation (with dates and name of implementer), and of all the resolutions, which are the explanations of how item was finally resolved. There's a resolution for every item, even if a recommendation wasn't made and even more important, if a recommendation was not followed upon. Although the latest resolution is the one that will be shown in the main table, all the history of the item from day one is available by clicking on the history button. Thus, the evolution of the reasoning of why the resolution stands as it is, is available, as well the justification for all the safeguards and IPLs that are part of the current process configuration. When making a change, it will be immediately obvious why a certain protection is in place. If a protection is removed or a new protection is added, the program will recalculate the risk.

Another very useful part of the Register is a list of all the safeguards/IPLs with their PFDs and SIL values (Figure 3). This list can be easily exported to Excel and serve as the basis for creating or checking the plant's instrument list as well as inspecting and maintaining the Cause

and Effect table. Since it is fully searchable any instrument or device can be found, and its participation in more than one Safety Instrumented Function (SIF) at a time scrutinized.

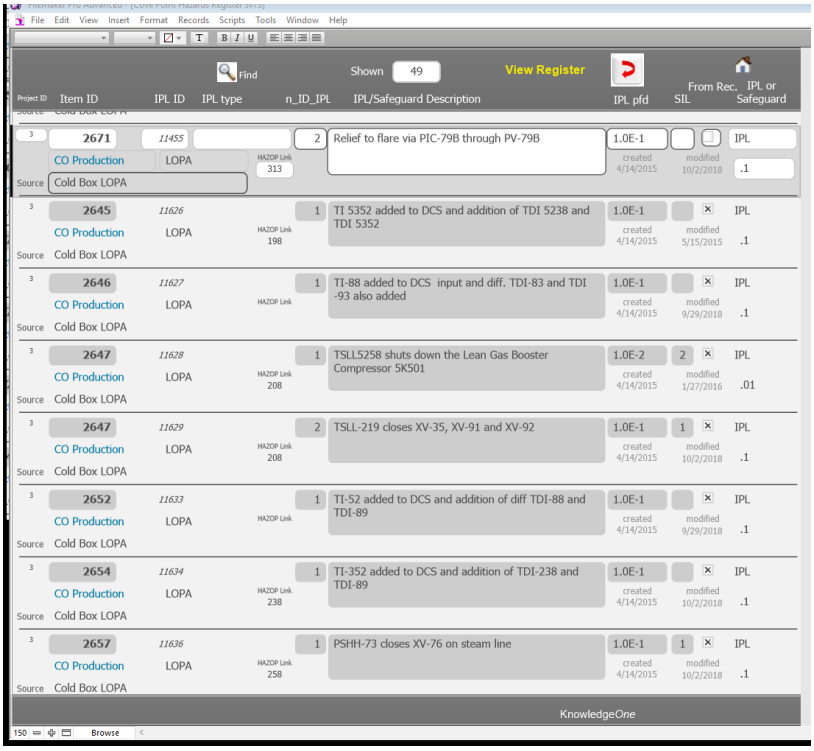


Figure 3. List of Safeguards/IPLs

In summary, the Hazards Register that was created maintains in one place all the hazards and related risks of the facility. The basis and reasoning for resolving the hazards through time is available since when the first safety study was imported. This is essentially in order not to forget the intent of an instrument or protection layer which could be later be changed, unintentionally increasing the risk of the facility. Since it resides in a database with simultaneous access to all, and is fully searchable, all the data can be easily found and continually used to maintain a safe design throughout the life cycle of the plant.

This Hazards Register was successful used in a very large EPC project ($4 billion) that lasted over three years. The database contained about 2,300 c-c pairs and 9,000 safeguards/IPLs and it was to track resolution of all these items. At the end of the project the data was incorporated in the new facility's information. The Register could be seamlessly transferred to the facility and continued to be used.

REFERENCE

1. CCPS, "Layer of Protection Analysis: Simplified Process Risk Assessment", October 2001.
2. CCPS, "Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis", November 2013.
3. CCPS, "Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis", February 2015.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

The Application of Bow Ties for a Robust PSM Program

Marisa Pierce and Tatiana Norman
DNV GL USA, Inc.
1400 Ravello Dr.
Katy, Texas 77449, USA
E-mails: Marisa.pierce@dnvgl.com, Tatiana.norman@dnvgl.com

Keywords: Barrier-based risk management, Bow ties, PSM, OSHA

Abstract

The fourteen elements of OSHA's Process Safety Management (PSM) program underpin so much of facility operations. PSM programs grow in complexity over time and can become increasingly disembodied from the operational elements that form their robustness. Often new PSM programs are modeled from organically grown existing programs rather than tailored to the specific risks of the operation introducing more than necessary complexity from the beginning. Barrier-based approaches can revitalize an existing PSM program or serve as a platform to build a simplified PSM program.

Bow ties reestablish direct connections to operations in a quickly visualized way transforming the perception of a PSM program from an operational albatross into an engagement tool to inspire ownership at all levels of the organization. This paper walks through each of the fourteen PSM elements highlighting the application and value of applying a barrier-based approach to the development or implementation of a PSM program.

Whether working with a robust PSM program that has become more complex over time or building a simple program based on the broad PSM concepts, bow ties can help a company focus their efforts on efficiently addressing deficiencies in their management systems and managing their most important risks.

Acronyms and Abbreviations

API RP	American Petroleum Institute Recommended Practice
BSCAT	Barrier Systematic Causation Analysis Technique
CCPS	Center for Chemical Process Safety
CFR	Code of Federal Regulations
EI	Energy Institute
HAZOP	Hazard and Operability
LOPA	Layers of Protection Analysis
MAE	Major Accident Events
OSHA	Occupation Safety and Health Administration
PHA	Process Hazards Analysis
PSI	Process Safety Information
PSM	Process Safety Management

Introduction

The fourteen elements of OSHA's Process Safety Management (PSM) program underpin so much of facility operations. PSM programs grow in complexity over time and can become increasingly disembodied from the operational elements that form their robustness. Often new PSM programs are modeled from organically grown existing programs rather than tailored to the specific risks of the operation introducing more than necessary complexity from the beginning. Barrier-based approaches can revitalize an existing PSM program or serve as a platform to build a simplified PSM program. Bow ties are commonly used to communicate the major accident hazards at an onshore or offshore facility.

Development of bow ties often follows the completion of a Process Hazards Analyses. Bow tie workshops use teams of experienced and knowledgeable people from various disciplines to develop the bow ties and select the barriers, previously identified in the PHAs, that meet the criteria for Major Accident Events (MAE) of being effective, independent, and auditable (Ref. /1/).

The focus of this paper is to show how bow ties can be used in other ways to drive success in a company's management system, regardless of where that company or facility may be in its process safety journey. This will be accomplished in the following ways:

- Lay out a process for developing or updating a relevant process safety management system for both OSHA PSM covered and non-covered facilities by engaging personnel in various levels of a company.
- Demonstrate how a bow tie can be used to develop or update a piece of the management system program associated with one of the 14 PSM elements.
- Present examples of how to tap into the additional benefits of bow ties to engage employees and improve a company's management system program. Examples are shown for some of the PSM elements.

The approach presented in this paper will include use of bow ties at the corporate level as well as at the manufacturing facility level. The principles discussed in the Center for Chemical Process Safety's (CCPS) Guidelines for Risk Based Process Safety (RBPS) are used in the development of this topic.

Using Bow Ties to Develop or Update a Management System

Bow ties can be used in developing a PSM program or updating an existing program for both OSHA PSM covered and non-covered facilities. The following benefits for using bow ties for PSM program development include:

- Illustrating the barriers associated with MAEs.
- Showing the impact of compromised degradation controls to barriers.
- Engaging employees in barrier and degradation control quality
- Encouraging employees' appreciation for their role in identifying and maintaining barriers and degradation controls.

Figure 1 shows how bow ties can be incorporated into the development or improvement of a management system program. This process is based on a company's knowledge of the three factors discussed in CCPS's Guidelines for RBPS specific to their company's business (Ref. /2/):

1. Identification of risks
2. Level demand of process safety activity work compared to resources available.
3. Existing process safety culture

The steps are discussed further in this section.

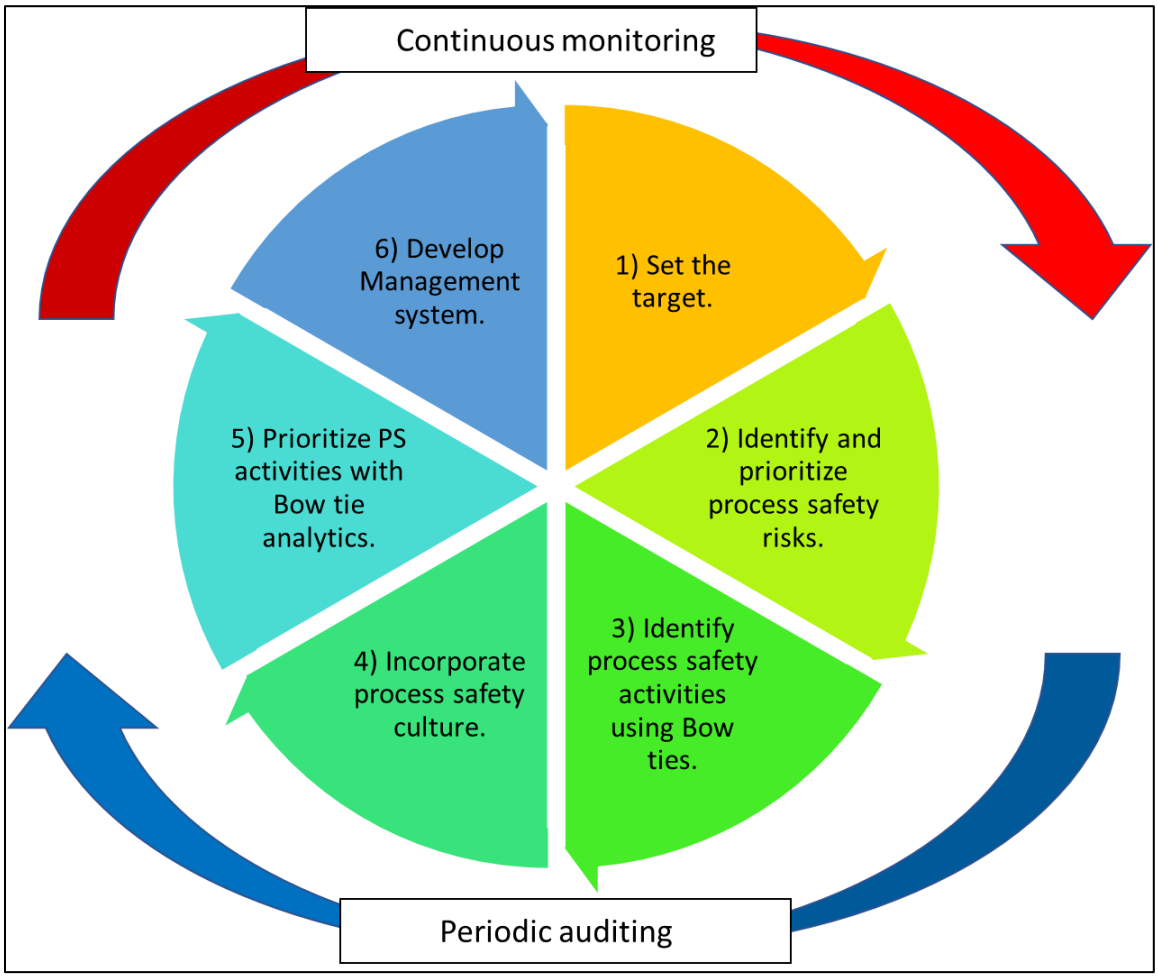


Figure 1 General Workflow for Bow Tie Application to PSM Program

Step 1: Set the target.

The target for a company's PSM program will be determined by regulatory requirements. OSHA PSM requires that companies develop program management systems that address 14 elements. A company may further decide to use Guidelines for RBPS to determine what level of rigor is needed for each element of its management system. Facilities that are not covered by OSHA PSM, still choose to have management systems as a best practice, and may use a risk-based approach to build their management system program.

Step 2: Identify and prioritize process safety risks.

The next step is to sufficiently understand the risks, which is the first factor on which process safety practices are founded (Ref. /2/). Many companies use various PHA methodologies to identify and assess risks at their facilities with Hazard and Operability (HAZOP) studies being one of the common types used. Bow ties and Layers of Protection Analyses (LOPA) are often used to identify the effective, independent, reliable and auditable barriers. Bow tie workshops go one step further in that the Bow tie workshop team members identify the degradation factors[1] and degradation controls[2] needed for the barrier be available illustrated in Figure 2. Bow tie workshops are convenient settings to engage the same people, who are assigned to the upkeep of barriers, through the activity of identifying specific degradation controls for each barrier.

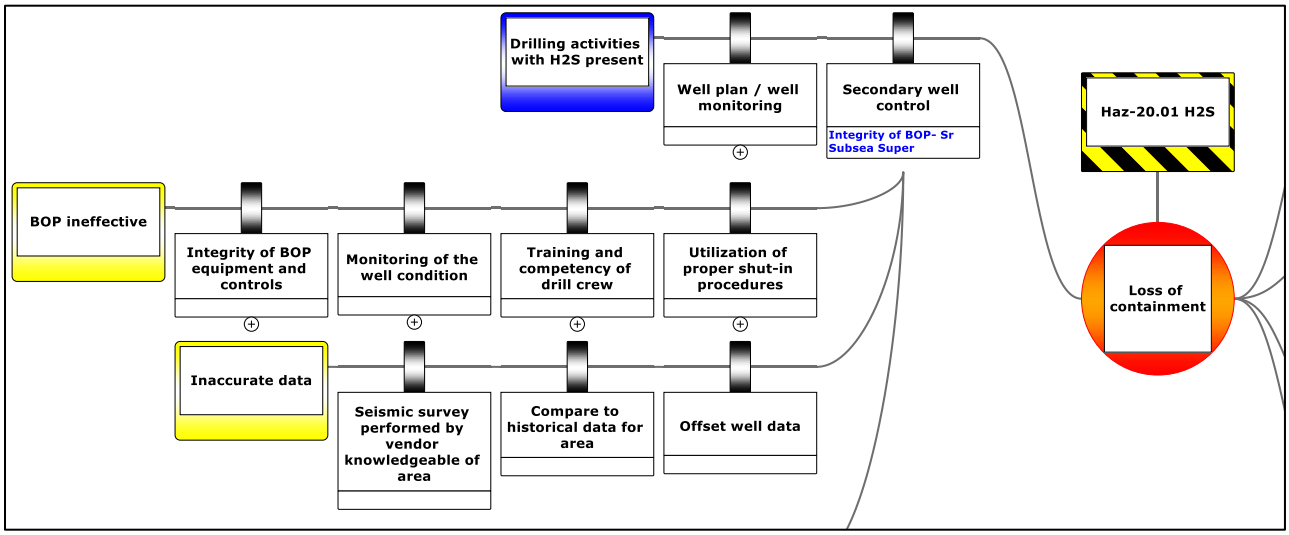


Figure 2 Bow tie Diagram Showing Barriers along with Degradation Controls

It is equally important for companies to identify process safety risks all levels of its operations including corporate and regional support levels. Bow tie diagrams can be useful for Corporate and Regional entities as well as manufacturing facilities.

Step 3: Identify process safety activities using Bow ties.

After identifying the risks and completing the bow tie workshops, the next factor to be addressed per RBPS Guidelines is the level of demand for process safety work activities needed compared to resources available (Ref. /2/). To determine the process safety activities, it is important to confirm that process safety practices associated with the degradation controls are in place. All process safety activities identified should be listed and linked to a management system element.

---

[1]Degradation controls are measures which help prevent the degradation factor impairing the barrier. They lie on the pathway connecting the degradation threat to the main pathway barrier. Degradation controls may not meet the full requirements for barrier validity (Ref. /1/).

[2] Degradation factor is a situation, condition, defect, or error that compromises the function of a main pathway barrier, through either defeating it or reducing its effectiveness. If a barrier degrades then the risks from the pathway on which it lies increase or escalate, hence the alternative name of escalation factor.

This activity can be completed as part of the bow tie workshop or separately. The outcomes would include the following:

- Short-term: A list of degradation control process safety activity gaps for existing barriers (e.g., missing PSI, out of date operating procedure, no maintenance procedure) and recommendation plan to address the gaps
- Long-term: A list of process safety activities based on maintaining degradation controls
- Time estimates for completing each process safety activity

The outcome from such a workshop may look like that shown in Table 1 (following page). The information can then be used to calculate the process safety activity demand time associated with its respective management system element for all barrier degradation controls identified. Examples are shown in Figure 3, Figure 4, Figure 5, and Figure 6 (on the page following Table 1).

Figure 3 shows the process safety activity demand currently associated with each management system element for the degradation controls. Figure 4 shows the additional process safety activity time needed to ensure the barrier degradation controls are in place long-term. Figure 5 shows projected long-term process safety activity demand time for the barrier degradation controls. Long-term process safety activity time is the summation of the additional process safety activity demand time in addition to the existing process safety activity demand time. This will help a company see which management system elements need more resources long-term.

Figure 6 is the time needed to implement the actions needed for the longer-term process safety activities. It helps prioritize resources short term.

Step 4: Incorporate process safety culture findings.

In addition to determining process safety activity and resource demand, is understanding the process safety culture (Ref. /2/), which may be accomplished through process safety culture assessments and review of leading, near miss and lagging indicators such as those discussed in API RP 754 *Process Safety Performance Indicators for the Refining and Petrochemical Industries* or CCPS's Guidelines for Process Safety Metrics.

Once process safety culture is understood across the organization, it is possible to determine how to prioritize which elements of the management system to focus on first.

Table 1 Process Safety Activity Identification Outcome Worksheet

Hazard and Top Event	Threat	Barrier	Degradation control	PSM Element	In place or active	Deficiencies?	PS Activity Time (per year)	Action	Time to implement action
Loss of Containment – High Pressure Natural Gas	Overpressure	PSV-01A – Pressure Safety Valve on Natural Gas Inlet Line	Inspection procedure, FAC-01-MNT-01	Mechanical Integrity	Yes		2 hours	None	N/A
Loss of Containment – High Pressure Natural Gas	Overpressure	HIPPS-01 High-integrity Pressure Protection System on Natural Gas Inlet Line	Maintenance procedure, FAC-01-MNT-02	Mechanical Integrity	Yes	No	2 hours	None	N/A
Loss of Containment – High Pressure Natural Gas	Overpressure	HIPPS-01 High-integrity Pressure Protection System on Natural Gas Inlet Line	Training requirements, HIPPS testing training and competence	Training	Yes	Yes; 2 out of 4 I&E technicians are trained	4	Provide training to J. Smith and A. Rogers (instrument technicians) hired in Q1 2018.	16 hours
						Total	**8 hours**		**16 hours**

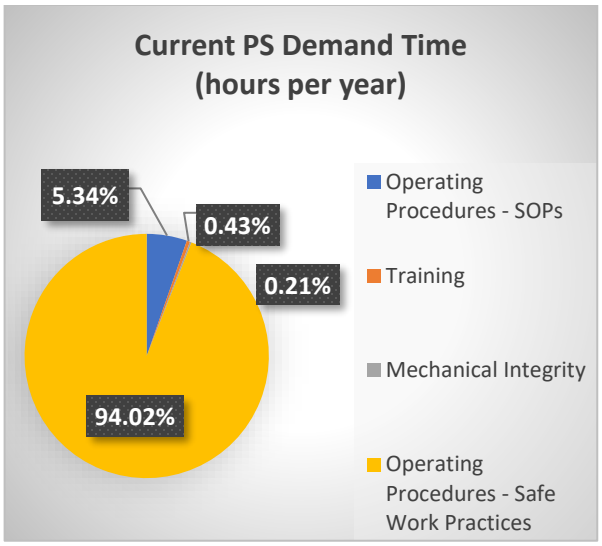


Figure 3 Current Process Safety Demand Time for Barrier Degradation Controls

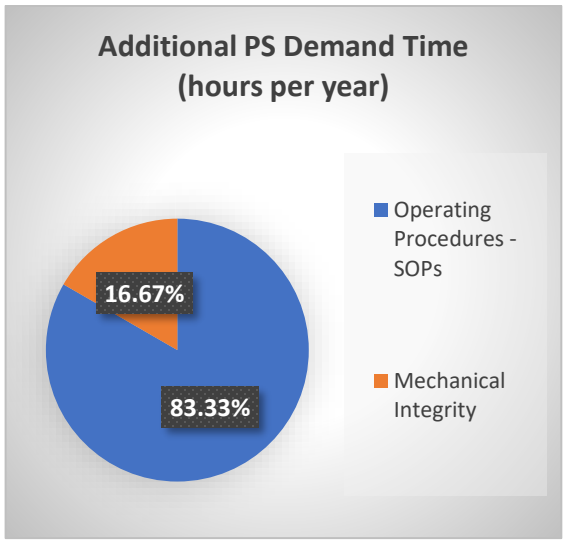


Figure 4 Additional Process Safety Demand Time for Barrier Degradation Controls

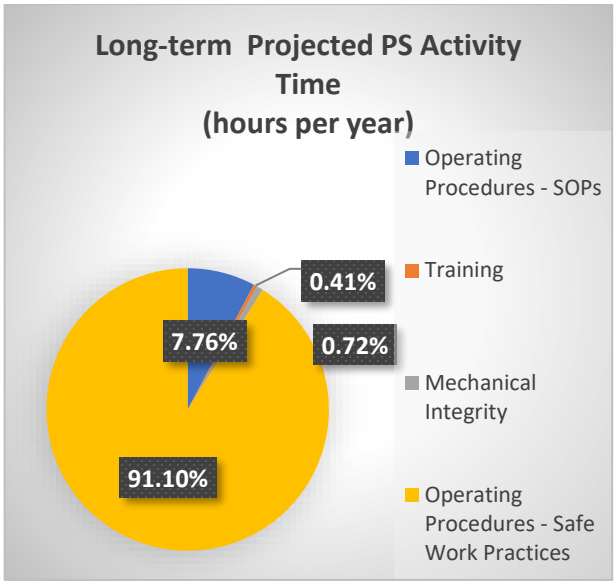


Figure 5 Long-Term Process Safety Demand Time for Barrier Degradation Controls

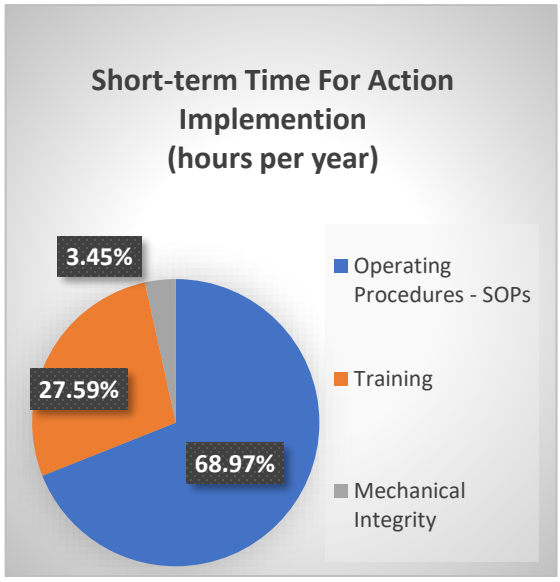


Figure 6 Short-Term Time for Action Implementation Time

The roles of the responsible resources can be assigned to each degradation control and corresponding management system. It can also be possible to see how the emphasis of a person's role can change with respect to management system elements.

How much time a person's role will change with respect to process safety activities vs. daily routine activities (if the breakdown of a resource's role in there is known). This may help a company determine if additional resources are needed or how to better prioritize the resources they have.

Step 5: Prioritize PS activities
Once the process safety activity demand and resource has been determined, the process safety culture rating can be used to help a company determine which process safety activities to focus on first with respect to their management system.

Step 6: Develop Management system
The findings from the facility level and corporate level assessments can be combined to an overall perspective of a company's management system to see company-wide, systemic patterns with current and long-term process safe activities.

Evergreen activities
Bow ties, barriers and degradation controls should be reviewed periodically to determine where process safety activities should be modified and to change the resourcing as needed. Continuously monitor barrier degradation control integrity, ensuring procedures are up-to-date, inspections on barriers or degradation controls are not overdue and maintenance activities are being performed at designated intervals. If deficiencies are noted with lagging or even leading indicators, the process safety activity demands and resourcing availability should be reviewed. When changes are made to equipment and associated barriers, bowties should be modified. If bowties are modified, this could impact the process safety activity demands associated with the barrier's degradation controls as well as the resources need to keep up the degradation controls.

Consider periodically reviewing the management system using the review of bowties, barriers and degradation controls periodically to assure that the management system is addressing the current risks with optimal resources.

Bow Ties to Design, Maintain and improve Management System Effectiveness

Bow ties can be used at a high level to develop or update a piece of the management system program associated with one of the 14 PSM elements especially at the Corporate level as mentioned in Step 2 in the previous section.

Once a company has determined the contents to be included or areas of improvement needed for the Employee Participation element of their management system, they can create a bow tie that can be reviewed periodically to determine areas of strengths and weaknesses. Figure 7 shows a bow ties that was developed using the contents of CCPS Guidelines for RBPS for Workforce Involvement (Ref. /2/). The Hazard is based on the attitude of the employees (i.e., their perception that their feedback does not matter and will not change safe work practices or safety culture). The top event is the result of the attitude which is "Lack of employee participation", which is the opposite effect of what the management system element is aiming to achieve. The threats on the left-hand side are based on a breakdown or lack of key principles needed to implement an Employee Participation Program. These key principles are discussed in CCPS's Guideline for RBPS (Ref. /2/). The preventive barriers are based on the possible work activities described for each of the key principles. To prevent breakdown of the preventive barriers, the degradation mechanisms for each barrier should be identified and controlled (Ref. /2/).

Figure 8 shows the degradation factors (i.e., Inconsistent Implementation) and degradation controls (i.e., Owner of Employee Participation Element) associated the preventive barrier of "Consistent implementation" to prevent "Lack of dependable work practice" (Ref. /2/). It is worth

noting that a bow tie like this can be created to assess the effectiveness of any company's management system elements using the information in Guidelines for RBPS. In a workshop setting, senior management and workers validate the existence of the barriers, assess the effectiveness of those barriers, review selected metrics, and develop recommendations to improve the existing Employee Participation program.

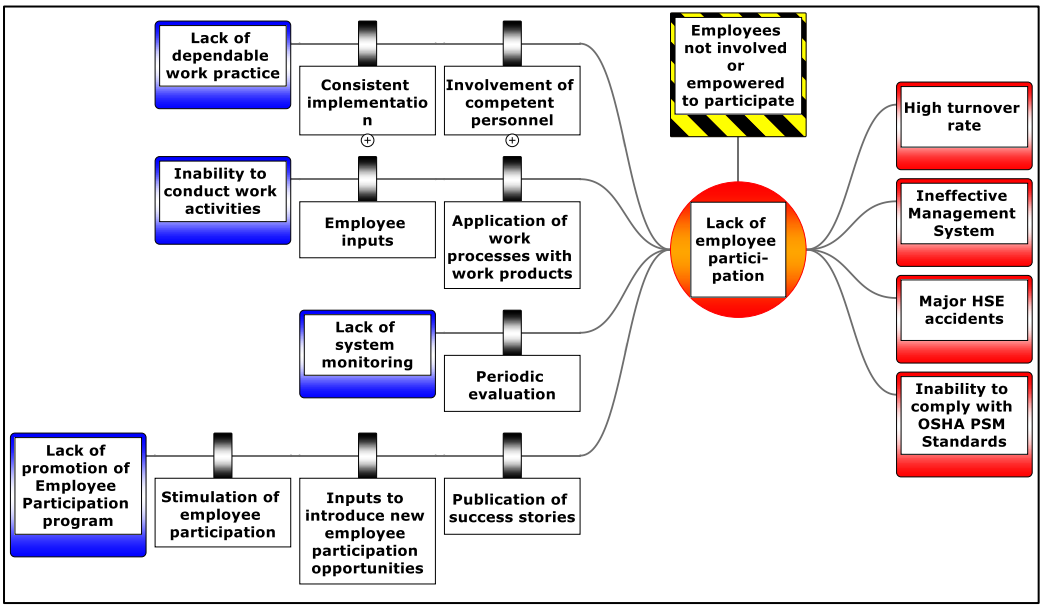


Figure 7 Bow Ties for Employee Participation Management System Element (Ref. /2/)

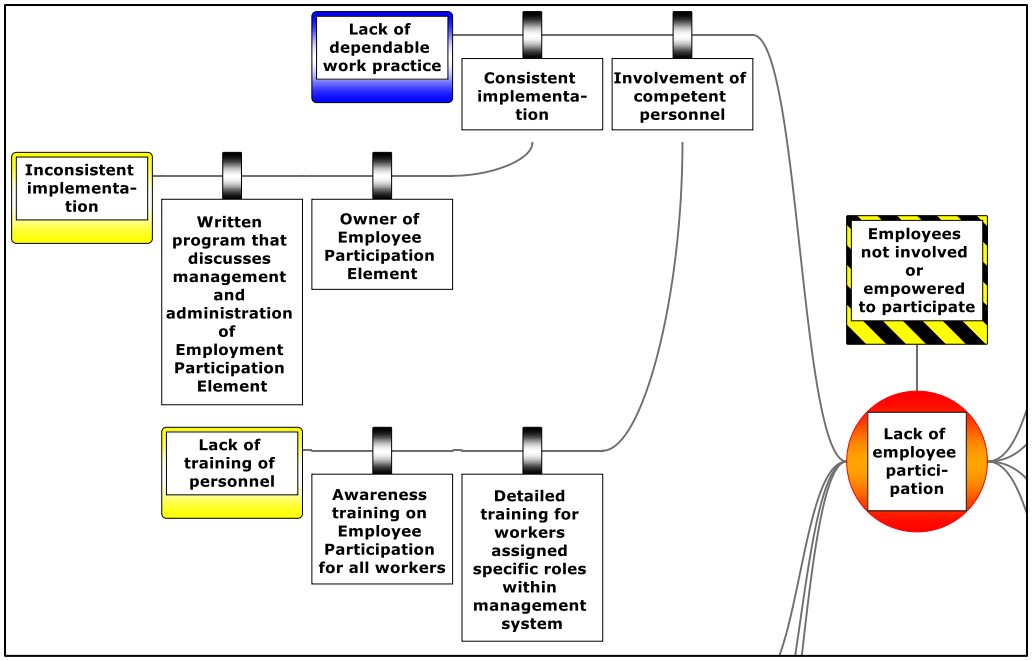


Figure 8 Bow Tie for Employee Participation Management System Element (with focus on Dependable Work Practice) (Ref. /2/)

Various Applications of Bow Ties to Support OSHA PSM Elements

Bowties can be used in other ways to engage employees in implementing the elements of a management system. This section shares some examples of how this can be accomplished.

Employee Participation

Bow ties can be used to monitor the success of an existing program in engaging the workforce at a high level as well as monitor the success of workforce involvement within each Management System Element. An example of an element-specific bow tie for Process Hazards with focus on employee participation is shown in *Figure 10* (on the following page). Figure 10 shows the degradation factors and degradation controls associated with the preventive barrier of “PHA activities” and “Involvement of competent personnel” to prevent “Lack of dependable work practice” (Ref. /2/).

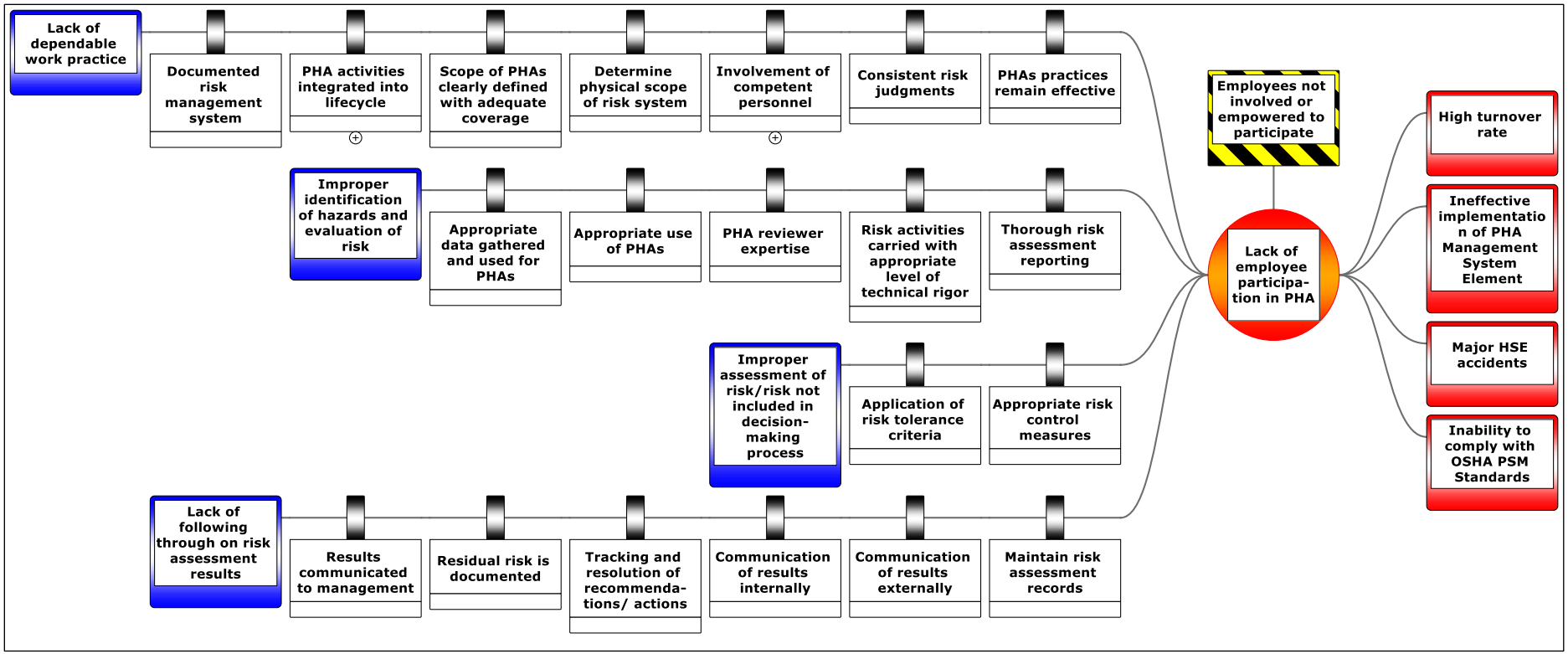


Figure 9 Bow Tie for Employee Participation within Process Hazards Analysis Management System Element (Ref. /2/)

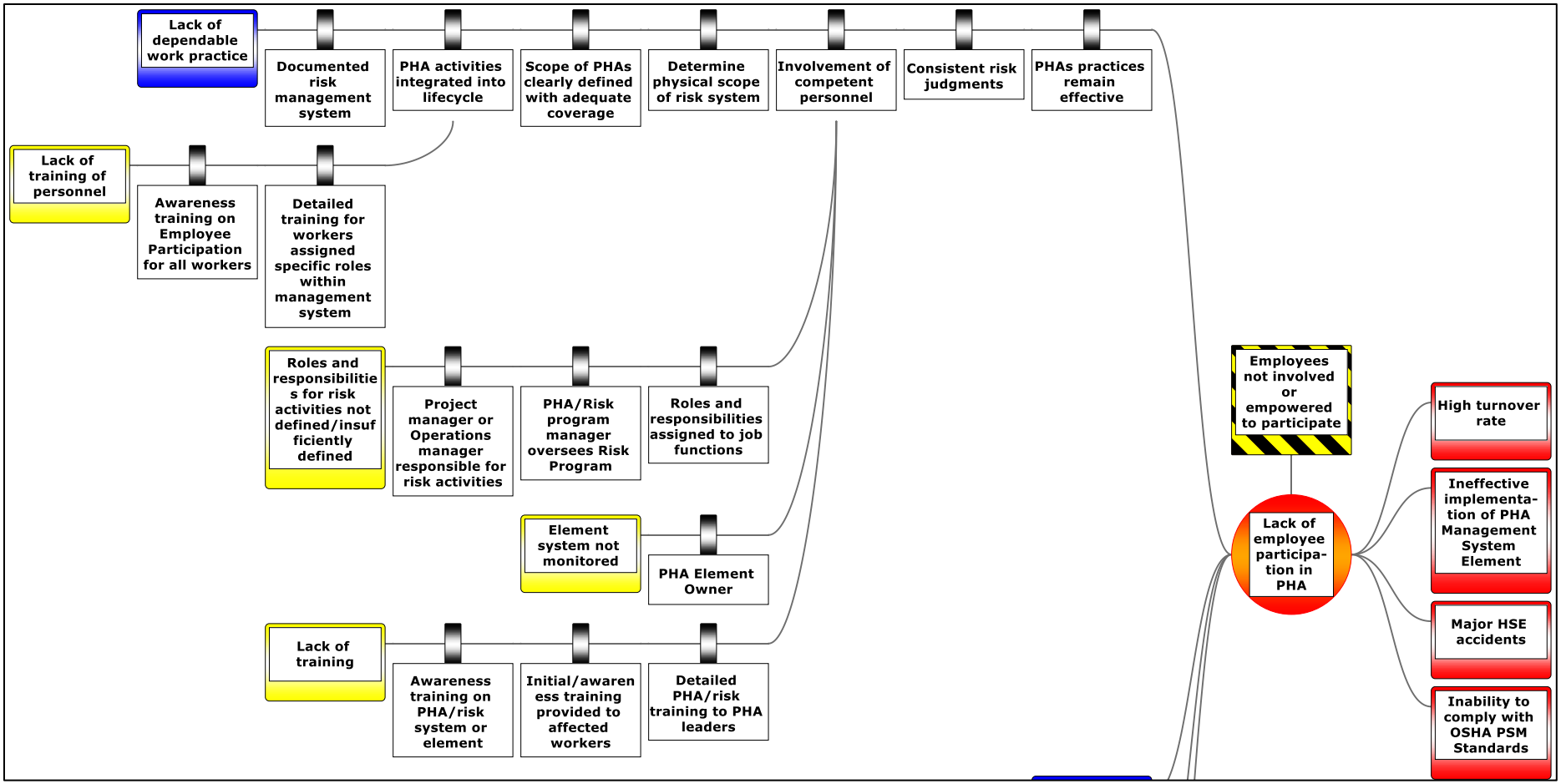


Figure 10 Bow Tie for Employee Participation within Process Hazards Analysis Management System Element (with focus on Dependable Work Practice) (Ref. /2/)

Process Safety Information

Established Process Safety (PSI) and relevant standards employed are required for covered processes in accordance with OSHA PSM 1910.119 (d). A bow tie can be an accountability tool for PSI and compliance with relevant standards associated with barriers. This type of information is referred to as barrier metadata in the joint publication by CCPS & Energy Institute on *Bow Ties in Risk Management: A Concept Book.* If PSI for a barrier or degradation control is missing, a barrier can be considered as not in place during the bow tie workshop. Therefore, the bow tie could be considered incomplete until the PSI is verified or acquired. It should be noted that the bow tie would be used as a mapping tool, not a repository for documents.

Operating and Safe Work Procedures

The employer must develop and implement written operating procedures, consistent with the process safety information, that provide clear instructions for safely conducting activities involved in each covered process in sections in accordance with OSHA PSM 1910.119 (f). OSHA PSM 1910.119 (k)) specifically focuses on the requirements for hot work. Procedures must be established to assure that there are no deficiencies in the barriers. The existing standard operating procedures and safe work procedures and relevant sections of the procedures can be documented in the bowtie. This shows the connection of the procedural steps to the bow tie to enforce the criticality of the procedure and specific sections or steps in preventing or reducing the likelihood of a major accident event. Procedures are shown as a degradation control. A poor or missing procedure can degrade a barrier. The use of bowtie for operating and safe work procedure is illustrated in Figure 11. The degradation control "Neighbouring firefighting units in remote areas" references the "Bridging Document" as necessary for the barrier "Active firefighting system" to be in place.

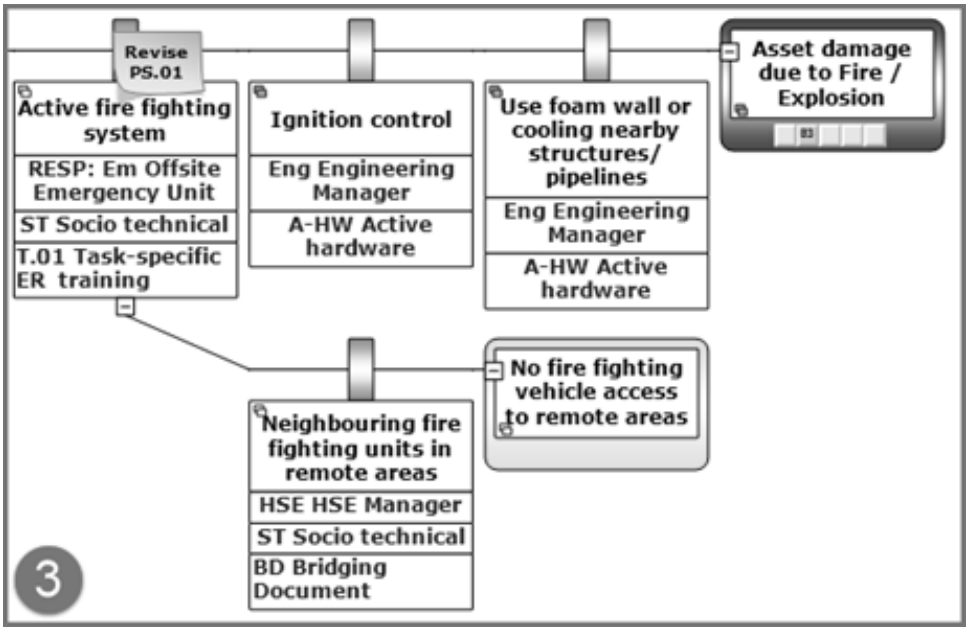


Figure 11 Illustration of Bow Tie with Operating Barrier Degradation Controls

Training

OSHA 1910.119 (g) states that the implementation of an effective training program is one of the most important steps that an employer can take to enhance employee safety. Training programs with periodic refresher courses should be established to assure that there are no deficiencies in the barriers. The company can include the applicable bow tie barriers or degradation controls critical to an employee's role or more specifically to a task or procedure. This is illustrated in Figure 11. The barrier "Active firefighting system" references "T.01 Task-specific ER training" as necessary for the barrier to be in place as an example, since personnel at the facility will need training to address a fire scenario. Additionally, the roles of personnel can be connected to barriers, also shown in Figure 11. The HSE Manager is assigned to the degradation control "Neighbouring firefighting units in remote areas"; it is the HSE Manager's responsibility to assure that firefighting units can access the facility otherwise, the barrier "Active firefighting system" may not be in place during a fire.

Contractors

OSHA PSM 1910.119 (h) includes special provisions for contractors and their employees to emphasize the importance of everyone taking care that they do nothing to endanger those working nearby who may work for another employer. Contractors can be provided copies of the bow ties applicable to their area of work. The company can orient the contractor supervisors and employees on the bow ties and discuss how the successful execution of their activities is important to keeping the facility safe.

Pre-Startup Safety Review

OSHA PSM 1910.119 (i) requires the employer to perform a pre-startup safety review (PSSR) for new facilities and for modified facilities when the modification is significant enough to require a change in the process safety information. The bowties can be effective during PSSR review in the following ways:

- illustrations to PSSR team members for importance of barriers in the process,
- review of the outstanding PHA actions, especially those actions related to barriers that address risks with MAEs, and
- assist in assigning priority to PSSR action items

Mechanical Integrity

Companies must maintain the mechanical integrity of critical process equipment to ensure it is designed and installed correctly and operates properly, per OSHA PSM 1910.119 (j). Mechanical integrity program must be established to assure that there are no deficiencies in the barriers, this is especially important with relief valves, SIS, and other safeguards. Bow ties can be used in the same way for tracking maintenance procedures and the associated roles of personnel as it can for the Operating Procedures by associating the maintenance and inspections procedures and roles of personnel to the applicable bow tie barriers and degradation controls.

Management of Change

OSHA states that changes to a process must be thoroughly evaluated to fully assess their impact on employee safety and health and to determine needed changes to operating procedures (1910.119 (l)). When changes in the facility include barriers, the use of the bow tie can illustrate the impact

of these changes to the barriers and its associated degradation controls. A barrier may need to be modified after an MOC review. It could be the case that the MOC procedure needs to be modified to ensure impacts on barrier effectiveness are adequately considered in the risk assessment.

Incident Investigation

OSHA requires the investigation of each incident that resulted or could have resulted in a catastrophic release of a highly hazardous chemical in the workplace (1910.119(m)).

Barrier-based Systematic Cause Analysis Technique (BSCAT) is the use of a bow tie to map out the events based on failure of barriers during each part of the scenario. Root causes of barrier failures and near-miss barrier failures can be mapped to the related management system element to determine where there are deficiencies. BSCAT diagram is shown in Figure 12 (shown on the following page) for the Lac Mégantic train incident in Canada (2013). A close-up of the left-hand side is shown in Figure 13 (shown on the following page). The barrier "Locomotive Temporary Repair" between the Threat "Locomotive Fault (8 Months Before)" and Immediate Event "Locomotive starts to smoke badly on July 5" was not effective at that time in preventing the next immediate event since Management System Factor (MSF) "MSF10.1 Maintenance Program" did not address follow up of temporary repairs, in the example shown. In this case, there were systemic issues with Mechanical Integrity.

Emergency Planning and Response

OSHA requires emergency pre-planning and training to make employees aware of, and able to execute, proper actions (1910.119 (n)). For this reason, an emergency action plan for the entire plant must be developed and implemented in accordance with the provisions of other OSHA rules (29 CFR 1910.38(a)). Bow ties can be used as communication tools for onsite employees as well as municipal emergency responders to help all parties understand the MAEs and the importance of having a robust emergency response plan as well that is executed periodically through drills.

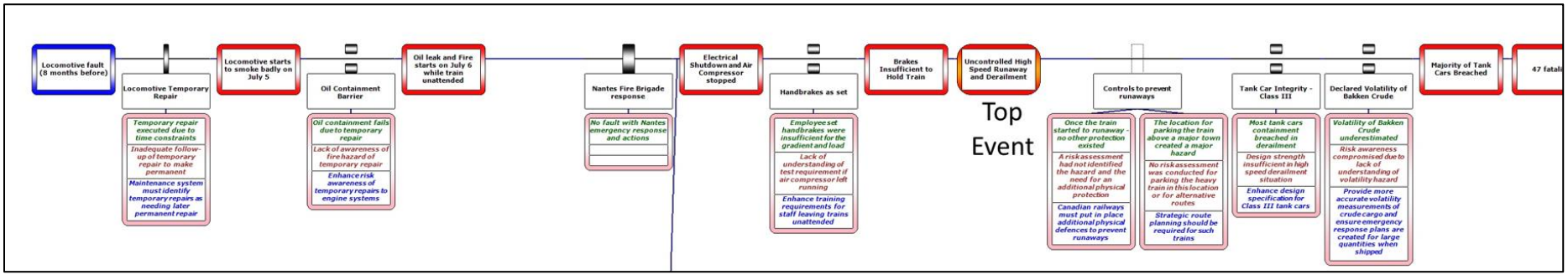


Figure 12 Illustration of BSCAT for Lac Mégantic Accident (Canada, 2013) (DNV GL)

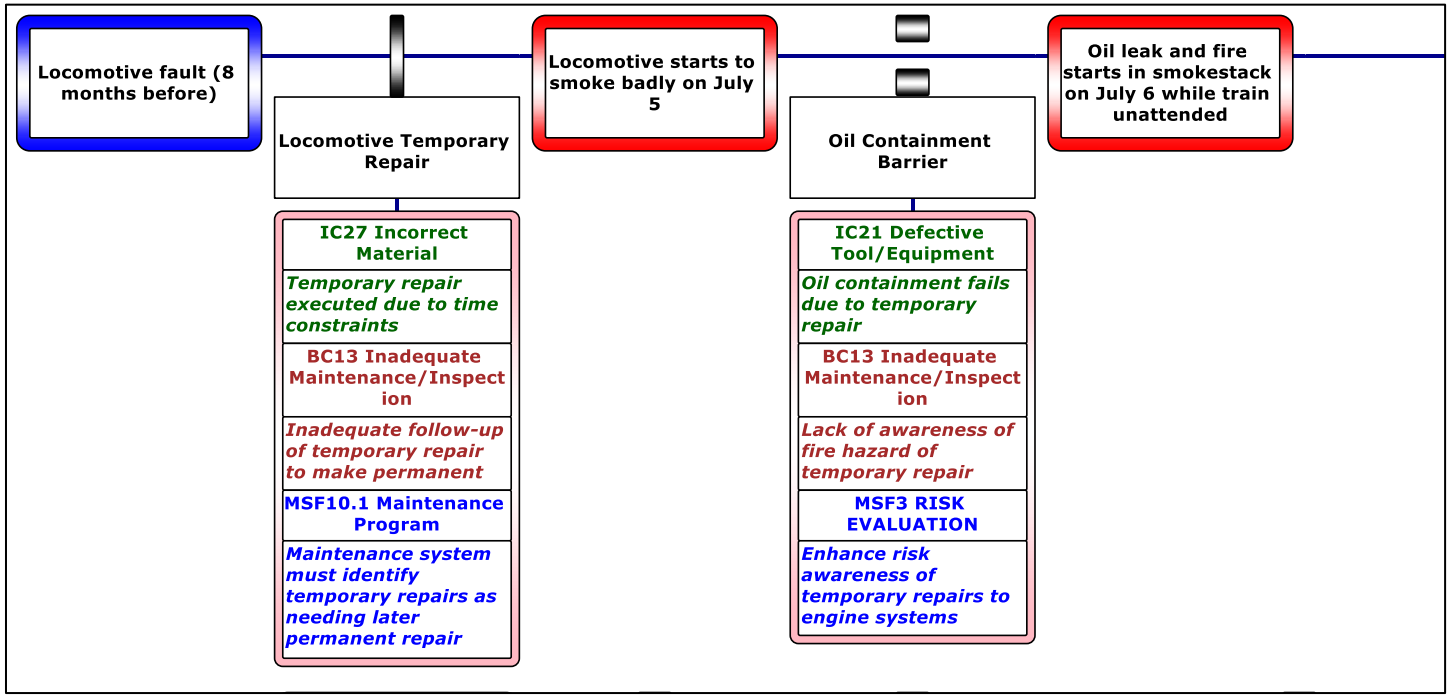


Figure 13 Close-up of Left Hand Side of BSCAT for Lac Mégantic Accident (Canada, 2013) (DNV GL)

Trade Secrets

OSHA states that employers must make available all information necessary to comply with PSM to those employees who are responsible for compiling the process safety information, those developing the process hazard analysis, those responsible for developing the operating procedures, and those performing incident investigations, emergency planning and response, and compliance audits, without regard to the possible trade secret status of such information (1910.119(p)). The completed bow ties are a demonstration that relevant information is being shared.

Conclusions

Bow ties reestablish direct connections to operations in a quickly visualized way transforming the perception of a PSM program using an engagement tool that can inspire ownership at all levels of the organization. Bow ties can help a company focus their efforts on efficiently developing a management system, maintaining a management system and addressing deficiencies in their management systems to manage their most important risks. Bowties can be applied to the assure a management system covers the fourteen PSM elements in various ways.

References

1 Center for Chemical Process Safety (CCPS) & Energy Institute (EI). *Bow Ties in Risk Management: A Concept Book for Process Safety. American Institute of Chemical Engineers*, Hoboken, NJ, USA: John Wiley & Sons, Inc. 2018.

2 Center for Chemical Process Safety (CCPS). *Guidelines for Risk-Based Process Safety.* Hoboken, NJ, USA: John Wiley & Sons, Inc. 2007.

3 Center for Chemical Process Safety (CCPS). *Essential Practices for Creating, Strengthening, and Sustaining Process Safety Culture.* Hoboken, NJ, USA: John Wiley & Sons, Inc. 2018.

4 OSHA Process Safety Management, 29 C.F.R. § 1910 (2013). https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

What to Do if PSM/HSE Performance Flattens Out? Resuming Your Drive to ZERO

Steve Arendt, P.E., Vice President, Rick Curtis, Sr. Risk Consultant
ABS Group
16855 Northchase Drive
Houston, TX USA 77060
+1-281-673-2914, +1-281-673-2963
Emails: sarendt@absconsulting.com, rcurtis@absconsulting.com

Abstract

Most companies have a continuous improvement expectation in their PSM/HSE mission and values. Many companies measure PSM/HSE performance with lagging and leading metrics. Some companies are pursuing Operational Excellence. And some companies have adopted some form of "drive to zero". But, what happens when their performance flattens out? People will wonder why, and there will be pressure from many directions - internal and external. Key issues that must be addressed are:

- Can you believe your measure data and methods?
- If so, can you improve the performance based upon these indicators?
- Then, how can you sustain it - How to resume driving to ZERO?

This paper/presentation presents an approach and case study that describes (1) where the company PSM/HSE performance plateaued and (2) what they did to resume their drive to ZERO that included the following steps:

- Examine learning mechanisms and corrective action processes
- Incident reporting and investigation root cause analysis effectiveness
- Audit effectiveness
- Action item completion work processes and results
- Examine leading indicators to see if they have PSM/HSE improvement value vs. just things easy to collect and are really being used to drive performance
- Examine the effectiveness of existing behavior based safety (BBS) program - many BBS programs lose value and need to be re-energized
- Do a PSM/PSM/HSE culture disease screening - determine whether there is evidence of chronic problems that never stay fixed

- Conduct an PSM/HSE culture evaluation
- Then, improve the areas where the problems are

Following this approach allowed for efficiently diagnosing performance problems, and the company was able to improve their PSM/HSE culture and resume their drive to zero with a two-year period.

1. INTRODUCTION

Companies have been taught many times that organizational factors have been important contributors to PSM/HSE/process safety performance. Some of those organizational characteristics have to do with not having a proper safety culture, failing to exhibit strong leadership to support the culture, and not creating the consistent operational discipline at all organizational levels. One theme common to all three of these aspects has been the failure of companies to learn from experience – either from their own or from others.

In order to address their "learning disabilities", companies should strive to improve operational discipline, leadership, and eventually their culture. The following sections describe examples of each of these aspects and how to improve them. This paper presents an approach and case study that describes (1) where the company PSM/HSE performance plateaued and (2) what they did to resume their drive to ZERO that included the following steps:

1. Examine learning mechanisms and corrective action processes
    a. Incident reporting and investigation root cause analysis effectiveness
    b. Audit effectiveness
    c. Action item completion work processes and results
2. Examine leading indicators to see if they have PSM/HSE improvement value vs. just things easy to collect and are really being used to drive performance
3. Examine the effectiveness of existing behavior based safety (BBS) program - many BBS programs lose value and need to be re-energized
4. Do an PSM/HSE culture disease screening - determine whether there is evidence of chronic problems that never stay fixed
5. Conduct an PSM/HSE culture evaluation
6. Then, improve the areas where the problems are

The following sections describes the company's journey to discover, diagnose, and correct the root causes of its PSM/HSE performance stagnation and the resumption of its drive to ZERO.

2. IMPORTANCE OF PSM/HSE CULTURE IN CONTINUAL IMPROVEMENT

Companies are usually motivated to improve PSM/HSE performance by the one or more of the following reasons:

- Recent major accident
- Series of incidents
- Regulatory – new rule or enforcement actions

- Industry group membership obligation
- Peer pressure/comparisons of existing practices
- Perception that risk is not tolerable/increasing
- Resource pressures
- Company policy of continuous improvement

Over the years, the following figure illustrates the three strategies that companies have adopted to attempt to drive continuous performance improvement.

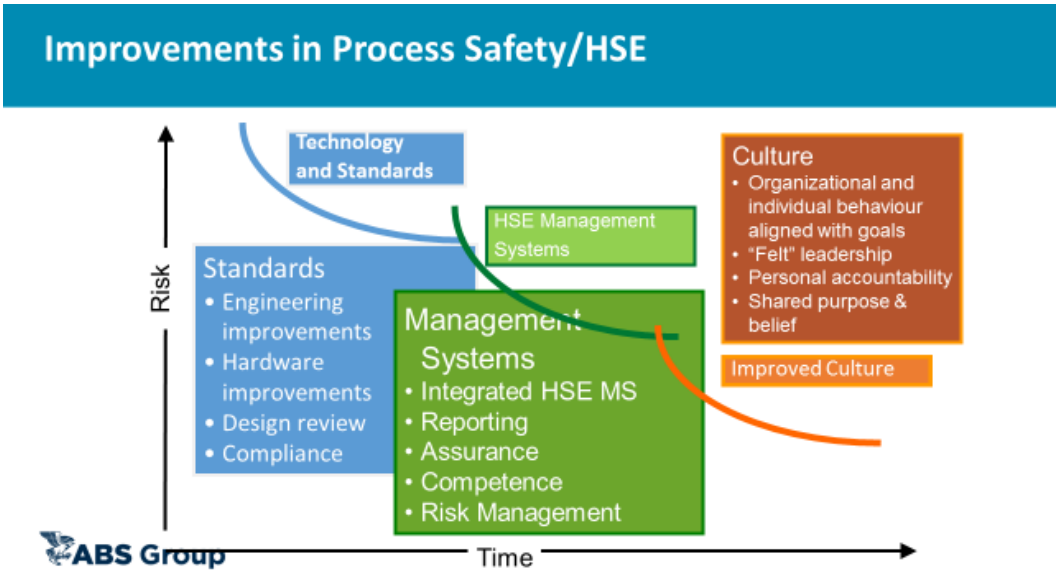


Figure 1: Continuous Improvement Strategies

As you can see from the figure, unless a company attempts to address behaviors and culture, they have no hop to break through performance stagnation and continue to drive to ZERO.

Arendt definition of culture is – ***"Culture is the tendency in all of us – and our organization - to want to do the right thing in the right way at the right time, ALL the time – even when/if no one is looking."*** Leadership is an essential feature of a good culture. Operational discipline (or the lack thereof) is a behavioral result of your culture and leadership. So, a company that analyzes its performance problems, seeks out root causes, and determines a path forward will eventually realize that it needs to evaluate and improve its PSM/HSE culture.

3. FRAMEWORKS FOR UNDERSTANDING PSM/HSE CULTURE

The CCPS made "culture" an official safety management system (SMS) element for the first time when it published its ***RBPS Guidelines***.[1] CCPS safety culture working group and ABS Consulting evaluated major organizational accidents and prepared a Safety Culture Awareness tool, which has been widely distributed via CCPS's web page. Subsequently, Process Safety Culture was defined as an element in the ***RBPS Guidelines*** that created a culture management practice and laid out the "Twelve Essential Features of a Good Culture."

Table 1 - CCPS Process Safety Culture – Essential Features

1	Establish safety as a core value
2	Provide strong leadership
3	Establish and enforce high standards of performance
4	Formalize the safety culture emphasis/approach
5	Maintain a sense of vulnerability
6	Empower individuals to successfully fulfill their safety responsibilities
7	Defer to expertise
8	Ensure open and effective communications
9	Establish a questioning/learning environment
10	Foster mutual trust
11	Provide timely response to safety issues and concerns
12	Provide continuous monitoring of performance

Our belief is that while the CCPS culture feature framework is the most complete one, ultimately, it will not matter which framework you follow, but that you excel in the aspects of any one of them. When this doesn't happen and a poor culture persists, here are some lessons the authors have learned about why and what needs to be done.

- If you have poor culture, marked by mistrust or needs large improvement, the worst thing you can do is too just start "talking" about it at the top
- The "top" needs to first start "behaving" better to address culture weaknesses; then, the talk will build up from the bottom
- If you survey, do it anonymous and voluntary; you should commit to sharing the results – quickly
- Any education/training, etc. should extend to ALL of the workforce, including contractors
- BUILD OWNERSHIP

One way to do this is look for evidence that culture problems exist and have been causing performance issues. The following are some examples you can look for to do "culture disease screening":

- Chronic work backlogs
- Problems that never seem to get better
- Poor reporting
- Investigations identify symptoms, not root causes
- Many incidents involve "people not following procedures"
- Repetitive barrier degradation patterns
- Repeated root causes – over and over and over…
- Corrective actions don't address root causes
- Fixes don't stay fixed

If any of issues are prevalent, then your performance problems are likely root in PSM/HSE culture disease.

4. HOW TO MEASURE PSM/HSE CULTURE

PSM/HSE culture is hard to measure and more difficult to change. There are few direct indicators of PSM/HSE culture, and because of its nature, it cannot be evaluated very frequently. Leadership and operational discipline are essential attributes of sustaining a healthy PSM/HSE culture. So, how do you know if better culture or operational discipline is needed? What evidence would lead you to believe that you need better operational discipline and that you need a ConOps element? Typical ways to get a handle on PSM/HSE culture are:

Employee surveys – Surveys are the most frequently used method. Typically, a company will prepare an anonymous survey (20-70 questions, shorter is better) for both hourly employees and management. The content of the survey historically has been focused more on occupational safety issues, but recently they have been adapted to address PSM/HSE issues. Survey questions are developed to see how employees "feel" about important PSM/HSE-related matters. Respondents are given a choice of five answers to gauge the strength of their feelings about the issues – strongly agree, agree, neutral, disagree, strongly disagree. Questions and results are normally placed in categories relating to the PSM/HSE issues of concern (Process Safety Reporting, Commitment to Process Safety, Supervision, Procedures and Equipment, Employee Involvement, Process Safety Training, and Safety Processes). Table 2 lists some best practices for developing/conducting PSM/HSE culture surveys.

Some difficulties with surveys are (1) that they should be voluntary, which may lead to insufficient participation to achieve statistical validity and (2) surveys cannot be repeated very often or else workers will become accustomed to it and can tend to feed back "what you want to hear" rather than what they are really feeling.

Interviews – another way to elicit PSM/HSE culture insights is through limited, representative, but targeted, interviews of company personnel. These interviews may last from 15 minutes to an hour. A disadvantage of interviews is that they are very time-consuming and resource intensive and the results are more difficult to pull together in a consistent framework for analysis.

Work observations – Process safety culture issues that deal with the tendency for employees to not following procedures, safe work practices, etc. can be identified via workplace observations. These can very effective, but are difficult to conduct in a consistent fashion using a large number of observers. The biggest limitation is that they are difficult to do without the person being observed knowing that they are being watched/evaluated. If they know, you are unlikely to get the "real" information about how the worker behaves "without anyone looking."

Process safety leading indicator metrics – More companies are using leading indicators of PSM/HSE as a window into PSM/HSE culture. For example, the rate of reporting of near-misses, the rate of close-out of action items, or the completeness of training compliance can be used to gage a company's leadership in PSM/HSE. Metrics are good because they can be refreshed frequently, but they are usually very "indirect" measurement of PSM/HSE issues.

Depending upon the situation, we typically use a combination of these means, anchored by some variation on a culture survey.

CCPS has recently published ***Essential Practices for Developing, Strengthening, and Implementing Process Safety Culture*** which condensed the ***RBPS Essential Features of a Good Culture*** into ten core principles. The following table compares the original features with the condensed core principles.

RBPS Culture Essential Features	Culture Core Principles
1.Process safety must be a core value	1. Establish the Imperative for Process Safety
2. Provide strong leadership everywhere	2. Provide Strong Leadership
3. Enforce standards of performance/accountability	9. Combat the Normalization of Deviance
4. Formalize the culture approach	10. Learn to Assess and Advance the Culture
5. Maintain a sense of vulnerability	5. Maintain a Sense of Vulnerability
6. Empower individuals	7. Empower Individuals
7. Defer to expertise	8. Defer to Expertise
8. Ensure open and effective communications	4. Ensure Open and Frank Communications
9. Establish a questioning/learning environment	6. Understand and Act Upon Hazards/Risks
10. Foster mutual trust	3. Foster Mutual Trust
11. Responsiveness to process safety issues	
12. Provide continuous monitoring of performance	10. Learn to Assess and Advance the Culture
Identical	
Word differences only	
Combined into one	
Possible gap	

Regardless of which of these two frameworks are used, a culture assessment should seek to use the selected framework items as measurement objectives for whatever survey, interviews, or observations are conducted.

ABS Consulting has devised an approach for connecting PSM/HSE culture survey results to PSM/HSE outcomes. This PSM/HSE **Performance Assurance Review** approach (Figure 2) categorizes the culture survey results and maps them to the 12 essential features of a good PSM/HSE culture, (b) categorizes the results from a review of recent and historical PSM/HSE performance at a plant (e.g., current PSM or PSM/HSE audit results) and maps these results to the same 12 essential features. The "weighted outcome" of the mapping of contributions of both the survey results and the PSM audit results to the 12 essential features are totaled and the most significant PSM/HSE culture issues are identified for the plant/company.

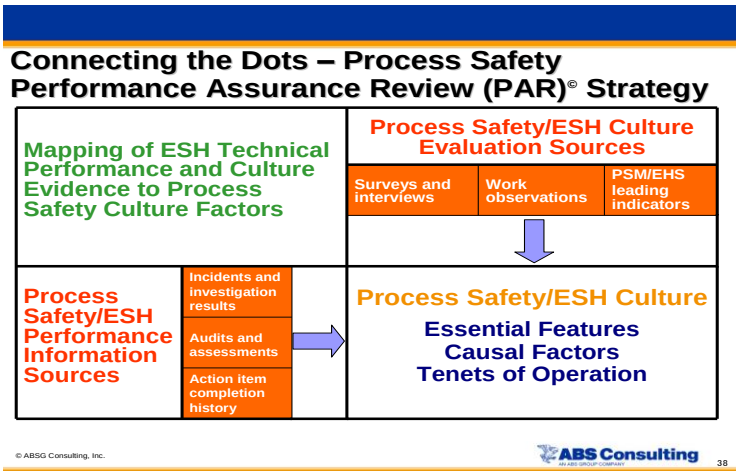


Figure 2: Process Safety Performance Review Culture Evaluation Approach

The results of the process safety culture survey are categorized into the 12 essential features of a good process safety culture, as shown by a typical results below

Figure 3: Example of Culture Evaluation Results

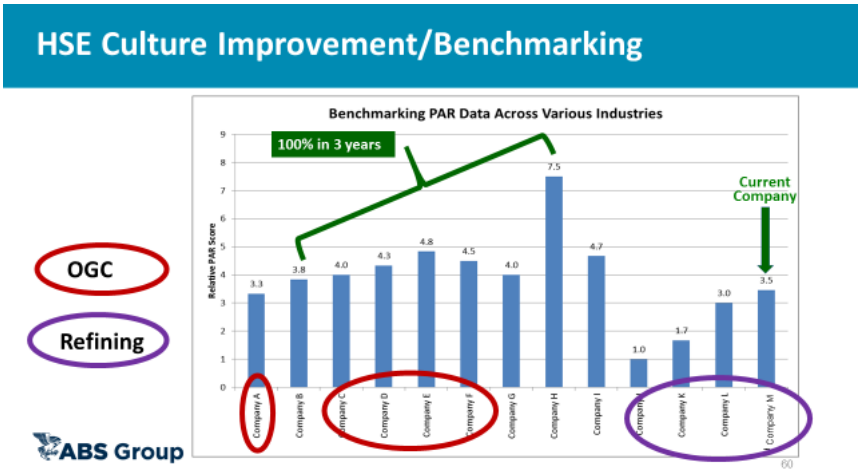


Figure 4: Example of General Improvement in Performance by Improving PSM/HSE Culture

5. CASE STUDY – HOW ONE COMPANY RESUMED IT'S DRIVE TO ZERO

The Responsible Care® program at a large multi-national chemical member company was directed towards a vision of zero – zero injuries, zero process incidents, zero distribution incidents and zero environmental incidents. Towards this end, they have created a "Goal Is Zero" culture among our employees that will push every individual towards a self-sustaining cycle of improvement in safety performance.

In 2008, the senior leadership expressed a concern that the employee injury/illness frequency rate had plateaued, and took steps to drive the frequency rate towards an ACC Best in Class level. A "Goal Is Zero Vision Statement" was created and communicated throughout the corporation. To facilitate improvement, the company committed to implement a Responsible Care Management System (RCMS) at all facilities world-wide that would encompass the Goal Is Zero vision and continual improvement. A Global Commitment to Responsible Care® was developed, signed by the Executive Management Team, and communicated. Within the RCMS model of continual improvement, they determined that the root cause preventing improvement in safety performance was failures in the underlying culture of Responsible Care®.

The Responsible Care® culture that the company desired is a tendency in all employees to want to do the right thing in the right way at the right time, ALL the time – even when no one is looking. (Arendt, 2007). In mid-2009 this company initiated the identification of behavioral and cultural causes of safety performance stagnation by retaining ABS Group to conduct a culture evaluation throughout the company and to visit representative company manufacturing, research, and office locations throughout the world to interview management and employees about their culture of safety. Incident summaries and statistics, EHS audit findings, and inspections were used to evaluate existing sources of historical safety performance. Based on the findings of the culture survey, interviews, and the evaluation of historical performance, company was able to identify "cultural causal factors" and rank their significance based on the results of the evaluation (Figure 5). Primary cultural causal factors were determined to be the lack of discriminating leading indicators based on quality rather than quantity of data, a normalization of deviance, and the perceived lack of management responsiveness to safety concerns.

Cultural Causal Factor	PAR Rank
11. Non-responsiveness to safety concerns	1
3. Not meeting performance standards – "normalization of deviance"	1
7. Not deferring to expertise	1
9. Lack of a questioning/learning environment	1
2. Not providing strong leadership	2
4. Not formalizing/celebrating the safety culture emphasis/approach	2
5. Lack of sense of vulnerability	2
1. Safety is NOT a core value	3
10. Lack of mutual trust	3
6. Not empowering individuals to fulfill their safety responsibilities	3
8. Not ensuring open and effective communications	3
12. Not provide continuous monitoring of performance	

Figure 5: Company PSM/HSE Culture Evaluation Results by Essential Feature

Based upon the identification of significant causal factors, company developed objectives to improve workforce at-risk behaviors and safety culture issues. Leading key performance indicators were established to evaluate the "health" of facility safety programs (Figure 6). Rather than require facilities to report a specific number of safety observations, each facility was given the task of developing their own goals, objectives, improvement plans, and reporting on the quality of their own program. Facilities were required to establish and report on the quality of safety near miss programs and the quality of observation and contact programs.

To increase management's responsiveness to safety concerns, company focused on near miss and incident root cause analysis, corrective action tracking, and communication of findings throughout the corporation. A web-based corrective action tracking system that allows all facilities to view all corrective actions corporate-wide has been implemented. In the event of an injury or serious near miss, the investigation, root cause, and corrective actions are presented to all Responsible Care managers, facility managers, business managers, and the executive management team. When appropriate, corporate-wide corrective actions are put in place. All employees are surveyed regularly for their opinion of management responsiveness.

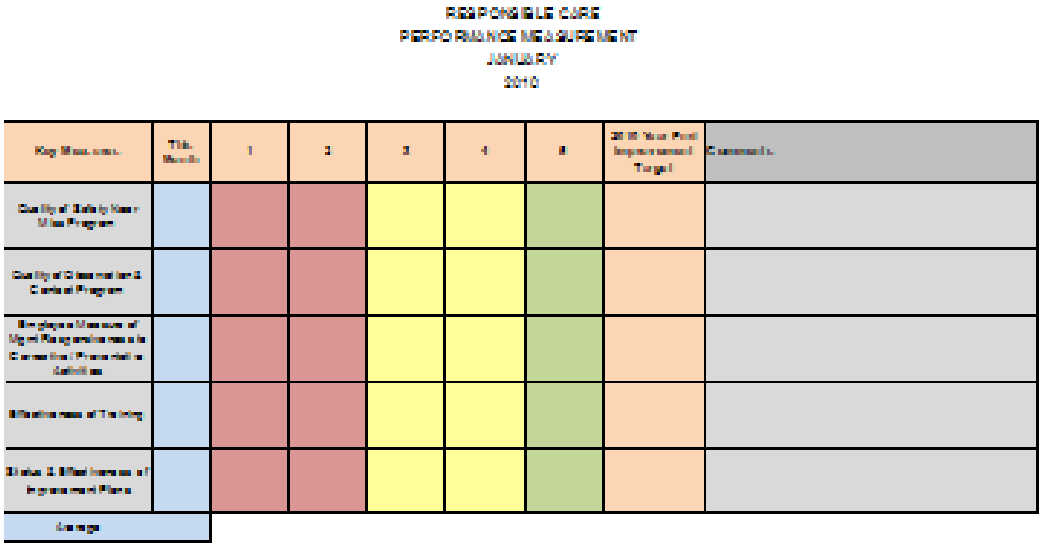


Figure 6: Company PSM/HSE KPIs Established to Monitor Culture Change

Facility key performance indicator improvement plans were required to be included in the facility RCMS goals and objectives. The status and effectiveness of the KPI improvement plans and progress against the RCMS goals and objectives are tracked monthly.

To roll out the improved Goal Is Zero program, a Global Responsible Care® and Operational Excellence Conference was held in September 2009. All Responsible Care® managers and facility managers were in attendance. Facilities began reporting on the program in January 2010. After one year, the culture evaluation was repeated in December 2010, and adjustments to the program were made as a part of the 2011 Corporate RCMS goals, objectives, and targets. All facilities were encouraged to review progress against their own programs and include KPI improvement plans in their RCMS goals, objectives, and targets.

When company began in 1999, their global employee recordable injury frequency rate was over 4.0 and in the fourth quartile for an ACC mid-sized company. The following figures show the improvement that the company made in PSM/HSE performance – all due to the PSM/HSE culture improvement initiative described above.

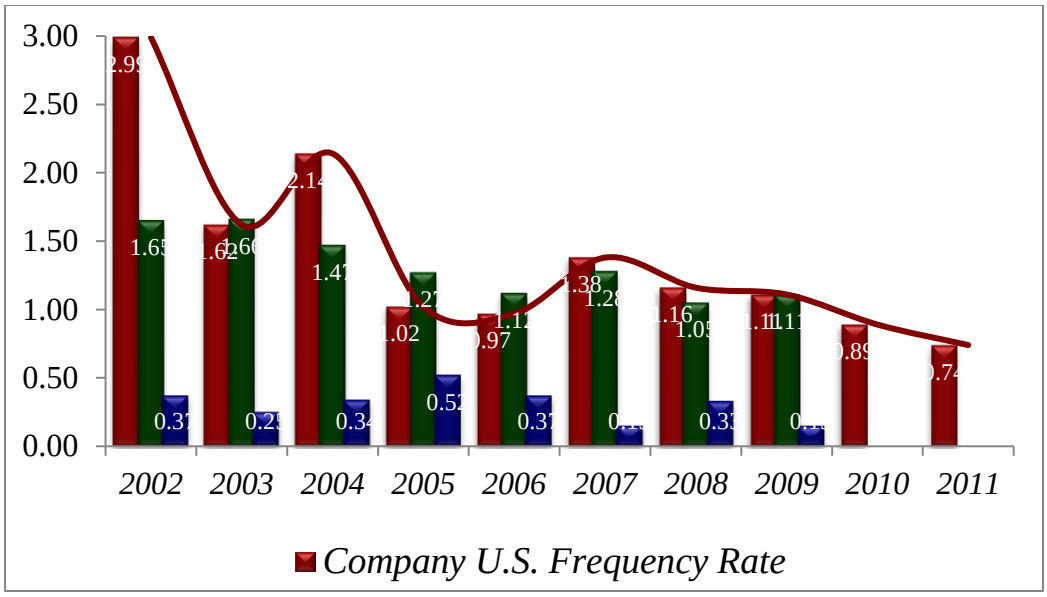


Figure 7: Company U.S. Employee Recordables Frequency Rate Improvement

Through its Goal is Zero initiative and other process improvements, the rate was reduced to near the ACC average. Since the renewal of the Goal is Zero initiative and the emphasis on the underlying safety culture which were linked to RCMS continual improvement initiatives, company employee injury/illness frequency rate has moved to the ACC first quartile (0.42), with every expectation of improving to an ACC Best in Class position. As of February 2011, company has achieved 33 months without a process safety incident, and 21 months without an environmental incident.

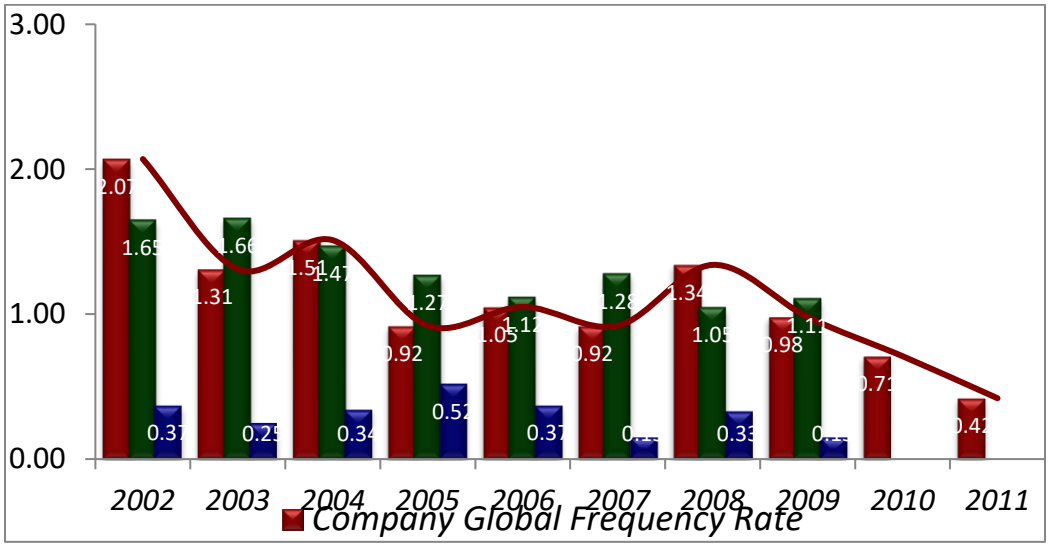


Figure 8: Company Global Recordables Frequency Rate Improvement

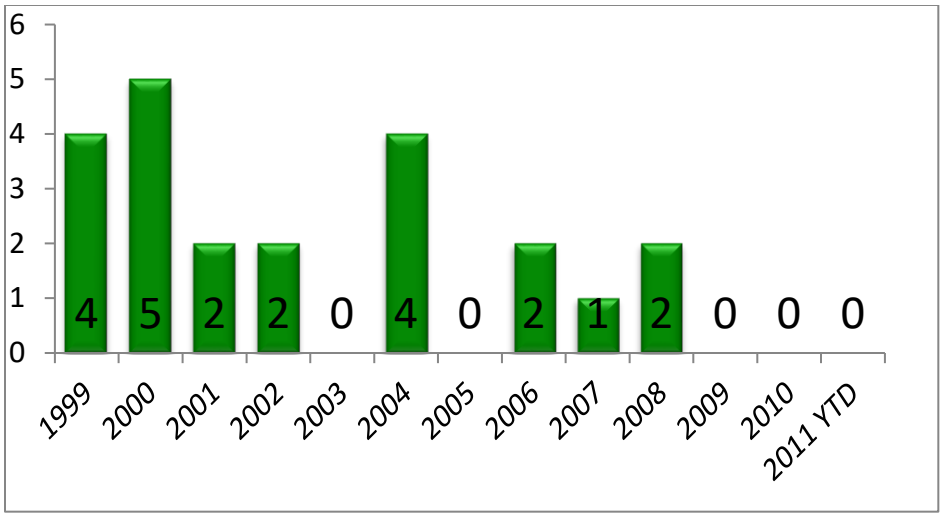


Figure 9: Company Process Safety Incident Rate

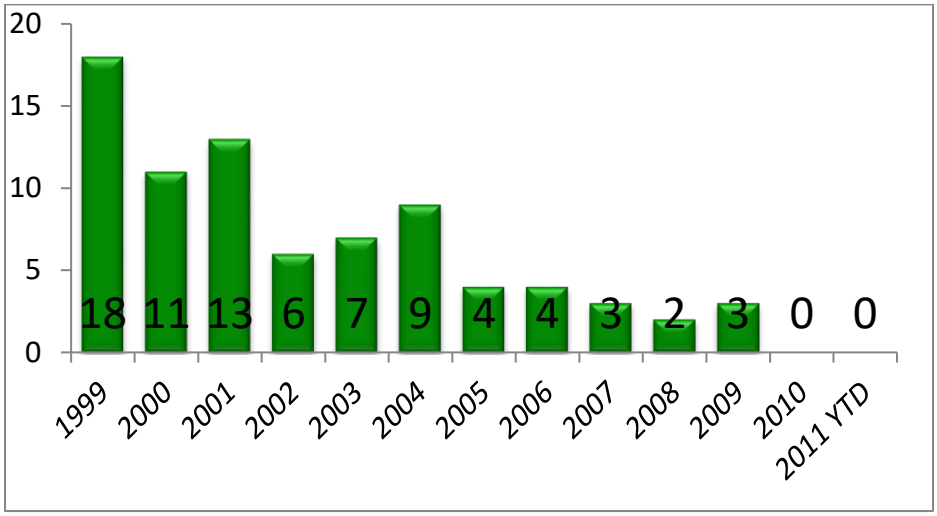


Figure 10: Company Environmental Incident Rate

7. CONCLUSIONS

Many companies have overall safety policies or visions that embody some sort of "pursuit of zero accidents". However, pursuit of ZERO is difficult and is often interrupted by organizational issues. This paper shows and example of one company that evaluated its PSM/HSE culture, took corrective action to address PSM/HSE culture weaknesses, and then resumed its **DRIVE TO ZERO**.

If you have PSM/HSE/process safety performance stagnation, indicated by chronic problems that never get/stay better, then you should consider examining your company's PSM/HSE culture and improving your chances of future continuous improvement of PSM/HSE performance.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Hazard Analysis Study of Vehicle Impacts in a Chemical Plant

Jaime Tseng, Ph. D., Carl Harrison
Formosa Plastics Corporation, U.S.A.
Email: JaimeT@ftpc.fbcusa.com

Abstract

Vehicles in chemical plants and refineries can be ignition sources for fires and explosions, particularly in situations involving crash impacts that cause chemical leakage. Generally, HAZOP methodology is used for facility risk evaluations, but HAZOP is inappropriate for mobile vehicles and normal protection systems or safeguards typically do not address such situations adequately. Thus, incidents caused by vehicle impacts can present a gap in a facility's hazard assessment process.

Hazards associated with vehicle incidents in a chemical plant were evaluated. An initial review revealed that there are few effective operational hazard-reduction actions that can be implemented, particularly for vehicle speeds over 40 mph. Therefore, speed control becomes the most important factor for risk reduction when selecting effective safeguards and providing hazard protection. Administrative actions such as controlling speed and limiting vehicle access to certain areas are suggested. Engineering controls include gate restrictions, ditches, berms, permanent and portable concrete barriers, guardrails, and bollards or posts to reduce risks associated with vehicle impacts.

A list of suggested administrative and engineering controls is presented, along with a guideline for varied speed limits directed at reducing vehicle impacts, hence their associated risks and consequences. Hazard analysis teams can consider using this information as they conduct their reviews and make their recommendations.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Achieving Operational Excellence by a Robust Sustainable Safety (process and people) Program

Chris Israni, Geni Stevens, Radhika Bompelly
ERM, City Centre 4
840 West Sam Houston Parkway, Suite 600
Houston, Texas 77024, USA,
+1-832-730-5514
Email: Chris.israni@erm.com

Abstract

Corporations have been consistently involved in the areas of process safety, people safety and risk management for several decades. These corporations have witnessed major and minor incidents, and their learnings have been consistently captured under various initiatives, some of which have also been responsible for introducing new regulatory regimes and have been game changers for the way companies operate. Another trend, emerged in the industries is the concept of sustainability.

Corporations have begun emphasizing their sustainability performance is tied into their safety program (process and people) which assists in reaching their goal of operational excellence. Hence, when a robust proactive risk management exercise is initiated during the concept of inception of the facility, and then carried out effectively and continuously until the demolition and decommissioning of the facility, it renders success towards the excellence program.

Another key component for success in safety program, is the appropriate management of safety culture within the organization. This includes the staff and the leadership. Irrespective of the hierarchy, it is important that the members of the organization understand and respect the hazards of their operations, on a day to day basis. These hazards maybe related to people safety or process safety.

This paper will discuss the influence of safety culture and leadership; along with the influence through the safety management systems (people and process safety management) that fall under the health safety and environment HSE domain of the organization. The authors will share their experiences and observations from the various sectors, and draw analogies. Their case studies will be examples of how to make these management aspects can be sustainable, without any compromises or breaches in the safety culture of the organization.

Keywords: Process safety, sustainability, operational excellence, risk management, risk identification

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Acting on Information from Small Incidents and Near Misses

Mike Munsil
PSRG, Inc.
800 West Sam Houston Parkway South
Suite 107, Houston, Texas 77042, USA
Email: mmunsil@psrg.com

Abstract

This presentation will look at moving beyond simply acquiring data from small incidents and near misses to addressing common mistakes made following collection of this data. Recording relevant and accurate data from small incidents is necessary, but often the opportunity to use the data to initiate meaningful change is missed. This presentation identifies three points at which companies fail in their handling of small incident and near miss data and presents responses to those common failures.

1. Focus on examining data recorded and identifying what data is dependable and relevant, then moving on to selection of techniques for sound statistical analysis.
2. Focus on taking the sound data acquired and the statistical methods applied and creating meaningful, understandable results.
3. Focus on presenting that information in a persuasive manner to management personnel who may be more focused on profitability than safety but are in a position to influence change.

Keywords: Incidents, Near Miss, Safety, Analysis

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Assessing Operational Excellence

Ian S. Sutton
Sutton Technical Books
PO Box 2217
Ashland, VA 23005

Email: ian.sutton@stb07.com

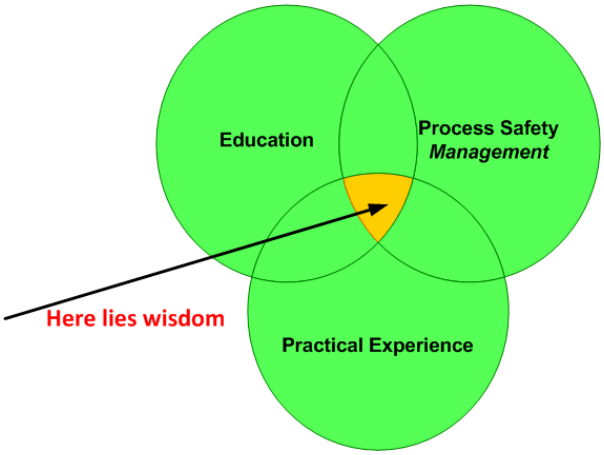
Keywords: Process safety, operational excellence, practical experience, process safety wisdom

Abstract

The discipline of process safety management is mature. For example, the OSHA (the United States Occupational Safety & Health Administration) standard was promulgated in May 1992; the standard is older than people who are now entering the energy and process industries.

The elements of process safety management are just one aspect of an effective, overall safety program. Other elements include formal education and practical experience. When combined they create what can be referred to as process safety wisdom as shown in Figure 1. They also move the program beyond just safety into overall Operational Excellence in which issues such as production, productivity and efficiency are considered.

Figure 1



Of the three elements shown in Figure 1 the one that is most difficult to systematize is practical experience — the knowledge and insights built up by people who have worked in industry for many years. In order to gather and assess such experience an Operational Excellence Assessment system has been developed. It is buit up of hundreds of questions to which there is no "right answer" — merely an expert response. This response is supported by the guidance and suggestions that an expert might provide.

This paper describes the development and application of an Operational Excellence System.

INTRODUCTION

Shortly before writing this paper I received an email from a colleague who works as a process safety professional in the offshore oil and gas industry. He also offers training courses to do with process safety. In response to one of his proposals for training the potential client said that all they needed was a two hour high level introduction.

My colleague was, not without reason, somewhat exasperated at this response. But, as he and I discussed what had happened we noted that the discipline of process safety management is mature, and, in spite of its successes, maybe it has become "just another program", indeed maybe it is becoming somewhat stale.

If that is the case then maybe we process safety professionals need to take at least some responsibility for this lackluster attitude. In an email I said,

> *Maybe the responsiblility lies with us — we need to make the discipline more relevant and interesting.*

If such is the case, then one of the challenges and responsibilities of process safety professionals is to introduce new ideas and initiatives that make their work more relevant and useful than it is now. And one of those initiativies lies in the theme of "Operational Excellence".

The term Operational Excellence covers a wide range of topics. This paper considers one of those topics — the incorporation of operational experience with other parts of process safety management to create something that might be called "Operational Wisdom".

MATURITY OF PROCESS SAFETY MANAGEMENT

Process safety management (PSM) has always been integral to manner in which companies in the process and energy industries operate. For example, they have always written procedures, trained their work force and conducted incident investigations. But, if the discipline is to have an formal start date, then May 26th 1992 is a good candidate. It was on that date that OSHA (the United States Occupational Safety & Health Administration) promulgated its standard 29 CFR 1910.119. The new regulation required many companies in a wide range of industries to implement a comprehensive and formal process safety program in an expeditious manner.

The new rule, along with other similar initiatives, also led to the creation of a process safety culture, involving not only the companies directly affected, but also organizations such as the

Center for Chemical Process Safety, the Mary Kay O'Connor Center, and a wide range of companies offering consulting and software services.

OSHA's PSM program is now 26 years old. That's a long time. If most professionals in the process industries enter the business at the age of 22, then for anyone younger than age 48 process safety is is not a new initiative — instead it is a part of the established way of doing things. The discipline of process safety management is mature.

It is a given that any company can improve its process safety performanc — after all, in a performance-based system the only way to achieve success is never to have an incident. And no company can claim to have reached that goal. (Which is why no company can be "in compliance". The only way of achieving that goal is never to have an event — something that can never be achieved.)

Nevertheless, in spite of the fact that some companies still have a lot of work to do, there have been major improvements in the quality of process safety programs since the year 1992. And, although catastrophic events occur only rarely, thus making it is difficult to measure progress with statistical confidence, the number of serious incidents does seem to have declined.

OPERATIONAL EXCELLENCE

A phrase that has gained increased use in recent years is "Operational Excellence" (OE). Although there is no universally agreed upon definition for this term an OE program is generally comprised of the following components:

1. A right or correct culture;
2. Continuous improvement;
3. An integrated management system; and
4. Operational discipline.

All four of these elements are part of process safety management (PSM). Therefore an existing PSM program can provide a sound basis for developing Operational Excellence.

Operational excellence goes beyond safety performance. If a company has a good process safety management program then it will also have a good overall management program — one that will help in other areas such as production, productivity and environmental compliance.

The Institute for Operational Excellence defines the operational excellence as follows.

> *Each and every employee can see the flow of value to the customer, and fix that flow before it breaks down.*

This definition bears similarities to the Employee Participation element of the OSHA PSM regulation. Paragraph (c)(2) of that element states,

Employers shall consult with employees and their representatives on the conduct and development of process hazards analyses and on the development of the other elements of process safety management in this standard.

So, if process safety already provides the basis of an OE program, what is needed is not a new management system *per se*, but better ways of "consulting with employees", such that every employee can see the flow of value to the customer (or organization).

THE REFINERY SUPERINTENDENT

A mid-sized refinery suffered an unexpected shutdown due the failure of a major piece of equipment. (There were no safety issues associated with this event.) The equipment was repaired and the refinery was ready for restart.

The refinery superintendent — who knew the facility intimately — had recently retired. But management knew that his expertise would be invaluable during the restart, so they asked him to return and direct the start-up activities. He did so, and, for a period of two days stood in the control room successfully directing the start-up just from memory — he did not need procedures or documentation.

This situation presented a huge opportunity for enhancing the process safety program and employee participation in particular. If management had installed a video camera in the control room and recorded his every command they would have had a wonderful training program for future operations personnel.

But they did not — the opportunity was missed.

This was just one incident. But it is probably fair to say that few companies have a system for capturing and recording the insights and wisdom that their highly experienced employess have garnered over many years of experience in the "School of Hard Knocks". Were they to do so they could make significant strides toward Operational Excellence.

PROCESS SAFETY WISDOM

The well-known literary critic, Harold Bloom of Yale University, once asked,

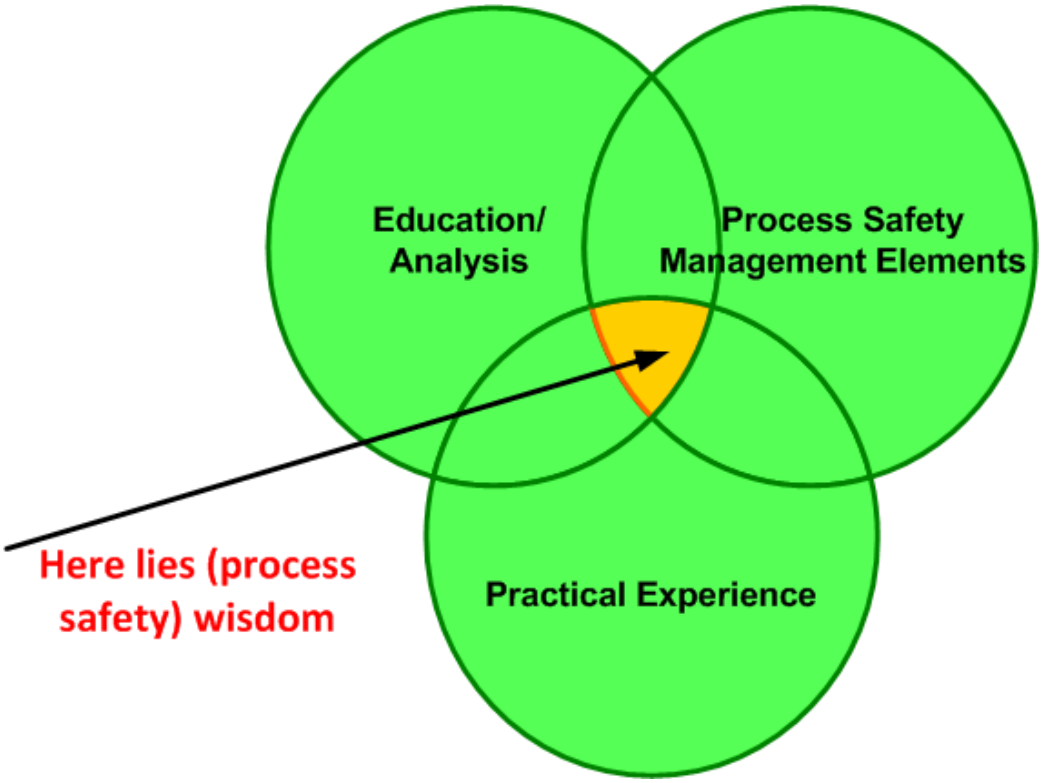
Information is endlessly available to us; where shall wisdom be found?

He posed that question in the early 1990s when the Internet was still in its infancy. The question possesses much greater urgency now than it did in those days.

Applying his insight to the world of process safety, information does indeed seem to be "endlessly available to us". But to what end if we do not know how to understand, digest and apply that information?

Or, to put it another way, "where shall process safety wisdom be found?"

One possible answer to this question is to divide the world of process safety into three areas, as shown in the Venn diagram.



The sketch consists of three overlapping components:

1. Education and analysis.
2. The elements of process safety management.
3. Practical experience.

Combined they create “Process Safety Wisdom” — the foundation for an Operational Excellence program.an Operational Excellence program.

1. Education and Analysis

The first source of knowledge — direct education — is the simplest to define and understand. For example, if a hazards analysis team has a question to do with the capacity of a pressure safety relief valve then someone with an education in fluid flow can calculate the rating of the valve and determine if it meets requirements or not based on well-established engineering standards.

Direct education is also needed when responding to regulatory requirements. Someone who wants to know if their system is in compliance with a regulation or standard simply needs to read the relevant documents and apply them to the current situation (although some interpretation is usually required).

Analytical techniques supplement the educational process. For example, in the case of the relief valve being reviewed by the hazards analysis team, the application of standards can be supplemented with detailed mathematical analysis.

2. Elements of Process Safety Management

Process safety programs are generally organized around management elements such as hazards analysis, operating procedures, prestartup reviews and management of change. The number and scope of the elements varies from company to company and from regulator to regulator. (The OSHA standard has fourteen.) In spite of detailed differences, they are all dialects of the same language.

It is in the development and implementation of these programs that great progress has been made in the last 26 years. And doubtless there will continue to be improvements in each of the elements. For example, the Bow-Tie and Layers of Protection Analysis methods for determining hazards and risk are both quite new and have both gained acceptance in recent years. Nevertheless, it is unlikely that there will be major changes in the manner in which the elements of process safety are managed. This is definitely an area of maturity.

3. Practical Experience

Education and an understanding of management principles are a vital and necessary part of any process safety management program. But they are not sufficient because they are general in nature — they cannot cover the details of every situation; they cannot provide specific guidance for all situations.

People who have worked at a facility or in a design office for many years generally have a good, almost intuitive, understanding of what works and what doesn't. (Which is the reason for telling the story about the refinery superintendent.) They have learned from their own mistakes and from the mistakes of others. They are graduates of the School of Hard Knocks.

Experience enables you to recognize a mistake when you make it again.

One large energy/chemical company demonstrated this insight in an ingenious manner. When a young professional first entered that company, no matter what their job was, no matter who their boss was, and regardless of the work that they were doing, for his or her first year their paycheck said, "Training Department". This was a neat way for the company to tell its new employees that they were not actually making a contribution because they knew very little about what they were doing in the "real world".

In the words of the bumper sticker, "There's no substitute for knowing what you're doing".

Industrial, practical experience includes not only a hands-on knowledge of industrial processes and equipment but also how to work with colleagues, subordinates and bosses; understanding the realities of client/consultant/contractor relationships; the resistance that managers can have toward spending money on safety; problems at the management/union interface; and how government agencies actually enforce regulations.

Therefore, perhaps the biggest opportunity for achieving "process safety wisdom" lies in finding ways of capturing and transmitting industrial, "real life" experience to those who are new to the business.

COMPLEXITY — NOT COMPLICATION

In order to capture the experience of seasoned professionals it is important to distinguish between the words 'complicated' and 'complex'. A complicated system has the following features.

- It is predictable; it can be understood by breaking it down into smaller parts, and then determining how those parts work, and how they interact with one another.
- A complicated situation can be quantified and understood through the use of metrics.
- A Command and Control management structure is effective at managing complicated systems.

Most process safety work addresses itself toward the management of complicated systems. For example,

- Once a method for writing operating procedures has been developed, then that method can be used throughout the organization for writing procedures for all types of facility and activity.
- Once a hazards analysis team has identified how a pressure vessel may rupture they can apply that insight into the operation of all other pressure vessels.
- Once an effective technique for analyzing incidents has been developed, that technique can be used for all future incident investigations.

A *complicated* system is 'understandable' and 'repeatable'. A complex system, on the other hand, is based on relationships, interconnection and evolution. It is fundamentally unpredictable. (Any system which involves human behavior — particularly the behavior of people in groups — will be complex.)

Complex systems do not have to be complicated — although most are. (Climate change is a good example of a system that both complex and complicated.)

Key aspects of a complex situation include the following.

- It comprises relationships that cannot be understood just by breaking a system into its component parts.
- The situation is fluid — surprises happen.
- 'Command and Control' structures will be limited in their effectiveness.
- It cannot be easily quantified — there are no effective metrics.
- It will often involve the unpredictable behavior of human beings, both as individuals and in groups.

Adding experience of the "real world" to Operational Excellence means understanding that the new management system is not just complicated, it is complex.

OPERATIONAL EXCELLENCE ASSESSMENT SYSTEM

One way in which experience can be captured is through the development of an Operational Excellence Assessment program. Such a program mimics the behavior of a professional if he or she is asked to evaluate a facility's performance. It consists of a large number of questions that are representative of what the expert would ask were he or she on site.

There are no right or wrong answers to the questions — opinions and judgment are welcome. The key to such as system is that the expert records what he or she is thinking and looking for when responding to each of the questions. His insights can then be structured in a manner suitable for educating personnel with less experience.

The Table illustrates the concept, in this case for when an expert is evaluating a Prestartup Safety Review program.

Question Number	Question	Response (Y / N / NA)
2.1	Are reviews conducted by a team?	
Discussion		

The question in the Table is a simple one: "Are the reviews conducted by a team?" In the discussion box the expert can speak to issues that would concern him. These could include:

- Is a team review always needed?
- Who should be on the team?
- What should their experience be?
- Who will lead the team?

The aim of these questions is to capture the experience of the expert and to understand why he answers the questions in the way that he or she did.

CONCLUSIONS

The following conclusions can be drawn from the above discussion to do with Operational Excellence.

- Process safety management programs already are, to a considerable degree, operational excellence programs because they incorporate the need for employee participation.
- An opportunity and a challenge will be determine how to capture the experience and insights of experienced employees in a system that is not only complicated, but complex.
- It is suggested that one way of achieving this goal is to develop an Assessment System for capturing the knowledge, opinions and judgments of experts in specific areas of process safety management.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Cybersecurity Consideration in Process Hazard Analysis

Addie Cormier, Christopher Ng
Siemens Energy, Inc.
Process Safety Consulting
Houston, TX 77027
Email: info.ogconsulting.energy@siemens.com

Abstract

Traditional process hazard analysis (PHA), such as Hazard and Operability (HAZOP) studies, typically includes a systematic assessment of initiating events and consequences affecting process facilities. Relationships among initiating events, safeguards, and consequences are evaluated in depth, but such evaluation is generally based on unintentional causes such as human error or some unexpected failure of equipment, instrumentation, controls, or safeguards. As the process industry evolves toward greater reliance on and integration with information technology, it is critical to also consider malicious and intentional disruption of process operations by parties who exploit the enhanced capabilities and integration of modern communication with process controls and operations.

This paper discusses the significance of considering cybersecurity threats during a PHA/HAZOP. A step-by-step and systematic technique is presented to show how a PHA team could assess the vulnerability of a system or facility to potential cyber threats, analyze adequacy of safeguards, and develop necessary countermeasures to resist cyberattacks. A typical refinery or chemical plant can have thousands of signals that are connected to a Distributed Control System (DCS) to ensure safe and smooth process operation. This arrangement could inadvertently present multiple pathways for malicious parties to intervene by manipulating signals or disrupting communications, potentially leading to severe process hazards and consequences such as a fire, explosion and fatality. Not only does incorporating cybersecurity in a PHA/HAZOP help identify the vulnerability of your system or facility, it could also be used to prioritize limited resources to ensure critical vulnerabilities are mitigated in a timely and efficient manner. The application of this technique will be demonstrated using case examples.

Introduction

Process hazard analysis (PHA) is an essential element of process safety management and widely adopted to evaluate systematically the hazards associated with process plant design and operation and to minimize the risks associated with such hazards. Traditional methods such as Hazard and

Operability (HAZOP) and What-If/ Checklists have been successfully applied by using a team based approach to evaluate potential design flaws or deviations from safe design and operational practices as well as to identify initiating events, assess potential consequences of such events, and implement acceptable safeguards or barriers to prevent or mitigate the consequences. Relationships among initiating events, safeguards, and consequences are evaluated in depth, but generally based on unintentional causes such as human error or some unexpected failure of equipment, instrumentation, controls, or safeguards.

As the process industry evolves toward greater reliance on and integration with information technology, it is critical to also consider malicious and intentional disruption of process operations by parties who might exploit the enhanced capabilities and integration of modern communication with process controls and operations.
Attacks using cyber technology on process facilities have been well-publicized, such as the socalled Stuxnet computer worm that might have infected industrial control systems in several countries, impacting plant operations and damaging plant equipment. Another cyberattack using so-called spear-phishing techniques has apparently occurred at a German steel mill, impacting both control and safety instrumented systems and resulting in physical damage to a furnace system. Common types of cyberattacks together with further details on the examples cited above are provided below.
Total costs to companies which are victims of cyberattacks are easily in the billions of dollars per year and are likely under-reported as companies seek to avoid negative publicity and loss of clients or business as well as many companies may not have resources to detect and recover from such attacks, let alone to prevent future attacks.1 Therefore, the impacts of cyberattacks have often been realized but not fully quantified.
A systematic method to integrate cybersecurity analysis as part of a PHA/HAZOP is presented in this paper.

Types of Attack

Cyberattack vulnerability could be traced to the exploitation of various complex network loop holes thus allowing malicious software to penetrate inadequate firewalls or be introduced into a computer network by means of a USB thumb drive. A list of some of the common cyberattack methods is highlighted below.2

- Malware: Code with malicious intent that typically steals data or destroys something on the computer.
- Phishing: Phishing emails include a link that directs the user to a dummy site that will steal a user's information. In some cases, all a user has to do is click on the link.
- Man in the Middle (MITM): Gains access through a non-encrypted wireless access point. They would then have access to all of the control information being transferred between both DCS and equipment.
- Malvertising: Compromise your computer with malicious code that is downloaded to your system when you click on an affected ad.
- Rogue Software: Malware that masquerades as legitimate and necessary security software that will keep your system safe.

- Drive-By Downloads: Through malware on a legitimate website, a program is downloaded to a user's system. It doesn't require any type of action by the user to download.

While it would be unreasonable to expect a typical PHA team to address in detail the vulnerability of a process plant to such cyberattack methods, the team should at a minimum check that such an assessment has been completed (outside of the PHA) and resulting findings adequately resolved. The PHA team could also check that a cybersecurity program has been implemented at the site, consistent with current industry best practices, such as the ISA/IEC 62443 series and particularly ISA/IEC 62443-3-2 standard (Security Risk Assessment and System Design) 3 which is pending ballot/ release.
Such assessment would include an extensive mapping of the control system network architecture, detailing how control and communication functions are implemented between the DCS and field devices such process sensors and actuators for control valves. In addition, communication links between the control system and the network or workstation operating system environment as well as with the business enterprise software and the outside world (through the internet) are mapped as well and then partitioned into zones with conduits allowing for communication between zones based on the type and criticality of function, access control, etc. Target security risk levels are assigned for each zone, and appropriate safeguards implemented to ensure target levels are met.

1. Case Study Malware Attack: The Stuxnet Virus Centrifuge Breach
   The Stuxnet was introduced by the infection of a computer and propagated to all other connected machines running Microsoft Windows. Stuxnet was a malicious worm virus.

   The virus apparently compromised the target systems at the Iranian Natanz nuclear plant and took control of the centrifuges, misleading operations by overriding the process variables and giving false feedback to the outside controllers (alarm and automatic safety shutdown system) and thus reportedly caused the impacted centrifuges to spin outside their safety operating limits and to fail eventually.

   Later, a separate operating company confirmed a potential Stuxnet virus breach on its machines, indicating the virus might have inadvertently spread beyond its intended target (Natanz plant) possibly due to a programming error and thus allowing the worm to spread from an engineer's infected computer to the internet. 4

2. Case Study Spear-Phishing Attack: Steel Mill Furnace Breach
   Germany's Federal Office for Information Security (or BSI), indicated the attackers gained access to a steel mill through its business network and then worked their way into the production network, gaining access to the control systems for plant equipment. 5 This type of attack is known as "Jumping" where the intrusion is in one area of the company's network but then jump to another. The breach was in the business network but leaped to the production network. The attack reportedly resulted in loss of shutdown control on one of the blast furnaces and physical damage to equipment.

As experts, in the cyber world, race to keep up with the evolving nature of the attacks, hackers are constantly deploying new ways to infiltrate and cause harm or damage. Beyond implementing robust information technology (IT) practices to detect and ward off malicious

software as well as recover from such attacks, it is also important to raise organizational awareness, identify vulnerabilities, and develop effective countermeasures by using all other available tools.

The PHA process lends itself well as an effective tool to support such efforts. By systematically evaluating the hazards associated with each section of the facility, the PHA team should already have a well-documented understanding of the type of consequences for various initiating events and the effectiveness of available safeguards. Historically, PHA's have been focused on preventing and mitigating consequences categorized usually in terms of safety, asset damage/business interruption, environment, and reputation. Cyberattacks have the potential to inflict any of such consequences, and traditional PHA's could be leveraged to help minimize them.

A traditional PHA team is comprised of representatives from different areas such as operations, engineering (different disciplines), and management who collectively review and discuss what could go wrong at a process plant and how to prevent the associated consequences. Equipped with the right mix of skillset among the PHA team members, the team should be able to recognize what types of initiating events are relevant to the undesirable consequences to be prevented and what safeguards would be considered effective. Using a typical nodal approach, the PHA team would evaluate each section of the plant systematically in this context and develop recommendations for improvement as needed.

Taking a step further, the PHA team could include an assessment of cybersecurity threats and vulnerabilities, their potential consequences, and safeguards under consideration. With qualified Instrumentation and Control (I&C) and Information Technology (IT) subject matter experts participating in the PHA's, weak points in the control and communication systems that might be exploited by hackers to gain access and cause harm could be identified and eliminated. A couple of general approaches are presented below.

General Approach

There are two general methods to perform a PHA integrated cybersecurity assessment.

- The first method is used to assess the basic process control system (BPCS) vulnerabilities as an independent node, such as by means of a Control Systems Hazard and Operability Study (CHAZOP) which could be extended to cover cybersecurity vulnerability.

This method controls the cyber risk through process controls network (PCN). For example, instrumentation or process measurements which are attached to the Distributed Control System (DCS) may be vulnerable to an attack, such as the MITM type of attack as reportedly deployed with the Stuxnet virus. For critical applications, emergency shutdown systems involving dedicated sensors, logic solver, final control elements, and communication pathways which are independent of the BPCS might be warranted such as those typically implemented as part of a Safety Instrumented Function (SIF) or automated Emergency Shutdown (ESD) system.

- The second method, based on an integrated cyber process hazard analysis, could also be used to assess the process system cyber vulnerabilities by integrating with a typical PHA and is applied to control the cyber risk by implementing non-hackable countermeasures.

The second method, integrated cyber process hazard analysis, will be described further in this paper. Adding cybersecurity analysis to a typical PHA requires a step by step systematic technique in the review of the cyberattack impacts and countermeasures. This approach could also be used as a “stand alone” or backup to the first method. If the BPCS is compromised, applications that have been reviewed using integrated cyber process hazard analysis method could lessen the overall risk impact.

This method considers the initiating event and safeguards to determine if they can be hacked and if the consequence is ranked significant. If so, the Process Hazard Team could specify instrumentation plus other mechanisms required to mitigate similar gaps using devices that could not be hacked. Device and instrumentation such as pressure safety valve (PSV), level gauges, pressure and temperature indicators that are not integrated into the DCS system and Operations External Monitoring could provide useful back-ups in the event of cyberattacks.

Table 1 shows an application of integrated cyber process hazard analysis. The initiating event is related to a pressure control valve located at the inlet of a pressure vessel and which could fail wide-open. Such failure would have been evaluated in a traditional PHA as possibly caused by mechanical or electrical malfunction. However, one could also observe that the operation of this control valve could also be vulnerable to cyberattack.

The Risk Ranking (RR) before safeguard consideration is an overall 6 based on severity level of 3 and likelihood level of 2. Based on the risk matrix used for this example, a scenario with an RR of 6 can continue to operate only if safeguards are in place to prevent personnel injury.

One might be tempted to take credit for a local pressure indicator/ gauge as a safeguard (SG). While this indicator is not vulnerable to cyberattack, it would require timely and reliable human intervention to be considered effective. The PHA team concluded that such instrumentation even together with human intervention would not be considered an acceptable safeguard as the indicator is not continuously monitored. Similarly, a pressure transmitter and its associated high-pressure alarm PAH-002, even if independent of the process control loop for the PCV-001 and continuously monitored, would also not be reliable as the pressure signal could be vulnerable to manipulation during a cyberattack.

A recommendation was then developed to install an adequately sized PSV to be routed to a safe location. Note that this PSV would not be vulnerable to cyberattack as its opening behavior is dependent on the vessel operating pressure as well as on the closing force exerted by the spring of the PSV.

Table 1: Example of Cyber Integrated

More Flow						Cyber Vulnerable?		Recommendations
Initiating Event (I.E)	Consequence	Risk			Safeguards (SG)	I.E.	SG	
		S	L	RR				
Pressure Control Valve (PCV-001) at inlet of Vessel V-101 fails wide-open due to mechanical/ electrical malfunction or possibly due to cyberattack creating an erroneous signal to force the valve open.	Potential overpressure of Vessel V-101 due to high upstream pressure source, resulting in release/ spill and loss of downstream feed.	3	2	6	Pressure Indicator (P-001) with Operator Intervention	Y	N	Team concurred that P-001 or PAH-002 would not be considered an acceptable safeguard. Therefore, the Team recommends installing an adequately sized PSV to be routed to a safe location.
					PAH-002 (High Pressure Alarm) with Operator Intervention	Y	Y	

While defending against all forms of cyber intrusion into the plant control system and operation is the ultimate goal, the integrated cyber PHA is also well-positioned to help plant personnel identify critical cyber vulnerabilities that could potentially expose the company to the most severe consequences with associated risk that might fail to meet the company's acceptance criteria and thus prioritize the allocation of scarce resources to enhance protection.

Safeguards

Performing an integrated cyber PHA requires one to control threats, vulnerabilities, and consequences. In order for a typical cyberattack to propagate from initiation to completion, it would typically require that both the initiating event and the safeguard(s) both be hackable. By making at least one of these two be non-hackable, the risk would substantially be reduced. By making both be non-hackable, the risk would be eliminated. For example, can a USB port be used to compromise the system? Then the first order of controls is to deactivate the ports. This would eliminate a conduit whereby the virus could intentionally or inadvertently be introduced into the system. Table 2 is an example of a Cyber Vulnerability Matrix that can be used during an integrated cyber PHA to assess system cyber weaknesses.

Table 2: Cyber Vulnerability Matrix

	Case 1	Case 2	Case 3	Case 4
Initiating Event Hackable?	N	Y	N	Y
Available Safeguards Hackable?	N	N	Y	Y
Likelihood of Consequence	N/A	Unlikely	Unlikely	Likely
Require Non-hackable Safeguard?	N	N	Decide based on risk tolerance	Likely

Note: N=No and Y=Yes

By understanding the different types of cyber threats that a process could be exposed to, one could then fully comprehend the in-place risks and develop effective mitigations to reduce or eliminate the risk. Staff training on cybersecurity awareness is essential to the understanding of cyber threats and safeguarding against them. Integrated cyber PHA could be used to enhance both awareness and readiness of plant personnel against cyber threats.

Table 3 contains examples of safeguards that would be resistant to cyberattack for different scenarios. To the extent that one could rely on devices that operate independently of the control system, common mode failure could be avoided. For example, a spring-operated PSV would relieve excess system pressure without relying on a signal from the DCS.

In terms of designing safeguards, there is a well-established concept called "defense-in-depth" which includes multiple independent layers of protection to protect against process hazards. In the context of cyberattacks, such layers might include but not limited to company policies and operating procedures, personnel training, network compartmentation, access restriction, physical barriers, installing software patches for operating systems, running up-to-date antivirus software, and continuous system monitoring to detect and contain intrusion.

With regards to SIS, IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector) 6 has implemented a new clause, requiring that a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. The PHA team could also check if this is being implemented for installed SIS.

Table 3: Examples of Cyber Secure

Scenario	Cyber Secure Instrumentation	Cautionary Remarks
Overpressure due to blocked outlet	Pressure Safety Valve (PSV)	Ensure appropriate design and sizing of PSV
BPCS failure	1. Safety Instrument System 2. Analog Back-up	Ensure SIS is independent of the BPCS.
Rotating equipment failure	Mechanical Overspeed Control/ Trip	Routine maintenance
Reverse Flow due to Pump or Compressor Failure	Non-return Check Valve	Routine maintenance
Critical (Shutdown) Valves	Back-up Hand Valve	Routine maintenance
Area H2S Monitor Failure	Back-up Personal Monitors	Routine maintenance
Level Alarm or Transmitter Failure	Level Gauge on Tank or Vessel	Routine maintenance and Operator rounds

Conclusion

Ultimately, the integrated cyber PHA results could help determine what countermeasures would be needed to lessen the cyberattack risks. In additional, the PHA along with a Layer of Protection Analysis (LOPA) could help with prioritizing resources for implementing required countermeasures. If the risk for a particular cyberattack is not considered significant, then it could be protected by using standard safeguards. However if a scenario has signification

consequences or risks and all safeguards could be compromised, the application would likely need at least one cyberattack resistant safeguard. Since the timing or type of a cyberattack cannot be fully predicted, the integrated cyber PHA could serve as a useful tool to reduce the overall risk profile of a process plant against such attacks.

References

1. Fernandez, I. (2013) “Cybersecurity for Industrial Automation & Control Environments, Protection and Prevention Strategies in the Face of Growing Threats”
2. Sullivan, M. "8 Types of Cyber Attacks Your Business Needs to Avoid”, quickbooks.intuit.com
3. ISA/IEC 62443-3-2 standard (Security Risk Assessment and System Design)
4. Kushner, D. (2013) “The Real Story of Stuxnet”, spectrum.ieee.org
5. Zetter, K. (2015) “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever”, www.wired.com
6. IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector)

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Addressing the Security Requirements in Functional Safety Standard IEC 61511-1:2016

John Cusimano, Tim Gale
aeSolutions
Industrial Cybersecurity
Greenville, SC
Emails: john.cusimano@aesolns.com, tim.gale@aesolns.com

Keywords: Industrial Automation, Process Safety, Functional Safety, PSM, PHA, HAZOP, LOPA, ICS, Cybersecurity, Cyber-threat, Cyber-risk, IEC 62443, ISA-99, IEC 61511

Abstract

The 2016 edition of IEC 61511-1: 2016 added two new requirements regarding the security of safety instrumented systems (SIS). The first requirement states that "a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS" and the second requirement states that "the design of the SIS shall be such that it provides the necessary resilience against the identified security risks". The standard directs the reader to ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010 for further guidance on how to comply with these requirements. While these documents are informative, the 479 combined pages do not provide concise guidance on how to address the specific security requirements. The purpose of this paper is to offer step-by-step guidance on how to address the security requirements in 61511 and to identify specific clauses in the reference standards for further information.

Why the Requirement for a Security Risk Assessment?

ISA/IEC 61511 is a functional safety standard which historically focused on random or systematic failures that could impact the ability of the safety instrumented system (SIS) to properly respond to a process demand. So why did the authors of 61511 add these new requirements for security assessments? The primary reason is that industries and governments now recognize that security threats, both physical and cyber, could significantly impact the integrity and availability of a SIS and that functional safety assessments do not historically address security threats such as physical sabotage or cyber-attacks (e.g. malware, hacking, etc.). This is particularly true for programmable electronic SIS with network communications. In other words, just because a SIS is SIL rated does not mean it is immune to physical or cyber threats.

Without performing a security risk assessment of a SIS, asset owners/operators may have a false sense of security regarding the safety of their operations.

Recent events have heightened the urgency of performing security risk assessments on SIS. Since 2010 there have been numerous publicized incidents regarding intentional attacks on industrial control systems (ICS) and SIS in critical infrastructure around the world. For example, the Stuxnet virus in 2010, the Shamoon virus in 2013, the attacks on the Ukrainian power grid in 2015 and 2016, and the Triton Malware targeted at a SIS in the Middle East in 2017.

The of Definition of Risk

Many people struggle with the term *risk* and what it means and what it doesn't mean. So, let's start with some definitions. The Oxford English Dictionary defines risk as "(exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility" (Oxford English Dictionary, 3rd ed.). This is good but it is a little too general. In risk analysis, risk is traditionally defined as a function of *probability* and *impact* where the probability is the *likelihood* of an event occurring and *impact* is a measure of the extent of the adverse circumstance (i.e. the *consequence*). The common formulaic way of expressing this is:

$$\boldsymbol{Risk = Likelihood\ x\ Impact}$$

This is also a good definition, but again, a little too general for applications where we want to assess security risk, particularly information security risk.

Security Risk

The thing many people struggle with when attempting to assess security risk, which is typically based on intentional actions, is that it is very difficult to estimate likelihood. In fact, I have heard people argue that it is impossible to assess security or cyber security risk because it is impossible to estimate the likelihood of a deliberate action. While I agree it's challenging, I disagree that it is impossible and fortunately most security professionals would agree with me. Otherwise, how would those responsible for national security or the security of major events such as the Olympic Games even begin their undertaking without some method of assessing security risk?

Actually, the solution to the "likelihood conundrum" actually quite simple. In the field of security risk analysis the likelihood component is broken down into its core elements: threats and vulnerabilities. The common formulaic way expressing this is:

$$\boldsymbol{Security\ Risk = Threats\ x\ Vulnerabilities\ x\ Impact}$$

National Institute of Standards and Technology (NIST) (Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments., 2012) explains this well by stating, "Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."

In addition to NIST, another organization called the FAIR Institute has developed a model for understanding, analyzing and quantifying cybersecurity and operational risk called the Factor Analysis of Information Risk (FAIR) framework. The FAIR framework factors security risk into

its elements making it easier to understand and more practical to assess. Figure 1 is a visual of the FAIR model that is provided by the FAIR Institute. As you can see, the model dissects likelihood (which FAIR calls loss event frequency) into Threat Event Frequency and Vulnerability. Sound familiar? The FAIR model further breaks down Threat Event Frequency into Contact Frequency and Probability of Action. Finally, Vulnerability is broken down into Threat Capability and Resistive Strength.

As you can see, it not impossible to assess cybersecurity risk. You simply need a good framework, methodology and guidance to get started.

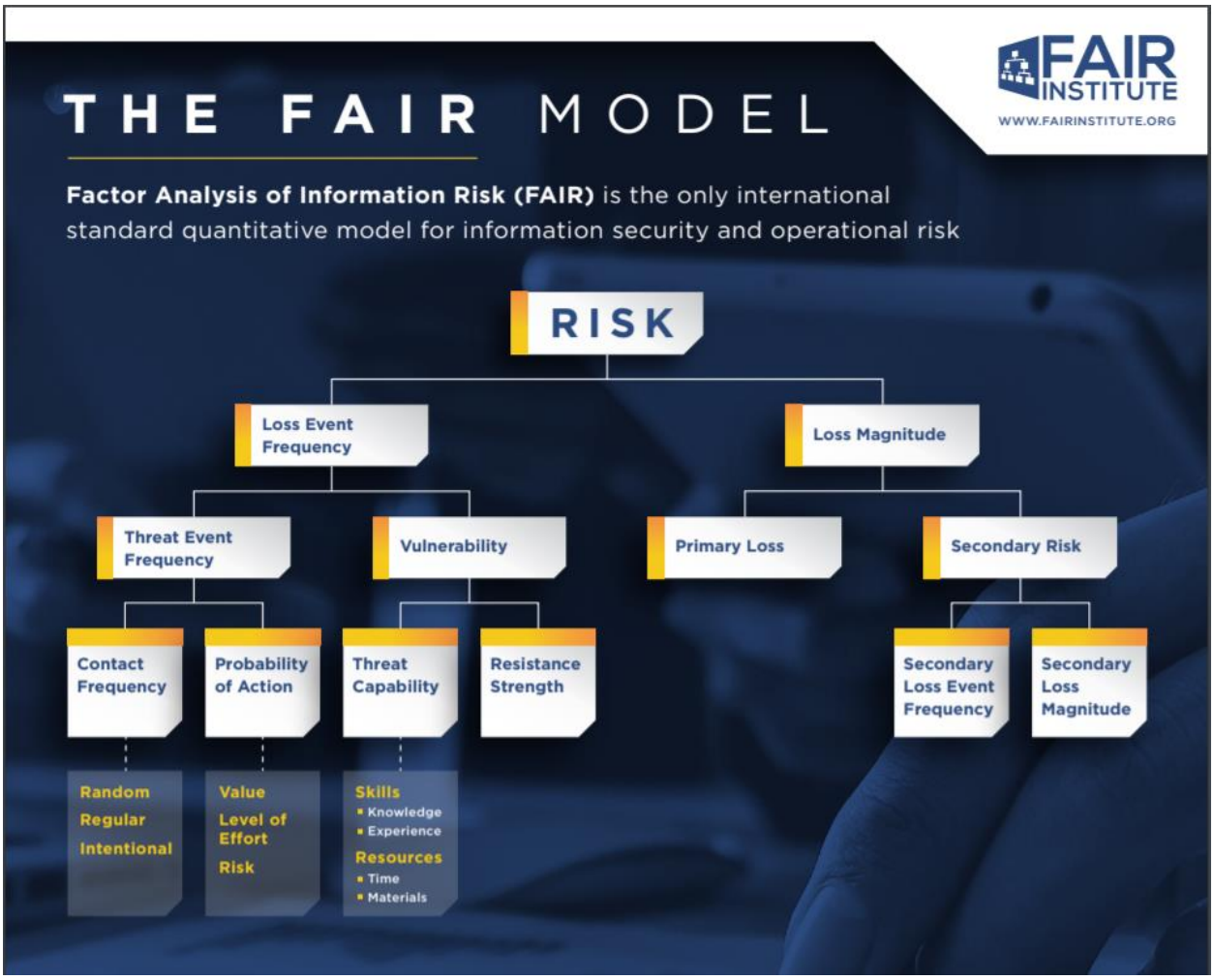


Figure 1: The FAIR Risk Model, Fair Institute, 2018 (cdn)

The 61511 Security Clauses

Now that we have established a good definition of security risk and its major components, let's take a deeper look at the security clauses in IEC 61511. Clause 8.2.4 states that a security risk assessment shall be carried out. It is followed by 6 sub-clauses that further specify the required elements of a security risk assessment.

If you read through clause 8.2.4 you will see that it requires the basic elements in a security risk assessment. For example, clause 8.2.4a requires that one define the *scope* of the assessment (i.e. the system under consideration) which is the SIS and any device connected to the SIS. Defining the scope is the first step in any security risk assessment methodology. Clause 8.2.4b requires identifying and describing *threats* and *vulnerabilities* while clause 8.2.4c requires a description of the potential *consequences* resulting from the security events and the *likelihood* of these events occurring. Clause 8.2.4.d states that the security risk assessment shall provide consideration of various system lifecycle phases such as design, implementation, commissioning, operation, and maintenance. Clause 8.2.4e states that the security risk assessment shall result in the determination of requirements for additional risk reduction. In other words, it shall define additional physical or cyber security countermeasures that will reduce the risk to tolerable levels. Lastly, clause 8.2.4f requires a description of, or references to information on, the measures taken to reduce or remove the threats. This, effectively is the documentation of existing or proposed security countermeasures. A security countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken (Countermeasure_Computer, n.d.).

Clause 11.2.12 simply states that the design of the SIS shall be such that it provides the necessary resilience against the identified security risks and refers the reader back to clause 8.2.4.

Additional Guidance

61511 clause 8.2.4 refers the reader to several standards for additional guidance (ISA TR84.00.09 and IEC 62443-2-1:2010). These documents can be helpful as they are aligned with general security risk assessment frameworks but incorporate the unique requirements of industrial automation and control system (IACS) and SIS applications. Another document that was not referenced but is a valuable resource is ISA 62443-3-2:2018 CDV, “Security for industrial automation and control systems – Part 3-2: Security Risk Assessment and Design”. The reason it was not referenced is that it was not available at the time that IEC 61511 second edition was published in 2016. This standard has been approved by both ISA and IEC and is currently being prepared for publication. It establishes requirements for:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing security level target (SL-T) for each zone and conduit; and
- documenting the security requirements.

How to Perform a Security Risk Assessment on a SIS

So, all of this background information and guidance is great but how do you *actually* perform a security risk assessment on an SIS? The answer is you need to select a security risk assessment methodology that has been tailored towards assessing ICS and SIS applications. The risk

management frameworks and discussed thus far (e.g. NIST, FAIR, etc.) apply generally to assessing cyber security and information security risk. They are, as their names imply, frameworks that define the core elements. They are not, however, methodologies. A methodology is a body of methods rules and postulates employed by discipline or, in other words, it is a particular procedure or set of procedures.

One methodology that that has emerged from all of the aforementioned standards and guidance is something known as a cyber PHA or cyber HAZOP.

Cyber PHA Methodology

A cyber PHA is a detailed cybersecurity risk assessment methodology for ICS & SIS that conforms to ISA/IEC 62443-3-2. The name, cyber PHA, was given to this method because it is similar to the Process Hazards Analysis (PHA) or the hazard and operability study (HAZOP) methodology that is popular in process safety management, particularly in industries that operate highly hazardous industrial processes (e.g. oil and gas, chemical, etc.).

A cyber PHA is typically performed in phases. Figure 2 depicts a typical cyber PHA risk assessment process. The process is scalable and can be applied to individual systems, or to entire facilities or even entire enterprises. It all depends upon the scope of the assessment which, if you'll recall, is the first sub-clause in IEC 61511 8.2.4a. In this paper we will focus on applying this methodology to the assessment of an SIS.

Figure 2: Example of a cyber PHA Risk Assessment Process

The Six Phases of a Cyber PHA applied to a SIS

1. Kickoff: Kicking off a project effectively puts both the site personnel and the assessment team on the same page with regard to project expectations, data exchange requirements and schedule. The kickoff is also where the scope of the assessment is established which the first requirement in 61511 Clause 8.2.4a. A successful kickoff meeting allows all personnel to discuss the current cyber posture of the facility based on existing policies, roles and responsivities, and the SIS components and architecture. Setting expectations on information requirements allows subsequent phases to progress efficiently.

2. Assess: The purpose of this phase is to gather information about the SIS and its connections to identify vulnerabilities. This phase satisfies the remainder of the requirements in 61511 Clauses 8.2.4a and 8.2.4b by documenting the SIS and its connections and identifying vulnerabilities. This is best performed through a site visit by the assessment team as it provides an opportunity to document data flows, equipment configurations, as-built system architecture, and to interview onsite engineering, operations and maintenance personnel. It is important that only non-invasive techniques be used during this visit as it is critical that the normal operation of the SIS not be interrupted or altered in any way.

Some vulnerability assessments techniques only involve interviewing site personnel and completing a questionnaire. In our opinion, such an exercise is inadequate when assessing the security of a system with health, safety and environmental consequences. Failure to assess the actual details of the physical attributes of a SIS and all of its connections (both physical and logical) jeopardizes missing critical information necessary to truly determine risk.

The site visit also provides an opportunity to perform a gap assessment providing valuable insight into the site's position in relation to compliance with relevant functional safety and cybersecurity standards such as IEC 61511, ISA/IEC 62443, and the NIST Cybersecurity Framework. This is valuable as a means of measuring progress as a cybersecurity program moves forward and also to benchmark against best industry practices.

3. Analyze: Analyzing the data acquired during the site visit, as well as any other information collected during the project allows the team to document potential vulnerabilities that may be exploited during a cyber event. These may include physical security gaps noted during the site visit, undocumented connections, unsecure protocols, misconfigured devices, weak access controls, anomalous communications captured during network traffic analysis, or vulnerable software found during computer analysis. These vulnerabilities are documented and used as part of the cyber PHA workshop on Phase 4 to ensure scenarios considered are valid.

During analysis, markups to the architecture diagram can be made in order to document the actual current state of the ICS. This is critical for use in the Cyber PHA Workshop so all participants are clear on the system's design.

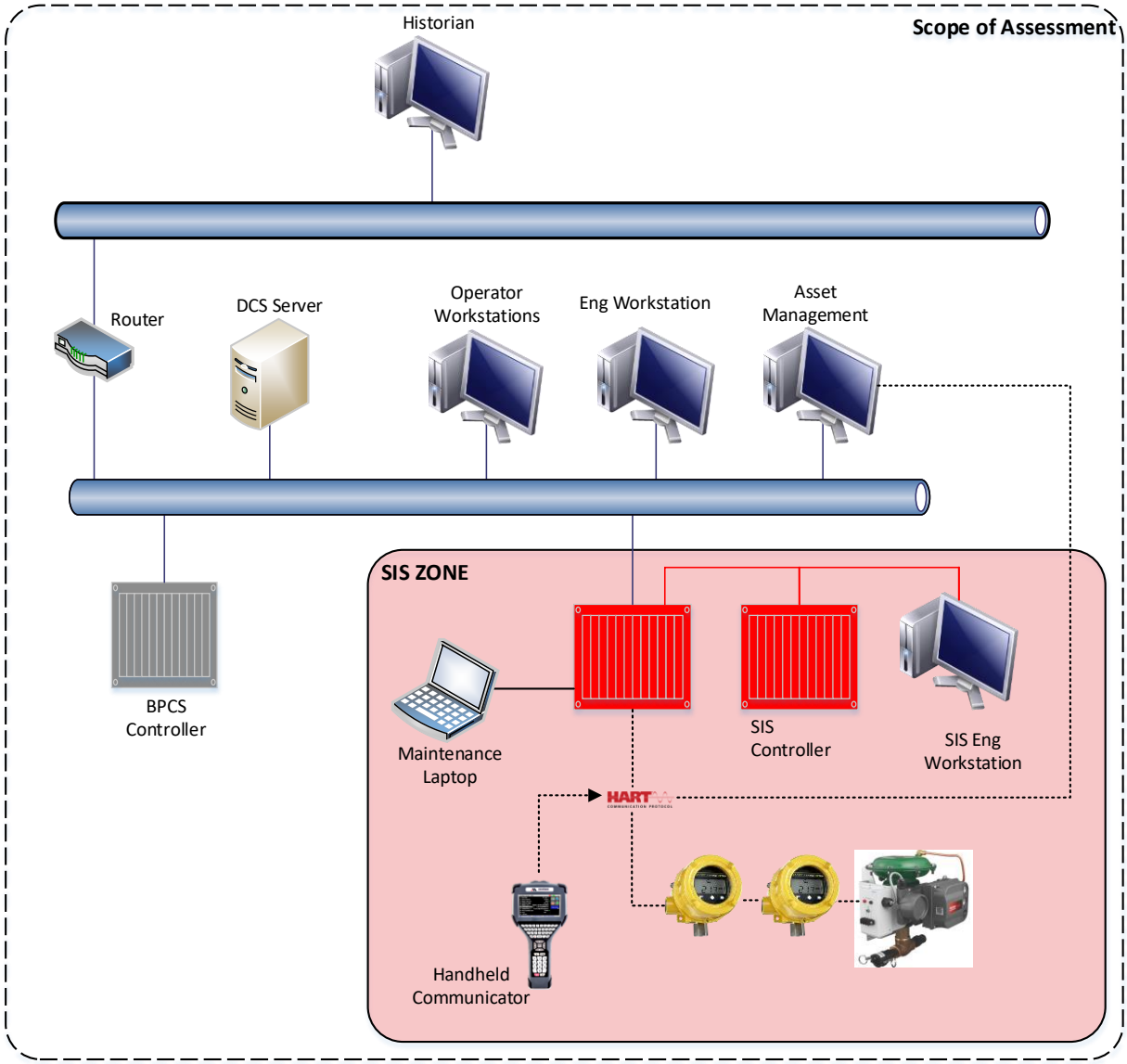


Figure 3: Example of Logical Network Diagram of Depicting the SIS and Connected Devices

4. Cyber PHA Workshop: The cyber PHA workshop is the heart of the process, where all of the information gathered and analyzed in Phases 1 – 3 is integrated with threat scenarios to develop a complete picture of risk. This phase satisfies the requirements in 61511 Clauses 8.2.4b, 8.2.4c, 8.2.4e and 8.2.4f by identifying and documenting threats, vulnerabilities, existing countermeasures, likelihood, consequences and recommendations for additional countermeasures for additional risk reduction.

The workshop is a group effort led by a facilitator and a scribe with expertise in the cyber PHA process as well as multiple subject matter experts who are familiar with the industrial process, the SIS and related ICS and IT systems. For example, the workshop team typically includes representatives from operations, engineering, IT and health and safety as well as an independent facilitator and scribe. A multidisciplinary team is important in developing realistic threat

scenarios, assessing the impact of compromise and achieving consensus on realistic likelihood values given the threat environment, the known vulnerabilities and existing countermeasures.

The facilitator and scribe are typically responsible for gathering and organizing all of the information required to conduct the workshop (e.g. system architecture diagrams, vulnerability assessments, and PHAs) and training the workshop team on the method, if necessary.

A worksheet is commonly used to document the cyber PHA workshop. Various spreadsheet templates, databases and commercial software tools have been developed to support the cyber PHA method. The organization's risk matrix is typically integrated directly into the worksheet to facilitate assessment of severity and likelihood and to look up the resulting risk score.

The workshop is conducted following a systematic approach where the system is partitioned into security zones and each zone is assessed to identify consequences of compromise and the threat scenarios that could lead to those consequences. Each scenario is assigned a risk score where risk is defined as the severity of a consequence versus the likelihood of that consequence.

First, a consequence must be defined. It include a description of what happens as a result of the scenario being considered. Typically, a consequence from the site's process safety PHA is selected where a control system failure is the initiator and/or the SIS is the safeguard. Additionally, non-safety but high impact financial consequences such as lost production or business interruption are also identified. It's important for the workshop facilitator to be familiar with process safety and cybersecurity so these scenarios are legitimate.

Next, the threat scenarios are defined that could lead to the consequence. The threat scenario includes threat actors, threat actions, and the vulnerabilities they may exploit to carry out the attack. Unlike the IT environment, cyber threats to the ICS include 3rd party contractors with high levels of privilege who may act maliciously or expose the system to non-secure laptops or portable media. These threats present a unique case were code can be changed creating safety incidents or infesting a system with a site wide malware outbreak causing an extended outage. Also, authorized users represent a significant proportion of ICS cyber attacks. These users have the potential to intentionally or unintentionally manipulate the controls in unintended ways.

Once the scenario is defined, the risk can be scored based on the severity of the consequence and the likelihood of each threat. Severity scoring uses the same system as a process safety PHA's. However, unlike process safety, there is no database of frequencies for cyber events. Likelihoods of threat scenarios are more relative to one another as opposed the more mathematical approach used in a process safety PHA. It's important that the facilitator has an understanding of this so the risk isn't under or over stated.

With a risk ranked scenario, the current state is documented by recording existing cyber countermeasures in place. Then, if required by the residual risk, recommendations are made that reduce the risk to acceptable levels. These new recommendations are directly tied to a real risk to the organization and are prioritized with the most effective countermeasures reported against the highest risk.

5. Report: Once the Cyber PHA is completed and its results analyzed, a comprehensive report is produced showing the risks to the enterprise and a plan to mitigate risk to the organization's acceptable level. A detailed risk profile provides a visual map of what zones in a

facility contain the highest risk. An executive summary provides the decision makers with a concise risk and remediation picture.

When conducing risk assessments across a number of assets (e.g. all SIS in a facility or company), a group of recommendations often become common to all the facilities. These are identified as baseline recommendations that become part of the organization's long term cyber remediation plan.

6. Mitigate: An effective remediation plan includes a prioritized list of actions, budgetary estimates, schedule and resource requirements. Typically, these plans include short term projects to mitigate high and critical risks and long term projects involving many resources, new equipment and training. Enterprises that possess multiple facilities often establish a specific project to roll out the baseline risk mitigations identified during the reporting phase. This phase satisfies the requirements in 61511 Clause 11.2.12.

Conclusion

We hope that this paper has helped clarify the purpose of performing a security risk assessment on a SIS and why it is important. More importantly, we hope that it has presented you with a proven methodology (cyber PHA) that will help you conform with the security requirements in 61511 as well as provided you with a sensible approach to assessing cyber security risk for any control system. More information on the cyber PHA methodology can be found in the whitepaper, "If it isn't Secure, it isn't Safe" **(Cusimano & Rostick, 2018)**.

Bibliography

(n.d.). Retrieved from cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf?t=1538069566530

Countermeasure_Computer. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Countermeasure_(computer)

Cusimano, J., & Rostick, P. (2018, April). *If it isn't Secure, it isn't Safe.* Retrieved from aeSolutions: http://www.aesolns.com/download/2087/

Oxford English Dictionary, 3rd ed. . (n.d.). Oxford University Press.

Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. (2012). Washington DC: National Institute of Standards and Technology (NIST) .

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Facility Security – Are you ready??

Bill Efaw
Dow Chemical
Freeport, Texas 77566
E-mail: WLEfaw@Dow.com

Abstract

Chemical Facility Security has become increasingly important after the World Trade Center attacks in New York City and a continued list of other terrorist attacks over the last 17 years on many other facilities and targets around the world, including petrochemical targets. Chemical facilities can pose a very real danger by the inherent hazards that can manifest in offsite impacts to the public. This presentation will briefly describe some of the current US regulations around Chemical Facility Security and several approaches used to meet these regulations. It will also describe the SVA-**S**ecurity **V**ulnerability **A**ssessment methodology used by many companies including Dow Chemical.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Team Cognition for Coordinated Decision-Making during Hurricane Harvey: A Case Study from Interviews with Responding Commanders

Jukrin Moon*, Changwon Son, Farzan Sasangohar, S. Camille Peres, Timothy J. Neville
Department of Industrial and Systems Engineering and Department of Environmental and Occupational Health, Texas A&M University, College Station, TX 77843, U.S.A.
*Presenter Email: jukrin.moon@tamu.edu

Abstract

To protect and assist threatened populations and infrastructures in response to natural and man-made disasters, emergency responders from diverse backgrounds collectively work as ad hoc teams. However, responders' coordinated decision-making in real-time has not been adequately addressed in terms of team cognition. Here team cognition is a binding mechanism that produces coordinated behaviors among responders (adapted from Fiore & Salas, 2004). We are particularly interested in cognition of an incident management team (IMT), an ad hoc strategic decision-making team of command-level responders co-located at the incident command post of major incidents such as Hurricane Harvey. To develop and provide an incident action plan to subordinate branch directors in the field, an IMT continuously manages information based on incoming cues from outside, following a cyclical planning process. Interestingly, an IMT is a team of functional sub-teams, and each sub-team is also a team of functional units.
The purpose of this on-going case study is to investigate the role of team cognition for coordinated real-time decision-making in emergency response, through a case study of a recent disaster, Hurricane Harvey. During the interviews with subject matter experts (SMEs, i.e., responding commanders worked during Hurricane Harvey), we asked how responding commanders as a cognitive system-of-systems (or a team-of-teams) continuously made coordinated decisions, especially in terms of communication and information management. In a prior work, a P·D·A (Perceive·Diagnose·Adapt) model, a theoretical interactionist model of team cognition in emergency response, was proposed as a proof-of-concept that depicts nonlinear, interdependent, and dynamic interactions observed within and among three functional sub-teams of a planning team of an IMT at a simulated incident command post (Moon, Son, Sasangohar, Peres, & Neville, 2018). Through interviews with SMEs, this case study is expected to validate the P·D·A model.

Keywords: Human Factors; Emergency Response; System Safety

References

Fiore, S. M., & Salas, E. (2004). Why we need team cognition. *Team cognition: Understanding the factors that drive process and performance*, 235-248.

Moon, J., Son, C., Sasangohar, F., Peres, S.C., & Neville, T.J. (2018, September 30 – October 05). *Modeling team cognition in emergency response via naturalistic observation of interactions.* Submitted to Proceedings of the 62nd Human Factors and Ergonomics Society (HFES) Annual Meeting. Philadelphia, Pennsylvania.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Assessment and Mitigation of Natech events caused by floods

Simone Vivarelli, Alessio Misuri, Valerio Cozzani*,
LISES – DICAM, University of Bologna
Bologna, Italy
*Corresponding Author: valerio.cozzani@unibo.it

Abstract

Recent events pointed out the relevance of threats deriving from natural events impacting on chemical and process facilities where relevant quantities of hazardous substances are present. The framework of climate change is also causing the increase in the frequency of floods and intense storms resulting in the damage of facilities and in the release of hazardous substances, causing concerns for the safety of population, the protection of the environment and asset integrity. The specific features of technological accidents triggered by natural events are recognized since several years and the term Natech (Natural events causing a technological accident) is now used to identify such accident scenarios. The present contribution presents and further develops the framework for the analysis of Natech scenarios, also with reference to recent events that took place in Europe and in the US. Beside the conventional approach based on scenarios caused by the damage of equipment, a new framework is introduced to identify and assess specific accident scenarios caused by the loss of critical utilities (nitrogen, instrument air, cooling water, steam, etc.). Natech events caused by floods and the related cascading events were addressed, in the light of the methods and tools available for quantitative risk assessment.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Designing Effective Emergency Response Plans: Lessons learned from investigating two major incidents

Scott Davis
GexCon US, Bethesda
Maryland, USA

Email: sgdavis@gexcon.com

Abstract

Emergency response plans are an essential, yet oftentimes overlooked, layer of protection for facilities where all other layers of protection failed to prevent an incident. While catastrophic accidents such as large releases of chemicals, fires or explosions are devastating for the process industry, experience investigating numerous incidents has shown that a lack of an effective emergency response plan can lead to an unnecessary and tragic escalation of the incident. More specifically, investigation of two recent incidents: (1) 2015 explosion on the FPSO Cidade São Mateus and (2) 2013 West Texas Explosion; will demonstrate how the lack of emergency planning resulted in devastating consequences that could have been avoided with the proper planning. More specifically, the FPSO explosion resulted in 9 fatalities, eight of which were responding to a leak of condensate, and the Danvers explosion that resulted 15 fatalities, most of whom were responding to the fire that preceding the devastating explosion. Lessons will show that deficiencies in the emergency response plan or implementation of the plan resulted in these fatal consequences that could have been avoided. In addition, while emergency response plans consider "maximum credible" scenarios, past events have shown that low probability high consequences should also be at least considered. Advanced tools will be discussed that can assist an owner/operator prepare an effective emergency response plan.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Computational Fluid Dynamics Study of Heat Flux from Large LPG Pool Fires

Hang Yi, Qingsheng Wang
Department of Fire Protection and Safety Engineering
Department of Chemical Engineering
Oklahoma State University
Stillwater, Oklahoma 74078, USA
Emails: hang.yi@okstate.edu, qingsheng.wang@okstate.edu

Abstract

Liquefied petroleum gas (LPG) is flammable and has risks of pool fires during its transportation, storage and applications. The heat flux radiated by LPG pool fires poses significant hazard to individuals and leads surrounded facilities to potentially fail. CFD (Computational Fluid Dynamics) can be an economic method to simulate and analyze pool fire behaviors, especially for large hydrocarbon fuel pool fires when comparing with large scale experiments. In this paper, three-dimensional CFD models have been carried out to simulate the heat flux of large LPG pool fires with four different diameters. The mesh independence and time step have been conducted firstly to ensure the accuracy and efficiency of simulations. Steady state and transient simulations have been carried out simultaneously to obtain reliable data. The simulation results have been compared with experimental data and classical flame radiation models. The results show that CFD models can validate the experimental data at acceptable relative errors and predict larger LPG pool fires properly. This work is funded by NFPA Research Foundation. The heat flux from simulations can provide NFPA 58 and 59 technical committees a better understanding of the radiation of LPG pool fires and be used in revisions to the next cycle of standards.

Keywords: LPG, pool fire, CFD simulation, heat transfer, storage safety

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Does a HAZOP reveal to us all the hazards we need to know, or are we overlooking serious threats?

Sunhwa Park*, Hans Pasman, William Rogers
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University
College Station, Texas 77843-3122
*Presenter Email: sunh9@tamu.edu

Abstract

The HAZOP process as part of a PHA has been well established and in LinkedIn groups discussions have been on the best supporting software and best practices; the latter, e.g., on different opinions whether a checklist and pre-population is desirable. Of course, all are apprehensive to missing a significant scenario. On the other hand, required time and effort is also a concern. That there is good reason for being concerned about hazard identification completeness appears from various studies over the years, e.g., in which in hindsight after an incident is analyzed whether the scenario had been predicted. In those studies figures of only half of the important scenarios identified are common. Over the years several efforts have been published of attempts to semi-automate the process. Intelligent/smart P&ID is a jump forward. A recent report on automated HAZOP from a highly experienced engineer who can look back on many years of using it, shows good success. More is in the pipeline. Yet, the experience, competence, spirit and ingenuity of a HAZOP team in brainstorming sessions remain needed to see and weigh the risks, although it can be doubtful that, as some assert, it is the single source. The present study comprehends a relatively modest attempt with means that are on every laptop to support a HAZOP study, given the availability of an intelligent P&ID. This Data-based semi-Automatic HAZard IDentification (DAHAZID), seeks to identify possible scenarios with a semi-automated system applying both HAZOP and FMECA. The new method will minimize the limitations of each method. This will occur by means of a thorough systematic preparation before the tools are applied. Rather than depending on reading drawings to obtain connectivity information of process system equipment elements, this research is generating and presenting in prepopulated work sheets linked components together with all required information and space to note HAZID results. Next, this method can be integrated with proper guidelines regarding process safer design and hazard analysis. To examine its usefulness, the method has been applied to a case study.

Keywords: HAZID, HAZOP, FMECA, DATA Mining, Safeguards, SQL, SmartPlant P&ID

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Distinguishing Offshore Drilling Safety Improvement through Engineered New Technologies versus Mandates & BAST – MPD Example

Robert M. Pilko
Blade Energy Partners
Houston, Texas
Email: bpilko@blade-energy.com

Abstract

Offshore drilling processes (personnel, methods & equipment) increase in complexity, yet improve continually by implementing new technology that brings enhanced safety via wellbore management. MPD – managed pressure drilling technology is one set of new techniques that provides multiple benefits, including measurement, detection, and mitigation of small wellbore influxes, and discrimination of these influxes from well kicks that require standard BOP well control practices (early kick detection). While quite applicable to some wells, and beneficial in certain portions of a well, MPD, similar to other new technologies, should not be mandated or considered BAST for every well or hole size. Using MPD as an example, this paper will discuss how offshore drilling safety is enhanced by a new technology, while distinguishing how mandated methods and technologies may reduce safety effectiveness.

Keywords: Integration with Operations, Process Design, Operations, Instrumentation, Risk Management, Matrix

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Dropped Object Risk Assessment for Fixed Offshore Platforms

Ali Sari, Ph.D., P.E.,
[1]*Omega Advanced Engineering and Risk Consulting, "Omega-Risk", 15700 Lexington Blvd #1650, Sugar Land, TX 77478*
Email: asari@omega-risk.com[1]

Abstract

Dropped object risk assessment quantifies the risk caused by accidental dropped objects on potential targets from topsides of a fixed offshore platform to seabed. The risk assessment evaluates both the likelihood of the dropped object accident and its consequence. Often a risk matrix is used in mitigation decision, i.e. high impact frequency and high consequence events require attention. The potential targets from platform deck to seabed pipelines define three types of dropped objects analysis (DOA): Topsides DOA, Appurtenance DOA, and Subsea DOA.

Topsides DOA involves the risk assessment for platform structural components and equipment while Appurtenance DOA includes any potential targets from the sea surface to the seabed, such as jacket legs. Subsea DOA is often of concern because of the high environmental and economic consequences as well as loss of human life, particularly gas release close to an offshore facility. This paper will give an over view of the dropped object risk in offshore lifting/drilling operations and how the risk is assessed in current practice of the oil and gas industry. Next, it will discuss a practical approach in which a two-stage Monte Carlo simulation is used to estimate the impact frequency for potential targets such as upper decks, jacket legs, risers, mooring lines, and pipelines on seabed. The two-stage Monte Carlo approach is an extension to DNV approach which does not take into account the randomness of dropped location on the sea surface. The two-stage Monte Carlo simulation estimates impact probability at different levels along the depth of the platform from sea surface to seabed. In the first stage, a random variable pair based on the drop point distance and angle with respect to the crane position is used. Crane extension is sampled from normal distribution, constrained by crane minimum and maximum radii. Crane rotation is sampled from uniform distribution, constrained by crane lifting arc. In the second stage, a probability distribution on level Z of the sea depth (including seabed) is used that is centered at the drop point on the sea surface. The point of impact is sampled using a normal distribution of the extension based on DNV-RP-F107 approach and a uniform distribution for the rotation angle. For the second stage, the parameters for the normal distribution of the extension radius change based on water depth, weight, and shape of dropped objects. The frequency of impact due to each dropped object is calculated by adding drop frequency and number of lifts per year. The accumulative impact frequency for jacket legs or pipeline is estimated by summing

values along the length (taking integral). The consequence analysis is done by means of advanced nonlinear finite element analysis which is believed to remove the conservatism in simplified approaches.

The paper seeks to discuss the asset risk assessment for dropped objects in offshore drilling operations in the oil and gas industry and proposes recommendations to common practice.

INTRODUCTION

In offshore drilling operations, the three main types of accidental collisions include dropped objects, helicopter collision, and ship impact. Among the three, the dropped objects are the highest threat and have constituted the great majority of potential and actual fatalities in offshore drilling operations. According to Ref. (1), overall dropped objects account for approximately 60% of high potential incidents. Tubular, overhead equipment, and tubular handling equipment items have accounted for the majority of the dropped object categories. The consequences of dropped object may include but not limited to human fatalities / injuries, offshore asset damage / failure, and environment / reputation and business impact. The objective of a dropped object assessment is to minimize the risk associated with the consequences listed above.

Risk assessment of accidental collisions involves two aspects: the probability/frequency analysis and consequence analysis. The frequency and consequences of an event are used against a risk matrix to assess the risk level associated with the event. High frequency and high consequence events require mitigation strategies. For example, to mitigate the consequence of dropped object to a subsea pipeline, a protection structure may be required and must be designed to sufficiently absorb the impact energy from the dropped object.

The objective of this paper is to focus on the dropped object assessment, both probabilistically and consequence-wise, of the subsea assets such as pipelines, X-mas tree, etc and discuss pipeline protection systems in cases where the risk due to damage from the dropped objects is intolerable.

METHODOLOGY

A safe design of offshore assets for accidental collisions requires the risk assessment of such events. Like any other risk assessments, the accidental collision assessment evaluates both the frequency of the risk (likelihood of the event) and the consequence of the event (human fatalities, structural integrity of the assets, impacts on environment, company reputation, and business). The following sections will discuss our approach for the frequency and consequence analyses for the risk assessment associated with dropped objects.

Frequency Analysis

Dropped Objects

There are often three types of dropped object analyses categorized based on the locations and targets of the drop. These include Topsides DOA, Substructure DOA, and Subsea DOA, as illustrated in Figure Error**! No text of specified style in document.-**1. Topsides DOA generally covers the topsides of the platform, i.e., main and production decks of a platform or vessel decks. The targets include deck structural members (primary and secondary steel, deck plates), topsides

equipment (e.g., fire water pump, diesel generators, etc.), laydown areas, stair towers, etc. Substructure DOA generally covers the components below topsides to above seafloor. The targets include top of TLP columns, pontoons, tendons, export risers/cables, jacket legs (fixed platforms), etc. Subsea DOA covers the architecture on the seafloor. Its targets include subsea pipelines, subsea cables, subsea architecture, and equipment such as wellheads.

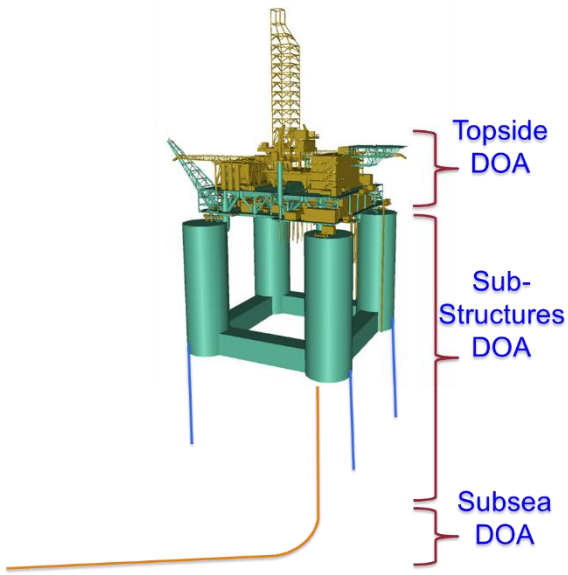


Figure Error! No text of specified style in document.**-1: Three Types of Dropped Object Analysis (DOA).**

In this paper the approach for dropped object frequency analysis is based on the extension of the approach outlined in DNV-RP-F107 (2). This approach uses a two-stage Monte Carlo simulation technique to estimate impact probability at different levels from the offshore structure deck to the seafloor. The frequency of impact due to each dropped object is calculated by multiplying drop frequency and number of lifts per year to the impact probability. The cumulative impact frequency for each target is estimated by summing the values over the areas occupied by the target, i.e., taking integral. Impact energy at any level can be calculated based on the assumption that the velocity at that level which can be linearly interpolated from the surface impact velocity and terminal velocity. The sea surface impact velocity is equal to square root of 2 times the product of the drop height and the gravitational acceleration. The terminal velocity is the velocity attainable by an object as it falls through the water column. It occurs once the sum of the drag force and buoyancy equals the downward force of gravity acting on the object.

The two-stage Monte Carlo simulation method is illustrated in Figure Error**! No text of specified style in document.**-2. The first stage occurs on the sea surface (or on the main deck if desired). In the first stage, a random variable pair (R_1, θ_1) based on the drop point distance and angle with respect to the crane position are used. Crane extension, R_1, is sampled from normal distribution, constrained by crane minimum and maximum radii. Crane rotation, θ_1, is sampled from uniform distribution, constrained by crane lifting arc as seen in Figure Error**! No text of specified style in document.**-3. The second stage can occur at any level Z from the sea surface to the seabed. Similarly, in the second stage, a normal probability distribution of the impact point on level Z that is centered at the drop point on the sea surface is used. The point of impact at the level Z is sampled using a normal distribution of the extension R_2 based on DNV-RP-F107 approach and a

uniform distribution for the rotation angle θ_2 (0-360 degrees). The parameters, for example the angular deviation, for the normal distribution of the extension radius are based on water depth, weight, and shape of dropped objects. Dropped object angular deviations as recommended by DNV-RP-F107 used for calculating the dropped object lateral excursion are summarized in Table Error**! No text of specified style in document.**-1. The definition of the angular deviation is shown in Figure Error**! No text of specified style in document.**-4.

Figure Error**! No text of specified style in document.**-5 shows the illustration of discretization of impact area on topsides/seabed (or any level Z) into 1mx1m cells. 1,000,000 or more drops can be simulated for each dropped object at different levels along water depth. Impact probability in each 1mx1m cell is calculated as the number of hits in the cell divided by the total number of hits (1,000,000). Impact frequency per unit area per year is then equal to the impact probability multiplied with drop frequency and number of lifts per year and adjusted for cell size and dropped object size (see equations below Figure Error**! No text of specified style in document.**-5).

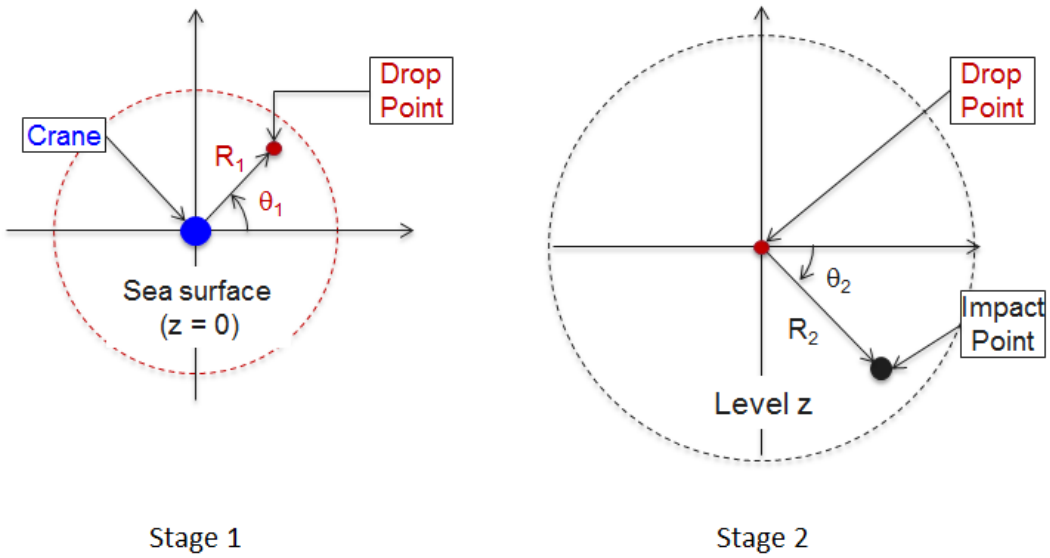


Figure Error! No text of specified style in document.**-2: Two-Stage Monte Carlo Simulations.**

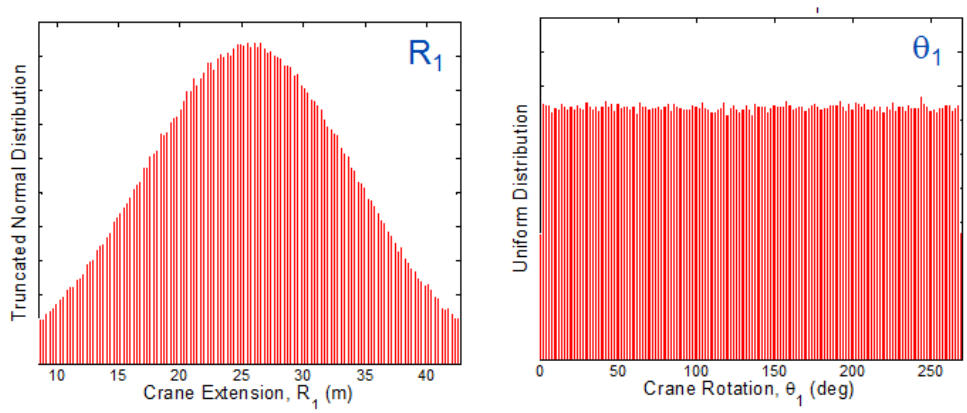


Figure Error! No text of specified style in document.**-3: Normal and Uniform Distributions for R_1 and θ_1.**

Table Error! No text of specified style in document.**-1: Angular Deviation of Dropped Objects (2)**

Object Description	**Weight (tonnes)**	**Angular deviation (α) (Deg.)**
Flat/long shaped	< 2	15
	2 – 8	9
	> 8	5
Box/round shaped	< 2	10
	2 – 8	5
	> 8	3
Box/round shaped	>> 8	2

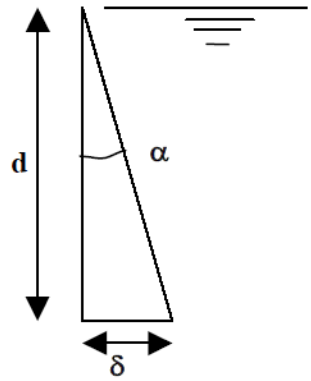


Figure Error! No text of specified style in document.**-4: Angular Deviation Definition (2)**

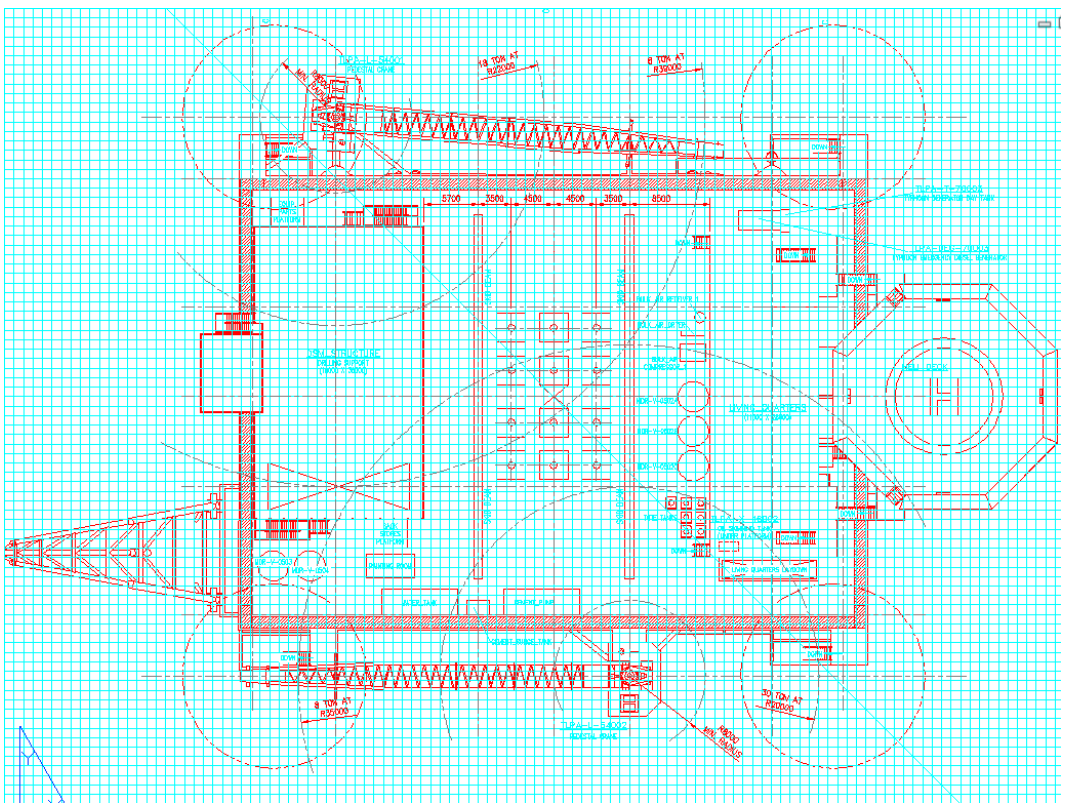


Figure Error! No text of specified style in document.**-5: Illustration of Discretized Impact Area on Topside/Seabed (or any Level Z)**

$$\text{ImpProb} = \frac{\text{Num Hits}}{\text{Total Hits}}$$

$$\text{ImpFreq} = \text{ImpProb} \times \text{Drop Freq} \times \text{Num Lifts} \times \frac{A_{DO}}{A_{Cell}}$$

where: A_{DO} = Dropped object impact area; A_{Cell} = Unit cell area

In the equations above, the drop frequency is often based on industry guidelines or standard such as DNV-RP-F107 or OGP Report 434-8 (3). For example, lifts performed using the drilling derrick are assumed to fall only in the sea, and with a dropped loads frequency as for ordinary lifts with the platform cranes, i.e., 2.2E-05 per lift (2).

Consequence Analysis

The consequence of an accidental collision event can be assessed in terms of human fatalities / injuries, asset damage / failure, or environment / reputation / business impact. For the safe design of offshore exploration and production facilities against accidental collisions, the structural integrity consequence is of interest. This section discusses the use of structural analysis for consequence aspect of accidental collisions.

The structural consequence of an accidental collision to an offshore asset is predicted using either simplified approach (if applicable) or advanced FE modeling. The FE approach is often used to remove the conservatism in the simplified approach. Advanced nonlinear dynamic structural analysis is capable of taking into account the effects of dynamic loading, geometric nonlinearity, material nonlinearities (strain rate effects, dynamic increase factor), and contact nonlinearity. Since dropped object loads are accidental loads, structural response of a target is not expected to remain in the linear-elastic range. Certain damage, i.e., material permanent plastic deformation, is allowed to absorb the impact energy. Hence, advanced FEA is more applicable in the design against collision loadings. A general finite element package such as Abaqus (4) is suitable for this type of analysis and was used for all of the consequence analyses in this paper. If the target can absorb the impact energy and damage caused by the impact is acceptable or tolerable based on performance criteria, no action is required. However, if the performance criteria are not met, either the target has to be re-designed or protection structures need to be provided.

Geometry Modeling

In FEA, impactors, i.e., dropped objects are usually modeled as rigid bodies with the initial impact velocity. The impact energy is calculated by multiplying the impactor's velocity with mass that accounts for the impactor mass and hydrodynamic added mass. The targets of the collision are often modeled as a deformable body with shell or solid elements. In this rigid impactor – deformable target set up, the impact energy is dissipated conservatively only through the plastic strains (unrecoverable deformation) of the impacted target. An example of an FE model for dropped object is shown in Figure Error**! No text of specified style in document.**-6.

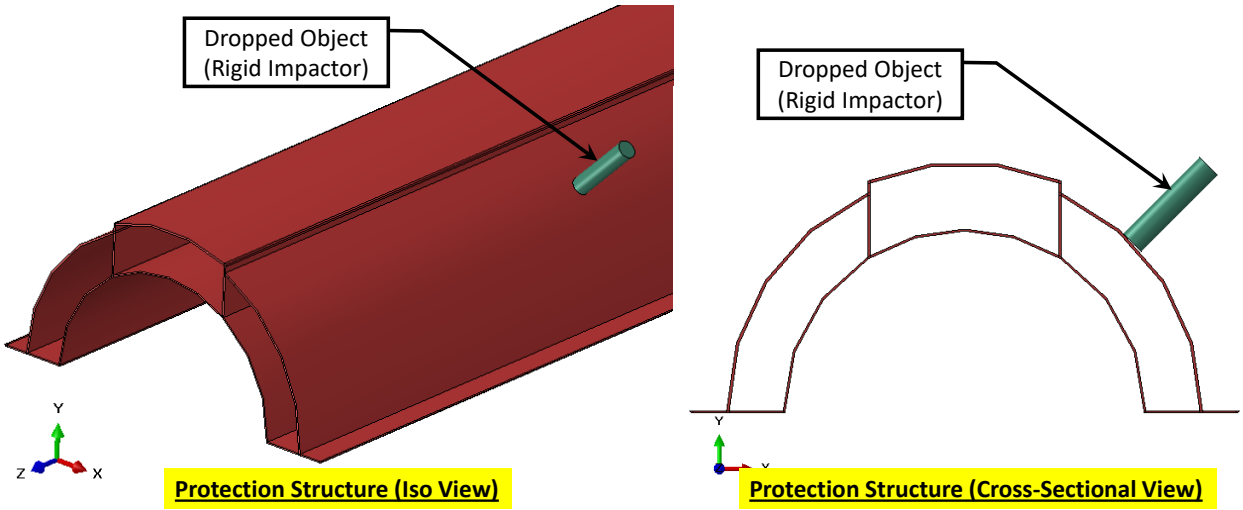


Figure Error! No text of specified style in document.**-6: Example FE Model: A Rigid DO Impacting a Deformable Structure**

Material Modeling

Excessive deformation is expected during accidental collision event. It is likely that structural components undergo large plastic deformation, even failure. Hence material plasticity/failure must be modeled to capture these nonlinear effects. Since impact loading happens in very short duration of time, rate-dependent plasticity should be taken into account. Figure Error**! No text of specified style in document.**-7 presents stress-strain relationships up to fracture for low-carbon mild steel at different strain rates (5). Yielding stress is also sensitive to strain rates, especially for high strength steels. Increase in yield strength due to strain rate effects is characterized by a dynamic increase factor. In Figure Error**! No text of specified style in document.**-8, the dynamic increase factor for yield strength versus strain rate is plotted for a mild steel (ASTM A36 steel with static yield stress of 250 MPa) and for a high strength, quenched and tempered steel (ASTM A514 steel with yield stress approximately 760 MPa).

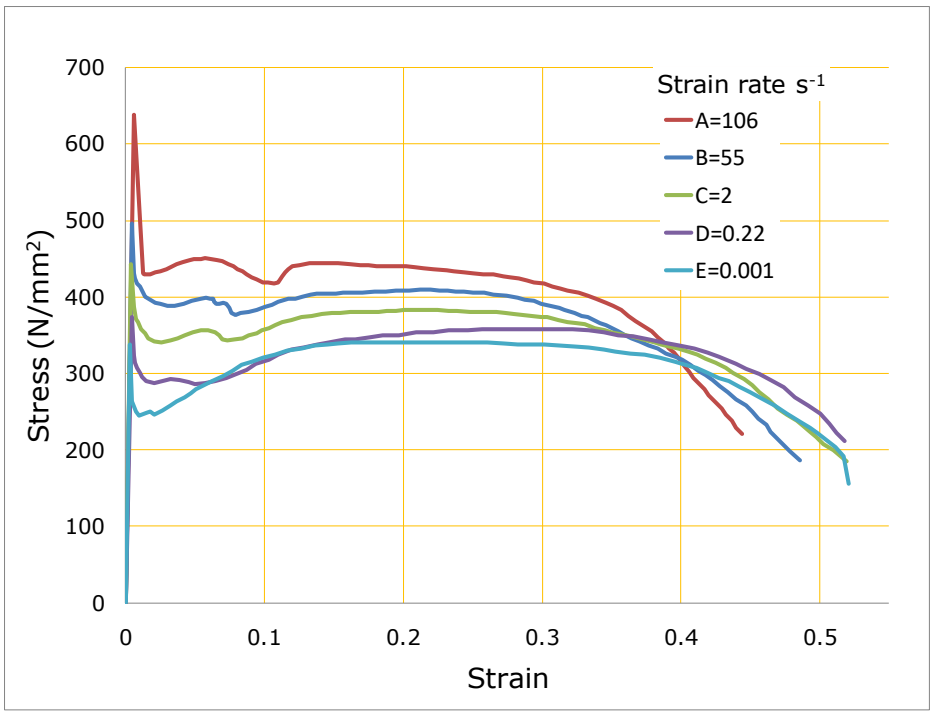


Figure Error! No text of specified style in document.**-7: Effect of Strain Rates on Behavior of Mild Steel (5)**

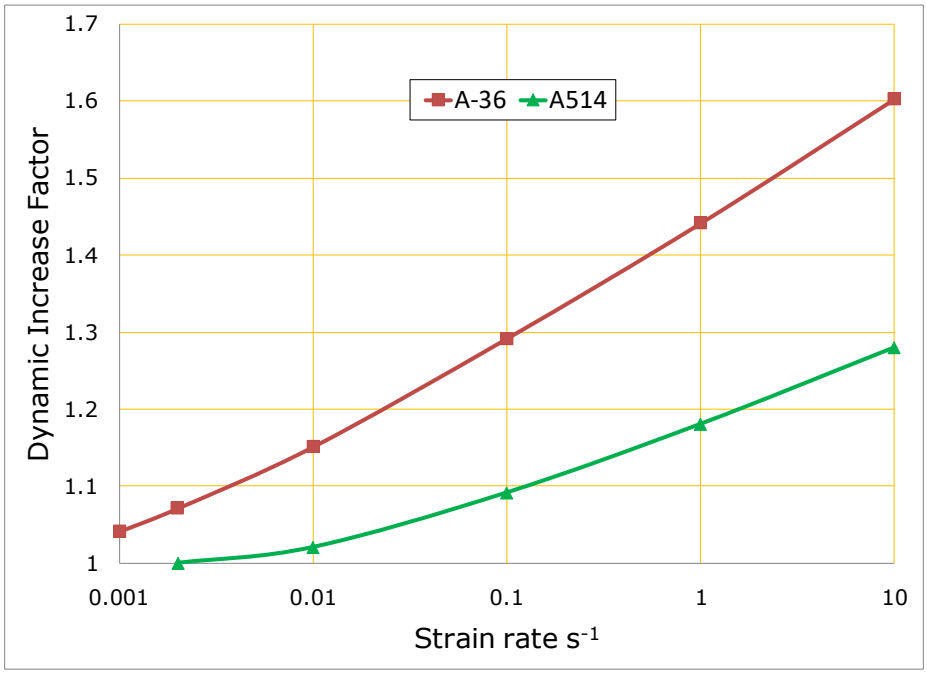


Figure Error! No text of specified style in document.**-8: Dynamic Increase Factor for Yield Strength of Mild and High Strength Steels versus Strain Rates (6)**

CASE STUDY

Dropped Object Analysis

The dropped object case study involved lifting operation during installation of a four-legged

fixed jacket platform. The water depth was 108.8 m. The lifting manifest that includes 14 lifted items is shown in Table Error**! No text of specified style in document.**-2.

Table Error! No text of specified style in document.**-2 – Lifting Manifest**

#	Item	Length (m)	Width (m)	Height (m)	Weight (ton)	Lifts/ year	Impact Energy (kJ)
1	Heavy lift	6.1	2.4	1.2	27.22	182	3485
2	Waste bins	6.1	2.4	1.2	1.81	130	103
3	Mini container	1.8	1.8	1.8	1.81	52	36
4	Food box	1.8	1.8	3.1	3.63	12	127
5	Tool box	2.4	1.2	1.2	0.91	12	24
6	Cylinder rack	0.9	0.6	1.8	0.91	12	27
7	MMSL tool box	1.8	1.2	0.6	0.91	52	23
8	Air compressor	3.1	1.5	1.2	3.63	12	153
9	Scaffolding Basket	6.1	2.4	1.2	6.35	12	443
10	Score tool box	1.5	0.9	0.6	0.91	26	24

Frequency Analysis

Based on the approach described in the methodology section, we used Monte Carlo simulations to estimate the impact probability due to each dropped object on the seabed. The results of the impact probability analysis for the dropped object "Waste bins" at seabed level are shown in Figure Error**! No text of specified style in document.**-9 as an example. The crane location is shown by a larger circle and the four jacket leg locations are denoted by four smaller circles. The probabilistic assessment was carried out for all 14 dropped objects. The contours of impact frequency at seabed for the 14 different dropped objects are given in Figure Error**! No text of specified style in document.**-10.

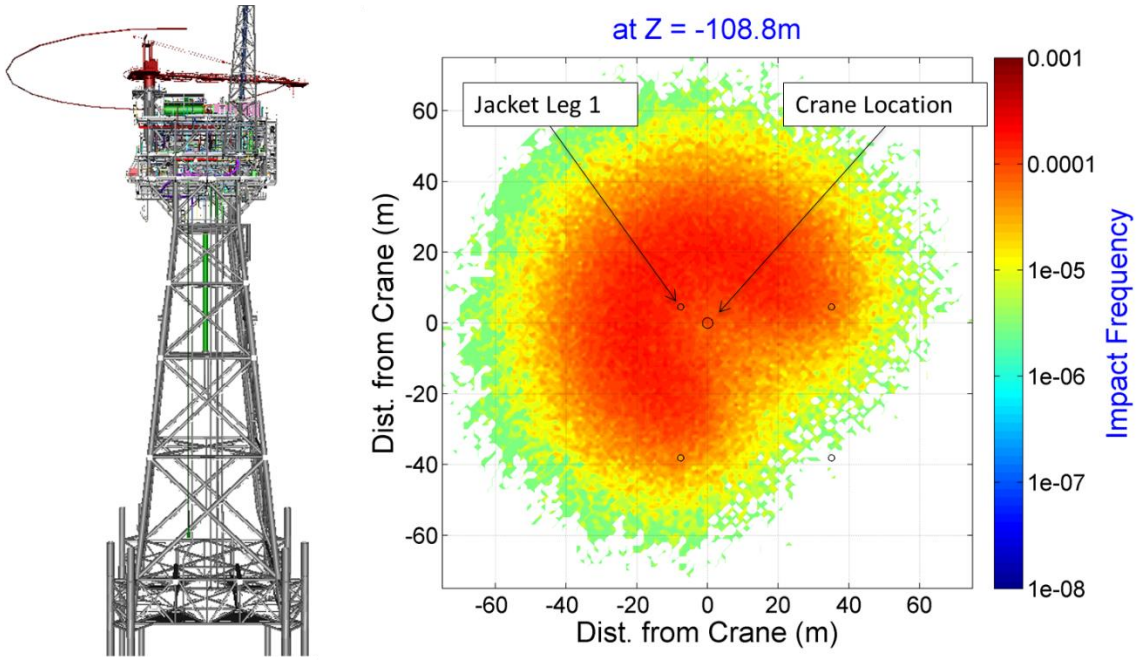


Figure Error! No text of specified style in document.**-9: Impact Frequency Contours on Seabed due to Waste Bins DO**

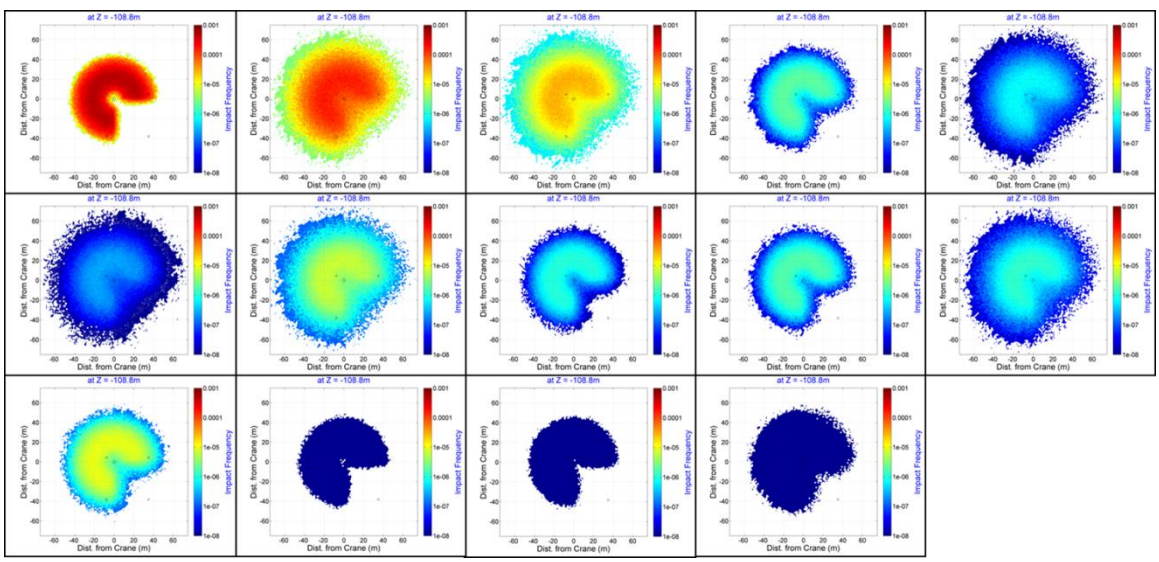


Figure Error! No text of specified style in document.**-10: Contours of Impact Frequencies for Total of 14 DOs**

Consequence Analysis

For an offshore platform, either fixed or floating, different types/scenarios of structural consequence analysis due to dropped objects could be done. These may include dropped objects on topsides upper deck plate members, equipment, on sub-structure components such as jacket legs, risers, mooring lines, or on pipelines on the sea bed. The goal of a structural consequence

analysis is to estimate the energy absorption capacity of the components within the performance criteria, i.e., acceptable damage level. As an example, Figure Error**! No text of specified style in document.**-11 presents the energy capacity as a function of deformation of a 26" flowline pipe with an elasto-plastic seabed assumption. In this simulation, the energy was dissipated through both pipe and soil plastic deformations. Figure Error**! No text of specified style in document.**-12 shows the comparison of the results between FE analyses with different assumptions and simplified approach outlined in DNV-RP-F107. In the FE sensitivity analyses, the seabed was modelled as rigid, elastic, or elasto-plastic. Two types of FE analyses were done: impact analysis and analytical analysis. The impact analysis simulated an impact event with possible "spring bouncing back" effect in which the deformable pipe acted as a spring. In the analytical analysis, the dropped object was pushed down into the pipe until failure of the pipe occurred. The analysis results indicate that DNV approach could underestimate energy capacity compared to an FE approach in which the seabed is assumed to be elasto-plastic (realistic assumption). Since the capacity of the flowline is around 363 kJ (before rupturing) which is less than the impact energies of certain dropped objects as shown in Table Error**! No text of specified style in document.**-2, a protection structure may be required if the risk is not acceptable or tolerable.

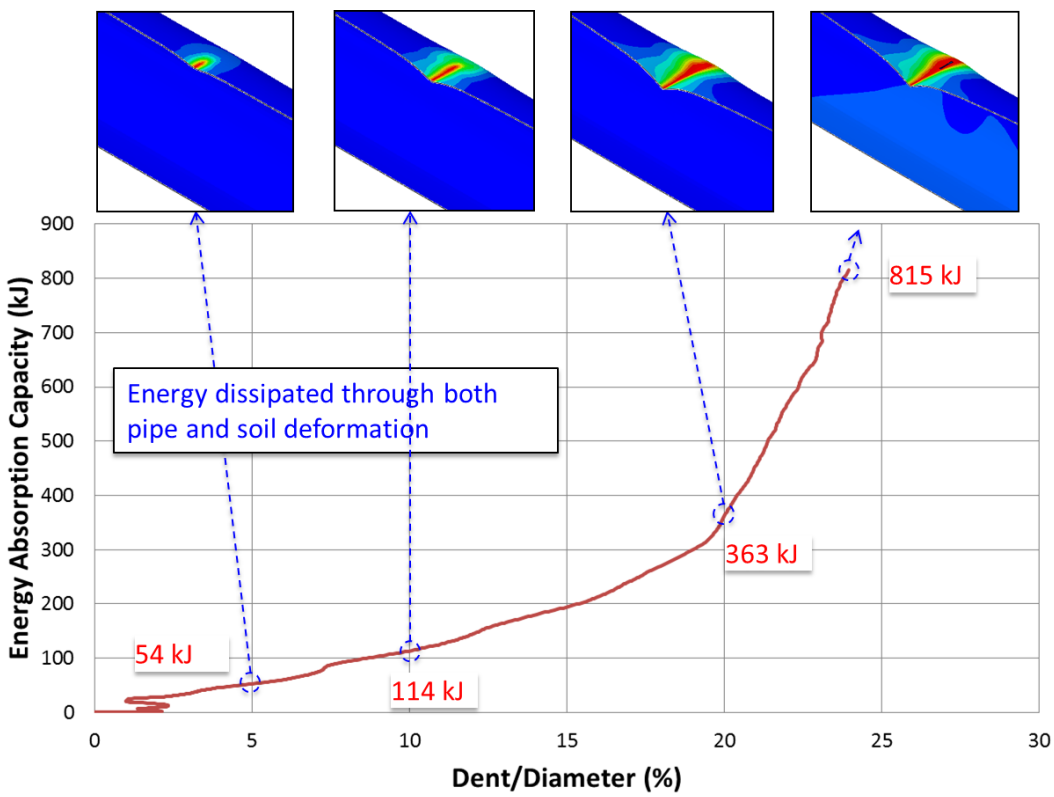


Figure Error! No text of specified style in document.**-11: Energy Capacity vs. Deformation of a 26" Flowline Pipe with Elasto-plastic Seabed Assumption**

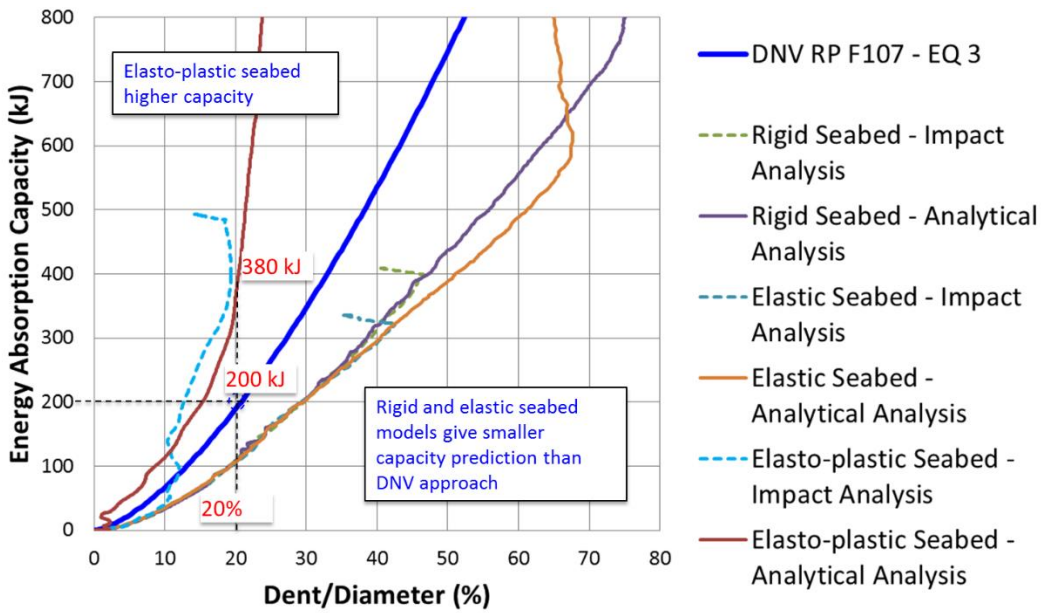


Figure Error! No text of specified style in document.**-12: Energy Capacity vs. Deformation of a 26" Flowline Pipe: FEA vs. Simplified Approach (DNV-RPF107)**

CONCLUSIONS

In offshore drilling operations, accidental loads such as dropped objects pose a high potential threat to human safety, asset integrity, environment as well as reputation and business of the operator. A safe design of offshore exploration and production facilities for accidental collisions requires the risk assessment of such accidental events. This paper proposes the methodology to assess such risk. For the frequency assessment part of the risk, the paper proposed an extended version of the approaches outlined in industry guidelines such as DNV-RP-F107. For the consequence analysis, it has been demonstrated that advanced analysis method is capable and suitable for understanding the response of structures to accidental loadings, not only to remove conservatism inherent in simplified approach but also to assure a safer and economical design.

REFERENCES

1. **Seward, Simon.** *PREVENTION OF DROPPED OBJECTS, presented at DROPS Forum Asia Singapore 6th Apr 2011.*
2. **Det Norske Veritas.** DVN-RP-F107 - "Risk Assessment of Pipeline Protection". October 2010.
3. **OGP.** *Mechanical Lifting Failure, Report No.434-8, March 2010.*
4. **Abaqus 6.14.** *Abaqus Documentation, Dassault Systèmes, 2015.*
5. **Campbell, J.D. and Cooper, R.H.** *Yield and flow of low-carbon steel at medium strain rates. Proceedings of the Conference on the physical basis of yield and fracture. Institute of Physics and Physical Society, London, 77-87 (1966).*
6. **Smith., P.D., Hetherington, J.G.** Blast and ballistic loading of structures. *Betterworth Heineman.* 1994.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Hazard Mapping Case Study on a Compressor House

William Pittman*, PhD
Fire and Gas Detection Consultant
Micropack Detection (Americas)
Chris Heaney
Fire and Gas Detection Consultant
Micropack (Engineering) Ltd.
Jim Scoggins
Regional Consultant
Micropack Detection (Americas)
*Presenter E-mail: williampittman@micropackamericas.com

Abstract

Compressors and pumps are amongst the most common sources of leaks in hydrocarbon processing facilities. Preventing leaks is the task of maintenance and inspection programs. Ignition sources are difficult to eliminate given the low ignition energy for most gases. So, when leaks occur, explosions and fires often follow. It is then the task of flame detection systems to sound the alarm quickly and possibly activate automated response systems.

The design of these detection systems is of critical importance. Owners and operators need to have confidence in the system and its ability to quickly identify fires in the area of interest. This requires conducting a geographic coverage assessment, preferably aided by well-designed software tools, to calculate coverage levels and identify any concerning gaps in coverage.
The authors present a case study where-in the detector layout of a proposed compressor house is assessed and optimized using 3D modeling. The assessment process and results are reviewed to highlight important aspects of the process and key outcomes.

Keywords: Case Study, Compressor, Fire, Normally Unoccupied Facility, Fire detection, Flame detection, Loss prevention

Introduction

Leaks from high pressure gas compressors are a common and potentially devastating occurrence. Compressor houses are typically sources of heightened concern for operators because they combine key risk factors. Hydrocarbon vapors are present at very high pressures with multiple potential leak locations packed into a relatively small geographic space. The typically high level

of congestion around the compressors further increases the risks associated with high pressure jet fires and vapor cloud explosions by making fire propagation and flame acceleration more likely. Even the best and most proactive preventative maintenance and monitoring programs at occupied facilities will not always succeed in keeping high pressure flammable gases and hydrocarbon liquids contained within the process equipment. When leaks occur, it is generally safe to assume that the resulting fuel-air mixture will eventually find an energy source sufficient for ignition. This can occur near the point of release, but this is often not the case and the consequences are generally far more severe when it is not. Where there are leaks fires and explosions will occur. It is the task of fire and gas detection systems to sound the alarm as quickly as possible and initiate mitigation systems, minimizing the resulting damage.

Fires and explosions tend to wake the neighbors, if there are any, and get the attention of local and sometimes national media - sometimes the attention of the US Congress as well. The rapid and effective operation of shutdown and blow down systems in compressor houses has the potential to not only limit losses and minimize downtime for repairs, but also make the operator look a lot better when the story hits the papers. Such was the case with a 2013 compressor station fire at a Williams facility in Pennsylvania. The role that automated safety systems played in mitigating the release and explosion received significant attention in an otherwise brief article that appeared in the local paper.[5]

Williams' track record since 2010 gives an unfortunate testimonial as to how often such incidents can occur and the losses they can inflict. A March 2012 explosion in Springville Township, Michigan blew a hole in the roof of a Williams facility. Just two weeks after the previously referenced incident in Pennsylvania - in the same calendar month - an explosion at another Williams compressor station in New Jersey injured two construction workers sufficiently to require hospitalization and lead to minor injuries for 13 others.[7,8] Yet another incident at an LNG facility in Washington less than two years later, in 2014, injured five workers and caused $69 million dollars in damage. Williams was less fortunate in that case as the fire and gas detectors at that facility had been disabled, unbeknownst to some of the personnel there, causing a delay in the activation of emergency shutdown systems.[9] Williams also lost three workers in an explosion at a Gibson, Louisiana gas facility in October 2015 though that incident was not attributed to the compressor house.[10]

Micropack was approached to assess the fire and gas detection requirements of a new compressor station a client was preparing to build. The client has had issues in the past with compressor fires at similar facilities including fires that went undetected for unacceptably long periods. The client therefore wanted to use a more rigorous design approach to verify the effectiveness of the design. This paper reviews the case study to provide an overview of the hazard mapping process, the results obtained and the benefits of such studies.

Optical flame detection evolved out of the need to provide faster and more accurate fire detection and to better protect equipment and personnel than what was previously possible with traditional smoke and heat detection technologies. The technology has now advanced to the point that 1 ft^2 n-heptane test fires can be detected at distances of 200 ft or more in 10 seconds or less.[2,3,6] However, for detection to occur the fire must be within range and within the effective field of view of the detector, established through standardized testing methods. This therefore makes the

design of detector layouts a critical and sometimes difficult process given the number of large and small obstructions in process areas that can prevent timely detection.

In the absence of assessment tools, fire detection layouts using optical-based detectors have traditionally been based on expert judgement - “eye-balling” it. This can be problematic if the designer is unaware or misinformed as to the field of view or effective range of the detector being used as these vary widely in the industry. It can be very difficult to determine which of two (or more) possible layouts provides the best coverage, or if any of the proposed systems actually provide a level of coverage that the system owner would consider acceptable. Documenting and auditing the design, and identifying discrepancies between the system as designed vs as installed could also be difficult. Geographic coverage assessments (GCA), or Hazard mapping, evolved from the need to address these issues. Early assessment methods used 2D drawings, pencils and paper. More recently computers and 3D models have begun to be used to improve the accuracy of the studies. GCAs are now used with increasing frequency in the oil and gas industry and beyond to ensure system performance meets expectations and to demonstrate compliance with performance-based regulations.

The methodology and target fire sizes used by Micropack and presented in this paper are consistent with the requirements for geographic coverage assessments in ISA TR 84.00.07.[1] As part of this process, Micropack reviews site plot plans, area classification drawings, P&IDs, PFDs, and H&MBs.

Model Sectioning, Conditioning and Review

Geographic coverage assessments (GCA) can be carried out using 3D models or 2D plot plans. Assessments conducted using 3D models of the actual facility are, of course, considerably more detailed and accurate and, therefore, greatly preferred. However, detailed 3D computer models are a relatively recent addition to the engineering and design process and as such are often not available for older facilities. Since the project discussed here involved a GCA on a newly planned and designed compressor station a 3D model had been made and it was provided by the client for the assessment. A screenshot of the client provided 3D model, viewed in Navisworks Freedom, is shown in Figure 1. The client-provided model also includes the surrounding topography of the site.

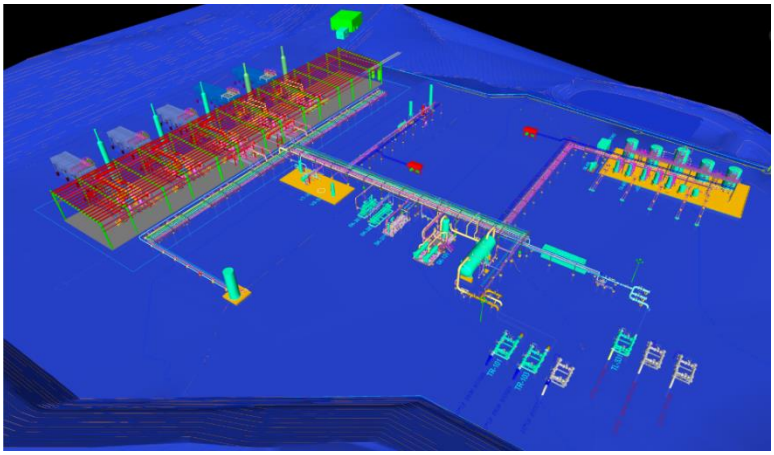


Figure 1: Complete 3D model of the onshore pumping station

3D models are often quite large with entire, multi-deck offshore platforms in one 3D file. While this is good from a visual and design perspective, these large models - often made of tens if not hundreds of millions of polygons - can be extremely difficult to work with without very expensive, high-end computers, and may be impractical to work with even then. It is therefore usually necessary to section the model, making separate 3D files for each fire area, allowing each area to be assessed individually.

For this project, the provided 3D model covered the entire pumping station. However, the scope of the assessment only covered the compressor house and a bunded area with several large storage tanks. The model was therefore sectioned to create separate model files for the compressor house and the bunded tank area with the out-of-scope areas removed. The sectioned models may require additional conditioning. This may include model simplification to reduce the number of polygons involved to make the software run faster and more smoothly. The model may also need to be converted into one of the file types supported by HazMap3D, the software used to conduct the GCA. These simplifications and conversions sometimes result in aberrations in the model and it is therefore necessary to review the final model, compare it to the original and confirm that the final model is acceptably accurate.

The model for the compressor house required some additional modification. The compressor house is designed to contain 6 compressors, but one of the compressors will be added in the future. The pumping station will only have five compressors when it comes online and the provided 3D model only includes five compressors with an empty bay for a 6th, shown in Figure 2.

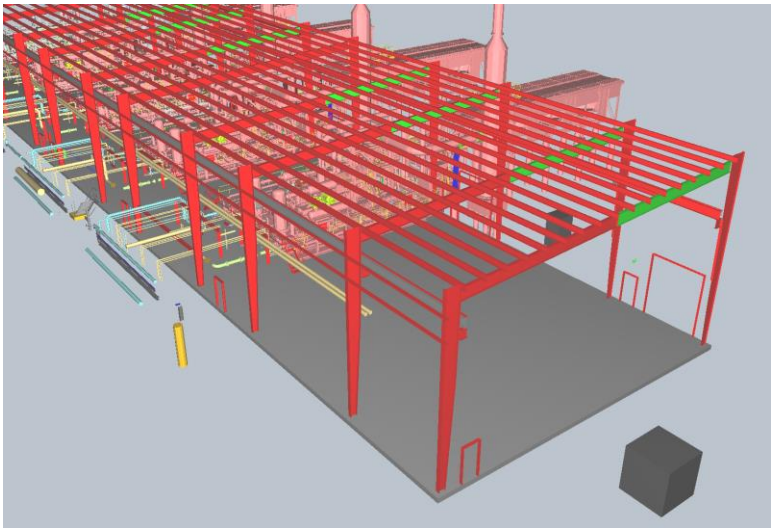


Figure 2: Vacant Bay in provided compressor house model

The client wanted the fire and gas detection system to account for the 6th compressor so that a reassessment is not required when it is added. The 6th compressor was therefore added to the model. An image of the final model, as it appears in HazMap3D, is shown in Figure 3.
Because the assessment model is created from the client-supplied model the coordinate system from the client model is preserved and used in the assessment model, even though large pieces of the original model have been removed. Figure 4 provides a look at a single compressor in the

model, showing the level of detail that can be achieved in the 3D model, which allows for a more accurate assessment of coverage volumes.

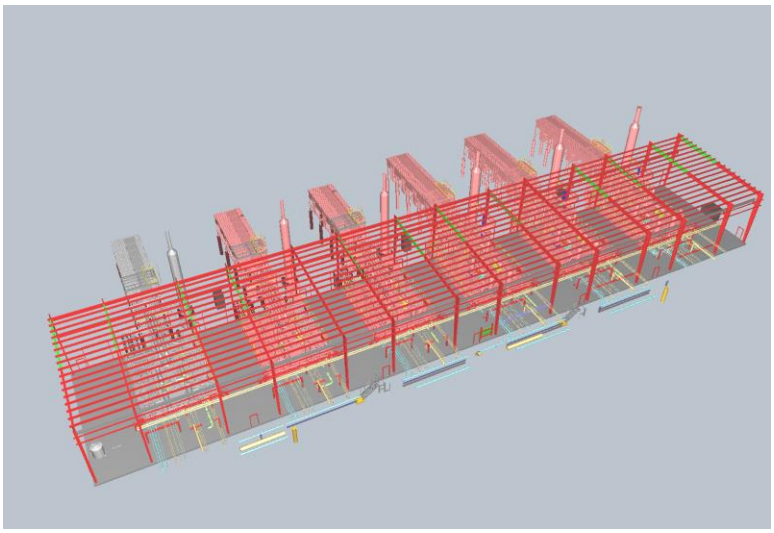


Figure 3: Bird's eye view of the Final 3D compressor house assessment model, as shown in HazMap3D, viewed from the East.

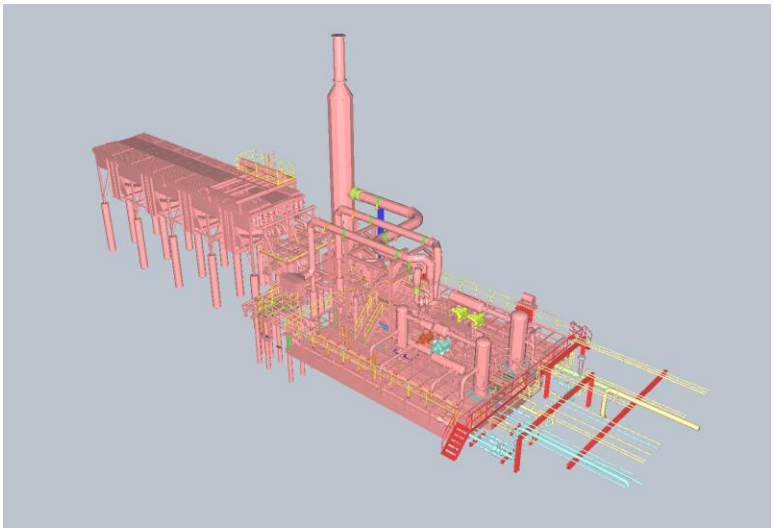


Figure 4: View of a single compressor, without the rest of the model, viewed in HazMap3D.

Part of the model verification process touched on previously should include a confirmation that the model dimensions have been properly specified during import into HazMap3D and the facility is modeled as being the correct size. The compressor house for the pumping station is relatively large, measuring approximately 100 m by 21 m with a ceiling over 10 m high. Using the wrong units during model import could result in a model that's only 8.5 m wide and 44 m long, if, for example, centimeters were used in place of inches during model import.

Risk Ranking and Grading

Pieces of equipment or process areas are typically assigned a risk ranking or grade as part of the geographic coverage assessment. The grade is assigned based on a combination of factors

including the materials, temperatures and pressures involved, the value of the equipment and surrounding equipment and the likelihood that the fire will spread and damage surrounding equipment. Risk rankings typically include low risk (LR), medium risk (MR), and/or high risk (HR) grades. Special Risk (SR) categories may be created to address unusual hazards that require additional attention and scrutiny.

Grades can be assigned by those conducting the GCA or specified by the client. In this case, the client assigned the risk grades based on their own in-house risk ranking and acceptance criteria. In cases where grades are assigned by the client Micropack still reviews relevant process information to ensure that no important fire hazards have been missed and will propose changes to the client grading where it is thought to be necessary or appropriate.

For this compressor house the key components of the compressors were designated as MR with no LR or HR graded equipment in the compressor house. Figure 5 shows the graded volumes for the entire compressor house. Figure 6 shows the graded volumes on a single compressor for clarity. The MR grade has been applied to the compressor engine as well as the scrubber, suction and discharge bottle for all three stages of each compressor. This effectively assigns a MR grade to the entire volume around and between the major components to each compressor. The internal volume of the engines and each of the small vessels in the compressors were excluded from the flame assessment to prevent an underestimation of the coverage level provided.

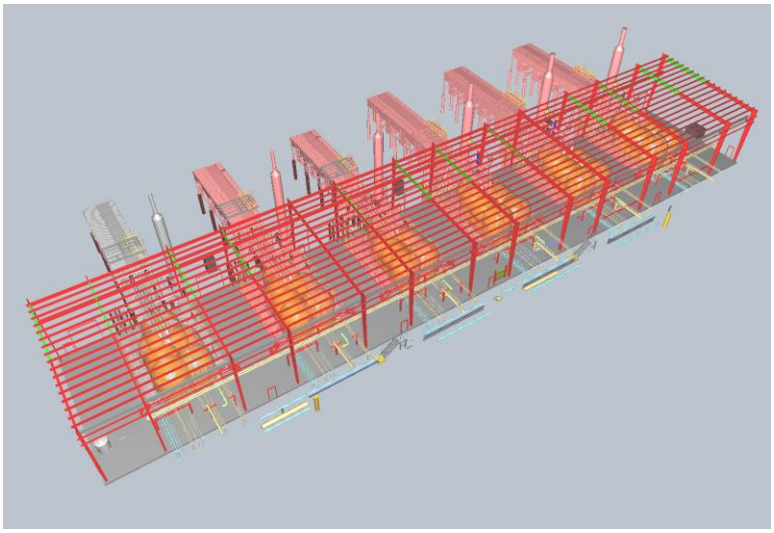


Figure 5: Graded volumes in the compressor house shown in HazMap3D

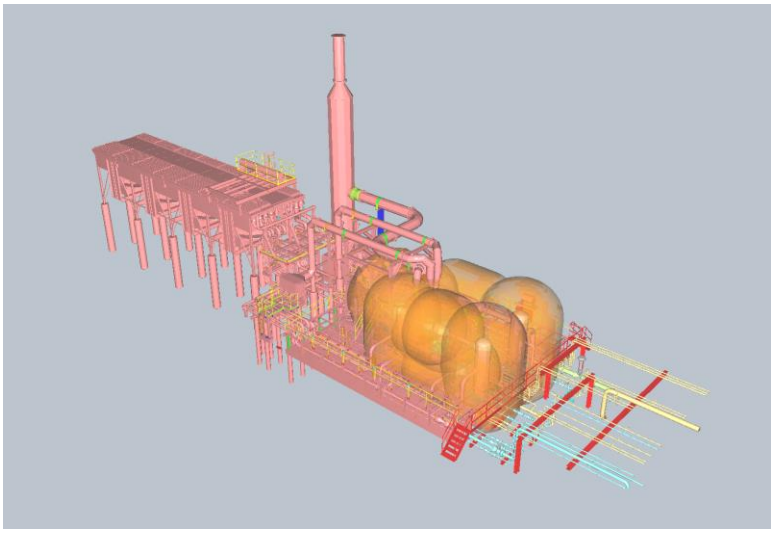


Figure 6: Graded volumes for a single compressor, viewed without the rest of the model in HazMap3D.

Once assigned, the grade of a piece of equipment or area can determine or affect, the size of the target fire the system should be able to detect, the size of the graded volume or area, and the level of coverage that is desired. For example, a LR piece of equipment may require that a 250 kW RHO fire trigger an alarm whereas an alarm is expected in response to a 50 kW RHO fire for MR equipment and 10 kW RHO for HR. Ninety percent coverage is usually desired with HR equipment where 60% or 70% is often considered acceptable for LR equipment. For this project, 80% coverage with the ability to detect and alarm in response to a 100 kW RHO fire was expected for MR graded equipment. These are desired levels of coverage that are used as a target to shoot for or as a rule of thumb, not a rigid target that must always be met.
The client specified fire and gas protection philosophy called for control action to occur with 1ooN voting and for stepped-up control action to occur in response to a fire confirmed with 2ooN voting.

Detector Selection and Placement

In some cases, 3D models of existing facilities will have flame and gas detectors incorporated into the 3D model. As the fire and gas detection system for this facility had not yet undergone formal design, no detectors have been installed and the detectors are not present in the model. Within the assessment software the flame detectors are represented by semi-transparent volumes that indicate the expected field of view of the detector. The size of this volume depends on the horizontal and vertical field of view and range of the specific detector being viewed as well as any desensitization factor that has been applied.

The hazard mapping software used in this study includes a database of FM Global certified flame detectors commonly used in the industry and it can therefore accurately model a wide range of detectors that a client might have installed at a facility or which they may have selected for installation. If a client is using a detector that is not currently included in the software's database this can usually be addressed through a minor software update. Where the type of detector is not known or where a detector model has not yet been selected, the software can model flame

detectors as a generic single-frequency IR detector with a typical, conservative field of view and an effective range or 10 or 25 m.

The client had elected to use the Drager Flame 3000 and Flame 5000 visual flame detectors in the compressor house. The decision was made to model all the detectors as Flame 5000 during the assessment. The Flame 5000 has a shorter detection range (44 m vs 60 m) as well as narrower horizontal and vertical fields of view as compared to the Flame 3000, but offers the possibility of supplying live video feeds to the control room and video recording of alarm events, which the Flame 3000 does not.[2,3] Therefore, modeling all the detectors as a Flame 5000 provides the maximum number of possible video feeds to the control center while also providing a conservative assessment of the provided coverage. Should the client decide to install Flame 3000s instead, higher coverage levels would be expected.

The client fire and gas protection philosophy calls for two detectors to be installed for each compressor, and would therefore call for twelve detectors to be used to monitor this compressor house. However, the layout of the compressors appeared to offer the potential for a smaller number of detectors to be used while still obtaining acceptable coverage. The assessment process allows for these options to be explored and for the coverage provided by competing layouts to be compared objectively. This is done by first modeling the existing or currently proposed detector layout, typically referred to as the baseline design. The software provides detailed information of the level of coverage, where gaps in coverage exist, and how much each detector contributes to the overall level of coverage. This information can then be used to modify or fine-tune the layout to address any unacceptable gaps in coverage or eliminate excessive redundancy.

Baseline Assessment Results

As the compressor station has not yet been built, there was no detailed information on the location and orientation of each detector in the client-proposed baseline layout. Because of this, the detectors were placed by Micropack based on information provided by the client in the project kick-off meeting. Twelve Drager Flame 5000 detectors were modeled in the compressor house as being mounted 8 m above the local deck (ALD) with a 10° downward tilt relative to the horizontal. Normal practice calls for the detectors to be positioned approximately 3 to 4 m ALD to allow for them to be installed and replaced using portable ladders. However, the detectors have been placed higher in this case because the compressors are also elevated. At an elevation of 8 m ALD the detectors can still be easily field tested from the ground using portable LED test lights. The detectors were situated so that they would be mounted to steel structural supports along the Eastern wall of the compressor house. These were thought to be the best available mounting points to avoid issues with excessive vibration.

The detectors were specified to face at a 45° angle relative to the eastern wall with six oriented towards the Northwest and six oriented towards the Southwest. Figure 7 shows the overlapping field of views for the detectors in the compressor house. The detectors are modeled with an effective viewing distance of 27.8 m (63% of the maximum) to account for desensitization. This desensitization factor was determined using a method widely used in the industry.[4]

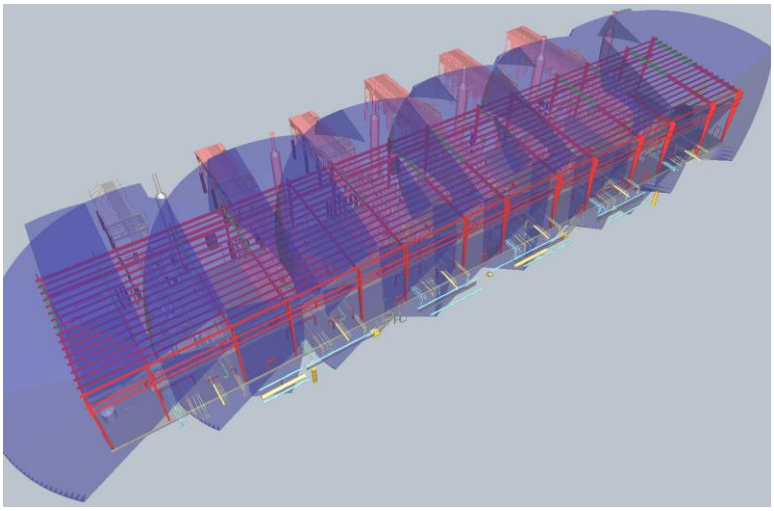


Figure 7: Detector Field of view for baseline detector arrangement.

This twelve-detector arrangement yielded a 2ooN coverage of almost 78% with 1ooN coverage for an additional 11% of the graded volume. The remaining eleven percent of the graded volume, mostly along the back and underside of the compressors had no coverage. Much of this area is difficult to obtain a clear line-of-sight to these areas because of obstruction from piping and equipment and the placement of additional detectors provide minimal improvements to coverage. For context, a 24-detector layout - using 12 additional detectors along the Western wall of the compressor house at 5 m ALD - only achieves 1ooN coverage for 92.8% of the graded volume and leaves 7.2% uncovered. It is hard to imagine many would argue a 5% improvement to 1ooN coverage is worth the addition of 1 or 2 detectors, much less 12, when the system already meets specified performance targets.

Figure 8 shows a graphical depiction of the detector coverage for the baseline layout overlaid onto the 3D model for one of the compressors. The baseline configuration can be seen to provide very good coverage of the upper and eastern facing sides of the compressor with coverage levels dropping towards the rear and underside of the compressor.

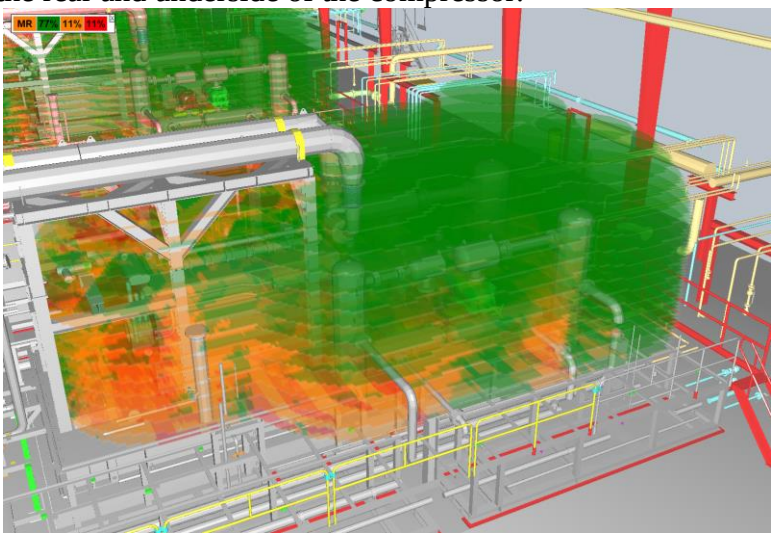


Figure 8: Visual depiction of geographic assessment result for the Southernmost compressor shown in HazMap3D.

Table 1 provides a numerical breakdown of the overall coverage and the contribution of each detector to the overall system. Pan and Tilt indicate the orientation of the detector. Pan ranges from 0 to 360 degrees with 0 degrees corresponding to an Eastern orientation. The tilt indicates the angle relative to the horizontal with a downward tilt being considered positive - flame detectors normally have a downward tilt of between 10 and 40 degrees. Because the assessment model is generated from the client-supplied model, the coordinates of the detector are defined and given using the same coordinates used in the client-model with the elevation defined relative to the local deck.

Table 1: Detector contributions to system coverage for the baseline layout

	Pan (°)	Tilt (°)	Individual	1ooN	2ooN	>2ooN
All Detectors				88.8	77.8	62.0
Det01	135	10	21.5	86.7	74.6	57.4
Det02	225	10	10.4	88.4	76.1	58.3
Det03	135	10	27.8	88.0	74.7	57.6
Det04	225	10	20.7	88.3	75.9	55.7
Det05	135	10	28.9	88.1	75.3	57.0
Det06	225	10	27.8	88.3	75.6	56.6
Det07	135	10	30.2	88.1	75.4	55.8
Det08	225	10	29.3	88.1	74.8	57.7
Det09	135	10	23.7	88.0	75.2	54.3
Det10	225	10	30.3	87.8	73.9	57.7
Det11	135	10	12.0	88.2	75.8	57.1
Det12	225	10	23.3	86.1	74.6	56.5

The 1ooN and 2ooN coverage columns in Table 1 give the percentage of the graded area that achieves that level of coverage if that detector is removed from the system. For example, if Det01 is eliminated, 2ooN coverage drops from 77.8% to 74.6%.

Based on Table 1, the baseline layout generated based on client practices detailed in their fire and gas protection philosophy and the project kick-off meeting is a good one. It meets and exceeds the 80% coverage level expected for MR areas with 1ooN coverage and nearly meets it with 2ooN coverage. The numerical breakdown in Table 1 also shows that the system has a sufficient level of redundancy that the failure or loss of any one detector does not significantly reduce overall coverage and does not cause the system to drop below the 80% coverage expected of it.

That 1ooN coverage for the targeted fire size is not achieved for 11% of the graded volume is not as concerning as it may at first appear given the size and location of the gaps, and the types of fires expected. The compressors handle high pressure gas. Jet fires are the most likely fire for the system to detect. Pool fires will not occur and fires on the underside of the compressor - where the largest gaps in coverage occur - are relatively unlikely. The remaining coverage gaps are relatively small and a high-pressure jet fire is unlikely to be able to “hide” within those small volumes.

Based on this, the baseline layout is a well-designed system. However, it may not represent an optimal layout. Table 1 suggests that it may be possible to eliminate several detectors with minimal loss of system performance. This can be inferred from that fact that Table 1 shows

3ooN coverage is achieved for 62% of the graded volume and the 3ooN coverage remains over 50% even with the loss of any single detector.

Detector Layout Optimization

Based on Table 1, Det02, Det04, Det06, and Det11 contribute relatively little to the overall system coverage and can likely be eliminated. Det05, Det07 and Det08 can also be seen to contribute only marginally to the overall coverage. Based on this, detectors Det02, Det04, Det08, and Det11 were removed and a new assessment was run. Table 2 shows the overall coverage levels and individual contributions of each detector for the reduced 8 detector layout.

Table 2: Detector contributions to system coverage for the 8-detector layout

	Pan (°)	**Tilt (°)**	**Individual**	**1ooN**	**2ooN**	**>2ooN**
All Detectors		10		86.3	65.2	41.6
Det01	135	10	21.5	79.9	57.1	34.6
Det03	135	10	27.8	85.1	59.7	28.9
Det05	135	10	28.9	85.5	61.4	30.6
Det06	225	10	27.8	82.6	56.8	30.5
Det07	135	10	30.2	85.2	60.7	29.2
Det09	135	10	23.7	84.8	58.4	34.3
Det10	225	10	30.3	83.9	60.9	34.6
Det12	225	10	23.3	82.5	59.3	35.4

The elimination of these four detectors resulted in an 8-detector layout with 2ooN coverage for 65% of the graded area and 1ooN coverage over an additional 21%, for a total 1ooN coverage of 86%. While the coverage provided is not as comprehensive as that provided by the baseline layout, the achieved coverage level still exceeds the desired coverage level of 80% specified by the client and does so with 33% fewer detectors. This 33% reduction in the number of detectors only reduces 1ooN coverage by 2% of the graded volume. Most of the loss of 2ooN coverage was seen on the outer sides of the Northernmost and Southernmost detectors. Figure 9 shows the coverage level on the southern side of the southernmost detector. While the level of redundant coverage in the system has been significantly reduced, Table 2 shows that the system can still tolerate the loss of any single detector while still maintaining 1ooN coverage at or above the 80% level desired by the client. The loss of Det01 has by far the most significant impact on system 1ooN coverage with the loss of Det06 causing the largest reduction in 2ooN coverage. The reduction in redundant coverage can be seen mostly clearly in Table 2 with the 20% reduction in 3ooN coverage as compared to the baseline layout.

Given that the detectors are designed to indicate a fault state and report a detected fault to the control room, and given the very high reliability of the detectors, it’s considered unlikely that two or more of the eight detectors will be in fault at the same time provided reasonable inspection and maintenance practices are adhered to.

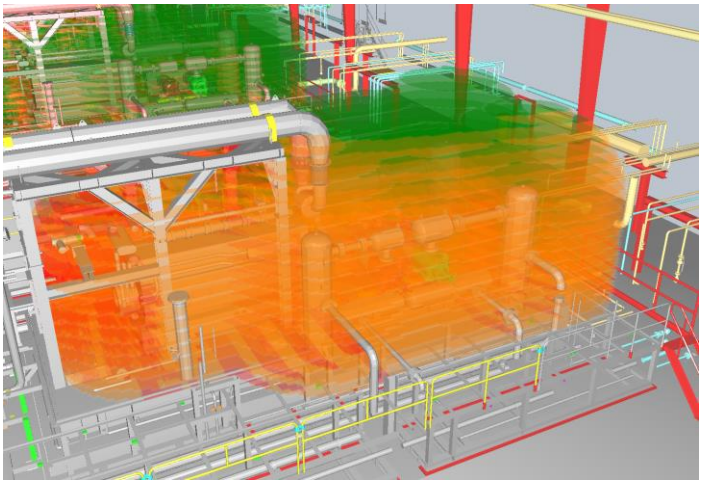


Figure 9: Coverage loss on the Southern side of the Southernmost detector shown in HazMap3D

Revision Based on Client Feedback

Soliciting client comments on and approval of the proposed changes is a vital part of any process that involves modifications to safety critical systems. Even if the system satisfies company specific or project specific performance goals, concerns may arise from the client, who may want to go beyond specified minimum coverage goals for any of a number of reasons.

While the 8-detector layout met the targeted performance level and the client was pleased by the prospect of reducing the detector count, the client was concerned about the gaps in 2ooN coverage at the far sides of the building and asked that two detectors be added to address the large gaps in 2ooN coverage on sides the Northernmost and Southernmost compressors.

Detectors were added to the Northwest and Southwest corners of the compressor house oriented towards these 2ooN coverage gaps, situated approximately 6 m ALD. The location and fields of view of these additional detectors is shown in Figure 10. This placement ideally situated these detectors to close the gaps in 2ooN detection on the sides of these compressors while also keeping them geographically separated from the detectors in the northeast and southeast corners of the compressor house.

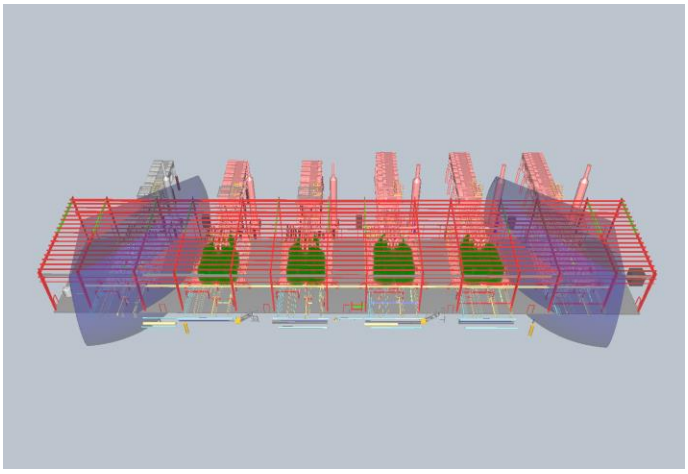


Figure 10: Field of view for detectors located in the Northwestern and Southwestern corners of the compressor house.

The additional detectors addressed the gaps in 2ooN coverage, resulting in a 10-detector layout that provided almost 74% 2ooN cover and over 88% 1ooN coverage, nearly matching the coverage levels achieved in the baseline layout - the two layouts are within 0.5% of each other for 1ooN coverage - while achieving a 16% reduction in detector count. Table 3 provides a breakdown of the layout and the coverages provided.

Table 3: Detector contributions to system coverage for the 10-detector layout

	Pan (°)	**Tilt (°)**	**Individual**	**1ooN**	**2ooN**	**>2ooN**
All Detectors				88.5	74.2	50.5
Det01	135	10	21.5	87.3	65.6	40.0
Det03	135	10	27.8	87.3	69.6	37.9
Det05	135	10	28.9	87.7	70.4	39.5
Det06	225	10	27.8	85.4	68.9	36.7
Det07	135	10	30.2	87.4	70.0	40.7
Det09	135	10	23.7	87.3	70.9	42.5
Det10	225	10	30.3	86.0	70.2	43.5
Det12	225	10	23.3	87.3	69.6	43.4
Det13	300	10	12.2	87.5	71.1	46.4
Det14	60	10	13.0	87.4	68.2	45.8

The hazard mapping software makes assessments like this possible by allowing an objective assessment of coverage levels provided for target fires of specified sizes. It allows practitioners to easily see where coverage gaps exist and then adjust detector locations or type or add additional detectors to address gaps. By providing information on the contribution each detector makes to the overall system performance, the software also makes it significantly easier to identify unnecessary detectors, detectors that are vital to overall system performance, and where more or less redundancy may be needed.

One of the chief hurdles that any engineering study or project has to overcome before being approved is justifying the expenditure of funds and resources. Each Drager Flame 5000 costs approximately $3,000. The installed cost of each detector can exceed $10,000 and each detector then incurs additional expense over it's lifetime for testing and maintenance, albeit a relatively small amount given the ease of testing and the high reliability of the device. Because of this, it can be relatively easy for a hazard mapping study to pay for itself in the form of reduced detector counts and costs. The cost of the system and the assessment both pale, however, in comparison to the risk of a fire going undetected and being allowed to propagate by a poorly designed detection system. With valuable equipment on the line, it pays to have a well-designed system based on an assessment by qualified engineers.

The effect of detector FOV on system coverage

The ability of the software to use the real, verified by test data, field of view and effective range of the detectors in conducting the assessment is critical to the quality of the assessment. The impact that detector field of view and range has on the effectiveness of the overall system and the number of detectors required to achieve adequate coverage deserves special emphasis. To

demonstrate this point, Table 4 lists the coverage levels achieved by the 10-detector system using the Flame 5000, and Flame 3000.

Table 4: Coverage levels obtained using different detectors with the proposed 10-detector layout.

Detector Type	1ooN	2ooN	>2ooN
Draeger Flame 3000	89.9	79.5	60.4
Draeger Flame 5000	88.5	74.2	50.5

Table 4 shows that the same layout - with no change in the number of detectors or the position of any detector - can provide significantly different coverage levels when different detector models are used, highlighting the importance of accurately accounting for field of view and range. Operators should be aware of this during the initial design and assessment of the system as well as during any MOC involving the replacement of a detector. The wider field of view and longer range of the Flame 3000 allows it to provide 2ooN coverage to an additional 5% of the graded volume when compared to the coverage provided by the Flame 5000. This is largely the result of the Flame 3000 having a wider horizontal field of view - 120° versus 90° for the Flame 5000.

Conclusion

The authors have provided a flame detection assessment case study for the purposes of detailing the hazard mapping process, also called a geographic coverage assessment, conducted in a manner consistent with the guidance provided in ISA TR 84.00.07. A client provided 3D model was modified as necessary for the assessment process and imported into the assessment software. Grades were assigned to hazardous equipment containing flammable hydrocarbons and a baseline detector layout was generated based on the client's fire and gas protection philosophy and discussion with the client. The baseline layout was then assessed, and modifications were proposed to reduce excessive redundancies in the system and thereby reduce the installation, operating and maintenance costs associated with the system. This case study demonstrates the ability of hazard mapping, assisted with software designed for such studies, allow for the rapid and efficient design and assessment of flame detection systems using good engineering judgement.

References

1. ISA TR 84.00.07. Guidance on the Evaluation of Fire and Gas System Effectiveness.
2. Dräger Flame 3000: Multi-Channel IR Visual Flame Detection. Dräger. 2016. Available at <https://www.draeger.com/products/content/9041484_flame_3000_pi_en_uk_ master_121012_fin.pdf>. Accessed on 3 Mar 2018.
3. Dräger Flame 5000: Flame Detection. Dräger. 2016. Available at <https://www.draeger.com/Products/ Content/flame-5000-pi-9046372-en-gb.pdf>. Accessed on 3 Mar 2018.
4. McNay, James. Desensitisation of optical based flame detection in harsh offshore environments. International Fire Professional. July 2014. No. 9. 12-14.
5. Kohut, Joseph. "Fire, possible explosion at Susquehanna gas compressor station thought to be accidental." The Times-Tribune. 16 May 2013. Available at <http://thetimes-

tribune.com/news/fire-possible-explosion-at-susquehanna-gas-compressor-station-thought-to-be-accidental-1.1489789>. Accessed on 22 Feb 2018

6. Multispectrum IR Flame Detector X3301 Instructions. Rev 1.1. Det-tronics. July 2014.
7. Bloom, Iris Marie. "Williams Compressor Station Explosion in New Jersey Injures Two Workers." Protecting Our Workers. Protectingourworkers.com. 31 May, 2013. Available at: <https://protectingourwaters.wordpress.com/2013/05/31/williams-compressor-station-explosion-in-new-jersey-injures-two-workers>. Accessed on 6 Mar 2018.
8. O'Brien, Walter. "Multiple injuries reported at Branchburg gas pipeline facility flash fire." Nj.com. 30 May 2013. Available at: <http://www.nj.com/somerset/index.ssf/2013/05/multiple_injuries_reported_at.html>. Accessed on 6 Mar 2018.
9. Powell, Tarika. "Williams Companies Failed to Protect Employees in Plymouth LNG Explosion." The Sightline Institute. sightline.org. Available at: <http://www.sightline.org/2016/06/03/williams-companies-failed-to-protect-employees-in-plymouth-lng-explosion>. Accessed on 6 Mar 2018.
10. Botelho, Greg and Sam Stringer. "3 dead after Louisiana gas plant explosion." CNN. CNN.com. 8 October 2015. Available at: <https://www.cnn.com/2015/10/08/us/louisiana-deadly-gas-explosion>. Accessed on 6 Mar 2018.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Enclosed Process Bay Vented Blast Loads and Impacts on Occupied Buildings

Mark Whitney, Chris LeBoeuf and Charles Vergara
ABS Group
Advanced Engineering Division
140 Heimer Road, Suite 300
San Antonio, TX 78232
(210) 495-5195
(210) 495-5134 fax
E-mail: mwhitney@absconsulting.com

Abstract

A typical approach to suppressing the effects of a vapor explosion inside an enclosed process building or bay is to use vent panels to relieve the confined blast pressures. This results in blast expanding outside the process building and reaching near-by buildings with potential hazardous consequences. Before the venting happens, blast also propagates within the process building itself and can load areas such as a control room. This paper examines blast wave characteristics (e.g., magnitude, shape, duration) of vented loads that are released after the vent panel is disposed of and the resulting blast loading on a near-by building assumed to be occupied. Blast propagation within the process building and loading on connected occupied areas (e.g., control room, break room) are also examined.

Keywords: CFD, Blast, Facility Siting, Structural Response, SDOF, Petrochemical

Introduction

A vapor explosion inside a fictitious enclosed process building was modeled using the Computational Fluid Dynamic (CFD) code FLACS[1]. The example CFD simulation tracked blast propagation within the process building and tracked loads vented to the exterior that reach a near-by building. The results of the CFD simulation are compared to predictions made using traditional vapor cloud blast curves. Example Single Degree of Freedom (SDOF) structural response calculations are made for common building constructions and the hazards to occupants summarized.

[1] Flame Acceleration Simulator (FLACS), Version 10.3r3, GexCon, Bergen, Norway, 2014.

Overview of CFD Model:

Figure 1 illustrates the example enclosed process building with two hazardous process areas (A & B). The facility also includes occupied areas such as a laboratory, change rooms, and control room. The various spaces are connected by corridors. In addition, there is an administration building connected to the process building by a breezeway.

It is assumed that the process building was not designed with blast in mind and that the structure was sized for conventional loads (e.g., wind, snow). The construction of the process building includes exterior walls that are metal panels supported by cold-for girts. Interior walls are 8-inch unreinforced masonry block. The roof is concrete on metal decking supported by open web steel joists (OWSJs). Doors at the process areas are assumed to be lightweight panels such as in Figure 2, while doors to occupied areas (e.g., laboratory) are conventional hollow metal doors. It is important to point out that the internal explosion will load wall and ceiling surfaces, resulting in pushing those components from the inside out, which is the reverse direction of conventional loads.

The Administration Building was assumed to be exterior brick over masonry block. It has a built-up roof supported by OWSJs. The building has conventional insulated glass unit windows.

Two flammable cloud locations were investigated, one each in hazard areas A & B (Figure 3). Each vapor cloud explosion involved propane as the flammable material in a moderate congestion level

Figure 4 illustrates the propagation of blast internal of the building, plus that which is vented to the exterior, with blast reaching the Administration Building. The following comments apply:

- The blast propagates away from the source, interacting locally with walls and roof.
- The most intense loading is in the room with the explosion.
- Blast quickly leaks through doorways into adjoining rooms and adjoining corridors.
- As time progresses the blast makes its way through the building failing weak walls and upheaving the roof. (See Figure 5 where failed walls are shaded red)
- Blast is also leaked to the outside through exterior wall and roof failures. Leaked blast loads reach the administration building. Leaked blast can also wrap-around and load external wall and room surfaces of the main building.

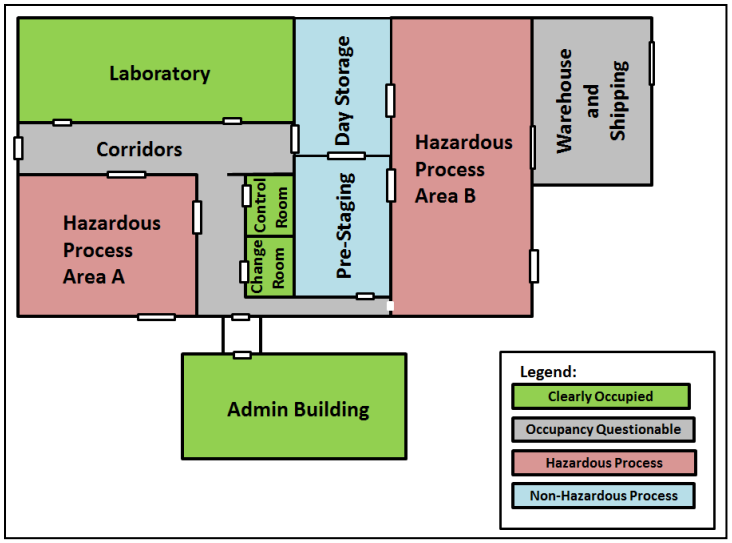
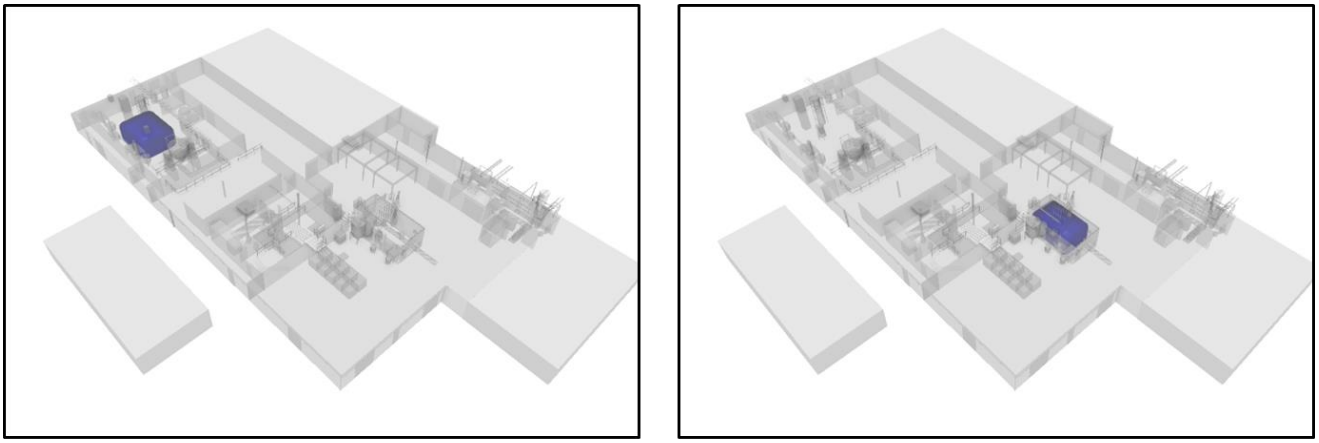


Figure 1. Example Building with Enclosed Process Areas

Figure 2. Typical Process Area Door



Explosion A **Explosion B**

Figure 3. Explosion Locations in Hazard Areas A and B

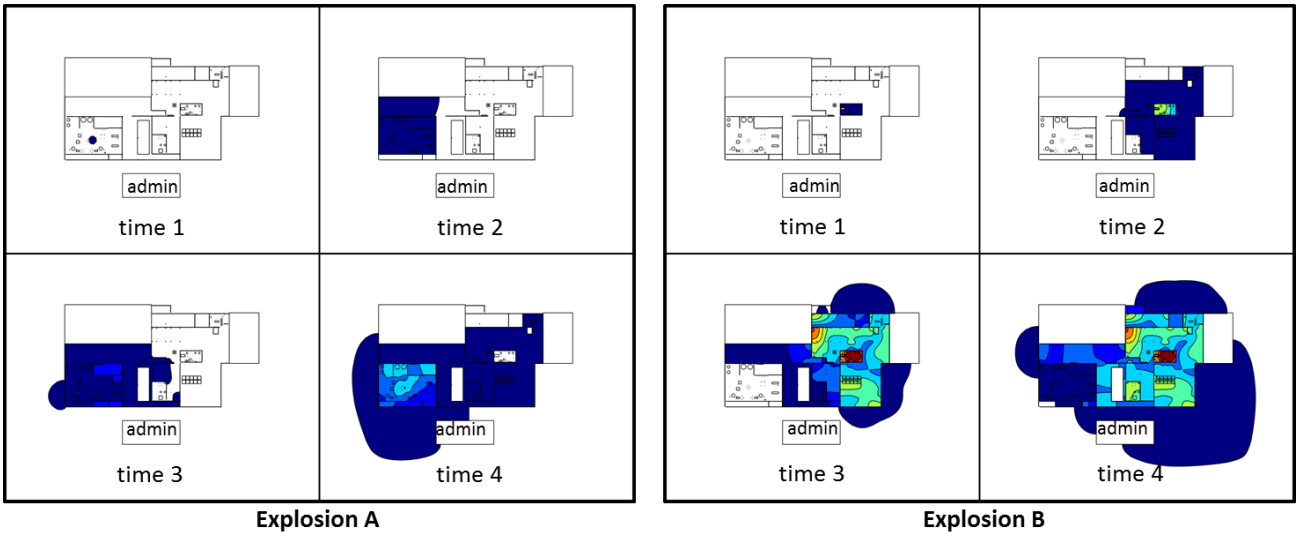


Figure 4. Blast Propagation Sequence

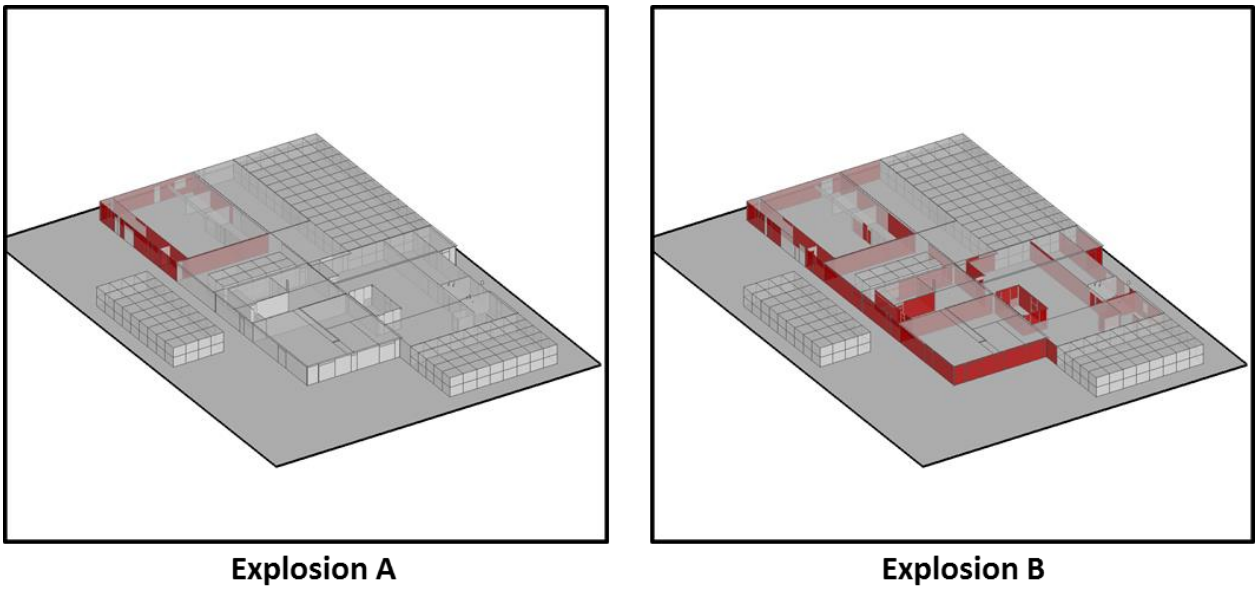


Figure 5. Wall Failures Patterns

Representative Pressure Time-Histories:

The process of blast propagation within the building results in the pressure wave reflecting off walls and floors. This results in a reverberation pattern in the pressure time-history[2]. Figure 6 shows two sample blast-recordings from the CFD simulation. Explosion A recording was taken at the Admin Building wall facing the process building. Explosion B was taken inside the

[2] The pressure axis values were intentionally left blank as only relative magnitude is germane to the discussion.

process building, away from the explosion center. Both reveal several peaks and valleys in the pressure history. Explosion A at the Admin Building is lower pressure (due to the increased separation from the explosion) and demonstrates several pulses as blast reflections in the building leak out over time. Explosion B shows a similar pattern but at higher pressure, as it is within the enclosed process building.

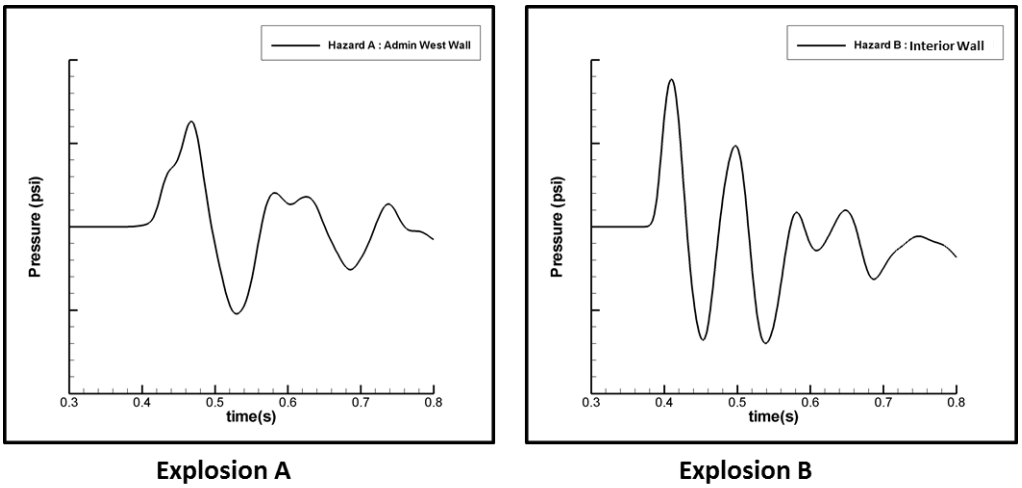


Figure 6. Pressure-Time Histories

Previous work investigated the structural response to blast histories comprised of multiple pulses. Previous work[3],[4] examined the effect of multiple shock pulses on structural response. That work compared a traditional triangular single pulse load to that of a load comprised of three pulses that decay with time. Single Degree of Freedom (SDOF) analysis was used to calculate responses and results were plotted as non-dimension terms in Figure 7, with the X axis representing scaled time (relating structural frequency and load duration) and Y axis as scaled maximum deflection (related to static deflection from peak pressure). The shock time history (duration and arrival time) are scaled to the natural period of the SDOF element. A single solution for a shock arrival/shock duration equal to 2.5 is shown. The triple pulse in Figure 7 is similar to the blast profile shown in Figure 6, indicating that the overall structural response can be enhanced over that from the initial pulse alone. Later shock reverberations cannot be ignored.

[3] DOE/TIC-11268, "A Manual for the Prediction of Blast and Fragment Loadings on Structures," Prepared for United States Department of Energy, Albuquerque Operations Office, by Southwest Research Institute and Wilfred Baker Engineering, Inc., under Contract with Mason & Hanger, and Battelle Pantex, July 1992.

[4] "Structural Response to Multiple Pulse Blast Loading," Whitney, Mark; Barker, Darrell; Waclawczyk, Jr., Johnny; Proceedings on the Sixth International Symposium on the interaction of Non-Nuclear Munitions with Structures; pages 122-127, May 1993

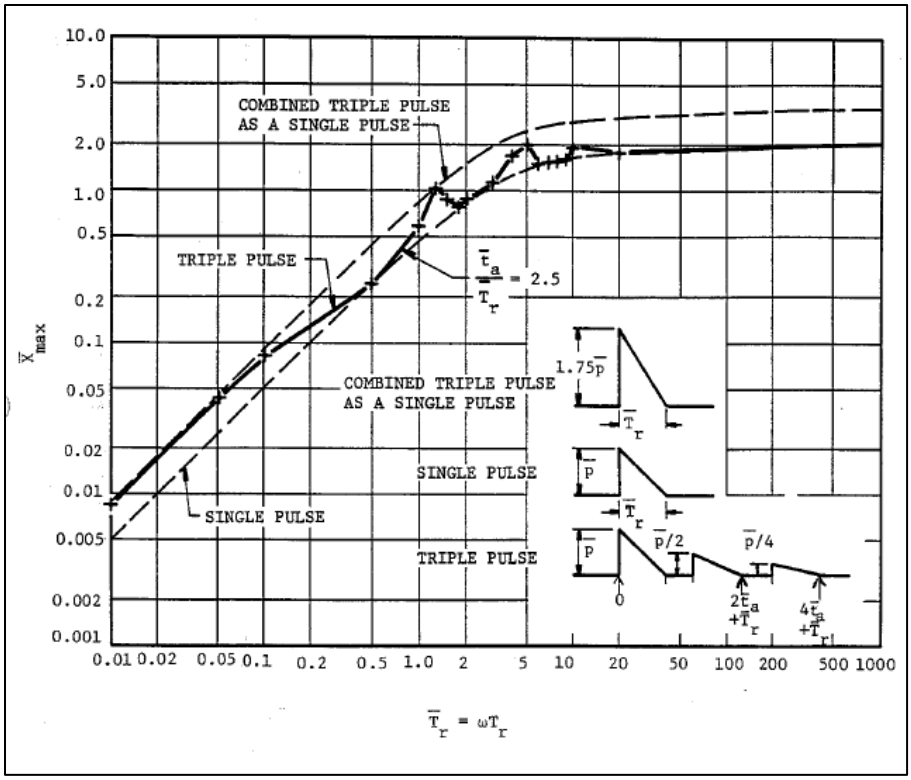


Figure 7. Triple Pulse Analysis (Taken from 3)

Construction Considerations

The following comments apply to conventionally constructed buildings:

- Provision of vent panels reduces blast load in the interior of the process building, but can increase blast loading on buildings near the vent location.
- Provision of vent panels does not eliminate blast loading on interior walls and ceilings and localized failures may occur unless design is provided to resist the loading.
- Brittle elements such as unreinforced masonry walls are unforgiving and can be driven to collapse. This is particularly troubling if the wall is load bearing.
- Brittle elements can be sensitive to pressure time histories with multiple shock reverberations such as those in Figure 6. In some cases, the element may not fail from the initial pulse but is driven to failure by the cyclic loading.
- Roof elements are designed to principally resist gravity loads. Some capacity is provided to resist uplift from wind loading; however, this is overcome by even modest blast loads. Roofs uplifted by blast result in a falling debris hazard after the blast load is relieved through venting.
- Some reinforced concrete cast-in-place slabs have greater reinforcement at the bottom to provide a tension component for gravity load. Interior blast loading can uplift the slab and ‘crack the back’ of the slab.

- Precast elements, such as double-Ts, typically have relatively weak connections to their supports. Also, double-Ts often have bottom pre-stressed tendons and relatively light top reinforcement. These are vulnerable to reverse loading.

Conclusions

This paper investigated explosions in enclosed process areas and how that affected blast propagation within the process building and vented blast that reached near-by buildings. A structural response should address the full pressure time-history of the loading. Examples are given to identify potential weaknesses in conventional construction to blast loading.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Development of Empirical Method to Calculate Natural Gas Pipelines Rupture Exposure Radius

Abdulaziz N. Ababtain, Dr. Arafat M. Aloqaily*
Saudi Arabian Oil Company
Dhahran, Saudi Arabia
*Presenter E-mail: arafat.aloqaily@aramco.com

Abstracts

Natural Gas pipeline location classification are designed following an approach similar to ASME B31.8, which considers segmenting the pipeline length and count the population in each segment within a given distance from the pipeline (width of segment). ASMEB 31.8 utilizes fixed distance of 400m for the segment width, while other operators use the pipeline Rupture Exposure Radius (RER). This is a distance determined by the consequences modeling for pipeline full rupture. Since, the population density within the segment width affects the design factors of the pipeline, i.e. wall thickness requirements, over-predicting the distance can have significant cost implications. Some operators use default RER values on conservative estimates, while industrial best practices allow for detailed dispersion to calculate representative RER distances.

Detailed dispersion modeling was performed for a large number of Natural Gas Pipeline scenarios, and an empirical formula was developed to estimate the RER for these pipelines as a function of the pipeline diameter and pressure. The dispersion calculations results show that the default RER values current used by some operators are very conservative, and that the cost of pipeline design/construction can be optimized by using the empirical formula developed in this work. The formula, which produces the RER value in terms of the distance from the pipeline to the point of ½ lower flammable limit is easy to use, and accurately represents the dispersion results. This eliminates the need to using sophisticated modeling software/tools to assess the RER values of Natural Gas pipelines. The formula also uses minimum number of data/information available about the pipelines (diameter and pressure only) increasing its effectiveness as a tool replacing the modeling software. In addition, for pipeline projects, lower RER distances result in more flexibility in route selection, lower pipeline location class and hence thinner wall thicknesses, less emergency isolation valves required and longer span between sectionalizing valves, which all translate to cost savings and reduces potential sources of leak (sectionalizing valves).

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Steam Drum Level Measurement Compensation through the use of Constant Head Chamber with Dynamic Compensation

Lianwei Zhong, Cindy Wei, Henry Johnston
Chevron Phillips LLP
Emails: zhongl@cpchem.com, henryjesusjohnston@yahoo.com

Keywords: Constant Head Chamber, Pressure Compensation, Tolerance, SIS

Abstract

The level measurement for high pressure steam drum, using differential pressure (D/P) transmitters, has been challenging and sometimes problematic because condensate/steam densities vary significantly with the pressure and the temperature. One additional source of measurement error is the difference in temperature between the differential pressure transmitter's reference legs. These factors could cause the level measurement to be off as much as 30% from the actual value for high pressure steam boilers, enough to exceed the tolerance established in the Safety Requirement Specification (SRS) for a Low-Low Steam Drum Level Safety Instrumented Function (SIF). The further the deviation from normal operating conditions, the greater the level measurement error. Because of this, the Low-Low Steam Drum Level SIF is not operative during the start-up, which is the riskiest operation mode.

This paper presents the use of temperature - equalizing columns (Constant Head Chambers) to minimize the temperature difference between the transmitter reference legs, and drum level compensated measurements through the use of dynamic selection of D/P range vs % Level depending on the steam drum operating pressure or dynamic calculation of saturated liquid/steam properties in SIS Logic Solver. This paper also addresses the challenges of implementing this method to meet measurement accuracy and safety integrity level requirements.

Introduction

Drum level measurement is one of the critical signals used in drum level control and drum level protection against hazardous scenarios. Typical DP based level measurement is shown in in Figure 1. Assuming the reference leg B is filled with water and its temperature is constant at the ambient conditions (68F or 100F etc.), the basic formulas are shown below:

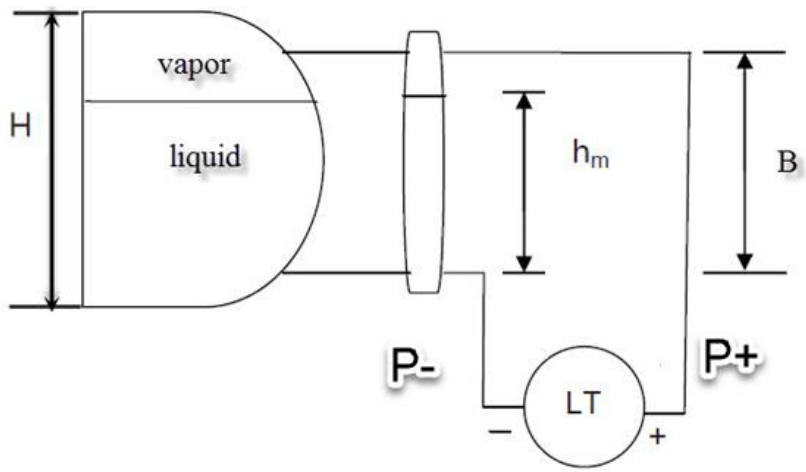


Figure 1: Schematic of Typical DP based Drum Level Measurement

$P_{upper\ leg} = P_+ = B * SG_B + (H - B) * SGv$ (Equation 1)

$P_{lower\ leg} = P_- = hm * SGw + (H - hm) * SGv$ (Equation 2)

$DP = (P_{upper\ leg}) - (P_{lower\ leg})$ (Equation 3)

$DP = [B * SG_B + (H - B) * SGv] - [hm * SGw + (H - hm) * SGv]$

$= [B * (SG_B - SGv) - hm * (SGw - SGv)]$ (Equation 4)

Where:

h_m: Actual steam drum level [inches]

h: Raw level measure by transmitter in SIS [inches]

H: The maximum steams drum height (inches)

B: The distance between upper tap and lower tap (inches)

SG_w: Specific gravity of saturated water inside the drum

SG_v: Specific gravity of saturated steam inside the drum

SG_B: Wet Leg water specific gravity at the ambient temperature

P: Hydrostatic pressure (inches W.C.)

The DP is measured and represented in DCS/SIS as raw drum level h typically; compensated level can be expressed as

$L=h_m/B=f\ (DP, SG_w, SG_v)= h_m=f\ (h, SG_w, SG_v)$ [%] (Equation 5)

Constant Head Chamber Level Measurement Analysis

As indicated in the above definition, Specific Gravity SG_B is based on the assumption that the temperature in the upper leg is near ambient. Such assumption is not accurate in some cases. One way to reduce the uncertainty in the determination of the upper leg temperature is the use Constant Head Chamber/Reservoirs. It is intended to reduce the difference in temperature between the upper leg and the measurement (lower leg) section via "pipe inside pipe" method as shown in Figure-2. The lower half of chamber and section below that are insulated to make those sections adiabatic to the ambient, but the upper half of the chamber is exposed to air. It makes the vapor and liquid inside the chamber stay saturated at normal operation. The inner tube (wet leg) is quickly full of steam condensate, the potential over fill spills into the outer tub and connects back with the drum liquid. The inner wet leg (upper leg) is always full of the saturated water which has the same specific gravity of the liquid inside of the drum, so it maintains "constant head" pressure in the reference leg.

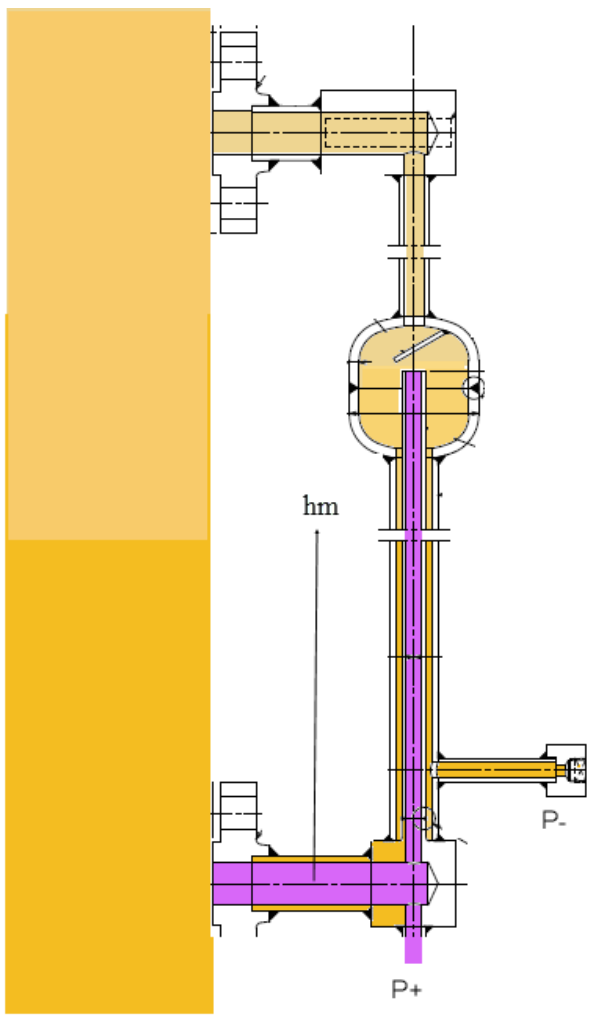


Figure 2: Schematic of Pipe in Pipe Constant Head Chamber (Permit from BBK Technologies)

Where:

Light yellow section: steam

Dark yellow section: liquid

Purple section: inner pipe filling of condensate, linked to transmitter lower pressure port

h_m: Actual steam drum level in the constant head chamber, linked to transmitter high port

Because of the use of Constant Head Chamber, we can now say:

$SG_B = SGw$ Equation (6)

Substituting Equation 5 in Equation 4

DP = $B * (SG_w - SGv) - \text{hm} * (SGw - SG\text{v})$ Equation (7)

Calling

ΔSG= $SG_w - SGv$ and substituting in Equation 6

DP= $B * \Delta\text{SG} - \text{hm} * \Delta\text{SG}$ Equation (8)

At 0% level hm=0, substituting in equation 7

$DP_{0\%} = B * \Delta\text{SG}$ Equation (9)

At 100%, hm=B, substituting in equation 7

$DP_{100\%} = 0$ Equation (10)

Pressure Compensation, Multiple Transmitter Ranges with dynamic switching

The linear relation between the differential pressure and the level is shown in Figure 3.

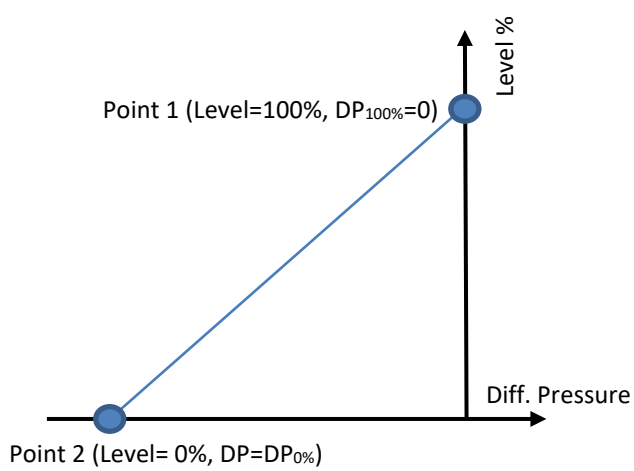


Figure 3. Linear Relationship of Differential Pressure vs Level

If two points of the straight line are known, the level at any point can be calculated as follows:

$L = L_2 + (L_2 - L_1 / DP_2 - DP_1) * (DP - DP_2)$ Equation (10)

Using the data from Figure 3: L_1=100%, $DP_{100\%}$=0, L_2=0%, $DP_2 = DP_{0\%}$

$L = -100\% / (DP_{0\%}) * (DP - DP_{0\%})$ Equation (11)

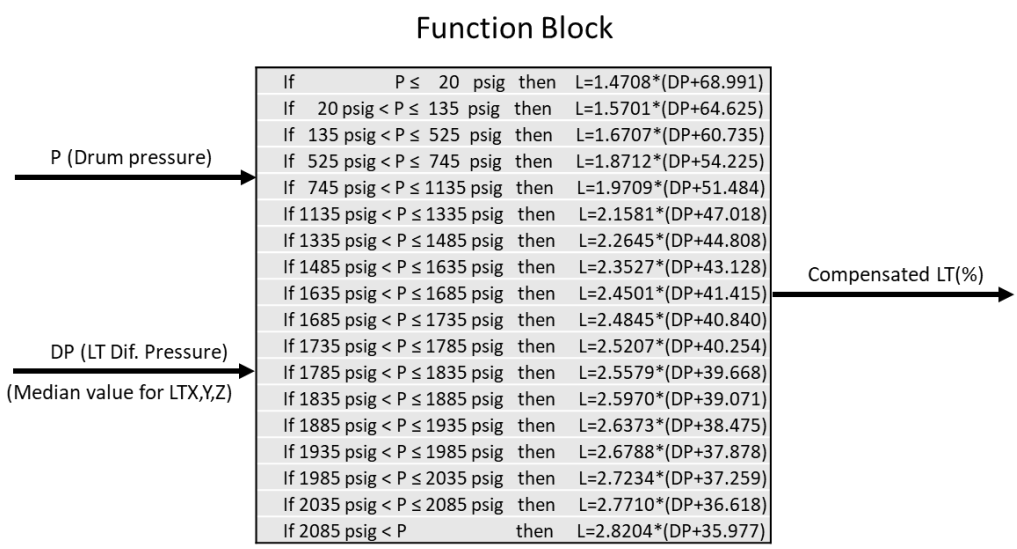
Substituting Equation 9 in Equation 11

$L = -100\% / (B * \Delta SG) * (DP - B * \Delta SG)$ Equation (11)

Where:

L: Actual compensated steam drum level [%] =hm/B

For a boiler with an operating range from start-up equal to atmospheric pressure to a design pressure of 2085 psig, 18 pressure segments were selected. For each one of those pressure segments a Level equation was calculated using Equation 12 and data from ASME Steam Tables. Within those segments the inaccuracy is limited within 2%.



This calculation bases on the traditional method using transmitter measured raw drum level h then compensated with saturation pressure, but it breaks the traditional link between uncompensated drum levels with transmitter settings. It measures D/P directly and uses dynamic value of $DP_{0\%}$ and $DP_{10\%}$ calculated from drum dynamic pressure.

Pressure Compensation using Function Block in SIS Logic Solver

Based on the similar idea of above, Equation 8 can be re-arranged to express hm as unknown

As now, $DP = B * \Delta SG - hm * \Delta SG$ Equation (8)

Moving hm *ΔSG to the left side of equation

$$\mathrm{hm} * \Delta\mathrm{SG} = B * \Delta\mathrm{SG} - \mathrm{DP} \qquad \text{Equation (8)}$$

$$\mathrm{hm} = \frac{B * \Delta\mathrm{SG} - \mathrm{DP}}{\Delta\mathrm{SG}}$$

$$\mathrm{L} = \frac{hm}{B} = 1 - \frac{DP}{\Delta\mathrm{SG} * \mathrm{B}} \qquad \text{Equation (8')}$$

In this method, as long as DP can be measured accurately from field transmitter, then by means of calculation capability of current SIS logic solver, the custom function blocks can be built to calculate differential specific gravity based on saturated pressure, then the drum level can be calculated and compensated correctly as well.

During the implementation, ASME Steam Table Compact Edition Table-2 is broken into 22 pressure segments. The algorithm determines which segment of the steam tables will be used based on the steam pressure from zero psig to 2085 psig. Another function blocks is built to calculate the drum level L based on Equation 8.

Building the function block of specific gravity differential curve with drum pressure utilizes the advance of computation capability in current DCS/SIS; it makes the relationship between drum level with DP and drum pressure simple and easy to understand. Furthermore, the measurement accuracy is improved with the full pressure range; the difference between the compensated readings and independent magnet level measurement is within 1%.

SIL Verification due to adding steam pressure compensation

The Steam drum pressure transmitter is a key element in the level compensated measurement. The switching between transmitter ranges depends on its indication. A false signal could cause a selection of an inappropriate range, which may not be able to meet the tolerance specified in the SRS, and probably defeating the protection. It is recommended to include such transmitter in the SIL verification. The input group voting should be 2oo2 of the pressure and level transmitters.

Conclusions

1. Constant header chamber's compensation reduces the temperature uncertainty of the differential pressure transmitter upper leg. Its main function is to equalize the condensate in upper leg and the steam drum water temperature. This equalization helps to simplify the equations used for pressure compensation.
2. This paper introduces a practical and convenient way of steam drum level measurement compensated by pressure, using multiple level equations with automatic switching depending on the pressure measurement.
3. This pressure compensation approach allows low-low steam drum level SIF functional during the start-up, design operation, off-design etc. operating modes.
4. modularity of functionality makes complex measurement/calculation easy to implement
5. The hardware used for pressure compensation (pressure transmitter) shall be included as part of the SIF and validated through the SIL verification.

References:

1. ASME Steam Tables Compact Edition
2. Power Industry Division Newsletter Spring 2012-- Steam Drum Level Measurement Temperature Equalizing Column Concerns, Dale P. Evelyn, P.E.
3. Instrument Engineer's Handbook--Process Measurement and Analysis, 4th Edition, Bela G. Liptak
4. ANSI/ISA-84.00.01-2004 Part 1(IEC 61511-1 Mod)

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

HAZID to SIL – Challenges in Hazard Identification Impacting SIL of SIF

Amit K Aglave, Vivek Gupta, Hemant J Patel
Fluor Daniel India Pvt. Ltd.,
New Delhi, India
E-mails: amit.k.aglave@fluor.com, vivek.gupta@fluor.com, hemant.j.patel@fluor.com

Abstract

Applying safety in design should begin at the conceptual phase of process design. In the early phase of the project, process engineering evaluates various design parameters such as process criteria, heat and mass balance, material selection tables, equipment data sheets and limitations to the design. Further, basic process control strategies and safeguarding philosophies are developed to prevent manifestation of hazard due to process upset or loss of containment.

Hazard identification, probability of its manifestation, and risk ranking through studies such as HAZOP is one of the important activities for verifying adequacy of proposed safeguarding philosophies. Proper hazard identification and risk analysis lay a solid foundation for determining the required protection layers to reduce risk to an acceptable level. Per hazard, several risk reduction layers are applied, one of which being safety instrumented functions (SIFs) implemented in Safety Instrumented System (SIS). The allocation of safety integrity level (SIL) requirements to SIFs is a commonly "understood" process. However, incorrect assessment of the hazards or risk ranking can lead to overrated or understated integrity requirements for SIFs. Either of this can be costly to the plant in terms of increased expenditure on assets or cost of salvaging the hazard manifested due to inadequate protection.

The paper reviews some challenges in current practices of hazard identification with a view to address those. This should help to establish realistic integrity and functional requirements for the safety instrumented functions. To address these challenges, it is important for functional safety engineers to influence process safeguarding strategies early in the design phase. This means identifying and moderating unrealistic safety constraints early in the design phase when it is still feasible to make significant process and mechanical design changes to lower the risks and, often, the total installed costs.

Introduction

Hazard and risk assessment (H&RA) is the first important phase of the SIS safety life-cycle phases and functional safety assessment stages as defined in IEC 61511-1 [1]. The objective of this phase as defined in the IEC 61511-1 [1] is to determine:

- the hazards and hazardous events of the process and associated equipment,
- the sequence of events leading to the hazardous event,
- the process risks associated with the hazardous event,
- the requirements for risk reduction and
- the safety functions required to achieve the necessary risk reduction.

This crucial phase, when executed properly, help the designers of the process plant apply correct safeguarding strategies for safe operations.

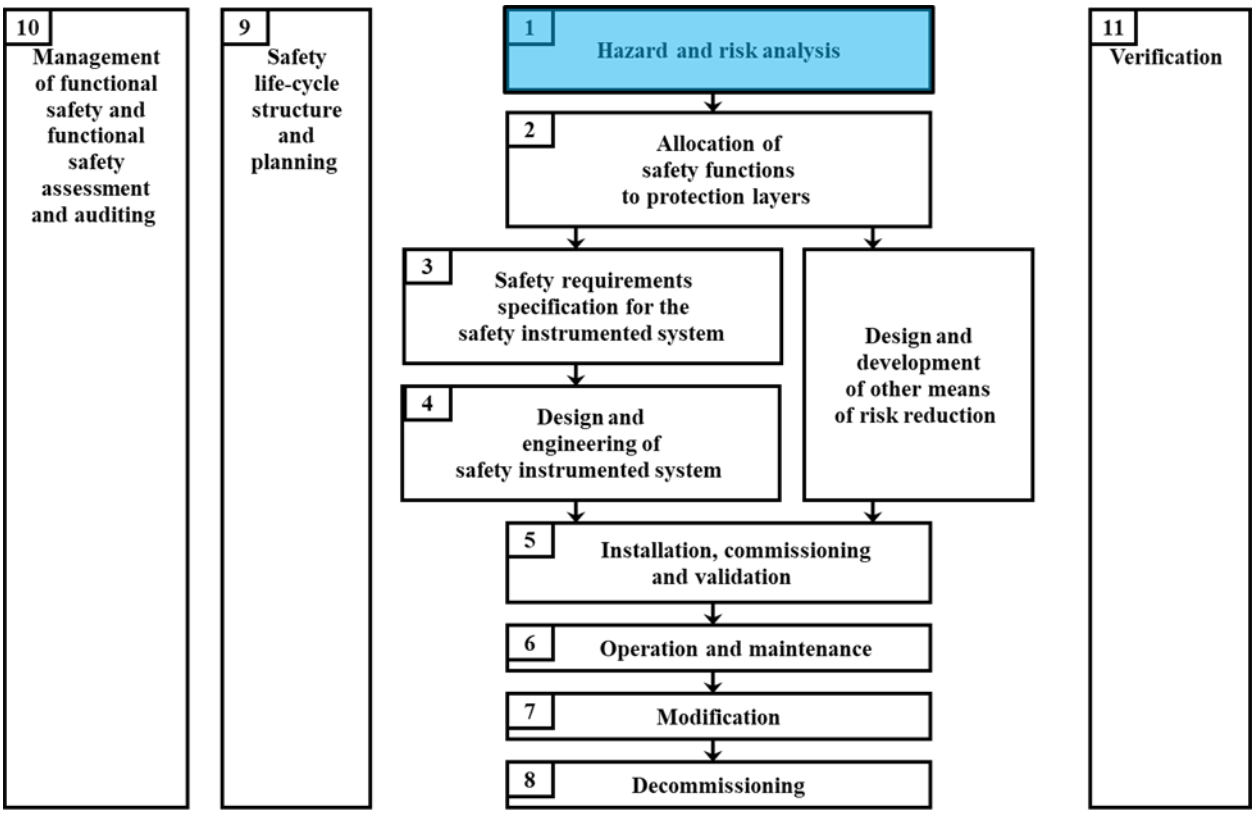


Figure 1. SIS safety life-cycle phases and FSA stages

Safety reviews, What if analysis, Hazard and operability study (HAOP), Failure Mode and Effect Analysis (FMEA) etc. are several ways for executing the H&RA phase.

Background

Operations in the process industry involve handling of fluids which can be flammable and / or toxic in both raw and finished forms and processing at extreme temperatures and pressure. Beginning with the conceptual phase through detail design engineering, H&RA is performed to

identify and address hazardous events that could occur under reasonably foreseeable circumstances. The knowledge obtained from H&RA studies helps to determine the required improvements in the design so that the risk can be reduced or eliminated. However in practice, the risk, in most of the cases can only be reduced or managed. Complete elimination may be become daunting task, making design impractical from operation and cost perspective.

It thereby necessitates the designers to provide a design which manages risk to an acceptable level. The likelihood of the operations free of incidents increases when the plants are designed with safeguards against each identified risk. For the design of these safeguards, proper understanding of the hazards and risks in operation is vital. This understanding of risk determines required robustness of the safeguards, i.e. the integrity requirement of the safeguards so that the risk is at the tolerable level. The figure 2 [1] indicates the possible safety layers which can be applied for the purpose of management of risk. Depending on the magnitude of risk to be managed, either a single or combination of these safety layers are put in place. The magnitude of the risk is established by conducting the hazard and risk assessment of the process.

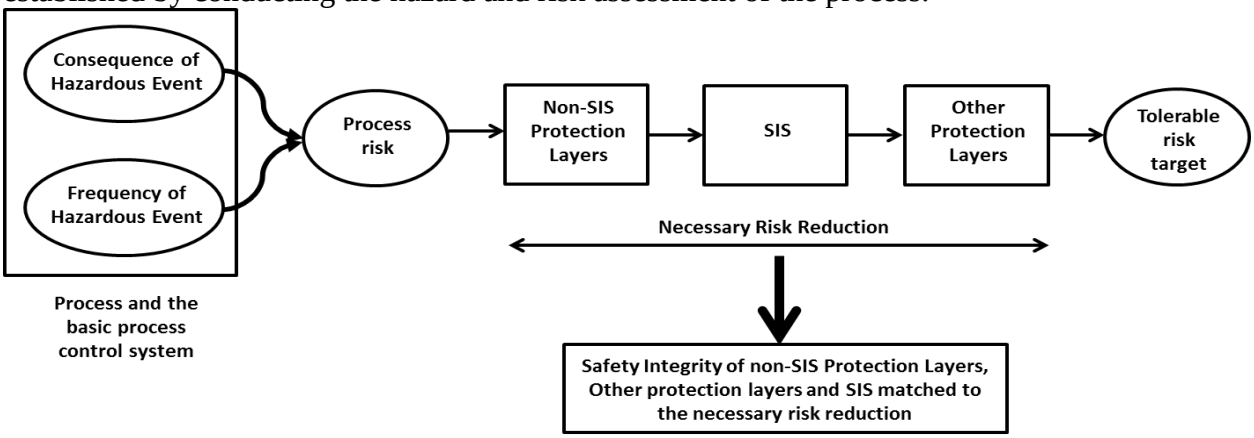


Figure 2. Risk and Safety Integrity concepts

How is Risk Assessed

A well understood risk during design stage is the backbone of the project moving forward to successful commissioning and operations.

The figure 3 [2] indicates important aspect of risk understanding and risk assessment which is vital for the performance of HAZOP.

- Historical-operational experience of the Design,
- Analytical Methods
- Knowledge of the Process Design

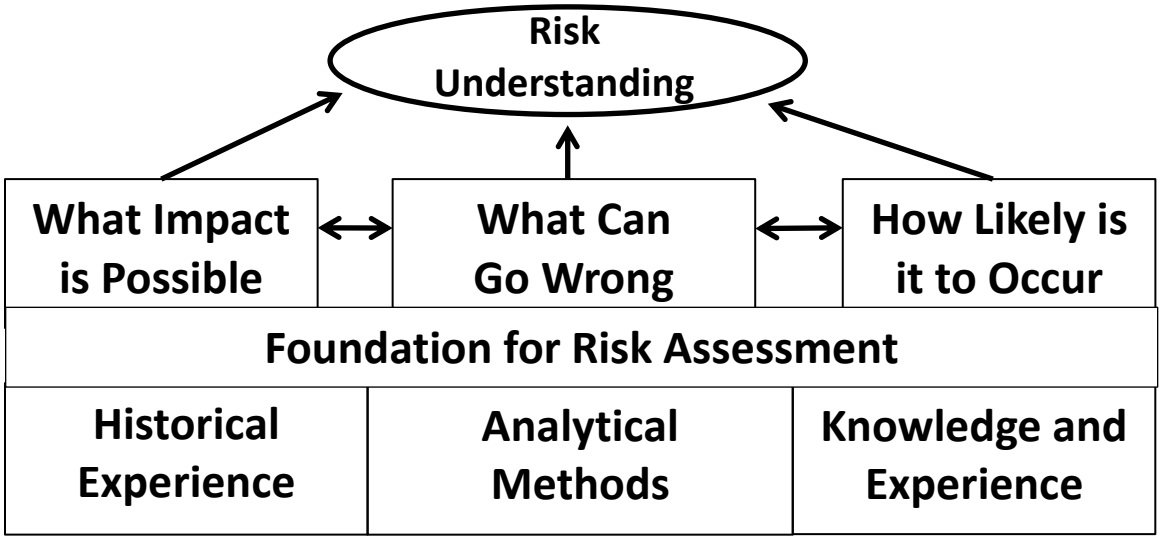


Figure 3. Aspects of Risk Understanding

Challenges in Design of SIS

Proper hazard and risk identification remains a challenge and opportunity in the process industry even after two centuries of experience in the design and operation of several process plants. Among several risk assessment studies, HAZOP is foremost and a team performed risk assessment activity and has been most widely used technique for carrying out H&RA. The process and methodology of HAZOP has improvised a lot since its conceptualization around five decades back.

However, the outcome of HAZOP studies is dependent on team performance and it may result into either underrated or overrated integrity requirements of the SIFs, often the later. Complying with these requirements becomes nightmare for the functional safety engineers who execute further phases of the SIS safety life-cycle. Often, to meet the requirements, changes to the design are made which results in overspending of effort hours, costly implementation of the safeguarding, schedule delays etc.

If the design remains underrated, the operations still carries the unmitigated risk which may lead to safety incident. If the design is overrated, management of functional safety during operations requires spending more than required resources apart from a costly implementation of the design, normally in terms of added instrumentation. It thereby becomes important to identify and understand the challenges in conduct of the HAZOP studies.

Why H&RA is Important?

"The traditional method of identifying hazards was to build the plant and see what happens - every dog is allowed one bite. Until it bit someone, we could say that we did not know it would do so. This method is no longer acceptable now that we keep dogs as big as Flixborough" - Kletz and Lawley.

The process industry has learned from past incidences that design should not proceed without proper identification of hazards and implementation of safeguards against these identified hazards. The findings of HAZOP lay foundation steps in the journey towards achieving goal of process

safety. The HAZOP studies have significant bearings on the risk ranking (or risk assigned) to a particular identified hazard leading from process upset or loss of containment. The risk rankings and safeguards available are further analyzed during SIL assessment studies.

Challenge in Present Execution Methodology of H&RA

With the installation of bigger capacities and complex process streams in oil and gas or chemicals plants than before, performing HAZOP studies and managing the design changes necessary to comply with its findings has become increasingly difficult over time. This is placing lots of pressure on performance of such studies and the quality of the HAZOP study may be impacted due to below mentioned factors:

- Scope of the study
- Schedule of the HAZOP
- Ineffective application of HAZOP ground rules
- Competence of personnel involved in HAZOP studies
- Risk perception of the stakeholders
- Process safety culture of the owner organization and / or personal belief of the person towards hazard-operability of a design.
- Execution method of the project
- Improper definition of tolerable risk and risk ranking criteria
- Improper reference of the historical data without consideration of the present design
- Regulatory and reference standards requirement
- Constraints imposed by process licensor, package vendors

As a result of one or more factors above, it is noticed that the HAZOP studies are often marred with incorrect risk ranking on higher or lower side. Ego clashes, endless debates on proving who is right (or wrong), delayed completion of the study, hushing up on the studies for completion due to wasted efforts in endless debates leads to re-performing the studies at times.

Present Execution Methodology vs. Improvised Approach of HAZOP

Effect of each of the above factor is reviewed to see how it influences the outcome of HAZOP and improvised approach.

Scope of Study

Scope is the most important factor to be defined first for the project being subjected to HAZOP review. Improper definition of the battery limits may impact the outcome of the study and lead to errors in design. If the scope boundaries are not clearly agreed, the team may be evaluating the parts of the process not requiring an evaluation or the parts requiring attention can be neglected.
It is also observed many a times that the HAZOP study is turned in to design review meeting. Discussions on the document on how the P&ID is should be corrected; narrative to be updated etc. can easily deviate from the main intent of the HAZOP.

Improvised approach - While scope for a greenfield project can be fairly defined, it can be challenging for a brownfield project HAZOP to limit identification of causes and consequences in

the design section being discussed. Some of the key areas of scope challenge to be overcome in a large and complex HAZOP study are:

- Mismatch in interfaces between different execution entities,
- Design cases for process operations to be considered,
- Providing written terms of the reference for the study to be conducted.

The necessary design reviews, and document reviews and approval should happen before beginning the HAZOP. This will ensure that the HAZOP outcome is to the expected level in finding of the all possible risk scenarios and its hazards.

Schedule of the HAZOP

In a large scale project with multiple units, the HAZOP durations can be very long and exhaustive. This may result into fatigue in the participating personnel due to the repetitiveness of the process.

If the schedule for completion is too compressed, then the personnel would always have pressure to complete without proper discussions of the risk scenarios.
In both the cases, the tendency in such cases is to avoid proper discussions which may result into missing important risk scenarios.

Improvised approach – The schedule of the HAZOP and teams has to be planned in such a manner that the participation remains focussed. Back to back sessions of HAZOP or HAZOP and SIL assessment need to be avoided. There should be realistic calculation of the effort days required for the performance of a HAZOP study. The team study should normally not exceed four to six hours a day. There should be off-day(s) gap when the HAZOP is likely to extend more than two weeks at a stretch. There should be break between the performance of HAZOP and SIL assessment so that a fair review of the recommendations impacting process safeguarding philosophies can be resolved.

Ineffective application of HAZOP ground rules

Ground rules formed for HAZOP study are both technical in nature and for workshop facilitation. In the absence of these ground rules or ineffective application of these ground rules, time allotted for review may be assigned to non-productive or inconsequential tasks. This would result in underrated or overrated risk rankings. Some of the ground rules often leading to such scenario are

- Consideration of each and every manual valves from their position in an operating plant
- Operator's behaviour deviating from plant operating procedures
- Not trusting the actions of interfacing process units
- Meeting conveying / re-conveying not on time after a break
- Other distractions such as use of laptop / mobile phone or near to work desk

Improvised approach – Before beginning of the HAZOP, the terms of reference with ground rules for the study should be mutually agreed between all stakeholders and be enforced by tea leader. During the workshop constant reminders towards ground rules and pace of the study towards timely completion should be highlighted by the team leader.

Competence of personnel involved in HAZOP studies

The competence of the personnel involved in HAZOP studies is an influential factor in the outcome of the HAZOP. As shown in figure 3 above, if the understanding of the risk is not correct, the risk cannot be analyzed properly. This means that the safeguards applied are underrated or overrated.

Improvised approach – It is important that the personnel nominated for participating in HAZOP should make up a team having sufficient background of the design, safety, maintainability and operability of the process under HAZOP. Further, the team should be provided orientation of the process before the HAZOP session begins.

It is often seen that the contractor and owner person nominate same resources in the HAZOP studies of different units on large scale project which are often scheduled one after other. As a minimum, the nominated personnel should have reviewed and understood the documentation such as material safety data sheets, heat and mass balance, process flow diagrams, piping and instrumentation diagrams (P&IDs), control narrative etc. which is usually available for HAZOP studies.

This is true for participants from all engineering disciplines and risk stakeholders such as owner, contractors, licensors and vendors as applicable.

Risk perception of the stakeholders

It is often noticed that the definition of tolerable risk is left open for interpretation. The common notion some participants carry is to always consider the probability of occurrence with a consequence of full magnitude for a given scenario. It is commonly seen that risk is underrated for familiar systems and overrated for complex and unfamiliar systems.

Improvised approach – Before beginning of HAZOP study, there should be documented agreement for the definition of the tolerable risk. Agreements on the tolerable risk, initiating event and its frequencies, maximum credit for safeguards should be defined. These definitions should be within the regulatory requirements and as per the guidance of the owner operating company. Deviations from the agreed conditions should be need based and documented with reasoning for doing so.

Several safety studies such as fire and explosion assessment, environmental assessment etc. are available to understand the presence and/ or the magnitude of a risk. The outcome of the risk values should be based on the design under consideration and should take credit of the applied safeguards.

Process safety culture of the owner organization and / or personal belief of the person towards hazard-operability of a design.

The process safety culture of owner organization indicates its approach and willingness to spend time and money towards identification and mitigation of process risk. For example organizations may choose automated system or stipulate administrative procedures to manage an identified risk

Improvised approach – The approach towards process safety should not be mere for compliance purpose, but should be understood that it helps operate with continued profitability. Major incidences in past has shown how big organizations can lose business, valuation and reputation post a safety incidence impacting human life as well as environment.

Execution method of the project

Depending on the nature of the contract, i.e. who manages and pays for the changes, often there is different behaviour observed from the stakeholders. If the contract is lump sum, then at times it is seen that the perceived risk is pushed towards higher side by owner representatives while contractors would try to defend lower risks. Both of this is not healthy sign for understanding of risk. At times, the behaviour reverses if the owner has to manage and pay for changes. The other aspect is the licensor of the process technology may have pre-conceived concepts of risk based on their standard design. Most of the debate happens when the perceived risk enforced by either of the stakeholder is on lower or higher side.

The way the HAZOP studies are structured segregates the HAZOP based on the contractor engineered scope and their package vendor scope. It often results in incomplete HAZOP done during the contractor engineered scope leaving open items for vendor HAZOP. During vendor HAZOP, all these open items are not reviewed considering that it is not part of this vendor HAZOP scope.

Improvised approach – The contracts between the owner, licensors, contractors and package vendors should be fairly written in order to avoid such scenarios. The focus should be on appropriate definitions of risk so that the plant is designed with optimum safeguarding. The risk rankings should be purely based on the design and operating conditions.

HAZOP of the unit should be looked in totality. Segregating HAZOP studies per engineering scope is incorrect approach. Examples of such instance can be:

- SRU unit where the main SRU unit and the blower vendor HAZOP are performed separately.
- Boiler unit in which the boiler feed water package HAZOP is performed separately.

The HAZOPs are to be scheduled in integrated manner to avoid any possible misses or misinterpretation.

Improper definition of tolerable risk and risk ranking criteria

The tolerable risk definitions should be drawn from the regulatory requirements, reference international standards and the corporate guidelines of the owner company. The stringent of these should be applied. However, before beginning of the process of risk assessment, the values of the tolerable risk and risk ranking criteria should be agreed and documented. The source of the values used and reason for selection of this should be documented.

Improvised approach – There is no change required in the approach on this part and the design should continue to follow the present approach.

Improper reference of the historical data without consideration of the present design

As explained in figure 3, the historical data provides foundation for the risk assessment. However, as is implementation would normally mean that the risk assessment remains improper and incomplete.

Improvised approach – Historical data should be used as a reference only. Actual risk should be evaluated based on the risk for the present design. There might be cases of newer risk induced though improvements from the past design. Varying risk might be due to change in feed, change in the philosophy of spare equipment(s), operation philosophy etc.

Regulatory and reference standards requirement
The regulatory or standards requirements may not cover all the aspects of the specific design of a process. These requirements are often at lag and updated based on findings or learning's from incidences worldwide. When the risk assessment requires a lean design, the regulatory or reference standard recommendations should take precedence. However, the reverse is not true. i.e. if risk assessment requires stringent design against requirements of regulatory or reference standards, the stringent design should be applied.

Improvised approach – There is no change required in the approach on this part and the design should continue to follow the present approach.

Constraints imposed by process licensor, package vendors
It is often noticed that when the risk assessment in the licensor or vendor packages is varying to their previous experience or their standard guidance, the findings are questioned and challenged. The risk rankings are brought up or down to comply with the recommendations without taking into design considerations, sparing philosophy, geographical location of the plant and operation philosophy.

Improvised approach – The representatives from licensor or vendor packages should be made aware of the possibilities of variations to risk ranking. The risk rankings cannot be pre-meditated and should take into consideration the target process and its conditions into consideration for proper assessment of risk.

Management of Change

As project transition from the early design phase to detail engineering, i.e. early identification of hazards and risks to HAZOP on the detail design data, any changes to the considerations of hazards and risks should be thoroughly reviewed. This review should be part of management of change process. Such reviews should be mandatory to establish that the risk levels considered early in the project have been sufficiently addressed either in terms of elimination or minimizing risk.

Consideration in the design based on other studies

Improvising on the performance of HAZOP is one aspect which needs to be reviewed for better assessment of risk. However, it is important to note that the knowledge about operational risk is made available as outcome of the different studies which are performed during the early phase of the project or parallel to HAZOP. These are:

- Fire Consequence Analysis
- Toxic Release Dispersion Analysis
- Explosion Overpressure Risk Assessment

- Environmental Impact Analysis(EIA)
- Quantitative Risk Assessment (QRA)

These studies reveal important parameters for the design of the plant. However, the knowledge captured from these studies is not carried in structured manner in H&RA. The findings of these studies can be applied for improvements in design so that the risk is reduced or mitigated. This means identifying and moderating unrealistic safety constraints early in the design phase when it is still feasible to make significant process and mechanical design changes to lower the risks and, often, the total installed costs.

The studies listed above can provide software based specific calculations or assessment on which scale of the impact from the risk manifestation of a hazard can be gauged. These studies can be conducted at an early stage when process flow diagrams of the process are available. Findings can be used in design to include SIS and non-SIS based layers well in advance.

Assessment of an uncontrolled fire, toxic gas release and explosion provide the heat intensity from a fire, IDLH (Immediately Dangerous to Life or Health) values of a toxic gas release or explosion overpressure damage to life and property both onsite as well as offsite.

EIA provides the environment framework based on which plant operations should manage various emissions both during normal operations and during process upsets. These values are to be kept below the stipulated emissions limits acceptable to the local authorities. Further, the EIA also provides guidance on requirements of containing the spills, management of hazardous waste, protection of water bodies etc. Taking cues from the EIA findings, early design should consider safeguards to limit well within acceptable limits so that consequence of an incident does not push risk ranking to a level where the SIL values are pushed up.

Owner corporate guidelines, codes and local regulations can help to define the threshold of the hazard. For example a fire in a flammable inventory which is either likely to be isolated or not likely to escalate to cause greater life and assets risk should not require to be dwelled upon in HAZOP studies. Further where secondary mitigation measures such as fire protection, drainage, containment, separation distance, area classification etc. are available these should be accounted in the consideration of plant or system safety.

These inputs help in categorization of risk in operation of a process unit which may be applied during hazard assessment study such as HAZOP or SIL assessment [3]. These risk categories, mentioned in table 1, are separated based on the level of consequences related to Health & Safety (H&S), Environment and Asset Loss & Production interruptions.

Level of Consequences (Risk)	H&S	Environment	Assets Loss and Production Interruptions
Low	No or minor Injury	Minor Env Impact with no agency notification or permit violation	Less than USD 100K
Medium	Single Injury possible lost time	Moderate Env Impact with agency notification or permit violation	100K to 1 million
High	One or more severe injuries	Major Environment impact (onsite and offsite)	1 million to 10 million
Very High	Fatality or permanently disabling injury	Serious Environmental Impact with long term effects/ irreversible	More than 10 million

Table 1. Risk Categories

The risk categorized for High and Very High consequence are the subject of mitigation measures so that residual risk is either brought down to acceptable risk or a risk as low as reasonable practicable (ALARP).

Inherent Safety – Can it be really applied?

"Those who want to spend more money to make a plant safer and those who think enough has been spent share a false premise: they both assume more safety will cost more money" – Trevor Kletz [4].

The findings of the many accidents in process industry reveal the loss of containment of hazardous material. The loss of containment can be avoided with better designed equipment and following the standard operating procedures. Both of these are susceptible to failures. The equipment can fail due to parameters such as corrosion even though it is designed for handling the suitable temperature and pressure. There can be lapses in following procedures due to human factor, omission, ignorance etc.

The inherent safety in design concept can be applied by either minimizing, substituting, moderating the use of such hazardous material or simplifying the chemical reaction process.
When feasible, elimination of hazard would be the best proposition rather than managing the risk with the residual hazards. This however is easier said than done.

Suggested Approach for Better Identification of Hazards

It is suggested to have a 3-step framework for identification of hazards.

- In 1st step, hazard identification is carried out at the concept phase of the project. The documents such as preliminary process flow diagrams (PFDs), material flow diagrams, and preliminary plot plan which are typically available during this stage are used to assess risk and provide broad level safeguards in design.
  The intent is to identify potential chemical and process hazards that require general considerations in order to increase level of safety in design and implement adequate safety measures. This step provides an opportunity for eliminating hazards while fundamental changes to the process are still possible and concepts of Inherently Safer Design (ISD) can be applied to reduce risk versus adding an active or procedural protective layer.
- 2nd step hazard identification is performed once the conceptual design is complete and project moves to preliminary or Front-End Engineering. At this stage of the project, risk identification should be much more specific to identify the safeguarding systems which can be applied in a cost effective manner in the next phase of the project.
- 3nd step hazard identification is performed when project documentation such as detail P&IDs, control and safeguarding narrative for the project are available. At this stage precise understanding of the risk is matched with the detailing of the safeguarding functions such as SIF and other means. Any unmitigated risk from hereon can adversely impact project progress or plant operations.

The intent of the 2nd and 3rd steps is to identify specific hazardous events that could occur during operation of the facility caused by a deviation from design intent.

Conclusion

Identification and active consideration of hazards and operability problems at the earliest opportunity in the project lifecycle is required to minimize the risk. This provides the leverage to implement risk mitigating or risk eliminating strategies early in the project and considerably lower costs when it is still possible to influence the design. The later the issues are known, the solutions placed would be for managing the risk than eliminating or minimizing it. This starts providing higher expectations on the SIL of the SIF.

When it comes to matters of process safety, having a proactive approach for design improvements is expected to avoid incidents like Flixborough. The findings from different studies in the early phase of the project should be considered for design improvements.

Principles of inherent safety in design should be thoroughly reviewed and applied to the design to check if the design is adding to the unnecessary risk.

The HAZOP study methodology need to follow a structured approach overcoming the challenges discussed above in the paper. Further, the HAZOP studies should consider covering the realistic risk so that the SIL targets for the SIF are not underrated or overrated.

References

[1] IEC, IEC 61511, Functional Safety of Instrumented Systems for the Process Industry Sector.
[2] Guidelines for Hazard Evaluation Procedures – Center for Chemical Process Safety
[3] Layers of Protection Analysis - CCPS
[4] What Went Wrong – Trevor Kletz

Acknowledgements

We would like to thank P.K. Midha, Control System & Electrical Head of Department, Fluor Daniel India Pvt. Ltd. for his continuous support and motivation in completion of this paper.
We would also like to thank Srinivasa Oruganti, Process Technology Head of Department, Fluor Daniel India Pvt. Ltd. for his continuous support and motivation in completion of this paper.
We would also like to thank Fluor New Delhi senior management for encouraging us to pursue writing of this paper.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Integration of Control Systems: A Focus on Safety

Mark Buchmann
Wood Group Mustang
Email: mark.buchmann@woodplc.com

Abstract

This abstract describes the importance of the design, integration and testing of control systems as a holistic structure in order to ensure process safety and operability.
As a byproduct of today's era of large projects, it is increasingly common in the design and integration of modern control systems that individual components of the control systems are developed independently as standalone elements. This current trend in development focuses less on the integration of the components as a holistic system- including process control, safety logic, packaged equipment control, and operator interactions. These components, though having independent primary functions, must synchronize harmoniously to operate a facility with reliability and safety. The downside of independent testing is that while the shutdown functions of a safety system might be adequately checked, the interaction with the process control system could cause unforeseen results, leading to the inability to start up a process unit in an acceptable timeframe or even at all.

Robust and standardized integrated testing of all components of a control system provides greater confidence in identifying potential operational or safety issues that could arise at commissioning or during operation, while allowing time to remedy with proper review and testing. Additionally, utilization of a process model or simulation can help to further strengthen confidence in the holistic system by simulating field devices to test logic in situ. Furthermore, this combined control system and process model can provide a higher level of operator training.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Changes in IEC 61511 2nd Edition

Paul Gruhn, P.E., CFSE
Global Functional Safety Consultant
aeSolutions, Houston, Texas, USA
Email: Paul.Gruhn@aesolns.com

Abstract

The ISA (International Society of Automation) 84 standard ("Application of Safety Instrumented Systems for the Process Industries") was first released in 1996. During the time of the development of ISA 84, the IEC (International Electrotechnical Commission) was working on the 61511 standard ("Functional Safety: Safety Instrumented Systems for the Process Industry Sector"). IEC 61511 was first released in 2003. ISA adopted the 61511 standard, with one additional clause, as ISA 84-2004. The IEC released a second edition of 61511 in 2016, followed shortly thereafter with a corrigendum (list of corrections) and an amendment that were finalized in 2017. The ISA 84 committee voted to accept the revised standard without modifications, and released it in mid-2018 as ISA 61511-2018. This presentation will summarize the changes in the new standard.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

The Importance of Properly Determining Consequences of Process Safety Incidents

Rhonda Schmidt
Phillips 66
Email: Rhonda.A.Schmidt@p66.com

Abstract

The purpose of this presentation is to communicate the importance of properly and consistently determining the consequence of potential process safety incidents. There are different methods to determine consequences such as dispersion modeling and industry data/experience and various process data needs to be factored such as pressures, temperatures, and proximity to workers and the community. Understanding the right consequence is critical in determining the risk of a scenario. Since the combination of consequence and likelihood are the factors for determining risk, consequence must be understood in order to understand and appropriately mitigate risk. The greater the consequence, it is likely that a more robust safeguarding scheme will need to be deployed in order to reduce the likelihood (and thus the risk) of the outcome from occurring. Further, key process owners must be aware of the pertinent safeguard schemes so they can manage and be assured that they are protected against the consequence of interest.

The presentation will focus on the importance of determining the right consequence, methods of doing so, and the implementation of the pertinent safeguard schemes commensurate with the consequence determination.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

PHA Guidance for Correlating H_2S Concentrations in Process Streams to Severity of Adverse Health Outcomes in the Event of a Leak

Anne Bertelsmann, P.E., Ph.D., *Marathon Petroleum Company LP*
Greg Knight, *ABSG Consulting Inc.*
Asheesh Tiwary, Ph.D., *Marathon Petroleum Company LP*
Austin Calico, *Marathon Petroleum Company LP*
Email: ABertelsmann@MarathonPetroleum.com

Keywords: PHA, Dispersion Modeling, Vaporization, Consequences, Health Hazards, Hydrogen Sulfide (H_2S)

Abstract

Process hazard analysis (PHA) teams are responsible for determining and categorizing the potential impact of a loss of containment. For streams containing hydrogen sulfide (H_2S), the health and safety consequences of a worker being exposed to H_2S are a function of airborne concentration in the breathing zone and duration of exposure. PHA teams often do not have the technical knowledge to link the known concentration of H_2S in the process stream to an adverse health outcome. This paper describes the methodology and the assumptions made in developing such guidance. H_2S concentration in the stream was correlated to concentration of H_2S in the breathing zone. Vapor releases used dispersion modeling, while liquid releases required additional modeling to determine the amount of H_2S liberated from the released liquid. Modeling was done on different process streams under a variety of conditions. Concentration in the breathing zone was linked to the most probable health and safety outcome by surveying relevant literature published by private and government sources. This correlated the stream concentration of H_2S directly to the consequence categorization used in the PHA. Results were summarized, providing simplified guidance that is valid over a wide range of process conditions and release scenarios.

1 Introduction

During a Process Hazard Analysis (PHA) or during incident investigations, teams need to rank the potential adverse health and safety outcomes based on a company's severity scale. This requires multiple steps – first, it needs to be established what the consequence would be; secondly, how it would affect any personnel in the area; and finally, how these effects would be classified per the company's risk standard. For hydrogen sulfide (H_2S) releases, teams would first need to predict the concentration in the area where personnel are located to determine the potential exposure and then define the effect on a person. That requires knowledge in dispersion modeling and toxicity of H_2S. This is typically beyond the skill level of a PHA team, thus leaving the team guessing with regards to severity. To achieve comparable risk rankings, it is important that the appropriate severity is determined consistently by different teams.

For risk ranking, the consequence should be based on the most probable worst-case outcome, not the worst possible. When consequences are overrated with regards to severity, it takes attention and resources away from the truly high severity cases. For H_2S, the hazards of exposure are emphasized in the safety training for anyone working in a refinery environment and there are many well publicized cases of past fatalities. This can lead teams to overestimate the consequences of H_2S exposure if there are no clear guidelines or data available to help them in their evaluation.

For a <u>qualitative</u> risk analysis, teams can compensate for overstating the severity by understating the frequency – based on the experience that the (overstated) consequence has never been observed. It does not matter for the overall <u>qualitative</u> risk ranking whether the consequence has not occurred because the failure never happened or because the failure did happen but was not nearly as severe as assumed. But when doing a <u>quantitative</u> risk analysis (for example LOPA or QRA), the frequency of the consequence is no longer selected by the team – but rather it is calculated from the probability of the event and the probability of failure of the safeguards. In this case, overstating the severity will result in overstating the risk. Selecting a realistic and most probable worst-case severity is now critical for a consistent risk ranking.

Marathon Petroleum Company, LP (MPC) with support from ABSG Consulting has performed a generalized analysis for predicting H_2S exposure and has developed guidance for use by risk assessment teams in estimating the probable worst-case severity for exposure in the case of leaks from process equipment containing H_2S. The following sections detail the methodology and the assumptions that were used to develop the guidance and show the conclusions that were reached based on the analysis.

2 Overview

To develop generalized guidance for the severity of H_2S leaks that is applicable for a wide range of process conditions, dispersion modeling was performed for liquid and vapor streams with a wide range of pressures and H_2S concentrations. Process conditions were varied between model runs, while other dispersion model parameters used constant values, representing typical conditions. The modeling provided the H_2S concentration in the air as a function of distance from the leak source for a variety of stream conditions. By selecting a representative distance, this function of distance is reduced to a single value thereby resulting in a direct correlation between stream conditions and H_2S concentration in the breathing zone of a person (right side in Figure 2-1)

A review of available toxicology data coupled with an assumption for the duration of the exposure linked the concentration of H_2S in the breathing zone to health effects for an exposed person. These health effects were then classified according to the severity definitions per the company's risk standard. This provided a correlation between exposure and the severity classification (left side in Figure 2-1).

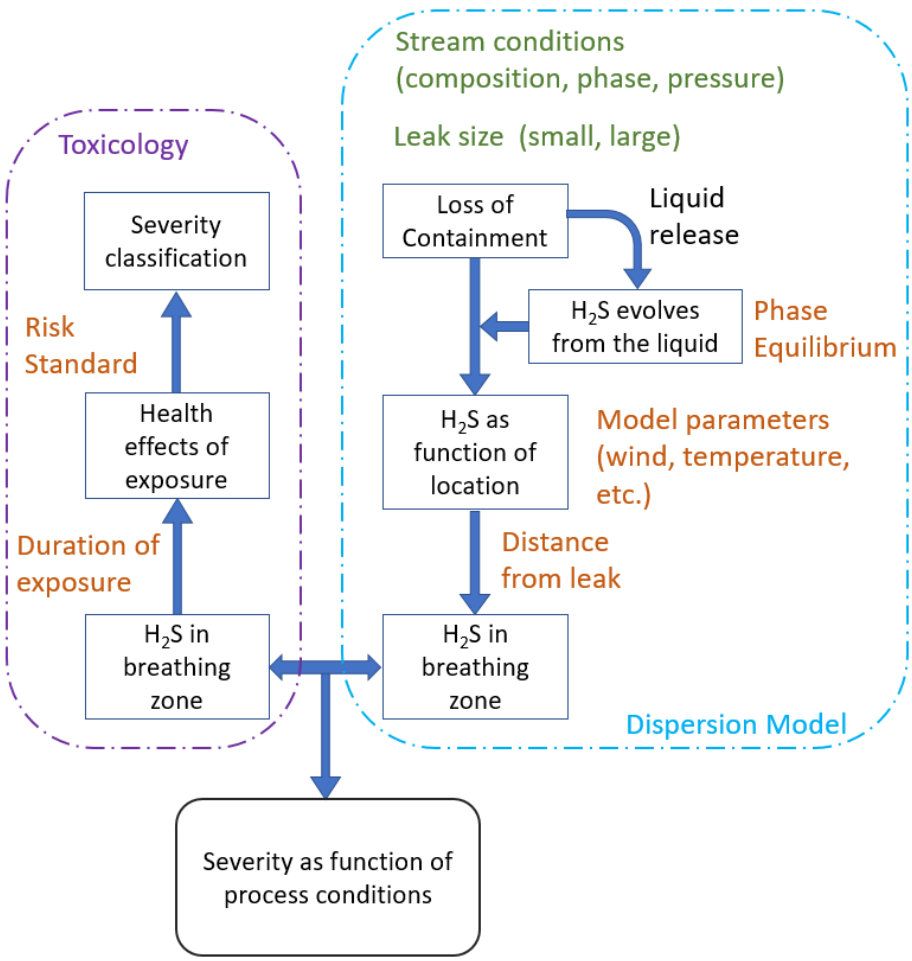


Figure 2-1. Correlating Dispersion Modeling and Toxicology

Combining the dispersion modeling with the toxicology review then allows to directly correlate the stream conditions of the leak with the severity outcome. Figure 2-1 shows an overview of the methodology. Green text in Figure 2-1 indicates inputs to the analysis that were varied. Orange text indicates inputs for which representative values were selected and then kept constant. The steps shown in Figure 2-1 are discussed in detail in the following sections.

3 H_2S Release from Liquid Phase Leaks

The H_2S concentration in the vapor phase of a release depends on two factors:

1. How much of the material vaporizes upon release; and
2. How the H_2S partitions into the vapor and liquid phases.

In answering these questions, the released material was broken into categories:

A. Hydrocarbons containing H_2S;
B. Sour Water (contains H_2S); and
C. Rich Amine (contains H_2S).

The fraction of a hydrocarbon that vaporizes upon release depends on several factors including its temperature, pressure, and bubble point. A stream's bubble point pressure relative to atmospheric pressure seems to have the largest effect on how much will vaporize: cold crude may vaporize very little, while hot naphtha may vaporize almost entirely.

Several streams around Crude Units, Hydroprocessing Units, FCCU, and Coking units were studied, specifically looking at streams that contain H_2S. Hysys, using the Peng-Robinson Equation of state, was used for modeling the phase equilibrium. For many of these streams, about 45% of the hydrocarbon vaporized, to where it is a useful approximation.

These same streams were studied to determine how the H_2S partitioned. H_2S is a vapor at standard conditions, so it was not surprising that about 98% of the H_2S was vaporized, with 2% remaining in the liquid phase. As a simplification, it was assumed that 100% of the hydrocarbon stream's H_2S is vaporized, which only minimally increases the H_2S concentration in the vapor phase as compared to a 98% vaporization rate.

The same analysis was conducted for sour water. Under most circumstances, the only vapor generated by the release was H_2S, and almost 100% of the H_2S evolved. As a simplification, the PHA team should assume that 100% of the sour water stream's H_2S is vaporized and that the generated vapor is 100% H_2S.

This analysis was also conducted for rich amine. Rich amine binds much of the H_2S, preventing much of it from vaporizing. In the event of a rich amine release, 3% of the amine vaporizes, with 35% of the H_2S vaporizing.

The hydrocarbon results were used as the basis for the dispersion modeling. The lower H_2S release from amine was not considered during the remaining modeling. This can result in overstating the severity of rich amine leaks, which was accepted for the sake of simplicity.

4 Dispersion Modeling

Dispersion modeling was performed to determine the H_2S concentrations to which a person may be exposed. The modeling was performed using PHAST (1) software along with spreadsheets and the data manipulation and extraction was performed using FACET3D (2) software.

In the analysis some parameters were fixed constants for all cases and some were variable to capture the range of conditions seen in the field. The below parameters were held constant for all cases in PHAST.

- 5 mph wind speed
- D stability level
- 68 °F ambient temperature
- 70% relative humidity
- 500 W/m^2 thermal flux
- 1 m surface roughness
- Horizontal (non-impinged) release direction
- 3.28 ft release height
- 100 °F stream temperature for vapor cases
- 200 °F flashed vapor temperature for liquid cases
- Instantaneous (Flammable = 18.75 sec) averaging time used when determining downwind concentrations

Parameters which were varied included the stream phase (liquid or vapor), H_2S concentration in the stream, leak size, and pressure as shown below.

- **Stream phase:** liquid or vapor; liquid streams used N-Hexane and H_2S while the vapor streams used Ethane and H_2S
- **H_2S concentration in the stream:** 25, 50, 100, 250, 500, 1000, 2000, 5000, and 50000 ppm
- **Leak size:** small leaks (0.5 inch) and large leaks (2 inch)
- **Pressure:** low (100 psig), medium (300 psig) and high (500 psig)

Vapor Releases

Vapor releases were straightforward and did not require any post processing other than extracting the H_2S concentration. Mixtures of H_2S and Ethane were used in PHAST *Vessel or Pipe Source* models with the *leak* scenario type. The PHAST case list feature was used to build cases with varying parameters. The H_2S component was tracked explicitly. Results of the dispersion were imported into FACET3D and a script was used to extract the centerline concentration at 3 ft downrange of the release. An example of the H_2S cloud and the extracted centerline concentration is shown below in *Figure **4-1***.

A distance of 3 ft from the leak was selected to represent the location of a person working on the equipment where the leak occurs (approximately an arm's length plus a wrench's length away). Personnel not working on the equipment, but just passing through the area would likely have a greater distance and thus lower exposure.

Liquid Releases

The expected H_2S evolution from liquid releases was described above in Section 4. Using those rules, the liquid release modeling in PHAST had the following approach.

1. Determine the liquid discharge rate for the given pressure and leak size.
    a. An artificially low temperature of 100° F was used such that no flashing occurred in the orifice, maximizing the liquid discharge rate.
    b. The releases used the same PHAST source models as the vapor cases but with mixtures of H_2S and N-Hexane.
2. Assume 45% of the hydrocarbon discharge mass turns to vapor and 100% of the H_2S discharge mass turns to vapor.
3. Create a user defined release in PHAST of just the flashed hydrocarbon and H_2S vapor. Use the same discharge expanded velocity as the liquid release. Use an expanded temperature of 200 °F (minimum to keep the N-Hexane a vapor for all cases). Use a new mixture of N-Hexane and H_2S which accounts for the higher H_2S percentage in the flashed vapor (since 100% of H_2S flashed but only 45% of the hydrocarbon flashed). In general, this vapor mixture had 2.2 times the H_2S ppm as the original case description.

Therefore, the final liquid release was modeled as an equivalent vapor release of H_2S and N-Hexane which represented the flashed hydrocarbons. The dispersion modeling of the equivalent vapor release was performed in the same manner as the pure vapor releases.

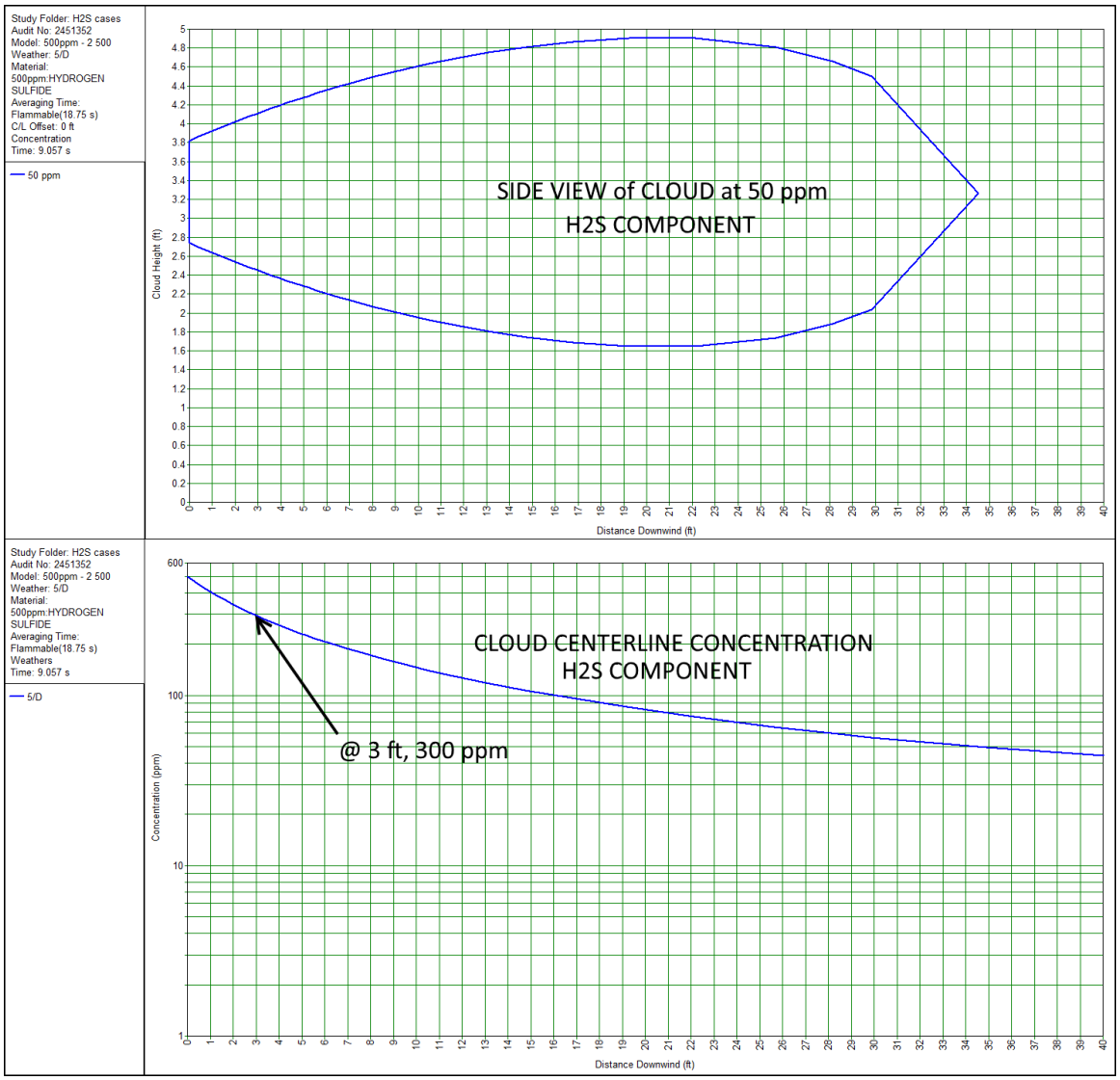


Figure 4-1. Vapor Release for 2" Leak and 500 psig with 500 ppm H_2S in Stream

Dispersion Results

Because of the large discharge rates seen in the liquid cases, a larger volume of vapor (H_2S + hydrocarbon) was released compared to the pure vapor cases. The liquid cases evolved 18% to 42% more vapor depending on pressure. Further, due to the higher concentration of H_2S in the flashed vapor from liquid cases (since only 45% of hydrocarbon flashed), the resulting H_2S concentrations downrange were 21% - 44% higher than equivalent pure vapor cases depending on pressure (higher pressures gave higher H_2S concentrations for liquid vs. vapor releases).

A comparison of the exposed H_2S concentration vs. the stream H_2S concentration is shown below in *Figure **4-2***. The following observations are made:

1. The exposed concentration can exceed the stream concentration for the liquid cases since the H_2S evolves at a higher rate than the hydrocarbon. This is analogous to a distillation

tower which produces a higher fraction of one mixture component at the top compared to the mixture entering the tower.

2. The vapor releases show increasing exposure concentrations with stream pressure while the liquid releases do not. The vapor releases had H_2S concentrations immediately downstream of the orifice (<1 ft) which were lower than the mixture H_2S concentration. This effect was larger for lower discharge rate releases. The liquid releases more closely matched the mixture H_2S concentration at all discharge rates immediately downstream of the orifice. It appears the high velocity vapor releases entrain more air which influences the initial downstream concentrations.

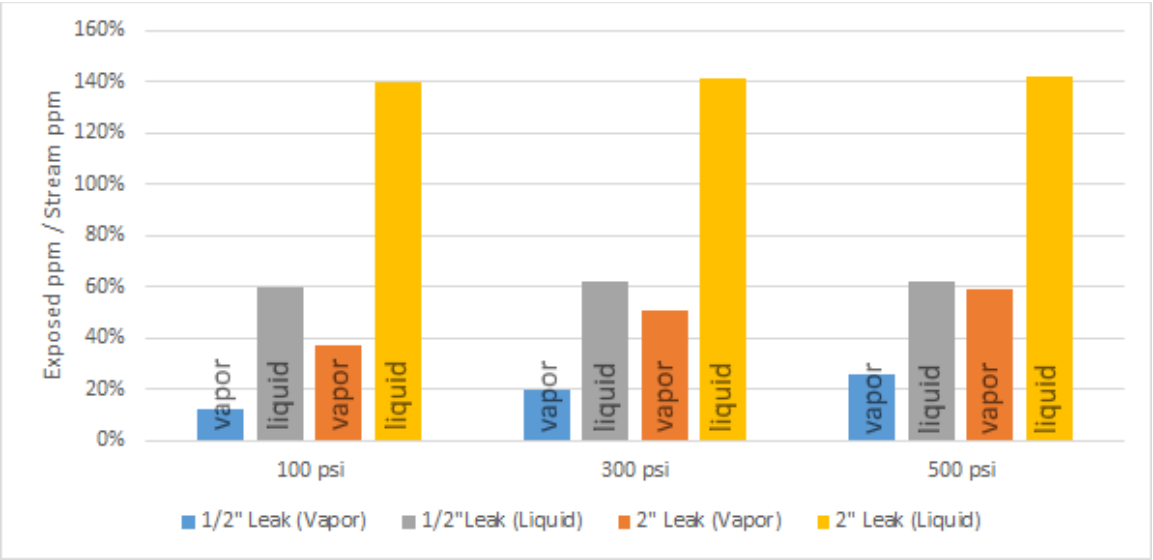


Figure 4-2. Exposed vs. Stream H_2S Concentration

5 Health and Safety Effects of Exposure

Hydrogen Sulfide (H_2S) is a colorless, flammable gas with a strong, irritating rotten-egg odor. H_2S is detectable by odor at concentrations significantly lower than those necessary to cause physical harm or impairment. The physiological effects of airborne toxic materials depend on the concentration of the toxic vapor in the air being inhaled, and the length of time an individual is exposed to this concentration. The most serious hazard presented by H_2S is exposure to a large release from which escape is impacted.

Occupational exposure to hydrogen sulfide is frequently encountered in various industries where H_2S may be released to the environment as part of the manufacturing/ treatment process. Some of these industries include natural gas production, municipal sewage pumping and treatment plants, landfilling, swine containment and manure handling, pulp and paper production, construction in wetlands, asphalt roofing, pelt processing, animal slaughter facilities, tanneries, petroleum refining, petrochemical synthesis, coke production plants, viscose rayon manufacture, sulfur production, iron smelting, and food processing.

H_2S and its metabolites are not long-lived in the tissues of exposed animals, indicating that longer-term exposures to low levels may not be as important as short-term peak events. H_2S is not considered a cumulative toxin since it is rapidly oxidized to sulfate, which is readily excreted in urine.

5.1 Animal data (short-term effects)

Results from animal inhalation studies indicate that H_2S is widely distributed in the body, primarily to the brain, liver, kidney, pancreas, and small intestine (3).

Effect Level mg/m^3 (ppm)	**NOEL mg/m^3 (ppm)**	**Duration of exposure**	**Effects**
35 (25)		Repeated, 3 h/day	Cumulative change in hippocampal type 1 EEG activity in rat
42 (30)	14 (10)	Once for 3 hours	Cytochrome oxidase inhibition in the lung
≥ 70 (≥ 50)	14 (10)	4 h	Inhibition of cytochrome oxidase in rat lung cells
100 (72)		1.5 h/day several	Various cardiac arrhythmias including ventricular extrasystoles in rabbits and guinea pigs
140 (100)		2 h, 4-day intervals, 4 times	Increasing inhibition of cerebral cytochrome oxidase activity and decreased protein synthesis in mouse brain
140 (100)		3 h/day, 5 days	Increased level of L-glutamate in hippocampus of rats
280 (200)		4 h	Detectable histologic lesions in nasal epithelium of rats
280 (200)		4 h	Increase in protein and lactate dehydrogenase in lavage fluids from rat lung
280-560 (200-400)	70 (50)	4 h	Particle-induced oxygen consumption reduced in pulmonary alveolar macrophages from rats
420 (300)		4 h	Marked abnormality in surfactant activity in lavage fluids from rat lungs
560 (400)		4 h	Transient increase in protein concentration and activity of lactate dehydrogenase in nasal lavage fluids or rats
615 (439)		4 h	Transient necrosis and exfoliation of nasal respiratory and olfactory mucosal cells in rat. Reversible pulmonary edema

Table 5-1: Summary of short-term non-lethal studies with H_2S (4)

5.2 Human data (short-term effects)

Separation of effects in humans due to odor nuisance vs. physiological effects is often difficult. Furthermore, most human studies lack the detailed exposure data to derive clear health hazard thresholds.

Effect level mg/m^3 (ppm)	**NOEL mg/m^3 (ppm)**	**Effects**
0.028 (0.02)		Minimum perception threshold
0.18 (0.13)		Generally accepted smell threshold
2.8 (2)		Non-significant effects in asthmatic subjects (exposure for 30 min)
4.2-7 (3-5)		Offensive smell
7 (5)	2.8 (2)	Increased muscle lactate levels during exercise (exposure > 16 min) and increased oxygen uptake
14 (10)		Exposure for 15 minutes did not alter the pulmonary function significantly.
14 (10)		Reduced oxygen uptake during exercise (exposure two times 30 minutes)
> 140 (>100)		No smell due to olfactory fatigue
700-1400 (500-1000)		Stimulation of carotid bodies
1400-2800 (1000-2000)		Paralysis of respiratory center and breathing stops

Table 5 -2: Summary of short-term human studies with H_2S (4)

6 Severity Correlation

The health effects of H_2S exposure detailed in the previous section needs to be related to the severity definitions used in a company's risk standard. For this paper, the severity definitions of "None" through "S4" shown in Table 6-1 were used.

The health effects depend on the duration of the H_2S exposure – longer exposure leads to more severe effects. For the purposes of the severity correlation, a maximum exposure time of five minutes was used. The value was selected based on the assumption that an exposed person would immediately be alerted to the exposure through their personal H_2S monitor and quickly evacuate upwind or crosswind once the monitor alarms. Five minutes provides sufficient time for egress even from spaces with limited accessibility.

Table 6-1 lists the severity categories and their definitions used in this paper, as well as the health effects from exposure that correspond to the severity definition and the H_2S concentration that would cause these effects.

Severity Category	**Health and Safety Impact Description**	**Effects of up to 5 min H_2S Exposure**	**Range of H_2S in breathing zone**
Very low / None	No health and safety consequence –	Up to Occupational Exposure Limit (OEL)	0 – 10 ppm
Low (S1)	First aid case	Up to Peak Exposure Limit (PEL); Below US EPA's 10-min AEGL of 76 ppm; Below AIHA's 1-hr ERPG-3 of 100 ppm	> 10 ppm to 50 ppm
Moderate (S2)	OSHA recordable incident with no lost time or hospitalization	Loss of smell, irritation of respiratory tract and eyes; Up to IADC's 300 ppm for 5 min survivability criteria	> 50 ppm to 300 ppm
High (S3)	Injury resulting in lost time, hospitalization or permanent disability	Difficulty breathing, serious eye damage and severe lung irritation	> 300 ppm to 700 ppm
Very High (S4)	Fatality	Rapid unconsciousness, collapse, potentially fatal within minutes due to respiratory paralysis; Threshold of human lethal effect for 10 min exposure (SPEL)	> 700 ppm

Table 6 -1: Severity Categories

It is important to keep in mind that this categorization is based on observed effects of exposure and represents a probable worst-case outcome – and not on the worst possible case or an exposure limit. The severity rating is for hazard evaluation purposes only and is not intended to indicate acceptable or safe levels of exposure.

If a company defines the severity levels differently than presented here, the correlation with the health effects and the corresponding H_2S concentration will need to be adjusted from what is listed in Table 6-1.

7 Summarizing the Modeling Results

Each severity category covers a range of H_2S exposure concentrations. This makes it possible to generalize the results from the modeling because variations in some of the parameters will not cause a significant shift between categories. A sensitivity analysis can indicate which parameters have the most significant effect on the predicted H_2S exposure and thus the Health and Safety consequences.

Based on the modeling, it was found that the H_2S concentration in the breathing zone mainly depends on the size of the leak; smaller leaks will result in a lower H_2S concentration at 3 feet from the leak. Also, vapor releases result in lower H_2S concentration in the breathing zone than liquid releases with the same H_2S stream concentration, since the non-H_2S components in the vapor release dilute the H_2S concentration in the air. Dependence on pressure was found to be insignificant for liquid releases.

As described in the previous sections, there are many parameters that can affect the analysis, many of which were assumed as constant. For guidance to a PHA team, the results of the analysis need to be simplified and summarized in terms of data that are most readily available to the team. These are generally the conditions of the process stream (available from the material balance for the unit) and the size of the leak. Of these parameters, the H_2S concentration in the stream, the leak size (small or large) and the phase of the stream (vapor or liquid) have the most significant impact on the severity outcome.

Combining the dispersion modeling results (Section 4) with the severity correlation for breathing air concentrations (Table 6-1) provides a correlation between the release conditions and the health and safety outcome. The following table summarizes the predicted severity outcome for a range of process conditions and leak sizes.

Phase and Leak Size	H2S Concentration in Stream							
	25ppm	50ppm	100ppm	250ppm	500ppm	1000ppm	2000ppm	5000ppm
Small Vapor Leak	**None**	**S1**	**S1**	**S2**	**S2**	**S2**	**S3**	**S4**
Large Vapor Leak	**S1**	**S1**	**S2**	**S2**	**S2**	**S3**	**S4**	**S4**
Small Liquid Leak	**S1**	**S1**	**S2**	**S2**	**S2**	**S3**	**S4**	**S4**
Large Liquid Leak	**S1**	**S2**	**S2**	**S3**	**S3**	**S4**	**S4**	**S4**

Table 7-1: Severity Table based on H_2S Concentration, Leak Size and Phase of Process Stream

If desired, the guidance can be further simplified by using worst case assumption for the leak size and phase, resulting in a simple table that only requires the H_2S concentration in the stream as input.

H_2S Concentration in the Stream	Health and Safety Consequence	Severity
≤ 10 ppm	No consequence	None
> 10 ppm and ≤ 50 ppm	First aid case	S1
> 50 ppm and ≤ 250 ppm	OSHA recordable	S2
> 250 ppm and ≤ 1000 ppm	Injury with restricted duty, lost time or hospitalization	S3
> 1000 ppm	Fatality	S4

Table 7-2: Simplified Severity Table Based Only on H_2S Concentration in the Stream

The simplified severity guidance given in Table 7-2 overstates the severities for small vapor leaks, but results in a simplified correlation for PHA teams that is easy to use. This table can be used as a starting point for the severity estimation. Teams may choose to use the more detailed Table 7-1 if they are concerned that the severity may be overstated or does not match what has been observed in the past, especially if the release comes from a small vapor leak.

8 Conclusions

It is not surprising that estimating the severity of the health and safety consequences of a potential H_2S release is difficult for PHA teams. The analysis presented in this paper shows the numerous parameters, assumptions, modeling, and toxicity information that is required for this type of estimation. However, by making conservative, but reasonable assumptions for most of these parameters, a generalized correlation between H_2S concentration in the process stream and the severity of the health and safety effects has been developed.

The generalized correlation provides guidance to PHA teams that is easy to use because it is only based on information that is readily available to them. It helps drive consistency in the severity estimation. PHA teams are often “out of their depth” when estimating consequences and are generally appreciative of clear guidance.

The development of the guidance tables shown in section 7 required multiple assumptions and is based on a specific risk matrix. The values in this table cannot be simply copied from one company to another but will need to be reviewed and adjusted to match each company’s risk standard.

9 References

1. *DNV GL, "PHAST," 2011.*

2. *ABSG Consulting Inc., "FACET3D," 2018.*

3. Sullivan and Krieger, 1992.

4. SCOEL. 2007.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Evaluating the Transient Radiant Heat Flux Impacts to Occupied Buildings

Jeffrey D. Marx and Benjamin R. Ishii
Quest Consultants Inc.
James W. Wesevich, Matthew Gomez, and Andrew Staszak
Thornton Tomasetti, Weidlinger Applied Science Practice
Emails: jwesevich@ThorntonTomasetti.com, mgomez@thorntontomasetti.com, astaszak@ThorntonTomasetti.com, jdm@questconsult.com, bri@questconsult.com

Keywords: facility siting, safety studies, consequence analysis

Abstract

Traditional methods of evaluating radiant heat impacts on occupied buildings typically rely on a threshold radiant heat flux value to evaluate occupant vulnerability. While this is acceptable within the methodology of fire hazard evaluation presented in the API RP 752 standard, the approach does not account for structure properties, the transient nature of the fire, or duration of exposure. These factors are an important part of describing the potential impact on occupied buildings, as well as the vulnerability of the building's occupants. Because API RP 752 does not provide any specific guidance on these topics, the specific evaluation of a building and its response to thermal radiation is left to the analyst. Previous work applied first principle numerical tools to define the impacts from continuous external fires. This paper continues that work to evaluate transient thermal loading on the building exterior and heat transfer through the building materials to better determine building occupant vulnerability. This work will help to define the limits of radiant heat dose for occupied buildings that may be exposed to external fires.

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 is specifically addressed towards exposure to fire radiation from continuous fires whose radiant impact changes over time (a transient heat flux).

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.

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

Of these fire types, jet fires and pool fires are typically the dominant types considered as a threat within a building siting study. Buildings within a vapor cloud fire are typically not exposed long enough to ignite the building, even if it is constructed of flammable materials. Fireballs, in addition to their short duration, are historically rare events and are typically not considered a credible threat to occupied buildings. It is the long duration jet and pool fires that pose a threat to buildings through flame contact or high levels of thermal radiation.

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 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.

The exposure of occupied buildings to high levels of fire radiation, such that it could adversely affect the building occupants, is the focus of this analysis, including the complex techniques required to evaluate building impacts due to fire radiation, such that the impacts to occupants can be evaluated. The precursor to this work[7] began addressing the issue of radiative loading to occupied buildings by evaluating a section of a typical pre-engineered metal building (PEMB) during external thermal radiation loading with durations up to an hour. The findings of that work included:

- Steady-state conditions were observed in the structural steel within about 10 minutes for the scenarios modeled.
- Insulated PEMBs may suffer damage to the exterior panels, but are not expected to experience any structural degradation under long-duration exposure to radiant loading up to 100 kW/m^2.
- Uninsulated PEMBs exposed to radiant heat fluxes greater than 35 kW/m^2 may experience a loss of structural integrity within about 5 minutes of exposure, such that building occupants could be threatened.
- Structural members in uninsulated PEMBs can reach temperatures that may be capable of igniting flammable materials in the interior of a building.

CONTINUING STUDY

To further evaluate the potential impacts to PEMBs, and thus the vulnerability of building occupants, this work sought to further investigate the potential impacts of transient heat flux loadings on a subject building.

Accidental Fire Loading

In order to study transient heat flux loadings, a dynamic system that is often found in process facilities was modeled to better represent realistic plant hazards. For this reason the modeling package CANARY by Quest® was used to calculate the transient release rate and the transient release conditions accounting for the thermodynamics of the releasing system. In addition, CANARY by Quest® was used to model the thermal radiation from transient jet fires.

The characteristic jet fires were modeled based on a release from a propane storage vessel. The vessel is used to store propane as a liquid, at atmospheric temperature and elevated pressure.

A two-inch hole is assumed to occur in the piping connected to the liquid side of the storage vessel. Within seconds, the release is ignited and forms a jet fire. The release flow rate drops quickly in the first two minutes as the system depressurizes. The rate continues to drop and at 28 minutes the flow rate reaches a value that is half of the initial flow rate. As the flow rate and pressure drop the jet fire shrinks in size, and the thermal radiation impacts shrink accordingly.

Figure 1 shows the thermal radiation at four separate points near the jet fire. The position of these four points are static relative to the release point (storage vessel). Not all points near the jet fire experience the same reduction in thermal radiation as the flame shrinks. As the jet fire shrinks the reduction in length is greater than the reduction in diameter or lateral dimensions. Thus, the points near the end of the initial flame will experience a larger drop in radiation than near the source of the jet fire.

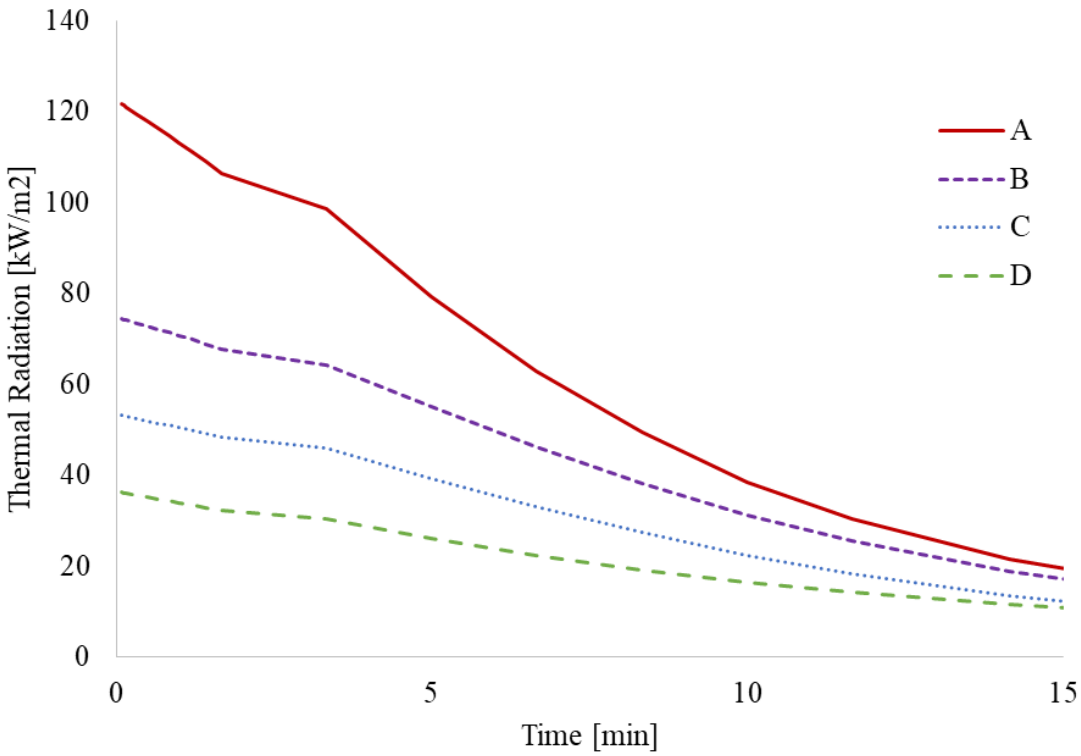


Figure 1. Transient Radiation Load Cases A-D

Complex Analysis

The potential impacts from fire radiation described above were investigated using the numerical heat transfer tools contained in a finite element analysis (FEA) model. Based on the FEA results, the temperature rise in construction materials exposed to an external fire can be estimated. Resulting temperatures can be used to determine the potential for ignition of construction materials, integrity loss of exterior construction elements, and integrity loss of the main structural framing members.

The performance of a typical PEMB exposed to transient thermal radiation loading external to the building is evaluated in this study. In the scope of this paper it is assumed that the fire event happens outside the building, exposing the building wall to a heat flux. The vertical cladding of such buildings would typically be constructed of exterior corrugated metal panels screwed to horizontal girts that span approximately 20 feet between columns. Depending on the building, insulation may be installed between panels and the building frame. This analysis will address both insulated and uninsulated structures, and it is assumed that a large portion of the exterior surface of the building wall is exposed to these heat fluxes.

Calculation Methodology

Heat flux from the fire flows from outside to inside the building wall. Due to the high temperature of the flame, radiation dominates the heat flow from the fire to the exterior surface facing the fire. Re-radiation of the exterior surfaces is also considered. External convective effects are ignored for this analysis due to the dominance of radiative heat transfer. At the exposed surface, heat is transferred through the solids by conduction. The interior surfaces, not exposed directly to fire radiation, release heat through radiation and convection to the surrounding interior air at low temperature (initially at ambient temperature). The air medium inside and outside the PEMB cladded wall are not explicitly modeled in the FEA.

To model heat radiation, for each radiative heat flux scenario, the methodology presented in the predecessor paper (reference 7) was applied. In each case, the equivalent incident thermal radiation equal to the values presented in Figure 1, varying with time, were applied to the external surface.

Conduction of heat through the solid body of the wall (construction material) results in a temperature change of the wall. The conduction equation is used within the FEA software to calculate the temperature change, where conduction depends on the specific heat, density, and most importantly, thermal conductivity, of the materials in the wall structure.

Once the temperature of the interior surface of the PEMB wall rises above its initial temperature, heat flows to the interior space through radiation and convection. Depending on how hot the wall materials get, internal heat flux may be dominated by radiation or convection. Since the air inside and outside the PEMB wall are not explicitly modeled, an assumption for the building internal temperature must be made, as well as emissivity of the internal surface and convection coefficient of the inside air.

Calculation Model

The PEMB wall considered in this study includes 26 gauge vertical spanning metal R-panels (structural panels used primarily for PEMBs roof and wall construction) screwed to horizontal 8x25z16 girts at 4 feet on center vertically. For the purpose of this paper, only a 2-foot by 4-foot area of the wall is modeled. Wall insulation is also modeled and it is assumed that the compressed thickness of the insulation at the girt location is ¾ inch, and elsewhere is a full 3 inches. It is assumed that the panel is screwed to the girt with #10 screws at every foot, and the equivalent area of the screws are included in the model. The Abaqus FEA software[8] was used to perform the

heat transfer analysis. Geometry of the model is shown in Figure 2. More specifically, 8-node linear heat transfer brick elements are used to mesh the geometry.

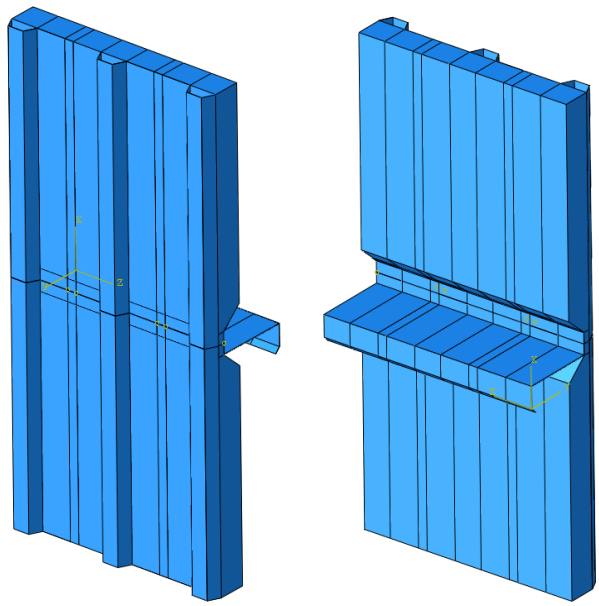


Figure 2. Geometry of the Modeled Portion of the PEMB Wall (Exterior and Interior, with Insulation)

Based on several manufacturers' available data, an R-value of R-10 was used for the 3-inch thick insulation. Squeezed insulation at the girt location is assumed to have R-value of R-5. Temperature dependent thermal material properties are used based on Eurocode 4[9] specifications. For all heat flux scenarios, the exterior face of the wall panel was exposed to heat flux for a duration of greater than 15 minutes according to the transient heat flux curves presented in Figure 1.

Overall, 5 different cases are defined. One case is a wall structure with insulation exposed to thermal load A at the exterior surface, and exposed to 25°C room temperature at the interior surface. Four other cases include a wall structure *without* insulation exposed to thermal loads A-D at the exterior surface, and exposed to 25°C room temperature at the interior surface.

STUDY RESULTS

The results of the simulations show the transient temperature variation in the modeled portion of the wall exposed to a range of transient heat fluxes. The results of an insulated wall exposed to thermal load A is shown in Figure 3. For comparison, a wall without any insulation with exposure to 50 kW/m^2 after 2 hours is shown in Figure 4. The uninsulated wall shows considerably higher girt flange temperatures.

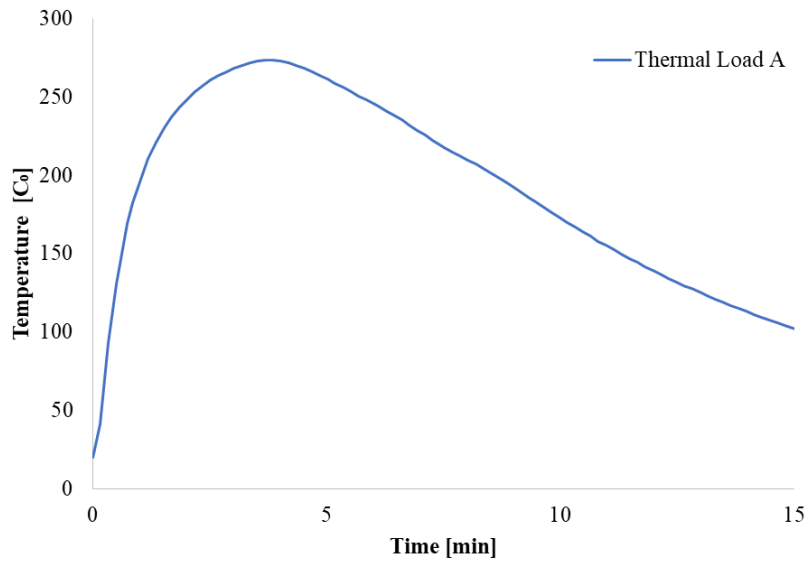


Figure 3. Temperature Variation at the Hottest Point of the Girt for a PEMB Wall *with* Insulation

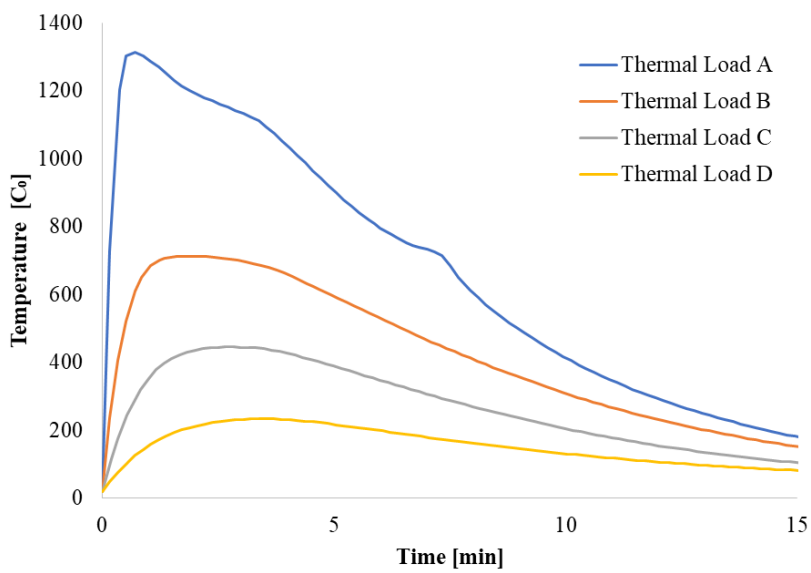
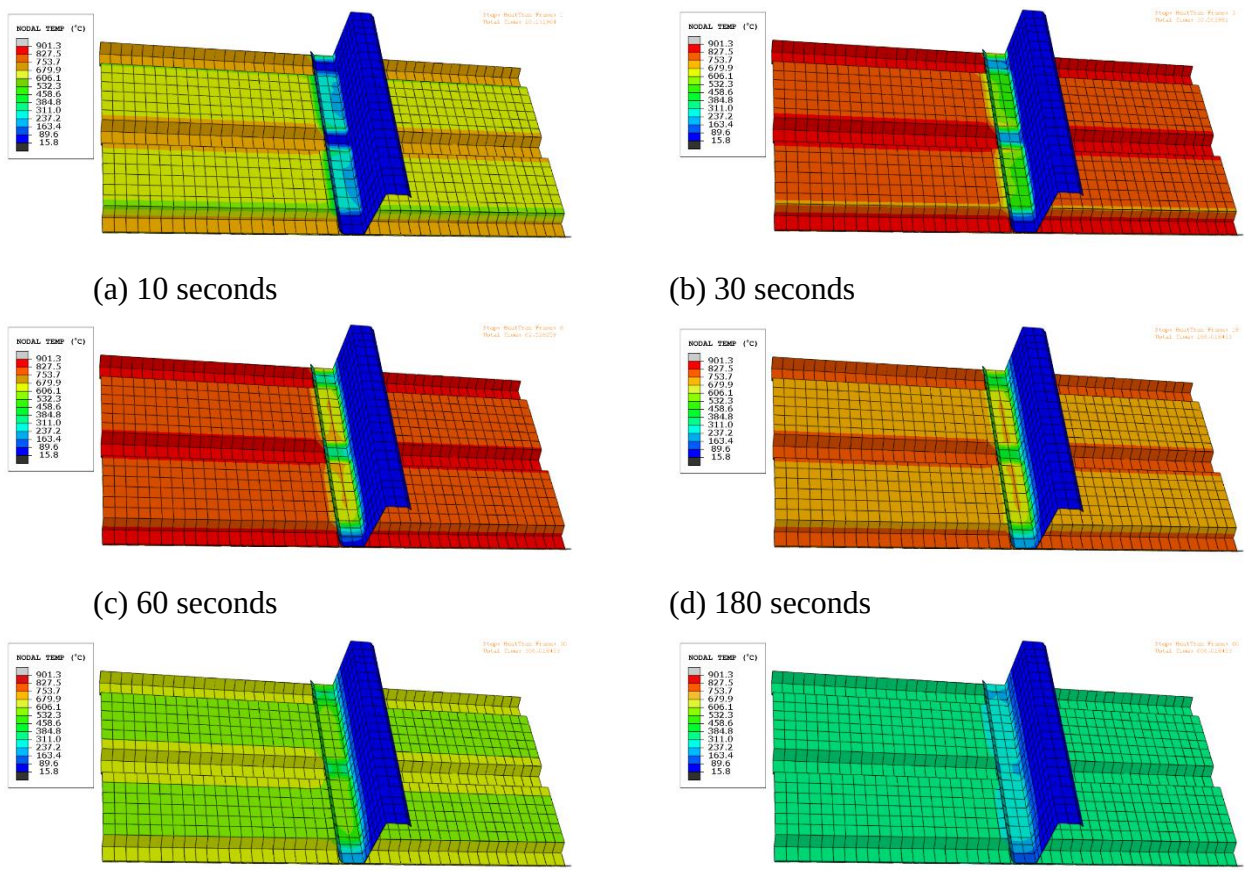


Figure 4. Temperature Variation at the Hottest Point of the Girt for a Wall *without* Insulation for Varying Transient Heat Flux Loads

Variation of temperature in the PEMB wall is plotted in Figure 5 for the uninsulated case, at six different times, for the Thermal Load B case.



(a) 10 seconds (b) 30 seconds

(c) 60 seconds (d) 180 seconds

(e) 300 seconds (f) 600 seconds

Figure 5. Temperature-time History of PEMB Wall Segment – Transient Loading B

To evaluate the effects of temperature on the steel structural members of a building, it is helpful to understand how the properties of steel change as temperature rises. The reduction factors presented in Table 1 (below) provide an indication of how the stress-strain relationship changes when the steel structural members heat up, based on the Eurocode 4 publication[6]. For example, at 600°C, the steel's modulus of elasticity is 31% of the modulus of elasticity at the standard temperature (20°C). Likewise, the steel's yield strength is 47% of the yield strength at standard temperature (20°C). Ultimate strength of the steel is approximately 25% higher than the yielding stress at temperatures below 400°C. At temperatures above 400°C, steel loses its hardening capacity. Ultimate strength and yielding stress of steel have essentially the same values at these temperatures.

Table 1. Reduction Factors of Steel Stress-Strain Relationship Parameters at Different Temperatures Based on Eurocode 4

T (°C)	Young's Modulus Reduction Factor	Yielding Stress Reduction Factor	Ultimate Strength Reduction Factor
20	1	1	1.25
100	1	1	1.25
200	0.9	1	1.25
300	0.8	1	1.25
400	0.7	1	1
500	0.6	0.78	0.78
600	0.31	0.47	0.47
700	0.13	0.23	0.23
800	0.09	0.11	0.11
900	0.0675	0.06	0.06
1,000	0.045	0.04	0.04

FINDINGS

Based on the analysis results provided above, the following conclusions and observations are drawn:

- When insulation is present, a transient heat flux peaking above 120 kW/m^2 (thermal load A) results in a maximum temperature of around 275°C, at the hottest location of the girt. At this temperature, the girt strength is not reduced structurally, although the girt stiffness may be reduced by 10-20%. Therefore, it could also be assumed that the integrity of the vertical columns and the frame would not be compromised.
- If insulation is <u>not</u> installed on a PEMB, a transient heat flux peaking above 50 kW/m^2 (thermal load C) results in a maximum temperature of around 450°C, at the hottest location of the girt. At this temperature, around 20% of the steel strength is lost, and around 35% of the girt's stiffness is compromised. The structural integrity is expected to be intact for typical structural loading. Therefore, it could also be assumed that the integrity of the vertical columns and the frame would not be compromised. A similar results are found with an uninsulated building with thermal load D.
- If insulation is not installed on a PEMB, temperatures exceeding 700°C in the girt may be reached for transient heat fluxes exceeding 70 kW/m^2 (thermal loads A and B). At 700°C, around 75% of the steel strength is lost, and around 85% of the girt's stiffness is compromised. Structural integrity is compromised for most structural loadings.
- For the uninsulated case, there is significant variance for the final girt temperatures from one level of fire heat flux to another. For all considered fire heat flux cases, since both the wall panels and the structural members radiate heat toward the building interior, there will be a potential for high heat fluxes to impact building occupants. The authors recommend

performing computational fluid dynamic analysis, explicitly modeling the interior air, to further investigate the non-insulated case to quantify the potential impact on building occupants.

Some further observations, based on the expected building response are:

- Insulated buildings may suffer damage to the exterior panels, but are not expected to experience any structural degradation, given the transient loadings presented in this paper. Therefore, building occupants are not vulnerable to structural collapse given the external heat flux examples evaluated here.
- Uninsulated PEMBs exposed to transient radiant heat fluxes beginning at greater than about 60 kW/m^2 may experience a loss of structural integrity depending on the specific transient load. Static loads at this level (even those that are sustained for greater than about 3 minutes) are sufficient to induce a loss of structural integrity in the element, such that building collapse is possible.
- Structural members in uninsulated PEMBs can reach temperatures that may be capable of igniting flammable materials in the interior of a building. Further investigation into the temperatures reached by exposed surfaces of structural members and additional factors that influence the transfer of heat to interior elements is warranted.

The previous work (reference 7) found that under static loading, the building structural elements reached a steady-state temperature in less than five minutes. In this work, the peak temperature is reached in less than five minutes due to the transient loading patterns that were applied. These transient loading patterns are considered typical for jet fires following accidental release from hydrocarbon systems. Consequently, the building structural response is expected to be known within about 5 minutes from the beginning of the fire radiation exposure.

Finally, for both insulated and uninsulated PEMBs, the exterior paneling reaches temperatures where failures may be likely. While it is not well understood how a failure may manifest, failure of exterior panels have the potential to allow exposure of the building's interior elements. Consequently, this is another area for further investigation.

SUMMARY

Based on the analysis presented in this paper, the differences in insulated and non-insulated PEMBs are found to be significant. Insulated PEMBs provide a higher level of protection to structural elements as opposed to uninsulated PEMBs. Insulated buildings should be able to withstand thermal radiation greater than 100 kW/m^2 in both static and transient loading without suffering structural degradation. While an uninsulated building exposed to static radiant flux loadings greater than 35 kW/m^2 may have structural steel elements that reach temperatures exceeding 400°C, transient loadings of the type evaluated in this paper can reach up to 60 kW/m^2 before the same effects are realized. Above these values (35 kW/m^2 static loading and 60 kW/m^2 for a transient peak) significant damage to the building structure could occur, and structural failure may be possible.

Further building analysis, using computational fluid dynamic analysis and explicit modeling of the interior space, is recommended to better describe occupant vulnerabilities. For both insulated and uninsulated PEMBs, the potential failure modes of the exterior paneling requires further investigation to ensure that such failures would not result in exposure of the interior space to radiation.

Given that the building's structural response can be known within about 5 minutes of the beginning of a fire, something resembling a dose-response relationship can begin to be formed from these results. However, more investigation and calculations must be done before this relationship can be quantified.

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] Abaqus (2014). Abaqus Unified FEA, Version 6.14, Dassault Systèmes, 2014.

[9] Eurocode 4 (2005). Eurocode 4: Design of Composite Steel and Concrete Structures – Part 1-2: General Rules - Structural Fire Design, BS EN 1994-1-2: 2005, British Standards Institute, 2005.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

CAROL - Robotic Catalyst Removal

Christopher Jansen*
Program Manager
WorleyParson,
12 Creek St, Brisbane, QLD 4000

Andrew W. Sloley
Principal Consultant
Advisian (WorleyParsons Group), Energy Center II,
575 N Dairy Ashford St, Houston, TX 77079

Scott Schroeder,
Senior Technical Consultant
Advisian (WorleyParsons Group), Energy Center II,
575 N Dairy Ashford St, Houston, TX 77079
*Presenter Email: christopher.jansen@worleyparsons.com

Abstract

WorleyParsons has developed the industry's first commercial robot for catalyst unloading from refinery and petrochemical vessels. The development of CAROL™ (Catalyst Removal Amphirol) responds to increasingly stringent requirements to reduce human risk in inert confined-space entry. It is the culmination of a three-year development effort from conception and design to prototyping and testing and represents a potential game-changer in the industry.

The number of fixed-bed catalytic vessels in the global refining and petrochemical industry is estimated to exceed 58,000. Based on current technology a rough estimate of the number of worker days of risk exposure due to confined-space entry during catalyst unloading exceeds 10,000 days per year. Current practices for catalyst removal from each of these vessels pose a risk to safety and/or the environment. CAROL provides an alternative option that minimizes risk to workers.

CAROL is a simple, one-of-a kind machine that has been demonstrated to achieve vacuum catalyst removal without the placement of workers inside the vessel. A review of operating characteristics in a single bed test vessel is provided. Additionally, two case studies from commercial field trials are presented.

This paper showcases the challenges associated with current catalyst removal techniques, and the inherent safety advantages that CAROL has shown. The presentation includes video of the test vehicle operating characteristics and discussion on industry acceptance progress and preliminary test results.

Abbreviations

ATEX	Atmosphere Explosibles
CAROL	Catalyst Removal Amphirol
HAZID	Hazard Identification
HMI	Human Machine Interface
HPU	Hydraulic Power Unit
IEC	International Electrotechnical Commission
LEL	Lower Explosive Limit
LNG	Liquefied Natural Gas
RSI	Reactor Services International

Introduction: The Problem

Catalyst Unloading

A refinery or petrochemical plant can have up to 100 vessels containing fixed beds of catalyst, adsorbent or other granular material. These beds include reactors, contaminant adsorbers and filters. Vessel entry periods vary from six months to five years. Work requiring vessel entry includes bed replacement, vessel inspection, and internals repair or maintenance.

Catalyst unloading is a potentially hazardous and time-consuming activity. Many vessels require inert conditions throughout the catalyst unloading process for various reasons. For example, pyrophoric scale can autoignite in the presence of oxygen. Other hazards include residual hydrocarbon in the catalyst, hydrogen sulfide, mercury, and other toxic compounds depending on the application. Until now, catalyst unloading has typically been performed by catalyst contractors who enter the vessel equipped with breathing apparatus because the inert nitrogen atmosphere does not support life.

Catalyst removal is most commonly achieved by a worker standing on the catalyst and manipulating the end of a high-volume vacuum hose (Figure 1). Material is removed via the vacuum hose to a vacuum truck located adjacent to the vessel (Figure 2).

Figure 1: Manual vacuuming

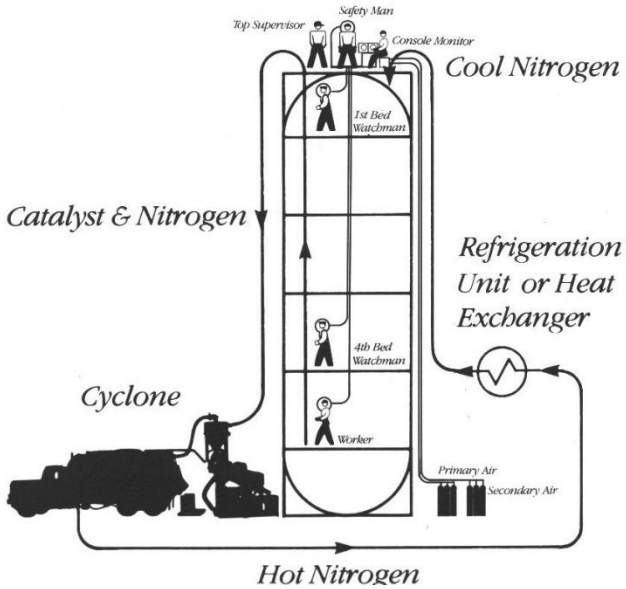


Figure 2: Set up for manual catalyst removal

An alternative method of removing spent catalyst or adsorbents from vessels is gravity unloading through either a side or bottom dump nozzle. Gravity unloading leaves residual material below the dump nozzle or in a talus-like slope extending away from the nozzle. In short, wide vessels, up to 40% of the residual catalyst can remain in the vessel after dumping.

Water flooding is a method to avoid confined space entry under inert conditions. The vessel is filled with water which suppresses the volatile components. The water level is dropped and the catalyst is then vacuumed in an open-air environment. Water flooding typically increases the catalyst unloading duration due to the time it takes to fill and empty the vessel which is often required several times. It also poses an environmental impact associated with disposal of the contaminated water.

Potential Hazards

Confined-space entry, particularly with inert conditions, is considered hazardous. Fatalities continue to occur due to asphyxiation, exposure to heat, fire, falling from heights, pressure build-up, and engulfment under catalyst (1). Specialized contractors are usually hired to work in inert atmospheres.

A study conducted by the U.S. Chemical Safety Board identified 85 nitrogen-exposure incidents in the U.S. between 1992 and 2002, resulting in 80 deaths and 50 injuries (2). Despite significant technological advances in the last 25 years, personnel entry into crude oil storage tanks and petrochemical vessels remains commonplace. Maintenance activities at industrial facilities continue to put workers at risk who enter the equipment.

In 2014, a worker was killed at a refinery in Germany. The worker was vacuuming catalyst under inert conditions at the bottom of the reactor. A wall of catalyst collapsed and completely buried him. 10 m^3 of catalyst had to be removed for the body to be recovered.

The industry has an obligation (not just requirement) to maximize personnel safety. The industry should not tolerate manned inert entry as the de facto technique.

CAROL Development: The Solution

Roles & Project Objectives

The vision was to apply robotic technology to transform personnel safety and to revolutionize how refinery and petrochemical vessels are unloaded of hazardous materials. WorleyParsons, as program manager, combined the robotics expertise of Canadian company, Mecfor, with the oldest catalyst handling company in the US, Reactor Services International (RSI).

CAROL

Through the use of cutting-edge technology, the project team developed CAROL, the Catalyst Removal Amphirol. This represents the culmination of a three-year development effort from conception and design, to prototyping and testing.

The CAROL robotic catalyst removal process is similar to the conventional method. However, instead of a person holding the vacuum, the vacuum hose is connected to a screw-propelled vehicle. This light-weight and simple device is lowered in to the vessel on a winch. It moves with precision on top of the catalyst surface (Figure 3), maintaining an even catalyst surface, controlled by an operator stationed outside of the vessel (Figure 4).

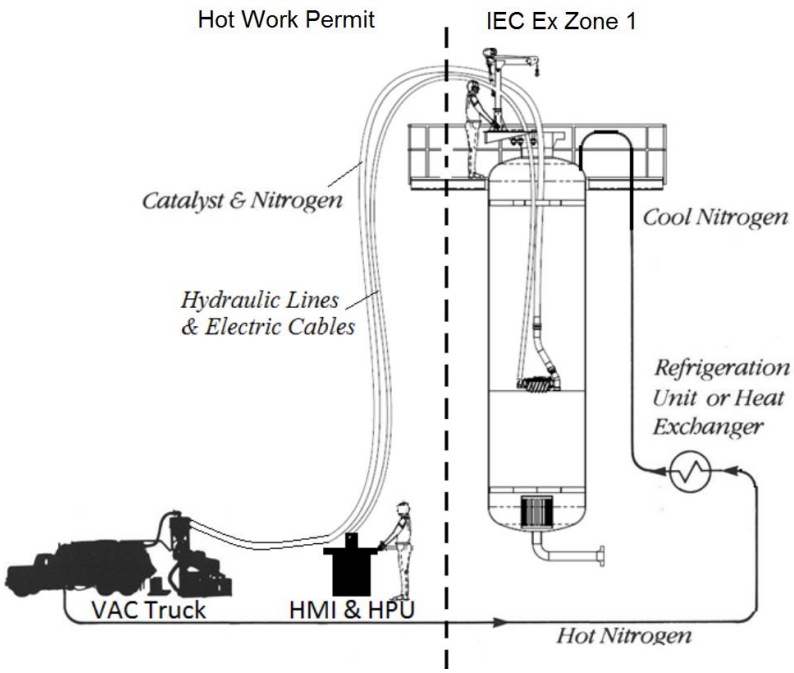


Figure 3: CAROL Prototype **Figure 4: Remote operated catalyst removal system**

The amphirol (screw propelled vehicle) design allows CAROL to move in all directions and to turn on a dime. The screws were manufactured using 3D printing. This allowed for optimization of the ribs and the ellipsoidal ends. The aluminum frame is critical to minimizing the weight. The result is a device that essentially floats on the catalyst, causes minimal damage to the catalyst and rarely gets stuck. It has a low center of gravity to prevent it from flipping over. If it does flip over

or gets stuck, then it is easily lifted using the winch cable, and then lowered back to be right-sided.

CAROL is controlled remotely via a joystick and monitored using video screens. The motors are hydraulically powered and the cameras and sensors have a Zone 1 hazardous area rating suitable for use globally with IEC Ex, ATEX and AEx (Class 1 Zone 1) approvals.

One advantage over the traditional manual process is that CAROL can be used in temperatures not suitable for human entry. Typically, human entry is prohibited if the vessel temperature exceeds 40°C (104°F). CAROL can be operated in temperatures of up to 75°C (167°F).

While the key driver for this technology development is improving safety during catalyst unloading, it was important that newly introduced risks were identified and mitigated. The WorleyParsons risk management process has been adopted to generate a risk register for robotic catalyst removal technology. HAZID reviews by tier 1 operating companies have confirmed that no risks of unacceptable consequence and probability have been introduced.

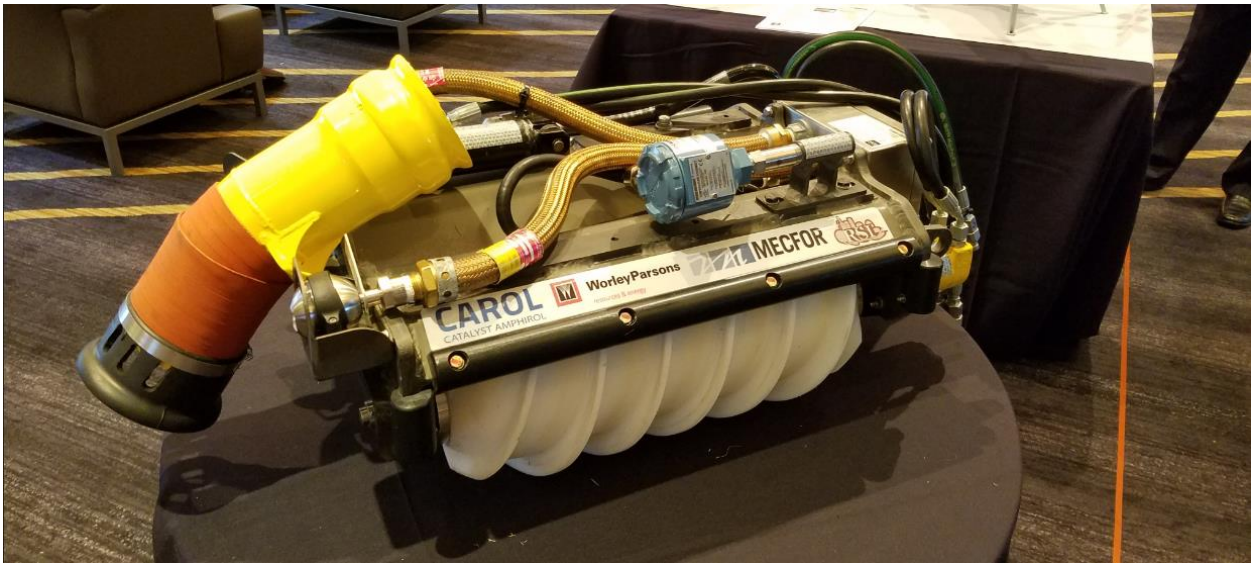


Figure 5: CAROL at the Energy Robotics & AI Network Conference in Houston, TX

Review of Operating Characteristics

Extensive testing has been carried out at test facilities in the United States and Australia. Rate of catalyst removal trials indicate that CAROL can achieve a removal rate that is at least equivalent to that of the current human operation with the same vacuum equipment. Over the total catalyst unloading period, it is estimated that 20-30% time savings can be achieved once worker fatigue and the requirement for breaks is considered.

CAROL has been tested on a range of material types. Bulk densities for the test media ranged from 625 kg/m^3 (Figure 6) to 1310 kg/m^3. Test media size ranged from 1mm diameter for ICR 130 catalyst to 25 mm for ceramic balls (catalyst support). The screws were shown to be effective operating on loose/random tower packing (Figure 7), on ceramic balls (Figure 8) and in

breaking up a slightly agglomerated material created using carbon and concrete. An endurance test was conducted using a reservoir and re-circulating the catalyst (Figure 9).

Figure 6: Molecular Sieve

Figure 7: Loose/random tower packing

Figure 8: Ceramic Support

Figure 9: 12 Hour endurance test set-up

Case Studies

Two commercial field trials are presented.

Case Study 1 - Australian LNG Facility

CAROL was used to remotely remove adsorbent from a dehydration vessel, avoiding the need for worker confined space entry under inert conditions.

Figure 10: Dehydrator Vessel

Figure 11: Control Station

Customer Challenge

The dehydration vessels, which remove water from gas before it is liquified, have previously been unloaded using a water flood method. The adsorbent is deactivated using water after which workers enter the vessel equipped with breathing apparatus and manipulate the end of a vacuum to remove the material. Other vessels at the plant must be unloaded under inert conditions – a nitrogen environment. The Client is seeking to minimize confined space entry, particularly under inert conditions.

The dehydration vessels at the Gorgon LNG Plant provide some unique challenges for the robotic catalyst removal technology. The manway is off-center, which means the robot needs to travel a long distance to the outer edge of the 4.1-meter diameter vessel. The top ceramic balls are on a steel mesh screen, and there are moisture probes located towards the bottom of the vessel, which the robot needs to navigate around.

Our Solution

CAROL was used to unload one of the dehydration vessels under inert conditions. This was the first time that CAROL had been used in a live operating plant. The use of CAROL removed the need to water flood the vessel and the associated issues of disposing of potentially contaminated water, while also minimizing the time spent by workers in the confined spaces.

Value delivered

CAROL remotely removed more than 95 per cent of the adsorbent from the vessel including the ceramic support material at the top of the bed. Inert conditions were maintained throughout and the requirement for confined space worker entry in the oxygen deficient atmosphere was eliminated. CAROL was also successfully deployed in another vessel under water flood conditions.

The successful trial of CAROL at the LNG Plant has demonstrated that WorleyParsons' robotic catalyst removal provides an alternative to inert confined space entry during catalyst unloading. It also provides an alternative to water flooding and the associated disposal of the potentially contaminated water. Lessons learned from the trial have been implemented in the revised procedures and design. Once implemented, CAROL should also provide schedule advantages compared with the current methods

Case Study 2 - USA Syngas Power Plant

CAROL was used to remotely remove built-up catalyst at its angle of repose with vessel temperatures exceeding 50 degrees Celsius.

Figure 12: Reactor and control system trailer

Figure 13: Top view of CAROL in reactor

Customer Challenge

Catalyst from the Gas Shift Reactor vessels is removed in the first instance using a dump nozzle located at the bottom of the catalyst bed. This allows for catalyst to be gravity dumped from the vessel however not all catalyst is removed. The residual catalyst can be up to 40% of the total vessel volume. It is difficult to unload manually by people entering the vessel with a vacuum hose because the material is built up around the vessel walls. Workers need to manually break down the mounds of catalyst whilst trying to avoid getting buried in the falling material. The pyrophoric material also tends to heat up if the nitrogen purge is insufficient to maintain inert conditions.

Our solution

CAROL was used to unload the residual catalyst material (post dumping) in one of the Gas Shift Reactor vessels. CAROL was operated in temperatures exceeding 50 degrees Celsius thereby reducing delays caused by the requirement to cool the vessel for the traditional worker entry technique. This was the first time that CAROL had been used in a live operating plant in the USA.

Value delivered

This use of CAROL demonstrated that the robotic catalyst removal technology can be used effectively in combination with gravity dumping, to minimize the time spent by workers inside confined spaces during catalyst unloading. In many cases, this will reduce the outage duration because CAROL can be used in vessel temperatures and toxic environments that are not suitable for worker entry.

Conclusions

WorleyParsons and its partners have developed the industry's first screw-propelled remote-operated catalyst unloading machine. CAROL (Catalyst Removal Amphirol) will reduce the associated risk with placing people inside vessels by phasing out the current manual-labor-intensive process.

CAROL has a straightforward design with few moving parts. By using screws for propulsion, CAROL moves freely on the surface of loose material. It is light weight and easy to maneuver inside the vessel using a joystick and live video feedback. CAROL facilitates effective vacuum removal of catalyst with no requirement for human entry during the bulk catalyst unloading phase of vessel change-out.

WorleyParsons have challenged the status quo that catalyst unloading must rely entirely on personnel–CAROL has the potential to radically alter what has been done the same way for almost 75 years.

References

Malewitz et al. (2015). A Deadly Industry. Available at: http://www.ehstoday.com/safety/deadly-industry [Accessed 10 Jan 2018]

MacCarron, C 2006. 'Confined-space Fatalities', Doctor of Philosophy thesis, Edith Cowan University, Western Australia

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Connecting Progress Safety and the Dynamic Frontline

Simon Jones
Head of Professional Services
Petrotechnics Ltd
Email: simon.jones@petrotechnics.com

Keywords: Process Management for Safety; Digitalization; Connected Worker; Major Accident Hazard Management; Risk Assessment, Analysis and Management; Safety Critical Elements; Control Systems; Equipment Integrity; Petrotechnics

Abstract

The real world of operations is neither simple nor static. It's dynamic and can be difficult to manage. Deviations from management system or procedural practice, changing equipment status, hazards introduced through maintenance and repair work, and human and environmental factors can increase risk exposure which can escalate into a significant process safety event.

While process safety tools and techniques have enabled us to improve the design basis of our facilities, we simply do not provide adequate systems and solutions to help Operations prioritize their work and operate the facility in a way that proactively minimizes and manages risk.

In fact, according to Petrotechnics' 2018 survey on process safety and risk management, 86% reported a gap between how process safety is intended and the reality of its implementation in operations. In 2017, an overwhelming 90% said risk awareness and safety would be improved with access to real-time process safety risk indicators – and yet the 2018 survey reveals that today 60% of companies are not proactively monitoring and managing impaired process safety barriers.

While the current digitalization initiatives of the industry offer companies an opportunity for a more precise understanding of risk and provide a route map for the journey towards sustainable production, often the last people in the organization to be connected are the frontline work teams. This is all about to change – and process safety and operations teams need to prepare for a substantial digital leap.

A new category of Operational Risk Management (ORM) tools are emerging which seek to close this gap. This paper shares the approaches adopted by two major international oil industry

operators who are leveraging a new approach to process safety and operational risk management to achieve safer, more sustainable operations.

1. Introduction

Few would argue that process safety approaches developed and implemented over the past 20 – 30 years have enabled us to improve the design basis for our facilities. The use of a risk-based approach is commonplace and indeed a requirement of many regulatory bodies around the world. Yet we still see major incidents occurring at a steady rate [1, 2].

Operational risks arise from a complicated set of interrelated parameters and are viewed and managed in differing ways depending on the role and level in the organization. The challenge is simplifying this complexity, enabling all levels of the organization to collectively focus on the elements of risk that are most important.

2. Survey of process safety and operational risk engineers in 2018

Petrotechnics conducted its second major survey of process safety and operational risk engineers in 2018. 108 process safety, asset integrity and operational risk management senior leaders around the world participated, including representation from members of the Mary Kay O'Connor Process Safety Center. Figure 1 provides a few key facts about the contributors to this survey:

Figure 1 Respondents to a global study of process safety professionals in 2018

When asked in 2018 about the operational reality of risk from their viewpoint, the following figures emerge:

- 86% believe there are gaps between how process safety is intended and what actually happens on the plant/asset - up from the 2017 survey figure of 70%
- 56% suspected an increase in risk on their plant when undertaking periodic process safety reviews (for example, 3-5 year periodic reviews of PHAs, HAZOPs, HAZIDs, LOPA studies, etc.)

This speaks to the challenge when good design enters into service at the frontline – the operational environment drives processes, systems, and equipment to degrade over time, thereby increasing risk.

Concerning safety-critical maintenance:

- An average of 73% of scheduled safety-critical maintenance is achieved, and 22% of respondents do not think it's practical to achieve 100% scheduled safety-critical maintenance
- When asked why, conflicting priorities (75%) and limited resources (72%) are said to be the challenges to delivering planned safety-critical maintenance

This suggests that we know what needs to be done to maintain safety critical elements (SCE) and associated systems and equipment, but resource availability and conflicting priorities get in the way of real-world delivery.

Following up on two key pieces of feedback from the 2017 Survey [3]:

- "It's important that we understand hazards on a real-time basis and that the continual state of barriers is maintained as designed to reduce incidents."
- "Everyone would be more thoughtful on ensuring barriers perform to standards if they truly understood what the barrier was trying to prevent."

The 2018 survey found that only 38% believe industry operators proactively manage process safety - companies do not have effective systems in place for:

- monitoring and managing impaired process safety barriers (60%)
- monitoring and managing deviations from management system requirements or expectations (64%)

3. Can digitalization help close-the-gap?

There is increasing focus and attention on the potential for new digitalization strategies to deliver increased value and sustainability in the energy and petrochemicals sector. Over 73% of industry leaders recognize the power of digitalization to accelerate and provide sustainable operational excellence [4]. A reduction in operating costs, broader operational efficiencies, and fundamental transformation of the business are what is expected. The promises of data connectivity and analytics suggest continuous uptime, rapid response to risk exposure, incremental revenue gains, opportunities to better utilize assets, coordinate with operating and business needs and improve the efficiency of field service groups.

> *"The effective use of digital technologies in the oil and gas sector could reduce capital expenditures by up to 20 percent; it could cut operating costs in upstream by 3 to 5 percent and by about half that in downstream." – McKinsey [5]*

In many ways, the dynamic nature of the frontline is ripe for technology to better support decision-makers. In fact, according to a Verdantix study, Operational Excellence and Industry 4.0 strategies are among the top factors triggering operational risk management implementation today. Over 73% consider digital technology valuable, if not essential, for effective operational risk management [6]. An emerging category of Operational Risk Management enterprise software seeks to support safe and effective operational decisions by providing critical innovations [7], including:

- An enterprise ORM approach to barrier management, permit to work (PTW), management of change (MoC), incident management, risk assessments and process safety management - all accessible via desktop web applications and mobile devices for use in the field
- Wearable technology as a source of data for use in the field
- Industrial Internet of Things (IIoT) as a source of data from critical devices in the field
- Advanced modeling capabilities to create dynamic “digital twin” asset models
- Advanced analytics from big data and edge data to provide actionable insights on operational risk status and trends

4. A new model for Operational Risk Management

Operational risks can arise from critical equipment conditions - or non-conformances - and also from planned activities on the facility. A new approach to managing the cumulative impact of all these operational risks is to model their impact on process safety barrier groupings and associate them to the major accident hazards (MAH) under management. This simple, elegant approach enables operators to predict and better manage the outcome – whether that means to postpone a particular planned activity or accelerate maintenance to address the deviations or non-conformances on the facility [2].

At the heart of this model (Figure 2) is the need to carry out an operational risk assessment for any performance deviation or non-conformance identified on the facility. Examples include:

- Performance standard failure
- Verification inspection finding
- Overdue safety-critical maintenance
- Override of a safety-critical system or device
- Management of hydrocarbon leaks
- Temporary equipment
- The absence or inadequacy of a control system(s)

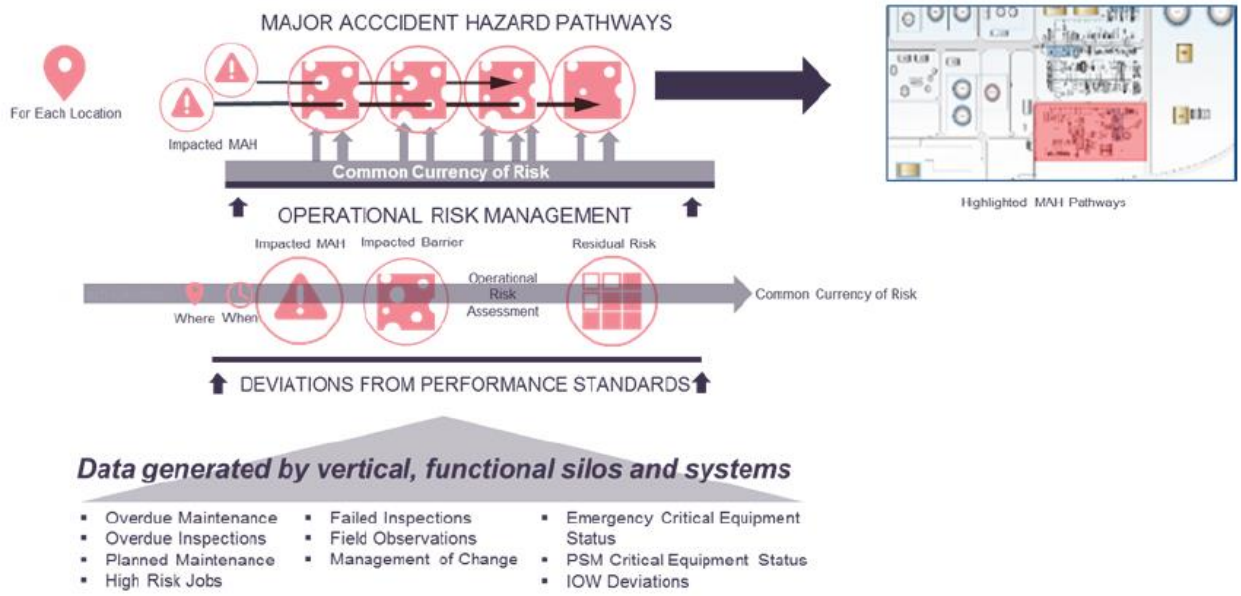


Figure 2 Deviations and non-conformances as sources of risk

An engineering technical authority typically leads the risk assessment process. This process identifies the major accident hazards under management, the fundamental barriers impacted, defines interim control measures and authorizations required and also the resulting residual risk associated with the individual deviation or non-conformance.

As illustrated in figure 2, deviations and non-conformances may be tracked and managed through many different business processes and systems, such as asset integrity inspection systems, maintenance management systems, operator rounds or management of change processes, inspection data and environmental control systems. Therein lays the challenge and the opportunity from an Industry 4.0 perspective: if we can map these operational conditions, from whichever business system they arise from, and provide a better illustration of their impact on operational risk and the major accident hazards under management, we help support better decision-making from a risk management perspective.

Connecting Activity Risks and Fundamental Barriers

Planned activity on the facility can also introduce potential process safety barrier impairments and increase risk exposure. These activities are typically planned and scheduled in a maintenance management system, and their execution is managed via a work permit processes, supported by a 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 operational activity can be modeled – for instance, if a planned isolation is needed to prepare for confined space entry. In this case, it is reasonable to assume there is a potential impact on the process containment barrier for the period in which 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.

Towards a common currency of risk
If we have carried out operational risk assessments for all deviations and non-conformances on the facility, and we also know the potential barrier impairments introduced by planned work, we can have a more complete view of all activity and risk and their potential impact on the asset's operational reality. And we can map this to a specific location, a given time/shift and see the MAH risks under management.

From an Industry 4.0 data and systems perspective, we can use this model to connect disparate sources of data that represent all activity, deviations, and non-conformances 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 proactively intervene to prevent major hazard events.

5. Connecting the complete view of all risks and all activities to the frontline

Once we have a common currency of risk and a comprehensive view of all of the activity and risk, the next challenge is to get this information into the hands of all those that can benefit. Enabling the connected industrial worker using mobile devices is the next opportunity in the "digital transformation" journey. From a process safety standpoint, we must take care to ensure the data presented to the frontline - through intrinsically safe mobile devices - offers the dynamic information work teams need to support process safety hazard management.

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.

Figure 3 The connected frontline worker

Figure 3 illustrates the typical use cases for a connected frontline worker using a appropriate mobile devices. For example, field workers can:

- Know when and where to execute work
- Carry out task risk assessments (JSAs) at the worksite

- Manage work activities and associated tasks – for example, gas test recording
- Update the details of an isolation plan – recording isolation status, lock and lockbox information in real-time

From a risk oversight perspective, users can:

- See when and where work and activity is happening on the facility
- Monitor real-time work execution and performance
- Understand the cumulative impact of all activity and risks on the facility, to support decision-making from an operational risk management perspective

5. Case Studies – applying the Operational Risk Management platform approach

Here we share case studies of two major international oil and gas industry operators who are implementing the advanced operational risk model using Industry 4.0 Operational Risk Management software.

Improving the quality of technical risk assessments and modeling their cumulative risk impact

A major international oil company operates multiple platforms offshore in the UK Continental Shelf (UKCS). This operator has a mature management system and a well-defined approach to process safety, asset integrity management and work control. By implementing their Operational Risk Management platform solution, a technical manager sought to further improve the risk assessments that are undertaken when critical equipment is not meeting its performance standard.

The existing practice was to immediately carry out an operational risk assessment once such a deviation had been identified from formal inspection, maintenance or operator activities. This initial risk assessment was approved by the local offshore installation manager and would be discussed with the engineering support team onshore.

A general criticism of the UKCS regulator (not specific to the operator) was that such risk assessments in practice rarely identified the true hazard related to the failure of the protective function of the critical equipment.

This operator had a well-defined approach to managing safety-critical elements (SCE) and associated components and equipment. A performance standard was defined for the identified SCEs on each installation, which is related to the risk reduction credit taken in the regulatory Safety Case.

To improve the quality of the initial risk assessment, the operator used its ORM software to present the assessor with templated risk assessments based on the type/category of SCE impaired. The templates helped to:

- Define the true hazard that the non-conforming equipment as a class gives rise to
- Provide typical mitigating measures for the assessor to consider to minimize risk based on the equipment class/function

- Present relevant SCE performance standard content as checklists – which encouraged the assessor to:
    - Identify the level of safety or integrity criticality the deviation represents
    - Consider other protective functions that might compound the problem – that is, other deviations that also impact the area and major hazard under management

The ORM software also helped the assessor define if the impairment would impact a local area of the facility, or the whole platform – for example single gas detector may have a localized risk impact, whereas firewater pumps unable to deliver required capacity impact the entire installation.

The ORM software was also used to drive a revised approval process:

- Formally involve the defined functional technical authority in the approval of the technical risk assessment, based on the equipment class/function; and,
- Based on the level of safety or integrity criticality identified in the assessment, indicate required approvals from asset and business managers, in addition to the local installation manager

The Operational Risk Management software is also used to manage all permitted activity on the operator's facilities. This provides a combined view of all equipment risks and all activity risks on a barrier model, highlighting MAH risk pathways.

Delivering a real-time view of critical equipment status and its impact on risk

A major national oil company is building and will operate a world-class refinery in the Middle East. Currently in the greenfield phase, the Operator has commissioned a significant Industry 4.0 initiative to develop and deliver a technology-driven approach to integrate a suite of business systems to better support asset and operations processes and management. The operator has a sophisticated safety management system and clear corporate standards and practices. The operator wishes to make a real-time view of operational and process safety risk a central element of decision-making from plant start-up onwards.

The operator is implementing an Operational Risk Management software platform to manage all permitted activity and deviations on the facility. The ORM software will integrate with three other business systems to deliver a real-time view of the risk status associated with critical equipment:

- Data historian – for near real-time status of critical equipment (this data historian is itself tracking the operational DCS and critical alarms systems)
- Maintenance Management System (MMS) - for inspection and maintenance records and associated plans and schedules
- Operator rounds system

Since the project is still in the design phase, the project team was able to access design package materials from the EPC contractors responsible for each refinery unit to identify the critical equipment. This includes bringing together a variety of information in useful formats.

- From design phase Hazop and asset integrity studies

- Health parameters associated with specific items of identified critical equipment
- Critical equipment types/categories mapped to the fundamental process safety barrier model
- Records representing all critical equipment were set up in the ORM software
- Through integration, the ORM software "listens" to the health of critical equipment, based on the above parameters, from three sources:
    - Near real-time status of equipment from the data historian
    - Inspection records for critical equipment from operator rounds and inspection management system
    - Deferred planned maintenance for critical equipment from MMS
- Non-conformances are mapped to the fundamental process safety barrier model

The ORM software is used to manage all permitted activity on the facilities. The integration described provides a combined real-time view of all equipment status risks and all activity risks on a barrier model, highlighting MAH risk pathways.

6. Conclusion

The oil and gas industry continues to experience major accidents, despite the application of mature approaches to process safety in the design phase of projects. There appear to be gaps that arise when this good design goes into operation. The dynamic nature of the frontline, coupled with the siloed nature of sources of information on planned activities and critical equipment can give rise to major incidents.

An emerging category of enterprise software system for Operational Risk Management seeks to close this gap by applying proven risk models to support all levels of operational decision-making with an improved approach to risk management - which is more pragmatic, simple in concept, and informed by real-time risk status.

The concept of the connected industrial worker mobility seeks to put real-time information in everyone's hands - through intrinsically safe mobile devices - to help keep people and assets safe and productive. From a process safety standpoint, such devices provide the opportunity to support process safety hazard management by ensuring everyone knows what is happening, where it is happening, what is impacting process safety barriers and what is truly driving the complete picture of risk on the facility.

7. References

1. *The 100 Largest Loss events 1978 - 2017 - Large property damage losses in the Hydrocarbon Industry*, 25th edition, Marsh & McLennan, 2018
2. Jones, S, *Do we really know how to manage risk?*, Proceedings of 2017 MKOC Process Safety Symposium
3. *2017 Survey on Process Safety Management and Operational Risk Management*, Petrotechnics, 2017 - https://www.petrotechnics.com/insights/petrotechnics-2017-survey-process-safety-and-operational-risk-management-report/

4. *Operational Excellence Index 2017*, Petrotechnics, 2017 - https://www.petrotechnics.com/insights/operational-excellence-index-2017-survey-report/
5. Choudhry, H. et al. *The next frontier for digital technologies in oil and gas*, August 2016, https://www.mckinsey.com/industries/oil-and-gas/our-insights/the-next-frontier-for-digital-technologies-in-oil-and-gas
6. *Operational Risk Survey 2018: Budgets, Priorities & Tech Preferences*, Verdantix, August 2018
7. *Smart Innovators: Operational Risk Management Software*, Verdantix, May 2018

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Using Process Historian Data to Understand and Assure Barriers

A.M. (Tony) Downes*, Prasad Goteti
Honeywell Performance Materials & Technologies
115 Tabor Rd, Morris Plains NJ 07950 USA
*Presenter Email: Anthony.Downes@Honeywell.com

Keywords: American Petroleum Industry (API), Computerized Maintenance Management System (CMMS), Key Performance Indicators (KPI), Loss Of Primary Containment (LOPC), International Electrotechnical Commissions (IEC), International Society of Automation (ISA), Independent Protection Layer (IPL), Layers Of Protection Analysis (LOPA), Occupational Safety and Health Administration (OSHA), Process Hazard Analysis (PHA), Performance Materials and Technology (PMT), Safety Instrumented Function (SIF), Safety Integrity Level (SIL), Safety Instrumented Systems (SIS), Safe Operating Limits Table (SOLT)

Abstract

Like many companies, Honeywell estimates the probability of control system problems and safeguard layer faults using the available reliability data. Probably like others, we have wondered how accurate these "standard numbers" are in our services. In our Advanced Materials division, we have been collecting real-world data on initiating events, Safety Instrumented Functions (SIFs) and other Independent Protection Layers (IPLs) in the data historians at two of our new low-global-warming Hydro Fluoro Olefin (HFO) units. Recently, we began using analysis tools to "mine" this data to see what it could tell us about our actual Initiating Event Frequencies and the Risk Reduction Factors being achieved. In essence, we are comparing the actual performance of our critical safety Layers of Protection with the performance that was intended by the PHA team.

In this paper we will describe the results of the Operation and Maintenance phase of the Safety Life Cycle and how we are using the resulting data in several important ways: to indicate the real-time health of active IPLs - watching for events like IPL degrading, and bypassing; to integrate the learnings as Key Performance Indicators (KPIs) to leadership and as inputs to our PHA/LOPA revalidations.

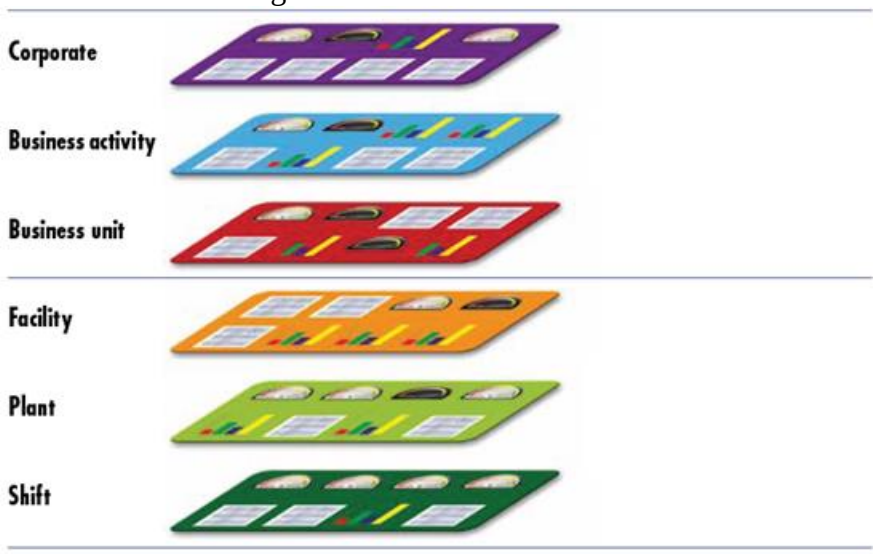
INTRODUCTION

Over the past 20+ years, improved understanding of process safety risk and decreasing risk tolerance has led to many more safety interlocks, particularly Safety Integrity Level (SIL) rated interlocks, being installed in process industry facilities. These have substantially reduced the probability and thus the risk of catastrophic incidents – generally by one or two orders of magnitude, possibly more. On the other hand, they have increased the number of trip activations – both real and spurious. And without a doubt they have increased the effort required to test and maintain these safeguards.

Standards like IEC 61511 / ISA 84.00.01*(ref 1)* and Recommended Practices like API RP 754 *(ref 2)* call for methods to identify and inform appropriate personnel at various levels in an organization on "Key Performance Indicators" (KPI) which could be either a leading indicator (before any incident or action occurs) or lagging indicator (after the incident or action). IEC61511 calls for Functional Safety Assessment of an installed Safety Instrumented System (SIS) after a few years of operation to make a judgement call based on such KPIs if the SIS is doing what it was supposed to.
Such KPI's are a useful measure to *(ref 3)*:

1. **Prevent major incidents** –KPIs released by an individual site to the company headquarters and later nationwide, the company (and other companies in the similar business) can analyze and learn what led to the Process Safety Incident, the root cause and how this can be avoided in the future.
2. **Improve Reliability –** Steps taken by a company to reduce major Process Safety Incidents help improve Reliability of Process Operations.[5]
3. **Avoid Complacency** – KPI's provide a measure of asset integrity. Just because there has been no major incident for a long time does not mean everything is fine. Leading KPI's could provide valuable information on the health of assets and indicate that it is time for maintenance on the asset.
4. **Communicate Performance –**KPI's could provide to the company and State / Country how the individual site is performing while **or** could asses performance internal to the individual site

Identifying key leading and lagging indicators at various levels in an organization and monitoring them on a continuous basis could give an indication of Process Safety performance at a site. These indicators, expressed as KPIs, are different at various levels in an organization. As an example, a major gas leak above the tolerable limits set by the local jurisdiction would be a lagging indicator and would be a KPI at the Corporate level while a demand on an SIS would be a leading indicator KPI for the Plant Manager and Shift Engineer indicating they should take a closer look at the process as to why a SIS Loop had to trigger on demand. See Figure 1 below.



KPIs at these levels are usually summarized and tend to be more of lagging and less of leading indicators

KPIs at these levels are usually more detailed and tend to be more of leading and less of lagging indicators

KPIs at various levels in an organization will be different.

Figure 1 (*ref 3*)

COMPANY LEADERSHIP CONCERNS

Is enough being done?

It's natural to focus our attention on identifying and tracking the individual risk scenarios that have the potential to lead to catastrophic outcomes. We need to find these, then identify solutions, budget for them and eventually design and install them. While our leaders will initially be looking at achieving the risk targets, they'll eventually ask whether these solutions are giving the intended level of safety – especially if an incident occurs. Have you gone digging in a PHA report to see what it said after something went wrong? We certainly have.

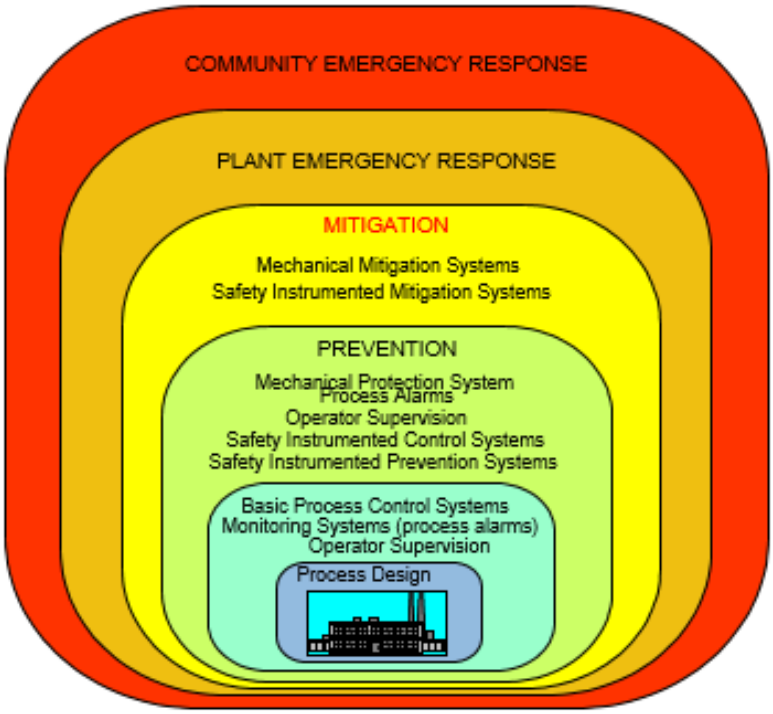


Figure 1 *(ref 1)* - The Layer of Protection Model, showing all layers

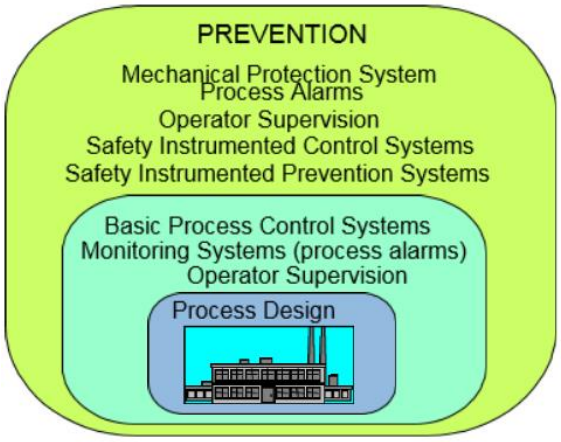


Figure 3 - Focus of this Paper

Are we doing the right things? Could we be doing too much?

For process safety staff, this is a tricky discussion. We have a tendency to think that there's no such thing as too much safety. But there are always multiple demands for capital and it's prudent to take a broader view. Certainly our leaders do. They recognize that reducing the risk of 10 scenarios by 1 order of magnitude (a factor of 10) is more effective[1] assuming ALL other factors are the same, than reducing 5 of them by 2 orders of magnitude (a factor of 100) and leaving the other 5 for later. Ignoring units for a moment, mathematically it looks like this:

Scenario 1, Mitigated Risk = 10 * 0.1 = 1

Scenario 2, Mitigated Risk = 5 *0.01 + 5 = 5.05

It's also why savvy leaders are looking for some proof that the investments they are making in process safety are paying off in reduced incidents.

1 There are enough caveats to this statement to fill another paper.

Moving from Rules-based Criteria to Data-based

Rules are important. They help the PHA teams obtain consistent results, and prevent most arguments. And we advocate for following the PHA rules in the vast majority of cases. But most operating companies allow their expert risk analysts to select partial credits for very well-understood and well controlled situations. If we are looking for optimal solutions, we need more accurate, "specific-to-our-application" data. In the past, we've looked solely to the Reliability Engineers to give us this, based on their testing data. It's still a good idea to include Reliability, but we can now provide ourselves with another source of raw data.

Is this system getting better than average Reliability? Or Worse?

Available industry standard failure rate data, such as CCPS's Process Equipment Reliability Database, has a wide range of values. In some cases more than 2 orders of magnitude from the lower values to the upper values. This makes sense given the wide variation in "quality" of something like a ball valve. Good ones tend to last longer. And, of course, services vary widely. High quality ball valves last even longer if they aren't in acidic mud ("severe") service. And the converse is true.

Most Layers of Protection Analysis (LOPA) teams struggle with these issues. If they choose to degrade the reliability from one of the "standard" values, they'll do it by a factor of 10. That may make sense, or it may be conservative. Or the actual performance may be even worse. You may have inspection results, or repair history, but it's time-consuming for maintenance to report this in great detail in their Computerized Maintenance Management System (CMMS), and it rarely gets down to the tag number of the particular instrument or valve involved. Even in the old days when paper records were kept, it was possible – though difficult – to extract reliability/availability information.

As a practical matter, you are depending on the opinion of the maintenance representative. Generally these folks remember the really bad actors IF they're close enough to the day-to-day work to know when a particular transmitter or valve required frequent repair because it failed in a "revealed" way. Only in rare cases do we get input about whether a particular valve had repeatedly failed in proof-testing even though it happens more frequently. So generally we are not getting up-to-date information in our Process Hazard Analysis (PHA) even though the information lies in our plant site's data systems.

EXAMPLES FROM A HONEYWELL PROCESS PLANT

The Problem

Honeywell's Performance Materials and Technologies (PMT) operating plants have been working on all the above issues, too. We've made it a requirement that our sites investigate each activation of a "PHA-Credited" Safeguard as a Near Miss. And IEC 61511 now asks the Functional Safety Engineers at the site to confirm the interlock worked properly as part of that investigation. Most of our SIS loops work reliably on demand once we install them. The demands on these SIS loops are also not frequent – especially as most are designed for "low demand mode". But in a business like ours, we want assurance both that the IEF is as low as we predicted and that the safeguards / protection layers are working at least as well as we predicted when we did the PHA. Here are a couple of examples – one good, and one not so good.

Example1

Pressure control loop on a distillation tower

This example considers a group of typical distillation columns. They have a Reboiler to provide heat and to boil up the liquid in the bottom. This is the most significant potential source of overpressure. Each column's vapor pressure is controlled by a simple overhead pressure control loop. A fault in that loop

could cause the column pressure to rise. Each column has a pressure safety relief valve (PSV) set to protect it by venting the contents of the column to a scrubber in case the control and alarm safety systems fail to prevent such an overpressure. In the past this might have been sufficient, but this system alone does not achieve Honeywell's current target risk level, so a High-High Pressure interlock[2] was added to shut off the reboiler heat source. This design met the risk target as designed.

Like a number of other companies, several years ago Honeywell adopted the leading practice of adding a Control Plan to its operating procedures. There is no "official" title for these. Some other companies use the term "Safe Operating Limits Table (SOLT)" and at least one company refers to this as an "Integrity Operating Window Table". See example Table 1 below.

CONTROL POINT	PROCESS VARIABLE	CONTROL METHOD	OPERATING LIMITS/ALARM SETTINGS		SAFEGUARDS	CONSEQUENCES of DEVIATION	OPERATOR ACTIONS / INTERACTION
PIC-101	Column Pressure		MAWP	450		Damage/Loss of Containment	
		Automatic: PSV calibrated	Never to Exceed	400	PSV-103	Will relieve pressure through RVs, causing release through relief scrubbers.	Ensure column is venting to LPS. Isolate column from any higher sources of pressure. Stop reboiler steam flow manually and increase condenser water flow to max.
		Automatic: Pre-programmed and cannot be altered without a MOC approval process	High High Interlock	350	SIS, At High High Pressure, PZIT-102 closes XZV-102 to stop heat to the Reboiler	Approaching pressure that will require relief through RVs.	Ensure XV-201 has opened and HIC-401 is allowing pressure to vent. Confirm XZV-102 has closed. Increase condenser water flow.
		Automatic: Operator inputs desired pressure setpoint. BPCS adjusts setpoint of flow control FIC-102 in a cascade loop	High Alarm	240	BPCS	May reduce flow from reactor or cause upset.	Check pressure in downstream column. Check reboiler and condenser are normal.
			Target	215-240 Typical: 230			Set pressure based on what gives good column performance and recovery of recycle material.
			Low	200		Can stop feeding forward to next column.	Ensure column is not venting to LPS. Check reboiler and condenser are normal.
			Low Low	--		Quality	
			Never to Exceed	--		None	

Table 1 : Example of Safe Operating Limits Table (SOLT)

[2] Where practical, Honeywell uses the Inherently Safer approach of selecting the MAWP of distillation columns such that the maximum potential pressure from the heat source would not challenge the vessel integrity.

The principle behind the table is to show important process parameters with the instrument loop which controls that parameter, as well as its normal set point and (often) some range in which the operator might vary the set-point or operate the system in manual - say, during startup or shutdown.

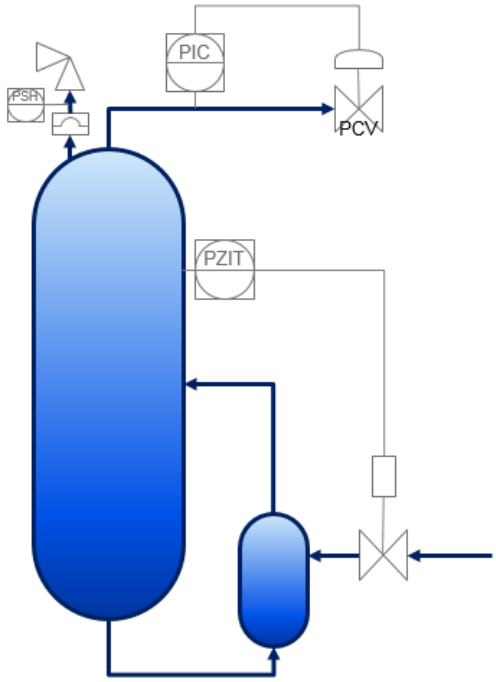


Figure 4. Typical Distillation Column with Safeguards

These fit well with Layers of Protection Analyses (LOPA) and provide direct mapping for the analyst checking the system performance.

Any Interlock activation (eg. PZIT102) needs to be “Validated” per IEC61511 (2015, Clause 5.2.5.3), and should be reported as a “Near Miss” per API754. It’s also a “Demand” of the Safety interlock also referred to as Safety Instrumented Functions (SIF), so it should be counted to compare these with the target frequency assumed in the PHA/LOPA.

So how well is it working in practice? Is the plant operating “in the Green”? This and nine other similar columns were checked. Only one fault was found anywhere in the control loops in more than three and a half years of operation. There’s a good chance that fault was due to an installation problem as it happened very shortly after start-up. Nevertheless that failure was counted as part of “all causes”. Thus the unit experienced 1 fault with 10 x 3.5 years of experience, so the failure rate was 1/35 or 0.029 faults/year. This is about 10x better than the standard LOPA assumed rate for similar cases. This is not a statistically large enough sample to consider changing the LOPA guidance for Initiating Event Frequency (IEF), but it is reassuring that the LOPA team assumption has not been found to be aggressive.

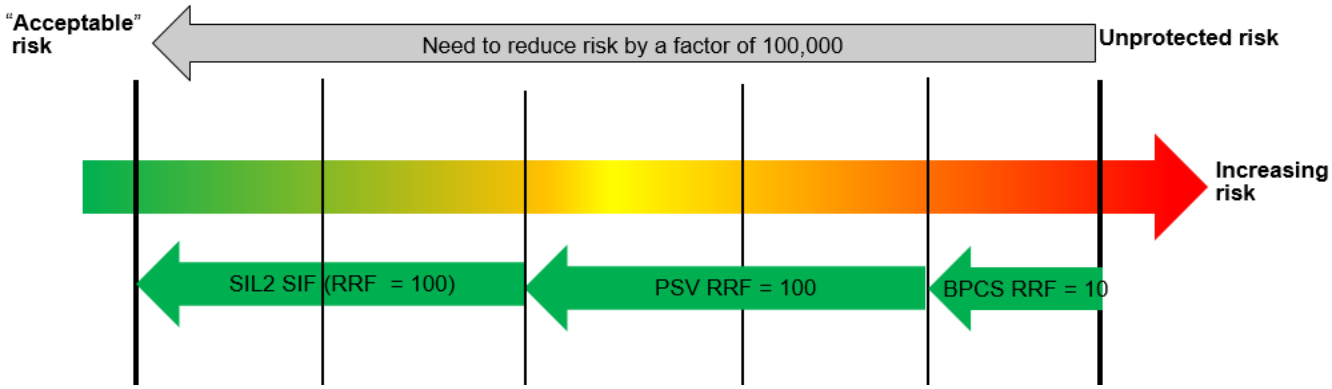


Figure 5. IPLs in a LOPA to reduce Risk

The Reliability and Availability of the SIFs were also checked. Based on the LOPA, the SIFs were designed to be SIL2 which would be a Reliability of 99% (refer Table 3 and Figure 5) in our scenario. To understand how Reliable they really are, the test records and the historian data were checked. The test records have shown all subsystems of the loops were functional at the end of each test interval. Thus it can be inferred that the interlocks were functional all the time they were in service since installation and would have operated Reliably on demand. This conforms to "more than 99%" reliability for which the SIFs had initially been designed.

SIL	**Risk Assessment**	**Protection Layers**	**Performance**
Safety Integrity Level	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD)	Reliability (1 - PFD)
1	10 to 100	0.1 to 0.01	.9 to .99
2	100 to 1,000	0.01 to 0.001	.99 to .999
3	1,000 to10,000	0.001 to 0.0001	.999 to .9999
4	>10,000	0.0001 to 0.00001	.9999 to .99999

Table 3. SIL in relation with other parameters

The Historian information was then checked for the amount of time the SIFs were in "Bypass mode". This was about 24 hours over the same period, so >99.9% of the period, the SIFs were Available to operate on demand. Figure 6 below shows Availability over a period of 60 minutes as snapshot.

At about 9:35 am, the Operator put the SIF input (100PZI4001) on "bypass" and at that instant onwards the input parameter shows "zero". All actions and events on the SIS are attributed with a "Risk index" number which is configurable based on user input. In this case, putting the Input value on Bypass is associated with a Risk index of "One" which means the process is running on a High risk because the SIF input is not being measured.

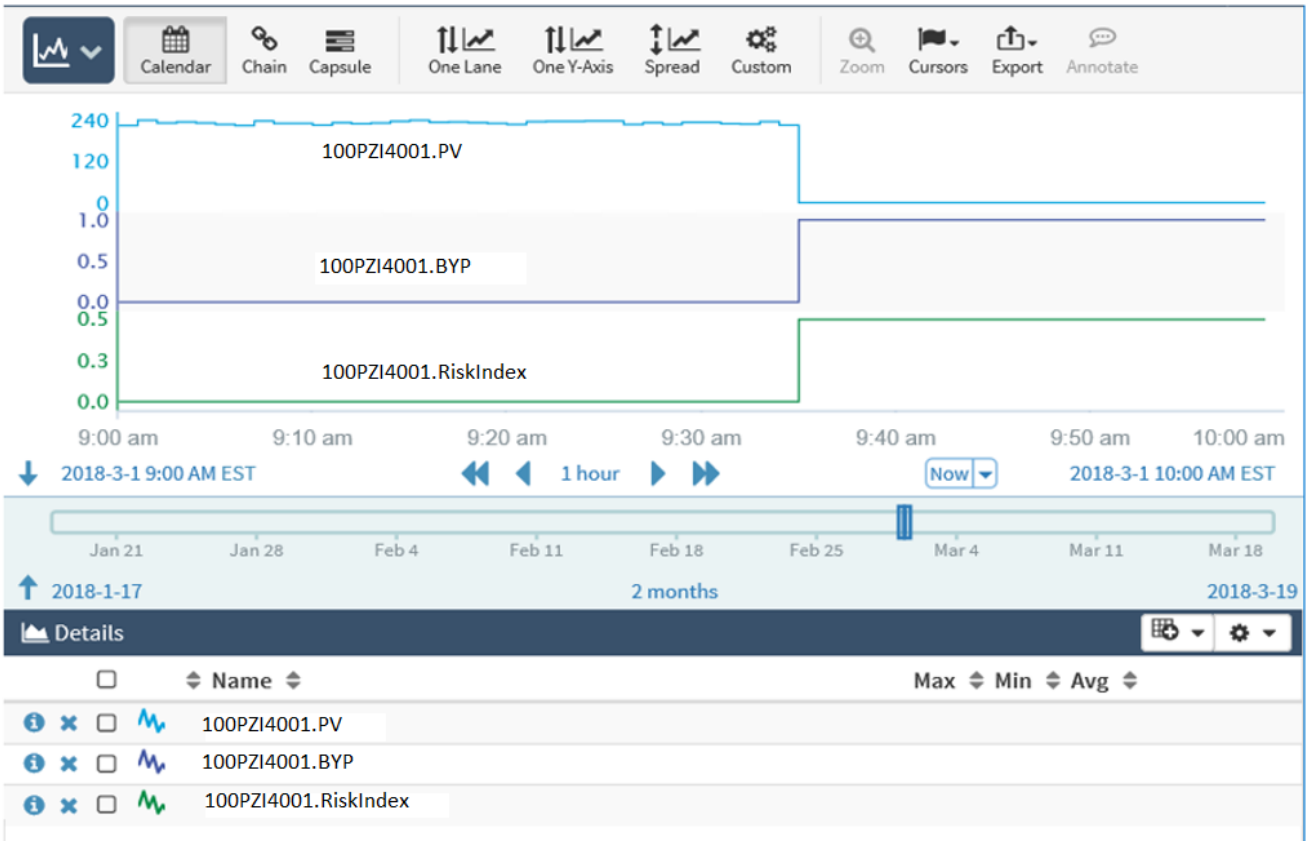


Figure 6. Safety interlock Availability over a 60 minute snapshot showing a change

Thus the analysis has validated that the LOPA target is being met for this scenario both in terms of Reliability and Availability

Other parameters that could affect Reliability or Availability of Independent Protection Layers (IPL) can also be monitored. Examples:

1. Safety Interlock in degrade mode due to failure of Input Transmitter signal (0 mADC) to the Logic Solver which could affect Reliability (See Figure 7). At about 9:35 am, the transmitter (100PZI4002) signal drops to 0 mADC and from there on the process value reads zero. The Risk index is configured to “0.5”, which means there is a redundant transmitter available for the SIF to function

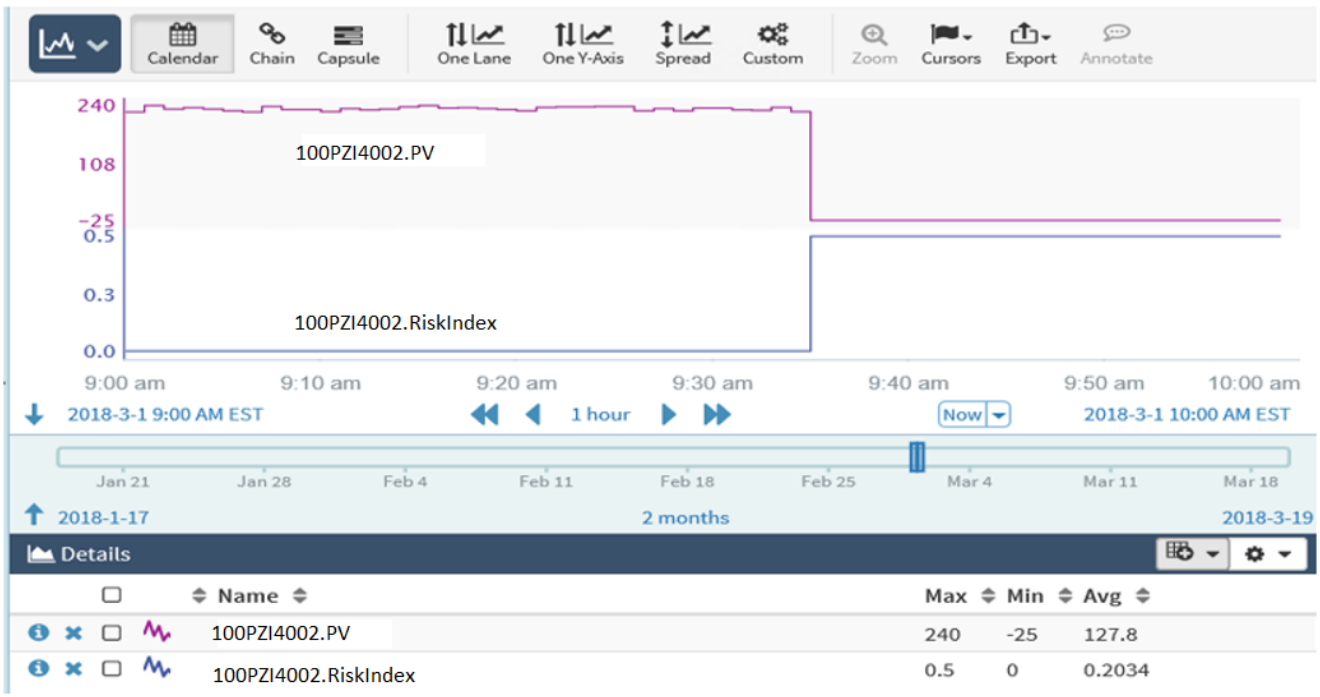


Figure 7. Safety interlock transition to Degrade mode due to transmitter failure over a 60 minute snapshot

2. Safety Interlock in degrade mode due to “frozen” Input Transmitter signal to the Logic Solver which could affect Reliability. The example below indicates two transmitters in a redundant configuration and one of the transmitters (100AZI4001A) is essentially “frozen” for the most part reading a process value of 200. The Risk index is configured to “0.5”, because there is a redundant transmitter available as part of the SIF input

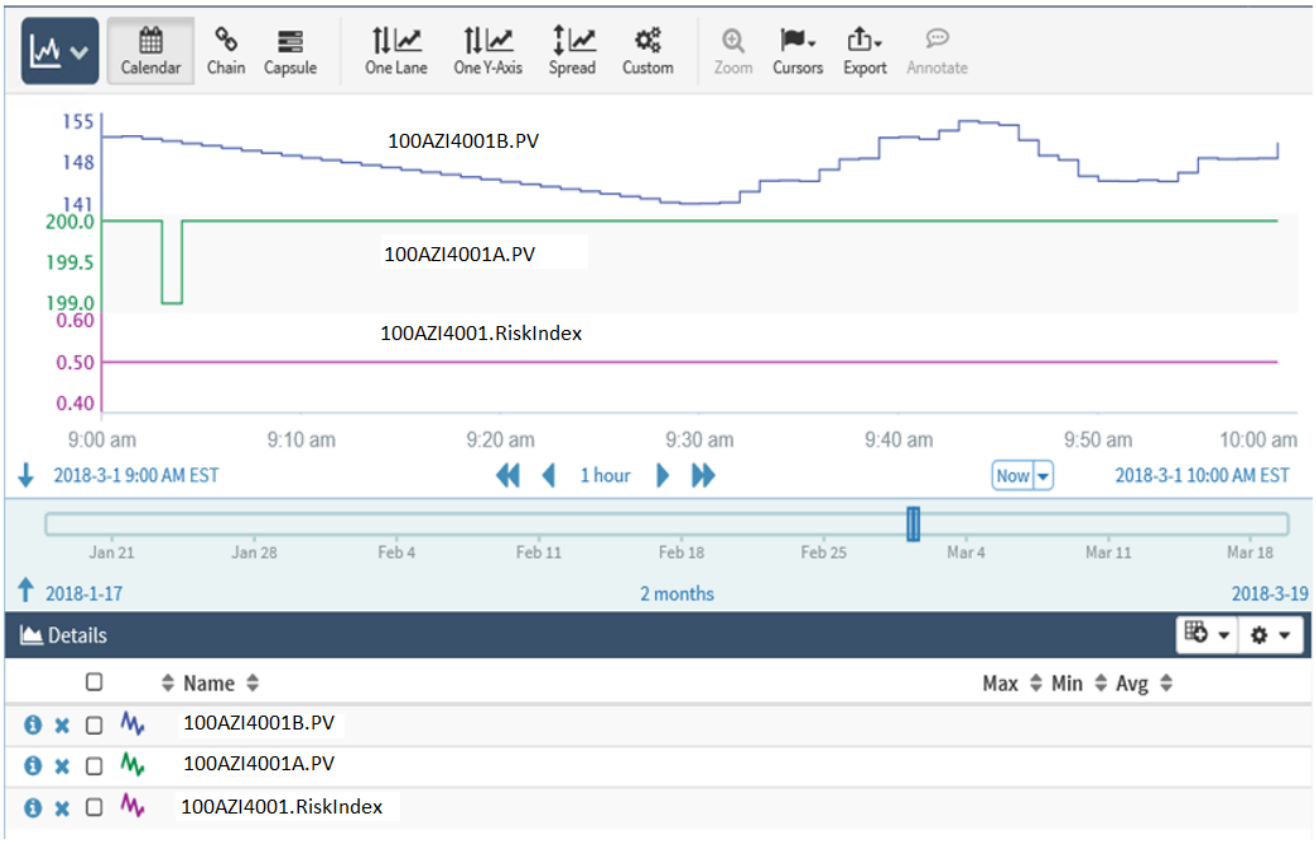


Figure 8. Safety interlock transition to Degrade mode due to transmitter signal “frozen” over a 60 minute snapshot

3. BPCS control loop in Degrade mode due to it being in “Manual” instead of “Auto” for a long time which could affect Reliability. In Figure 9, 100PIC4003 mode is changed to Manual at 9:41am. The controller output is manually changed to 100% and the process value starts increasing and saturates at 350 engineering units. The Risk index is configured to be “One” in this state.

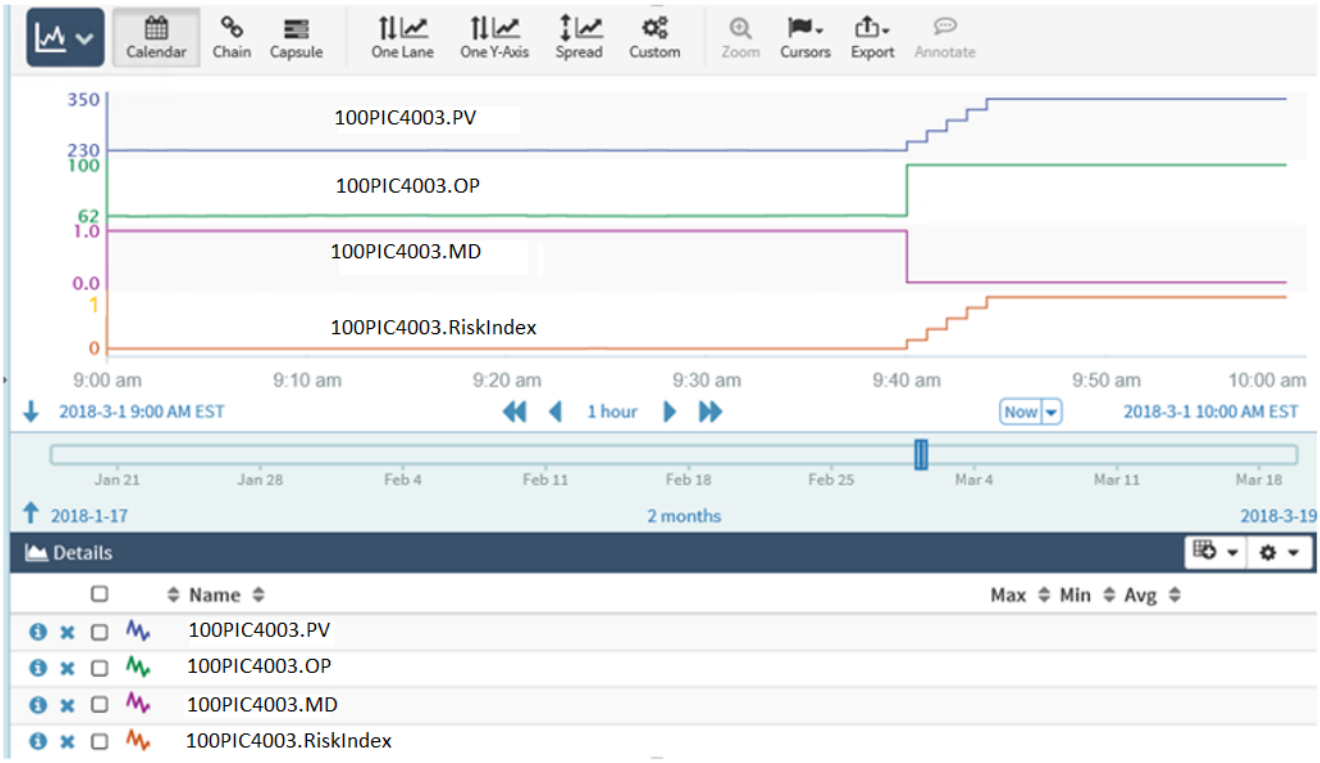


Figure 9. BPCS Control loop from “Auto” to “Manual” mode over a 60 minute snapshot

Example 2

Redundant Analyzers as inputs to SIF

If a heat exchanger in process service experiences a tube leak, it may put a hazardous material into the heat transfer fluid. It may be possible to detect the leak using analyzers such as for pH, Conductivity, depending on the properties of the process and heat transfer fluids. This is a useful capability, though analyzers tend to be relatively complicated systems with a number of potential fault modes and thus are generally considered to have relatively lower reliability/availability.

Here's an example of a "problem" set of Analyzers. The team estimated the IEF based on the LOPA table. They determined a safeguard should also be applied, so they added dual analyzers in a 1oo2 configuration. As it turned out, the tubes were more reliable than estimated and substantially more reliable than the analyzers that were meant to find any leaks. In one 5 week period, six of the analyzers had activated a total of 30 times, an average of once per week (Table 1). In fact, there had not been *any* leaks – as demonstrated by test and/or inspections after each activation. Thus all analyzer-triggered trips have been spurious. This High Spurious Trip Rate meant the Technology and PHA teams had to come back to the issue and find suitable alternates. There were two problems to be solved: the analyzers weren't reliable enough in this particular application to be part of a SIF and the spurious trip rate was causing significant business interruption.

.

Week Number	100AZIT1774A	100AZIT1774B	100AZIT1790A	100AZIT1790B	100AZIT1791A	100AZIT1791B	Grand Total
40	3	3					6
41	2						2
44			1	1	10	8	20
45	1						1
46	1						1
Grand Total	**7**	**3**	**1**	**1**	**10**	**8**	**30**

Table 4 - Demands for Analyzers in 1oo2 input configuration

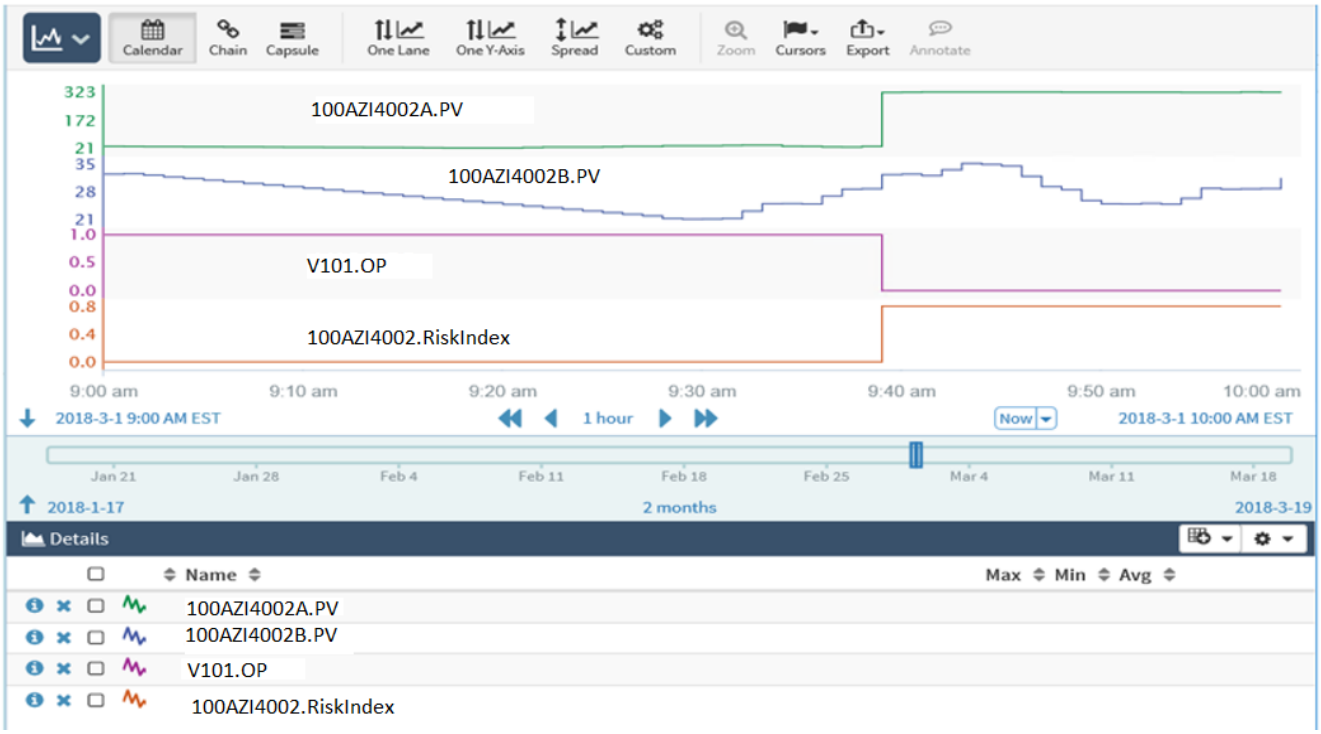


Figure 10. Spurious trip in a 1oo2 input configuration over a 60 minute snapshot

In Figure 10, at about 9:40 am, Analyzer 100AZI4002A spuriously senses the value as 323 engineering units when it is actually between 21 and 35 engineering units. Because of this reason, being in a 1oo2 input configuration with Analyzer 100AZI4002B, the output (Valve V101) trips. In this scenario, the Risk Index is configured to 0.8 as this is a Safe failure.

Emergency shutoff valves (XZVs) as Output Devices of a SIF

Emergency block valves go by many names: Emergency Shut-Down (ESD) valves, Remote Operated Shut-Off Valves (ROSOV), etc. Honeywell generally calls shutoff valves “XV’s” or “HVs”. The ISA convention is to put a Z in SIL-rated safety loops, so shutoff valves in SIL-rated service are XZV’s or HZV’s. XZV’s are generally provided with ZSO and ZSC limit switches at the “open” and “closed” end of their travel. Thus the time required for such a valve to travel from its active to its “safe” position can be measured using the data from the event historian. If a trend chart of the travel-time shows an increase, one may anticipate that eventually the travel-time will exceed the required Process Safety Time limit.

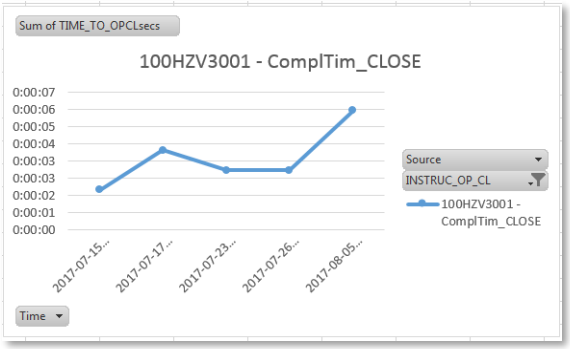


Figure 11. Travel time for an HZV to Close

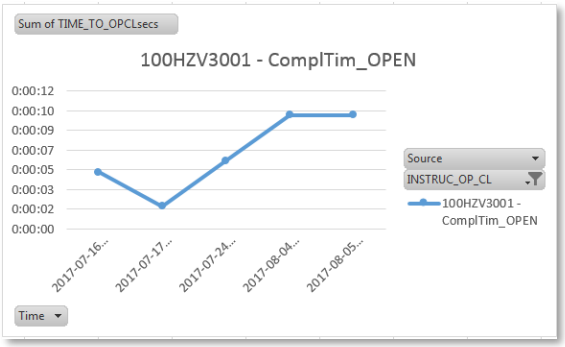


Figure 12. Travel time for the same HZV to Open

The increasing travel time may be an early warning sign of stickiness. Once it exceeds a threshold, Maintenance should take a look.

EMPOWERING PHA REVALIDATION TEAMS WITH THEIR PLANT DATA

The cases above show what can be done with historian data to either support the PHA/LOPA assumptions or to identify where non-conservative assumptions have been made. It may also reveal other opportunities like high spurious trip rates and overly conservative assumptions.
But anyone who has done this kind of analysis by hand, or using Excel, understands that it's time-consuming. In an era of financial constraints, the staff might not get to it. Fortunately, computer tools are available which can now search for and report these issues and opportunities, so the site's process safety and functional safety staff can spend their time solving problems rather that downloading data and developing pivot-tables – the techniques used for this paper. It's possible to get a report of demand rates and faults, area by area throughout the facility as input to the PHA teams.

How far can this concept be taken?

Scrutiny of the historian data enables some diagnostics to show when a degraded condition may have occurred. Honeywell is testing software that allows "degraded" situations to be diagnosed and flagged

in real time, so the controls and operations staff can see potential problems and take prompt action to fix them.

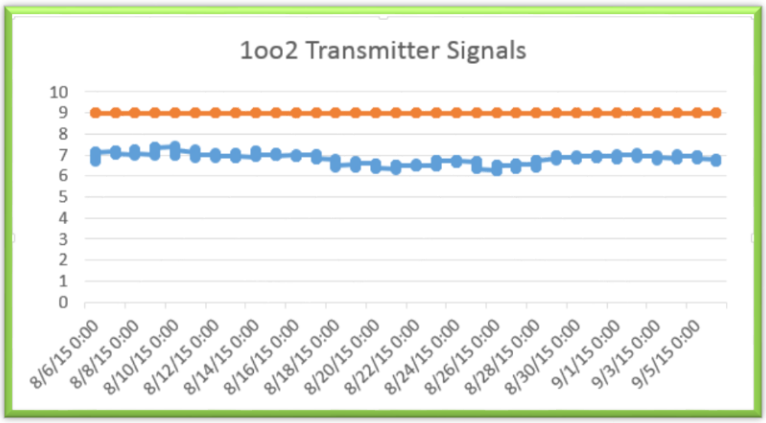


Figure 13 - Diagnosing a "flat-lined" transmitter signal

Analyzer and Transmitter signals, or Process Variables (PV's) generally change over time. If the signal is not varying in any way over a period of time, the analyzer or transmitter may have developed a fault. Maintenance Inspection/ recalibration is appropriate - once diagnosed. This is a reminder why continuous "analog" signals from transmitters are more valuable than the on/off signals from discrete switches where only a test can reveal a "covert" fault.

Similarly, if a control input is regularly in fault or Bypass mode while being repaired, it seems reasonable that the likelihood of an initiating event is higher than if it's controlling properly.
Could this kind of data analytics, especially if continuously provided to operations, have diagnosed and escalated the issues at Buncefield ahead of time? If the high, high level sensor were a continuous signal and if the data were in the historian, and all signals were being continuously analyzed looking from a process safety perspective, then it seems possible that it could have.

While this is of particular interest to the site level staff, the division-level staff will want to ensure these problems do not persist long-term. Generally site-level needs detail to support the analysis while senior levels of the organization need enough detail to know the site–level staff is able to promptly manage any issues which are identified.

Closing the loop back to the PHA

All this data feedback takes effort. The first studies within Honeywell were all done using Excel spreadsheets and manual techniques. This was effective, but too time consuming to be sustainable in the long term without significant additional staff. The rise of analytical computer tools enables the comparisons to be done regularly and much less expensively than using automation engineers to sift through the historian data once per month looking for issues.

Still, it's not without an effort. In order for the analytic engines to find issues, they have to be configured with the expected behavior. The Cause and Effect Matrix can be used as a data entry tool once it has been created in Excel. But it has to be created, maintained and updated if anything changes. The tools to look for flat-lined transmitters have to be configured to know which transmitters are protecting against high severity scenarios and thus are important enough to monitor.

How can we convey the expected behavior of our critical control, alarm and interlock protection layers? Today we do it manually by reviewing the LOPA and "programming" the analytics tools to look how these critical systems are behaving. But a new set of tools is emerging to help set these expectations.

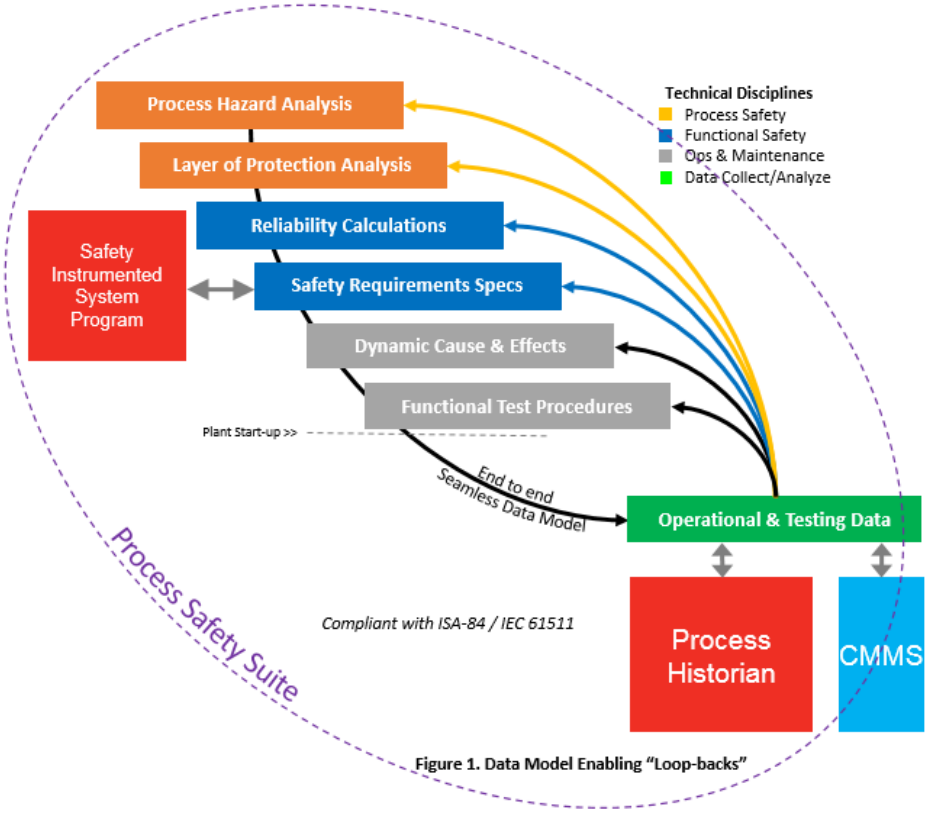


Figure 1. Data Model Enabling "Loop-backs"

The PHA and LOPA recording software can be used to manage this data. One such system is shown in the Figure above. This system is "programmed" by the PHA teams during the hazard reviews to understand the expected initiating even rate and the desired risk reduction factor for each barrier layer. The team needs to be diligent in recording control and interlock loop numbers properly so they can later be connected with the historian data, but the reward is significant. As with so many things today, bringing all this information into the digital realm enables much more to be done with it. The resulting "risk model" provides a real-time view into the actual risk on the site or at the division, regional or even the enterprise level.

CONCLUSION

The analysis shows that the data in the process and event historians can provide valuable insights into the actual safety of our operations as they stand today. Manual analysis showed that the design of the Safety Instrumented Functions looked at does provide the target amount of protection. In most cases the actual field performance of the SIFs also met target. However, a few did not. As it happened, this didn't matter as the Initiating Event Frequency was actually much better than anticipated by the

HAZOP/LOPA team. Nevertheless, analytics from field performance showed opportunities to improve the system in a few cases. The issues and opportunities were not apparent at first. Thus the analysis met it's intended purpose.

However, the manual analysis takes resources and time to complete. The addition of more advanced, and continuously-running computer analysis tools takes this into the realm of being practical to do all the time. And today's new enterprise-level integrated PHA/LOPA and SIL Calculation systems take this to the next level.

REFERENCES

1. IEC 61511 / ISA 84.00.01- Functional Safety – Safety Instrumented System for the Process sector
2. API RP 754 - Process Safety Performance Indicators for the Refining & Petrochemical Industries
3. OGP Process Safety – Recommended Practice on KPIs – Report # 456, Nov 2011
4. Occupational Safety and Health Administration (OSHA) Process Safety Management of Highly Hazardous Chemicals Regulation, 29 CFR 1910.119
5. CCPS "Guidelines for Integrating Management Systems and Metrics to Improve Process Safety" pp109

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Experimental Research on the Decontamination Effect of Aqueous Solutions Containing Organic Acids on the Release of Ammonia within Confined Space

Xuhai Pan*, M. Hua, X.H. Shen, J. Zhang, H.C. Jiang, X.M. Liang
College of Safety Science and Engineering
Nanjing Tech University, Nanjing 210009, China
*Presenter Email: xuhaipan@njtech.edu.cn

Abstract

Comparative tests between pure water curtain and water curtain which contains three CH_3COOH, $C_6H_80_7$, $C_4H_6O_5$ organic acids and surfactants were carried out in view of the release of ammonia in confined space. The results showed that the organic acids can promote the chemical decontamination effect of the water curtain on ammonia. The decontamination mechanism was physical absorption, air entrainment, physical block and chemical absorption. It was found that the addition of surfactant can improve the surface properties of the solution, reduce the surface tension, increase the contact area of the water curtain and ammonia, and efficiently promote the physical and chemical effect of the water curtain which contains organic acid additive. The causticity of organic additives was tested, and the results showed that three CH_3COOH, $C_6H_80_7$, $C_4H_6O_5$ organic acids have faint corrosive effect on the surrounding facilities.

Keywords: Ammonia, Water curtain, Decontamination mechanism, organic additives, corrosive effect

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Numerical Modelling for Effect of Water Curtain in Mitigating Toxic Gas Release

Dong Seok Min, Eui-young Oh, Seungho Jung
Department of Environmental and safety Engineering, Ajou University
Suwon, Republic of Korea
E-mail: processsafety@ajou.ac.kr

Abstract

As the chemical industry has developed, the use of toxic substances has increased, and leakage accidents have increased. Among various substances, hydrogen fluoride (HF) and ammonia (NH_3) are representative materials for the study since both are hazardous and important in the chemical industry. HF is a strong, pervious substance that is a stimulates on the body, respiratory system, and skin. HF is widely used in electronics manufacturing as a polisher and disinfectant. Since an HF release accident occurred in Gumi, S. Korea (2012) the Korea Occupational Safety and Health Agency (KOSHA) has emphasized that special attention and management is needed with respect to this toxic substance. NH_3 is widely used in the semiconductor industry and chemical processes. There have been about 20 large accidents regarding NH_3 around the world in last 10 years.

In this study, ANSYS Fluent, a computational fluid dynamics (CFD) program, was used to identify the effect of a water curtain as a mitigation system for toxic substances that are leaked from industrial facilities. Simulations were conducted to analyze how effectively a water curtain mitigated the dispersion of toxic substances. To verify the accuracy of the simulation, Goldfish experiment and INERIS Ammonia dispersion experiment were simulated and compared. Various water curtains were applied to the simulated field experiment to confirm the mitigation factors of toxic substances. The results show that the simulations and experiments are consistent and that the dispersion of toxic substances can be mitigated by water curtains.

1. Introduction

As the chemical industry has developed, the use of toxic substances has increased, and leakage accidents have increased. Among various substances, HF and NH_3 are representative materials for the study since both are hazardous and important in the chemical industry. HF is a strong, pervious substance that is a stimulates on the body, respiratory system, and skin. HF is widely used in electronics manufacturing as a polisher and disinfectant. Since an HF release accident occurred in Gumi, S. Korea (2012) the Korea Occupational Safety and Health Agency (KOSHA) has emphasized that special attention and management is needed with respect to this toxic substance. NH_3 is widely used in the semiconductor industry and chemical processes. There have been about 20 large accidents regarding NH_3 around the world in last 10 years [1-3].

In order to mitigate the impact from accidental releases of toxic chemicals, there are various systems equipped in the facilities such as dikes, secondary barriers, steam curtains, and water curtains. Among these, water spray system is known to effectively decrease the gas concentrations and prevent the movement of vapor cloud in the atmosphere after accidental toxic gas releases. To verify the effectiveness of water spray system, several researches have been undertaken with various field tests as well as Computational Fluid Dynamics (CFD). Dandrieux et al. (2001) verified the mitigation effect when using water curtains of the peacock tail type for 0.25 kg/s release rate of ammonia gas. Bouet et al. (2005) did 15 times of field test with physical barriers and water curtains for ammonia as well. [4, 5]. Kim et al. (2012) experimented LNG dispersions with the full cone type water spray curtains and compared the concentrations near the release source with CFD dispersion simulations. Cheng et al. (2014) also did field test for ammonia to compare CFD simulation results with the experiments [6, 7].

However, in these previous researches, the effectiveness to mitigate gas dispersions are significantly different for the peacock tail type. Dandrieux et al. (2001) showed very high mitigation efficiency in his experiment but there is almost no effect in the research of Bouet et al. (2005). It is mostly because;

1. Toxic gases were through water spray curtain area due to the high jet momentum.
2. Water spray curtain shape changed due to metrological conditions.

In this study, it is simulated to know the effectiveness of water spray curtains for accidental HF and NH_3 release cases using ANSYS Fluent 18.0. Also we analyzed how the precious two researched have to be judged [8]. Simulations were conducted to analyze how effectively a water curtain mitigated the dispersion of toxic substances. To verify the accuracy of the simulation, Goldfish experiment and INERIS Ammonia dispersion experiment were simulated and compared. After validation with field experiments, in order to avoid the concentration change of atmospheric condition, the meteorological conditions were fixed concentration was compared with the presence or absence of the water spray curtain. Various water spray curtains were applied to the simulated field experiment to confirm the mitigation factors of toxic substances. The results show that the simulations and experiments are consistent and that the dispersion of toxic substances can be mitigated by water curtains [9, 10].

2. Numerical simulation

ANSYS Fluent 18.0 is a program based on Navier-Stokes equations and capable of carrying out the physical modeling of fluid flow. In this study, we were to solve the relations of gas and water droplets so that we used Eulerian-Lagrangian method. We defined the problem as the steady state and solved it using Semi-Implicit Method for Pressure-Linked Equation method solver (SIMPLE).

2.1.Gas flow modeling

The governing equations are mass conservation, momentum conservation and energy conservation [11]. The equation for mass conservation can be written as follow;

$$\frac{\partial \rho}{\partial \mathrm{t}} + \boldsymbol{\nabla} \cdot (\rho \mathbf{u}) = 0 \tag{1}$$

Where ρ is the fluid density. Which can be expanded as follow;

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} = 0 \tag{2}$$

The equations for momentum conservation can be written as follows;

$$\frac{\partial (\rho u)}{\partial t} + \boldsymbol{\nabla} \cdot (\rho u \mathbf{u}) = -\frac{\partial p}{\partial x} + \boldsymbol{\nabla} \cdot (\mu \boldsymbol{\nabla} u) + S_{Mx} \tag{3}$$

$$\frac{\partial (\rho v)}{\partial \mathrm{t}} + \boldsymbol{\nabla} \cdot (\rho v \mathbf{u}) = -\frac{\partial p}{\partial y} + \boldsymbol{\nabla} \cdot (\mu \boldsymbol{\nabla} v) + S_{My} \tag{4}$$

$$\frac{\partial (\rho w)}{\partial t} + \boldsymbol{\nabla} \cdot (\rho w \mathbf{u}) = -\frac{\partial p}{\partial z} + \boldsymbol{\nabla} \cdot (\mu \boldsymbol{\nabla} w) + S_{Mz} \tag{5}$$

The above equations are for the conservation of momentum for x, y, z axis. μ is the viscosity term and S_{Mx}, S_{My}, S_{Mz} are terms for volumetric influences. The equation for energy conservation is as follow;

$$\frac{\partial (\rho i)}{\partial t} + \boldsymbol{\nabla} \cdot (\rho i \mathbf{u}) = -p \boldsymbol{\nabla} \cdot \boldsymbol{u} + \boldsymbol{\nabla} \cdot (k \boldsymbol{\nabla} T) + \Phi + S_i \tag{6}$$

2.2.Atmospheric boundary condition

For the atmospheric boundary condition, the wind power law relationship between the wind speeds at one height and those at another is written in eqns (7-10) which depend upon atmospheric stability [12].

$$U(z) = U(z_1) \times \left(\frac{z}{z_1}\right)^p \quad (7)$$

$$k(z) = \frac{(U^*)^2}{\sqrt{C_\mu}} \quad (8)$$

$$\varepsilon(z) = \frac{(U^*)^3}{\kappa z_1} \quad (9)$$

$$U^* = \left(\frac{\kappa\big(U(z_1)\big)}{\ln\left(\frac{z_1}{z_o}\right)}\right) \quad (10)$$

Where U is the wind speed, U* is sheared wind spend and κ is von karman constant of which value is 0.4 set for this study. z_1 is the known wind speed at a reference height and z_o is the surface roughness factor. We have used 0.1 as z_o for the C air stability class and 0.14 for the D air stability class as recommended by the EPA [13].

In this simulation, the realizable k-ε was employed for turbulence model. This model is the modified version of the standard k-ε turbulence model and improves to better predict the spreading rate of both planar and round jets. The standard turbulence model is based on separate transport equations for the turbulence kinetic energy (k) and its dissipation rate. The realizable k-ε model equations are described as follows [14]:

$$\frac{\partial}{\partial t}(\rho k) + \frac{\partial}{\partial x_j}(\rho k U_i) = \frac{\partial}{\partial x_j}\left[\left(\mu + \frac{\mu_t}{\sigma_k}\right)\frac{\partial k}{\partial x_j}\right] + G_k + G_b - \rho\varepsilon - Y_M + S_k \quad (11)$$

$$\frac{\partial}{\partial t}(\rho\varepsilon) + \frac{\partial}{\partial x_j}(\rho\varepsilon U_i) = \frac{\partial}{\partial x_j}\left[\left(\mu + \frac{\mu_t}{\sigma_\varepsilon}\right)\frac{\partial \varepsilon}{\partial x_j}\right] + \rho C_1 S\varepsilon - \rho C_2 \frac{\varepsilon^2}{k + \sqrt{\nu\varepsilon}} + C_{1\varepsilon}\frac{\varepsilon}{k}C_{3\varepsilon}G_b + S_\varepsilon \quad (12)$$

$$C_1 = \max\left[0.43, \frac{\eta}{\eta + 5}\right], \eta = S\frac{k}{\varepsilon}, S = \sqrt{2S_{ij}S_{ij}} \quad (13)$$

where G_k and G_b represent the generation of turbulence kinetic energy due to the mean velocity gradients and buoyancy, respectively; Y_M represents the contribution of the fluctuating

dilatation in compressible turbulence to the overall dissipation rate; μ is the molecular viscosity; μ_t is the turbulence viscosity; C_2, $C_{1\varepsilon}$ are constants; σ_k and σ_ε are the turbulent Prandtl numbers for k and ε, respectively. S_k and S_ε are the increasing rate by the source.

2.3.Water spray curtain modeling

The discrete phase model (DPM) was used to analyze the relationship between water spray curtain and toxic gas dispersions. DPM Eulerian-Lagrangian frameworks are the approach for CFD simulation of multiphase systems, and toxic gas (continuous phase) is solved by Eulerian method, and water droplet (discrete phase) is solved by Lagrangian. The equations for that are as follows in eqns (14-16);

$$\frac{d\boldsymbol{u_p}}{dt} = \frac{\boldsymbol{u} - \boldsymbol{u_p}}{\tau_r} + \frac{\boldsymbol{g}(\rho_p - \rho)}{\rho_p} + \boldsymbol{F} \tag{14}$$

$$\tau_r = \frac{\rho_p d_p^2}{18\mu}\frac{24}{C_d \mathrm{Re}} \tag{15}$$

$$\mathrm{Re} \equiv \frac{\rho d_p |\boldsymbol{u_p} - \boldsymbol{u}|}{\mu} \tag{16}$$

Where u is the fluid speed, u_p is the particle speed, μ is the fluid viscosity, ρ is fluid density ρ_p is the particle density, and d_p is the diameter of the particle.

The specification of water spray curtains were set based on INERIS tests performed in 2005. The peacock tail type has 1200 liter/min of water flowrate at 8 barg and the water droplet temperature is assumed to be the atmospheric temperature and the diameter of water droplets are calculated based on Britter's (2011) equation [16].

$$d_{pm} \equiv We_C \frac{\sigma}{\rho g u_{rel}^2} \tag{17}$$

We_C is Weber number and ρ_g is the density of surround gas. u_{rel} is the relative speed between the water jet and gas, d_{pm} is the average droplet diameter and σ is surface tension of the droplets. The more detailed of water spay curtain is in Table 1.

Table 1 Simulation specification of water spray curtain

DPM Input Data	
Parameter	Input Data
Injection type	Surface (semicircular ring)
Nozzle size (mm)	Radius : 70, width : 10
Water flow rate (kg/s)	19.9013
Droplet Diameter (μm)	935
Initial Droplet Velocity (m/s)	46

2.4.Actual field test used in validation

We used Ammonia large scale atmospheric dispersion experiments at INERIS from 1996 to 1997 for comparison of actual experiment with NH_3 and CFD simulation. Out of 15 total trials conducted in accordance with the size, height, direction of the leak and presence of protection devices, we have chosen 4th test for the reference and 11th test for two peacock tail type water sprays for comparing with the simulation. The two water sprays had been installed at 60 meters away from the source. In the experiment, compressed liquefied NH_3 was discharged from the pipe at a height of 1 m from the ground and was vaporized and diffused. The concentrations of liquefied NH_3 were measured by sensors installed at 20 m, 50 m, 100 m, 200, 500 m.

We have selected the Goldfish experiment conducted in 1986 in Frenchman, Nevada in the USA for the comparison of the actual experiment and the simulation was. In this experiment, which consists of three trials with different conditions as shown in Table 3, the compressed liquid HF was discharged through the pipe at a height of 1 m to the ground. The liquefied HF was vaporized and spread in the downwind direction in the form of steam clouds, and the concentrations were measured by sensors installed at 300 m, 1000 m, and 3000 m from the leak source.

Table 2 Information of Ammonia large scale atmospheric dispersion experiment

No.	Mass flow rate (kg/s)	Wind speed at 7 m (m/s)	Air stability	Temperature (℃)	Relative humidity (%)
4	4.2	3	D	12.5	82
11	3	5	C	24	24

Table 3 Information of Gold fish experiment

No.	Mass flow	Wind speed	Air stability	Temperature	Relative

	rate (kg/s)	at 2 m (m/s)		(℃)	humidity (%)
1	27.67	5.6	D	37.1	4.9
2	10.46	4.2	D	36.1	10.7
3	10.27	5.4	D	34.1	17.7

2.5.Simulation specification

For all comparisons, we unified the atmospheric conditions in order to minimize the variables. Actually, the temperature was about 5 to 24°C and the humidity was about 20 to 90% in the NH_3 field test. In the HF test, the experiment was conducted in a little bit higher temperatures and lower humidity. Since the tendency of gas diffusion differs greatly according to temperature and humidity, it was fixed at 25 ℃ and 50%. In the NH_3 and HF field tests, the different parts of the wind speed and reference height were set at 10 m height to 3 m/s and the atmospheric stability was applied to D class.

The following scenarios were set up to compare the effect of water spray curtain reduction on NH_3 leaks. First, in the INERIS field test, two water spray curtains were installed 6.5 m apart from the center line, but in this study, it was installed in the center line so that the toxic gas could contact the water spray curtain as much as possible. Based on this, we set up three different scenarios as follows;

1. Installed at 30 m and 60 m from the source simultaneously
2. Installed at 30 m
3. Installed at 60 m

In order to confirm the difference in efficiency of water spray curtain in existing field tests, we conducted the experiments with Dandrieux et al. (2001) at 0.15 m height, 0.25 kg / s mass flow rate and 5 m water spray curtain based on the test, we added a small scale simulation (W5). In HF, the leakage source and leakage were kept the same as the field test, and the other conditions were set the same as the ammonia large scale simulation.

ANSYS Design Modeler 18.0 was employed to generate the geometry for atmospheric diffusion modeling. The size of the external flow region is W × D × H = 580 × 80 × 40 m3 in the large scale simulation, width (W) × depth (D) × height (H) = 850 × 100 × 50 m3 in the validation case, In the small scale simulation, W × D × H = 100 × 40 × 20 m 3. As shown in Figure 1, the boundary conditions are the velocity inlet at the air inlet, the side and top, respectively, and the outflow boundary conditions at the outlet. The ground are set to be the wall boundary condition and the mass flow inlet is applied to the horizontal leakage source.

The mesh generation was performed by a polyhedral mesh using a meshing program and fluent meshing provided by ANSYS. A polyhedral lattice refers to a lattice created by dividing a flow region into polyhedral. The polyhedral grating can shorten the analysis time compared to the existing tetrahedral or hexahedral meshes, and can be produced with equal or better accuracy, and the grating generation time can also be shortened [17].

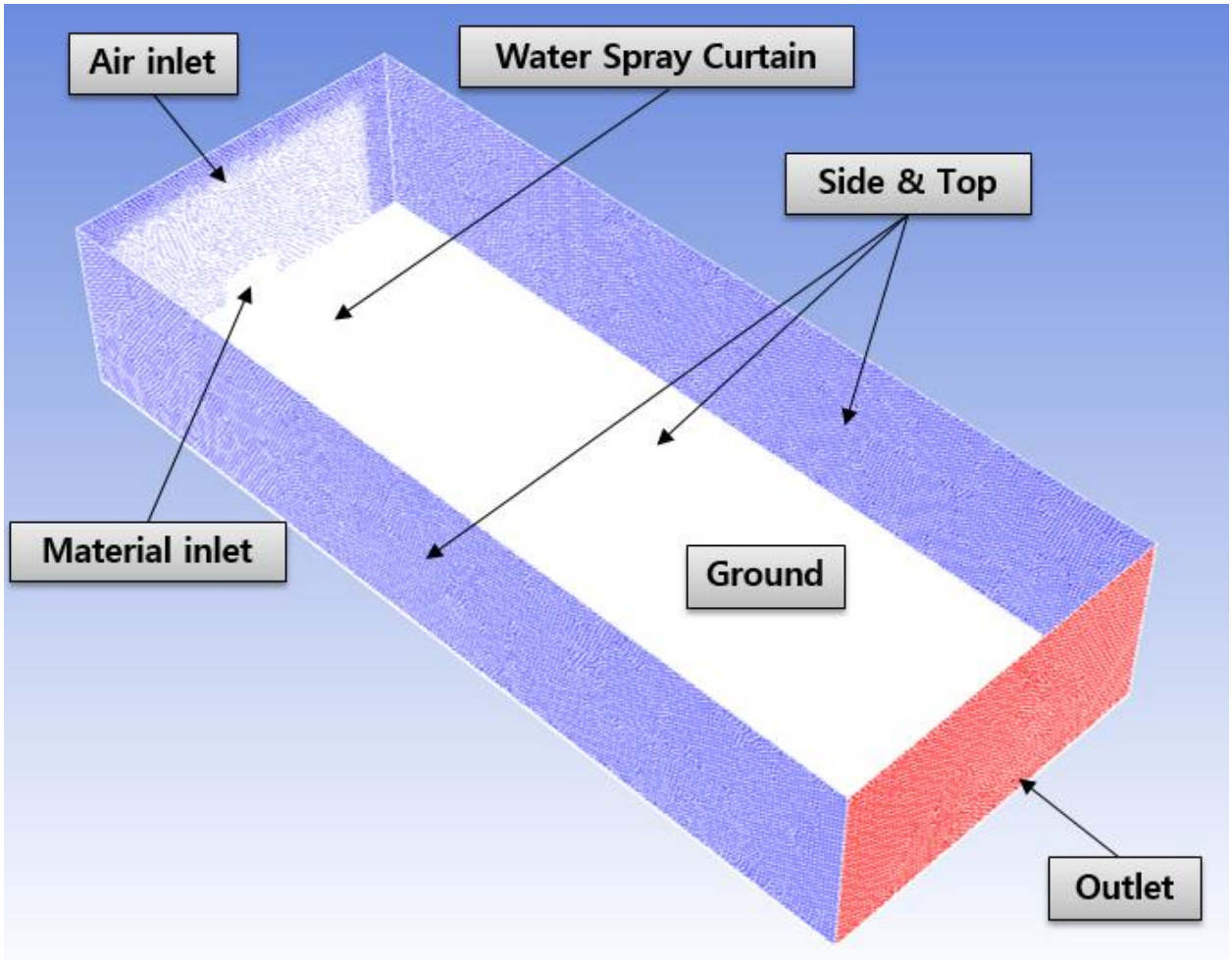


Figure 1. 3D Geometry and boundary condition of small scale simulation

3. Results

3.1. Comparison with field experiment

3.1.1. Comparison with ammonia field experiment

The results both of the field test for ammonia leaks and the simulation results are shown in Table 4. From the comparison of the concentrations for 6 locations at 1 m height, the differences between the reference (test # 4) and the simulation were between 71% and 117%. The difference of concentration was about 30% at the nearest (20 m) of the measurement points and within 20% at 50 m and 800 m. The difference between test #11 with the water spray curtain and the simulation occurred from as little as 68% to as much as 200%.

The comparison also showed that the difference in concentration was about 30% compared to the experiment at 20 m and within 10% of the experimental data up to 500 m. However, at 800 m, the concentration difference of the experimental versus simulation suddenly rose to 100%. Therefore, it was concluded that the efficiency of water spray curtain was effective up to 500 m in large scale simulation. Based on this, the analysis domain was defined.

Table 4 Comparison with field test and simulation for NH_3

Downwind Distance (m)	Test No. 4			Test No. 11		
	Experiment (ppm)	Simulation (ppm)	Ratio (Sim./Exp.)	Experiment (ppm)	Simulation (ppm)	Ratio (Sim./Exp.)
20	65000	46000	0.71	65000	44000	0.68
50	27000	27000	1.00	27000	25000	0.93
100	16000	17000	1.06	15000	13000	0.87
200	10000	8900	0.89	3500	3700	1.06
500	1200	1400	1.17	300	280	0.93
800	500	500	1.00	80	160	2.00

3.1.2. Comparison with hydrogen fluoride field experiment

Table 5 shows the comparison of simulation data with test #1 of Goldfish (HF leak) field test. Simulation results ranging from 300 m to 3000m showed similar trends to field tests, which is generally low in simulation results. Simulation results show that the concentration of 52% compared to the experiment at a distance of 300 m from the source of leakage, the concentration of 59% compared to the experiment at 1000 m, and the concentration of 56% compared to the experiment at 3000 m. Based on this, the model used for comparison with the water spray curtain field test results of ammonia was applied to HF as well.

Table 5 Comparison with field test and simulation for HF

Downwind Distance (m)	Test No. 1		
	Experiment (ppm)	Simulation (ppm)	Ratio (Sim./Exp.)
300	25473	13273	0.52
1000	3098	1842	0.59
3000	411	232	0.56

3.2.Mitigation efficiency of water spray curtain

The reduction effect of water spray curtain was investigated after verifying the simulation of NH_3 and HF with actual experiments. The reduction efficiency of the water spray curtain was calculated as shown in equation (18).

$$\text{Efficiency} = 1 - \frac{C_{w.}}{C_{No\,W.}} \tag{18}$$

$C_{W.}$ Is the concentration when water spray curtain is used and $C_{No\,W.}$ is the concentration when water spray curtain is not used. In the large scale simulation of NH_3, the concentration was measured at a height of 1 m from the ground. As a result, the reduction effect was observed at a distance of 100 m or less from the water spray curtain as shown in figure 2. However, as the measurement distance increases, the efficiency gradually decreases. When the distance reaches a certain distance, the efficiency becomes negative. Efficiency increases again after a certain distance. This is the same trend as the result of the INERIS ammonia leak field test.

In the large scale simulation of NH_3 of which concentrations were measured at a height of 1 m from the ground, the reduction effect was observed at 100 m or less from the water spray curtain as shown in Figure 2. However, as the measurement distance increases, the efficiency gradually decreases. When the distance reaches a certain distance, the efficiency becomes negative. The efficiency increases again after a certain distance, which showed the same trend as the INERIS ammonia leakage field test.

The efficiency of the water spray curtain installed only at 60 m was slightly higher when the water spray curtain was installed only at 30 m behind the leak source. Nevertheless, the overall reduction effect of toxic gases by water spray curtains was less than 20%. However, when the water spray curtain was installed both at 30 m and 60 m simultaneously, the efficiency becomes a bit better. Section where the reduction efficiency became negative is reduced.

The large scale simulation results of HF showed that the reduction effect did not occur near the water spray curtain as shown in figure 3, but the effect was increased as the distance

increased. The efficiency was less than 10% within 100 m from the leak source, but it increased gradually to approximately 30% at 500 m.

The efficiency of water spray curtain only at 30 m was higher than that of water spray curtain only at 60 m. The water spray curtains installed both at 30 m and 60 m were not significantly different from the water spray curtain installed only at 30 m.

In the small scale simulation of NH_3, the results of measured concentration for the height from 15 cm to 100 m are shown in figure 4 and Figure 5. Although a certain tendency was not found, the reduction efficiency was about 40~50% after 20 m of distance. This is much higher reduction efficiency compared to the large simulations. The efficiency of the small-scale simulation of NH_3 was more than twice to the large-scale simulation in the entire distances.

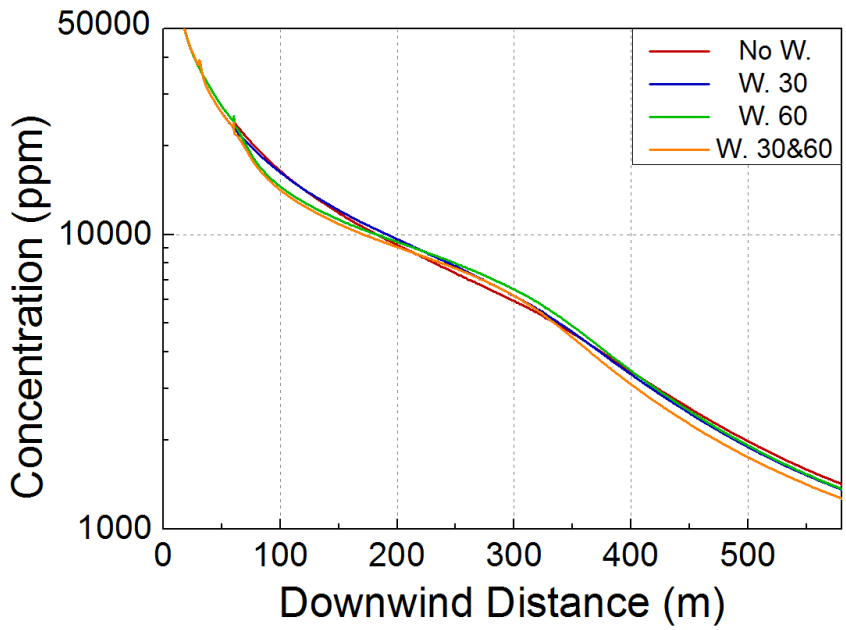


Figure 2. Variation of NH_3 concentration according to downwind distance by water spray curtain at large scale simulation

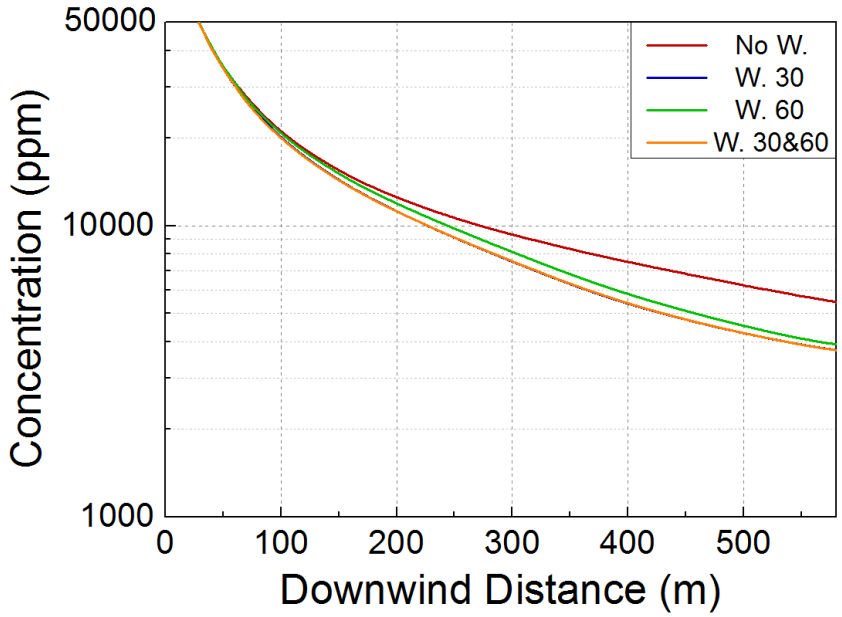


Figure 3. Variation of HF concentration according to downwind distance by water spray curtain at large scale simulation

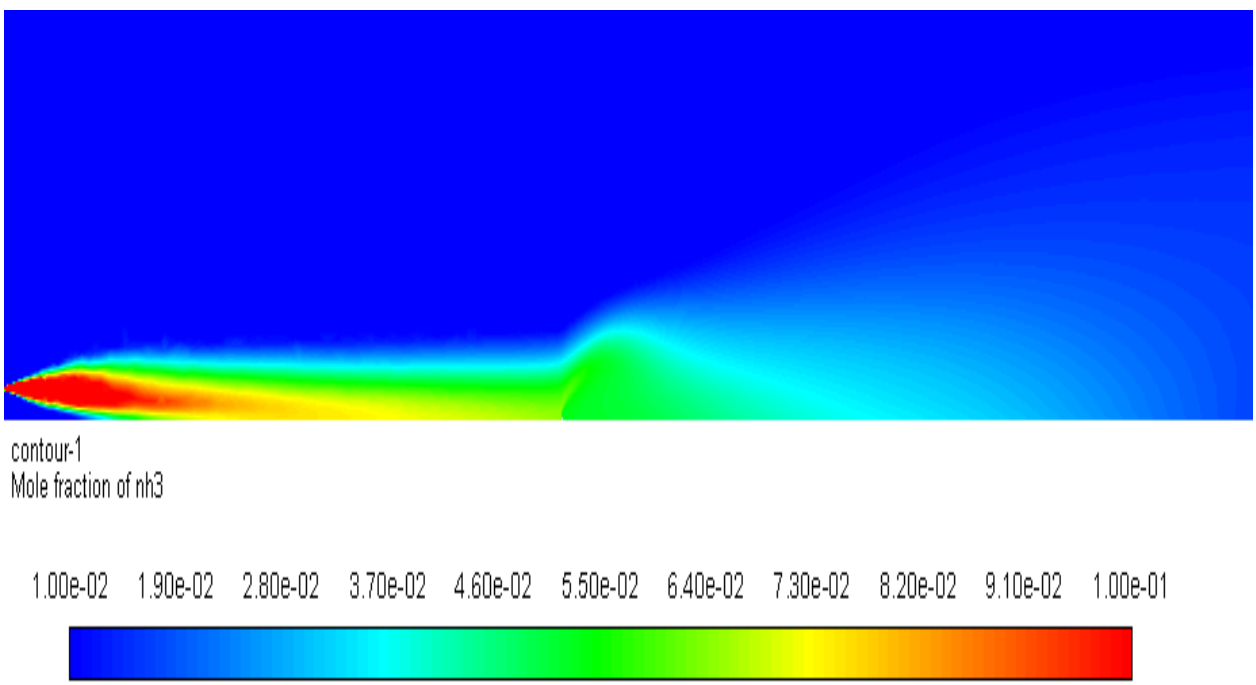


Figure 5. Mitigation effect contour of NH_3 concentration according to downwind distance by water spray curtain at 5 m

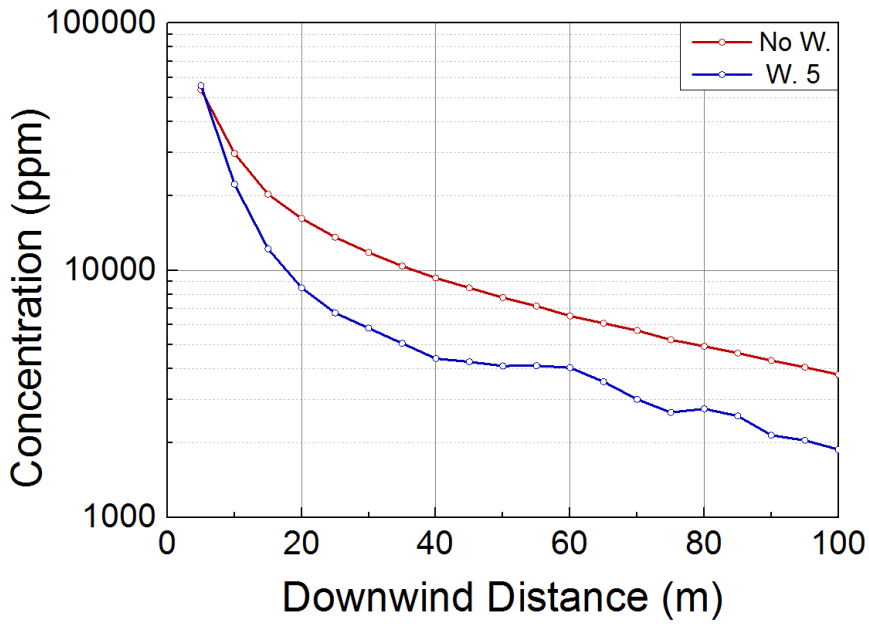


Figure 5. Variation of NH_3 concentration according to downwind distance by water spray curtain at small scale simulation

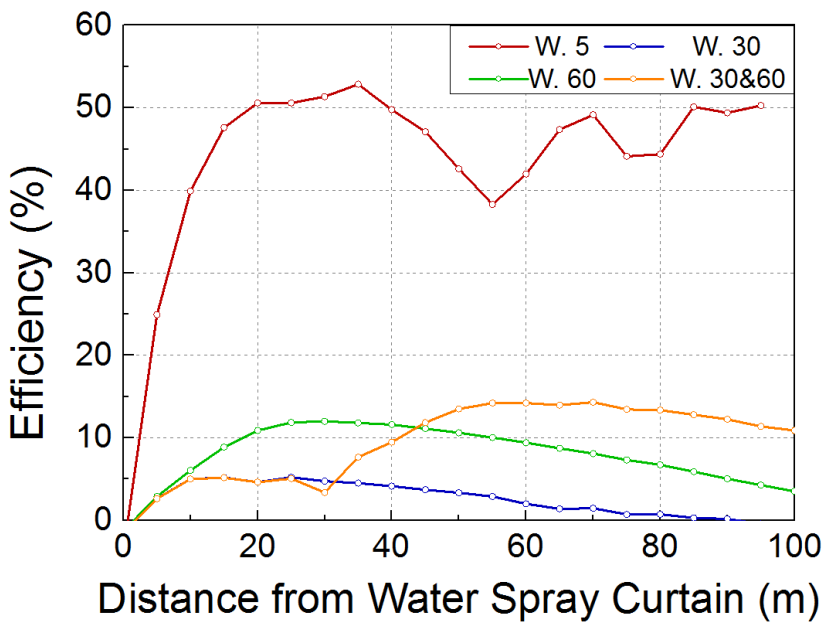


Figure 6. Efficiency water spray curtain according to distance from installation location at small scale simulation and large scale simulation

4. Conclusion

In this study, the effects of NH_3 and HF leakages with the peacock tail type water spray curtain were verified by simulations using computational fluid dynamics. We found the following results by analyzing the reduction efficiency of water spray curtain through the large scale simulation of NH_3 and HF and the small scale simulation of NH_3.

First, the efficiency difference of the water spray curtain of ammonia occurred according to the position of the leakage source. The closer to the point where the gas release source is from the water curtain, the more the concentration of the toxic material vapor is reduced by the physical effect.

The difference in the effect of water spray curtain according to the type of material was also confirmed. In the large scale simulation, the water spray for NH_3 shows good efficiency at a short distance and then declines with the distance. On the other hand, the efficiency for HF tended to increase with distance from water spray curtain in large scale simulation. The reason for this difference is thought to be the density difference of the material. Because of the low boiling point and the high molecular weight of NH_3 in the leaking state at the boiling point of the material, NH_3 with a high density was relatively less affected by the water spray curtain.

These results show that different applications of the water spray curtain are required depending on the type of material and the leakage distance. In this simulation, when the water spray curtain was applied to the NH_3 release, the reduction efficiency occurred at the relatively far distances over 400 m. Therefore, in this case, it is necessary to install the water spray curtain in a proper position in order to check the efficiency of the water spray curtain.

One of the applications is to install water spray curtains on the dike or physical barriers installed around the hazardous chemical storage facilities. In the case of water-reactive chemical or water-prohibiting substance, it should not be applied. This study would help how to install the water spray curtain in the optimal place depending on materials and situations in case of hazardous chemical accidents.

References

1. Bae, C.A., Chung, S.T., *A study on Awareness of Risks and Countermeasures for Chemical Accidents among Residents near Chemical Plants*. Crisisonomy, 2017. **13**(5): p. 123-134.

2. Anjana, N.S., Amarnath, A., Harindranathan Nair, M.V., *Toxic hazards of ammonia release and population vulnerability assessment using geographical information system*. Journal of Environmental Management, 2018. **210**: p. 201-209.

3. Yang, S., Jeon, K., Kang, D., Han, C., *Accident analysis of the Gumi hydrogen fluoride gas leak using CFD and comparison with post-accidental environmental impacts. Journal of Loss Prevention in the Process Industries*, 2017. **210**: p. 207-215.

4. Dandrieux, A., Dusserre, G., Ollivier, J., Fournet, H., *Effectiveness of water curtains to protect firemen in case of an accidental release of ammonia: comparison of the effectiveness for two different release rates of ammonia*. Journal of Loss Prevention in the Process Industries, 2001. **14**: p. 349-355.

5. Bouet, R., Dupletuer, S., Salvi, O., *Ammonia large scale atmospheric dispersion experiments in industrial configurations*. Journal of Loss Prevention in the Process Industries, 2005. **18**: p. 512-519.

6. Kim, B.K., Ng, D., Mentzer, R.A., Mannan, M.S., *Modeling of Water-Spray Application in the Forced Dispersion of LNG Vapor Cloud Using a Combined Eulerian−Lagrangian Approach*. Ind. Eng. Chem. Res., 2012. **51**: p. 13803−13814.

7. Cheng, C., Tan, W., Liu, L., *Numerical simulation of water curtain application for ammonia release dispersion. Journal of Loss Prevention in the Process Industries*, 2014. **30**: p. 105-112.

8. Chung, T.J., Computational Fluid Dynamics, 2002.

9. Goldwire, H.C., McRae, T.G., Johnson, G.W., Hipple, D.L., Koopman, R.P., McClure, J.W., Morris, L.K., Cederwall, R.T., *Desert Tortoise series data report: 1983 pressurized ammonia spills*, UCID-20562. Lawrence Livermore National Laboratory, 1985. Livermore, CA.

10. Blewitt, D.N., Yohn, J.F., Ermak, D.L., *An evaluation of SLAB and DEGADIS heavy gas dispersion models using the HF spill test data*. Proc. Int. Conf. on Vapor Cloud Modeling, 1987. AIChE, New York. p. 56-80.

11. Versteeg, V.K., Malalasekera, W., *An Introduction to Fluid Dynamics*. 1999. 2nd edition.

12. Blocken, B., Stathopoulos, T., Carmeliet, J., *CFD simulation of the atmospheric boundary layer :- wall function problems. Atmospheric Environment*, 2007. **41**(2): p. 238-252.

13. EPA, *RMP consequence analysis guidance*. 1996.

14. Shih, T.H., Liou, W.W., Shabbir, A., Yang, Z., Zhu, J., *A New k - ε Eddy-Viscosity Model for High Reynolds Number Turbulent Flows - Model Development and Validation*. Computers Fluids, 1995.**24**(3): p. 227–238.

15. Gosman, A.D., Ioannides, E., *Aspects of computer simulation of liquid-fuelled combustors*. J. Energy, 1983. **7**(6): p. 482-490.

16. Britter, R., Weil, J., Leung, J., Hanna, S., *Toxic industrial chemical (TIC) source emissions modeling for pressurized liquefied gases*. Atmospheric Environment, 2011. **45**: p. 1-25.

17. Symscape, Polyhedral, *Tetrahedral, and Hexahedral Mesh Comparison*. 2013. https://www.symscape.com/polyhedral-tetrahedral-hexahedral-mesh-comparison.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Risk Based Process Safety for Semiconductor Fabrication Operations

Steve Hawkins[1], Chris Israni[2]
ERM Midwest & ERM Gulf
[1]ERM Midwest - 9825 Kenwood Road, Suite 100, Cincinnati, Ohio 45242, USA &
[2]ERM Gulf - 840 West Sam Houston Parkway, Suite 600, Houston, Texas 77024, USA
Email: Steve.Hawkins@erm.com, Chris.israni@erm.com

Abstract

Most semiconductor manufacturing facilities do not contain quantities of highly hazardous chemicals in threshold quantities sufficient to be subject to the Occupational Health and Safety Administration's (OSHA) Process Safety Management (PSM) regulations. However, some organizations are applying Risk Based Process Safety (RBPS) concepts as a systematic means to not only ensure EHS risks are identified and quantified, but also to strengthen overall business performance and provide competitive advantages. Aging Fabrication facilities and infrastructure, their ever-increasing production demands, rapid innovation and need for process modifications are also business drivers for RBPS. The core RBPS concepts not only provide a holistic approach to protect employees from catastrophic accidents and releases; but in most cases also drive production efficiencies, increase equipment/tool reliability and life span, promote quality improvements, and enhance business continuity measures. This is accomplished by application of a wide range of process safety management elements, as applicable to semiconductor operations, which fall under the following four basic pillars of RBPS: Process Safety Leadership/Commitment; Risk Assessment/Identification; Risk Management; and Learning and Continuous Improvement. This session will discuss the basic concepts of RBPS, including a brief review of the 20 elements as provided by the Center for Chemical Process Safety (CCPS) framework, and present the benefits of developing and implementing process safety management systems for semiconductor processes. Case studies will be presented, as applicable, to detail the advantages, as well as the challenges, of RBPS for the semiconductor industry.

Keywords: Process safety, semiconductors, risk based process safety, risk management, risk identification

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Transient Large-Scale Chlorine Releases in the Jack Rabbit II Field Tests: Estimates of the Airborne Mass Rate for Atmospheric Dispersion Modeling

Tom Spicer*
Ralph E. Martin Department of Chemical Engineering
University of Arkansas, Fayetteville, AR
+1.479.575.6516

Graham Tickle
GT Science & Software Ltd.
Chester, UK

*Corresponding author: tos@uark.edu

Abstract

Sponsored by the U.S. Department of Homeland Security, the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense, and Transport Canada, the Jack Rabbit II tests were designed to release liquid chlorine at ambient temperature in quantities of 5 to 20 T for the purpose of quantifying the behavior and hazards of catastrophic chlorine releases at scales represented by rail and truck transport vessels. In 2015, five successful field trials were conducted in which chlorine was released in quantities of 5 to 10 tons through a 6-inch circular breach in the tank and directed vertically downward at 1 m elevation over a concrete pad. In 2016, three additional trials were conducted with releases of 10 tons also through 6-inch circular breaches at different release orientations. A final 20 ton test was conducted in 2016. Data from the test program is available. This paper summarizes assessment of the chlorine rainout and provides estimates of the mass of chlorine moving with the wind field as a function of time.

Introduction

Sponsored by the U.S. Department of Homeland Security, the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense, and Transport Canada, the Jack Rabbit II tests were designed to release liquid chlorine at ambient temperature in quantities of 5 to 20 T for the purpose of quantifying the behavior and hazards of catastrophic chlorine releases at scales represented by rail and truck transport vessels. In 2015, five successful field trials were conducted in which chlorine was released in quantities of 5 to 10 tons through a 6-inch circular breach in the tank and directed vertically downward at 1 m elevation over a concrete pad. In

2016, three additional trials were conducted with releases of 10 tons also through 6-inch circular breaches at different release orientations. A final 20 ton test was conducted in 2016. Data from the test program is available.

There are ongoing efforts to analyze data from the test program. One aspect of this analysis involves comparison of selected tests with predictions using available atmospheric dispersion models. For this comparison between atmospheric dispersion models to be most meaningful, it was desired to have a common set of model inputs including meteorological parameters and source parameters. This work represents the effort to prepare representative source parameters that can be applied in many different atmospheric dispersion models. Sections 1-5 below are summaries of previous work that analyze the test data (Spicer and Miller, 2018, and Spicer et al., 2018). Sections 6 and 7 discuss the extension of the present analysis to provide inputs for dispersion models used in the comparison exercise.

1. Liquid Volume as a function of Liquid Depth in the Disseminator

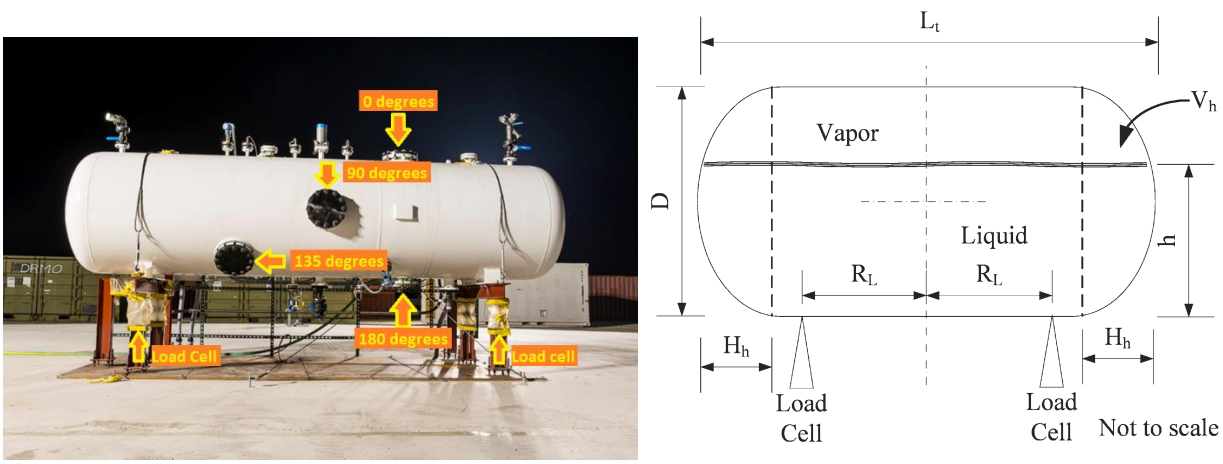


Figure 1. (a) Dissemination vessel on the 25 m concrete pad. (b) Schematic of the disseminator defining parameters.

The liquid volume (V_L) as a function of liquid depth in the vessel was calculated based on formulas (Couper et al., 2005) as follows,

$$V_h = \frac{\pi}{24} D^3 \tag{1}$$

$$V_L = (L_t - 2H_h)\left[\left(h - \frac{D}{2}\right)(Dh - h^2)^{1/2} + \left(\frac{D}{2}\right)^2 \cos^{-1}\left(\frac{D - 2h}{D}\right)\right] + 2\,V_h\left(\frac{h}{D}\right)^2\left(3 - \frac{2h}{D}\right) \tag{2}$$

where h is the liquid depth and D is the inner diameter of the cylindrical vessel, respectively (Figure 1b). The volume of one head is V_h, and the depth of each head is H_h (both quantities excluding the straight flange), so the length of the cylindrical middle is $L_t - 2\ H_h$ where L_t is the tangent-to-tangent internal tank length. For a 2:1 semi-elliptical head as specified for the dissemination vessel used here, the volume V_h of a single head is given by the formula above, and the head depth H_h is D/4. As written above, the formula for V_L is suitable for all values of h including the full volume (h = D). Using a tangent-to-tangent internal length of 5.61 m (221 in) and inside diameter of 1.35 m (53.1 in) with a uniform shell thickness of 12.7 mm (0.5 in), the calculated vessel capacity is 7.70 m^3 (2034 gal). DPG measured the volume of the disseminator by filling it with a metered quantity of water and found the volume to be 7.65 m^3 (2020 gal). In the calculations that follow, a volume of 7.70 m^3 (2034 gal) will be used for the vessel volume.
.

2. Dynamic mass and thrust measurements

The load cell measurements provided the most consistent measurement of mass in the vessel under static conditions, and the load cell measurements can also be analyzed as a function of time. The vertical release ports were positioned with a moment arm away from the center of mass of the tank and its contents to determine dynamic mass separately from the release thrust. From a position facing into the (historic) mean wind direction and also facing the tank (consistent with the orientation in Figure 1), the load cells were designated as front (north side), back (south side), right (west side), and left (east side). The vertical release ports (0° and 180°) were located on the right (west side) centered 0.94 m (37 in) from the axial tank center (center of mass), and the 135° release port was located on the left (east side) side also centered 0.94 m (37 in) from the axial tank center. The horizontal release port (90°) was located on the axial tank center (but never used due to program limits).

Assuming any load cell deflection changes were small during the release, the sum of the vertical forces and torques (about the center of mass) are zero:

$$\sum F_z = 0 = Mg - d_m T_z - (\sum F_E + \sum F_W) \tag{3}$$

$$\sum \tau = 0 = T_z R_T + d_t(\sum F_W R_L - \sum F_E R_L) \tag{4}$$

where M is the mass of chlorine in the vessel, g is the acceleration due to gravity, T_z is the vertical thrust due to the jet release with moment arm R_T (0.94 m or 37 in), F_E and F_W are the load cell forces on east and west ends, respectively, with moment arm R_L (1.91 m or 75 in; see Figure 1b), and d_m and d_t are constants reflecting the release direction. d_t is chosen so that all thrust values are positive (-1 for 0° and 135° releases since those ports would create a clockwise rotation of the disseminator and +1 for 180° releases which would create a counter-clockwise rotation of the disseminator as pictured in Figure 1), and d_m reflects whether the thrust increases the load cell measurements (-1 for the 0° release since this force acts downward and +1 otherwise since these forces act upward). Equation 4 does not account for the vertical change of the center of mass as the vessel empties (which has been shown to result in small changes in liquid level along the axis of the disseminator). Also, the downward force due to atmospheric pressure on the top of the vessel opposite the jet is ignored. The load cell forces were tared with

measurements after the release was complete. The vertical thrust is found from Equation 4, and the chlorine mass from Equation 3. (The load cells measuring horizontal forces were not analyzed here.) There was some scatter associated with the processed data as was anticipated (particularly at the start of the release). In addition to the data acquisition system failure during Trial 5, load cell recorded values between (roughly) 38:59 and 39:02 during Trial 4 did not change indicating additional data acquisition problems. In Trial 6, data from the improved acquisition system show a sinusoidal variation which likely reflects (axial) liquid level variation in the disseminator (sloshing).

To determine the (essentially constant) average initial release rate, an averaging time period was used. The start of the time period was taken to be the last set of recorded values before the release, and the end of the time period was chosen to match the slope of the recorded mass as a function of time. The mass rate was calculated as the difference in mass between the beginning and end of the time period divided by the time period so that the derived values will match the mass remaining in the vessel. Table 1 summarizes these initial (constant) mass rates ($\dot{M}_i$) and the averaging time period.

Table 1. Jack Rabbit II Mass Release Parameters

Trial	Initial Mass (kg)	Initial Rate (kg/s)	Averaging Time for Initial Rate (s)	Inventory after Initial Rate (M_x) at Time t_x (kg @ s)	Time Constant τ_x (s)	Power p	Heel (kg)	Data Rate (Hz)
1	4,545	224	14	1,524 @ 13.5	6.80	1	0	1
2	8,192	273	23.4	1,968 @ 22.8	7.20	1	0	10
3	4,568	275	11.3	1,988 @ 9.39	7.24	1	0	10
4	7,017	271	20.7	1,784 @ 19.3	6.59	1	0	10
5	8,346	not available					0	10
6	8,391	260	24.9	1,779 @ 25.4	6.83	1	0	25
7	9,072	259	23.9	3,175 @ 22.7	10.5	1	446	25
8	9,120	170	3.12	8,591 @ 3.12	23.9	0.867	6,698	25
9	17,700	not available						

The time period when the initial mass release rate ($\dot{M}_x$) was (approximately) constant was followed by a period when the rate steadily declined. While the mass rate could be obtained directly from the data during this later period, this would be cumbersome in practice, so this interval was fit using standard least squares to:

$$(M - M_h) = (M_x - M_h)\, exp\left(-\left(\frac{t - t_x}{\tau_x}\right)^p\right) \tag{5}$$

where M_x is the inventory at time t_x, M_h is the release heel, and τ_x and p are parameters determined in the fitting process (in Trials 1-4, 6, and 7, p = 1 proved a sufficient fit of the data). Equation 5 can be differentiated to determine the mass rate as a function of time (as long as $p \geq 1$), but this rate so determined could create a discontinuity at time t_x with $\dot{M}_x$ because $M_x = M_i - \dot{M}_x t_x$ where M_i is the initial disseminator inventory. This issue can resolved by simultaneously fitting t_x and τ_x to the data using the values for $\dot{M}_x$ as obtained previously. Table 1 includes data obtained for all trials. It is important to note that the integrated dynamic mass measurements were consistent with (static) mass measurements before and after the release.

For Trial 7, the release port chosen was 45° below horizontal, and consequently, mass remained in the vessel (heel in Table 1) after the first (primary) release. As in the previous trials, the end of the primary release was modeled using Equation 5 up to t = 84.1 s when the remaining heel was slowly releasing chlorine due to heat transfer to the remaining (subcooled) liquid. The heel was taken to be the average chlorine mass remaining in the disseminator measured between 84.1 and 94.1 s. The remaining heel was dumped from the disseminator using a remotely operated valve at 11:07.43 (after the primary release was deemed to be complete at the time of testing). It is worth noting that the maximum amount of chlorine that could remain in the vessel after a release from this orientation is 686 kg (i.e., the potential inventory when the liquid level would be at the same elevation as the bottom of the release opening), and since only 446 kg (65%) was measured to remain, 35% of the potential inventory actually flashed during the primary release. Video records indicate that the chlorine leaving the disseminator at the end of the test was flashing as opposed to simply being pushed out of the vessel by liquid swell.

In Trial 8, the release was vertically upward with significant mass remaining in the vessel after the primary release. During the initial phases of the release, a vapor (only) release would be expected since the opening was in the vapor space. Based on choked ideal gas flow at the storage conditions, the mass release rate is predicted to be 39 kg/s, and prior to the release, the vapor space was 1.30 m^3, so the vapor space would have been emptied in about 0.6 s. In the video record, the initial speed of the release clearly decreases after about 0.6 s and becomes stable at around 2.4 s. The load cell data seemed to be more consistent after 3.12 s (slightly later than video observations), so the initial phase of the release (first 3.12 s) was modeled assuming a constant release rate. As in the previous trials, the end of the primary release was modeled using Equation 5 (with p = 0.867) up to t = 100 s when the remaining heel was slowly releasing chlorine due to heat transfer to the remaining (subcooled) liquid. The heel was taken to be the average chlorine mass remaining in the disseminator measured between 90 and 100 s. (Since $p<1$, $\dot{M}$ cannot be calculated at t_i using Equation 5, but a simple approximation would be to assume the constant rate $\dot{M}_i$ applies up to 3.146 s where Equation 5 can be differentiated and would be the same mass rate.) As in Trial 7, the remaining heel was dumped from the

disseminator using a remotely operated valve at 15:30.53. In Trial 8, the maximum amount of chlorine that could remain in the vessel after a release from this orientation was the tank inventory (in this case 9,122 kg); 6,698 kg (73%) was measured to remain, and consequently, 27% of the potential inventory actually flashed during the primary release.

3. Time Varying Mass Release Rate

As discussed above, the time period when the initial mass release rate ($\dot{M}_x$) was (approximately) constant was followed by a period when the rate steadily declined. Equation 5 can be differentiated to find the mass release rate (-dM/dt) as a function of time after t_x:

$$\left(-\frac{dM}{dt}\right) = \frac{(M_x - M_h)}{\tau_x}\, exp\left(-\left(\frac{t - t_x}{\tau_x}\right)^p\right) p \left(\frac{t - t_x}{\tau_x}\right)^{p-1} \tag{6}$$

which reduces to

$$\left(-\frac{dM}{dt}\right) = \frac{(M_x - M_h)}{\tau_x}\, exp\left(-\left(\frac{t - t_x}{\tau_x}\right)\right) \tag{7}$$

when p = 1 (in Trials 1-4, 6, and 7). To summarize, the mass release rate ($\dot{M}_R$) is given by:

$$\begin{aligned} \dot{M}_R &= \dot{M}_x && for\ t \le t_x \\ &= \left(-\frac{dM}{dt}\right) && for\ t > t_x \end{aligned} \tag{8}$$

where -dM/dt is given by Equations 6 or 7. Note that Equation 7 should be used for all trials except Trial 8.

4. Impact of Rainout and Subsequent Re-Evaporation

Temperature measurements from the 2015 test season indicated the liquid that rained out formed thin liquid puddles that evaporated while remaining at the liquid chlorine boiling point. There were indications that the force of the release pushed liquid that rained out toward the periphery of the pad (surface temperatures at Pad 2 near the release were consistent with direct exposure to the aerosol because the measured temperature was significantly colder than the chlorine boiling point).

Video recordings in the 2016 test season were less obstructed and provided an opportunity in Trial 6 to determine the area coverage of the liquid. Trial 6 is also worthwhile to study because the infrared video shows that the liquid was contained on the concrete pad (some potential, limited overflow to the gravel is indicated on the IR images). During the initial phase of the release from containment, the aerosol cloud effectively shields the rained out liquid from solar radiation or heating by the air, so the majority of heat transfer to the liquid is by conduction from the concrete pad (effectively modeled by conduction in a semi-infinite solid with a constant

surface temperature boundary condition). The IR video was not used because cold concrete cannot be easily distinguished from concrete covered by liquid.

The following assumptions are used in this analysis:

1. The total deposition is equal to the total mass evaporated by thermal conduction from the concrete slab.
2. Because the deposition process is driven by the primary release from containment, assume the deposition rate is proportional to the release rate over the duration of the deposition.
3. Heat conduction from the slab will exceed the deposition rate initially, but after a brief period ($t = t_e$), the rate of evaporation will be controlled by the rate of heat conduction from the concrete pad.
4. The time when deposition/rainout ends (t_d) must presently be determined from the video record. For Trial 6, the jet angle changes at about 38.83 s, but the color of the jet is unchanged (indicating the presence of aerosol continues). At 48.2 s, the color of the jet changes in a manner consistent with the initial phase of Trial 8 when the release begins as a vapor but makes the transition to aerosol, and this would correspond to $t_d = t_x + 3.34\tau_x$. Video from the other trials showed a similar transition ranging from $t_d = t_x + 3.09\tau_x$ (Trial 1) to $t_d = t_x + 3.56\tau_x$ (Trial 2). Based on the average of the vertically downward jet releases, assume that $t_d = t_x + 3.4\tau_x$. The transition seems to occur at a later time in Trial 7, so for this trial, $t_d = t_x + 3.7\tau_x$.
5. The concrete pad seems fully wetted (covered by liquid) up to $t_w = 41.4$ s as indicated by visible video frames when the first dry concrete can be observed. After 41.4 s, the area covered by liquid is observed to decrease in regions where the pad can be observed. The view of the concrete pad is unobstructed by vapor puffs after 50.2 s. (Assuming complete coverage by the liquid will tend to overestimate the evaporation because the Pad 2 temperature measurements from 2015 indicated that there was likely no liquid coverage near the release point caused by the force of the release. This region is also partially obscured at 41.4 s in the visible video. Pad 2 is at a radius of 4 m from the release, and if the area inside a radius of 4 m was not covered, this would represent 10% of the concrete pad area or a coverage of 0.9.) Based on the observations above, $t_w \approx t_x + 2.35\tau_x$.

To summarize, the evaporation rate is equal to the deposition rate from $t = 0$ to t_e. From $t = t_e$ to t_w, liquid covers a large portion of the concrete pad surface, and this area coverage is assumed to be approximately constant. After $t = t_w$, the visible area of the liquid covering the pad decreases in time until the last puddle has evaporated. Deposition occurs up to $t = t_d$. Based on the video record, the visible area of liquid covering the pad begins to decrease before the deposition is complete.

Under a constant surface temperature boundary condition, the heat flux from a solid can be calculated using Fourier's law

$$q''(t) = \frac{k\,\Delta T}{\sqrt{\pi\,\alpha\,t}} \tag{9}$$

where the temperature difference ΔT is $T_p - T_o$, and T_p is the pad temperature. The pad temperature was estimated from the average temperature over the 1 minute interval prior to the release at 3 mm below grade averaged over all three pad locations (provided data was available except Trial 1 when the measurements at 6 mm below grade were used since the 3 mm measurements were not available). Pad temperatures were 19.8 C, 24.2 C, 22.4 C, 22.4 C, 22.4 C, 22.9 C, 19.4 C, and 16.7 C for Trials 1-8, respectively. Provided that the area covered by liquid chlorine can be quantified as a function of time A(t), the total amount of heat transferred from the concrete Q(t) at time t is given by:

$$Q(t) = \int_0^t q''(t)\, A(t)\, dt = \int_0^t \frac{k\, \Delta T}{\sqrt{\pi\, \alpha\, t}}\, A(t)\, dt \qquad (10$$

Consequently, the total mass evolved or evaporated from the surface $M_e(t)$ is given by:

$$M_e(t) = \frac{k\, \Delta T}{\Delta H_v} \int_0^t \frac{A(t)}{\sqrt{\pi\, \alpha\, t}}\, dt \qquad (11$$

Based on the visible video analysis, the concrete pad area fraction covered by liquid is shown in Figure 2. The solid line indicates a best fit to an exponential decay (with time constant τ_e):

$$\begin{aligned} A(t) &= f_{a,0} A_p & 0 \le t \le t_w \\ &= f_{a,0} A_p e^{-(t - t_w)/\tau_w} & t > t_w \end{aligned} \qquad (12)$$

where $f_{a,o}$ is the initial fraction of pad area covered by liquid and A_p is the area of the concrete pad. As indicated in the figure, a value of $f_{a,o} = 0.9$ fits the data well ($\tau_w = 297$ s).

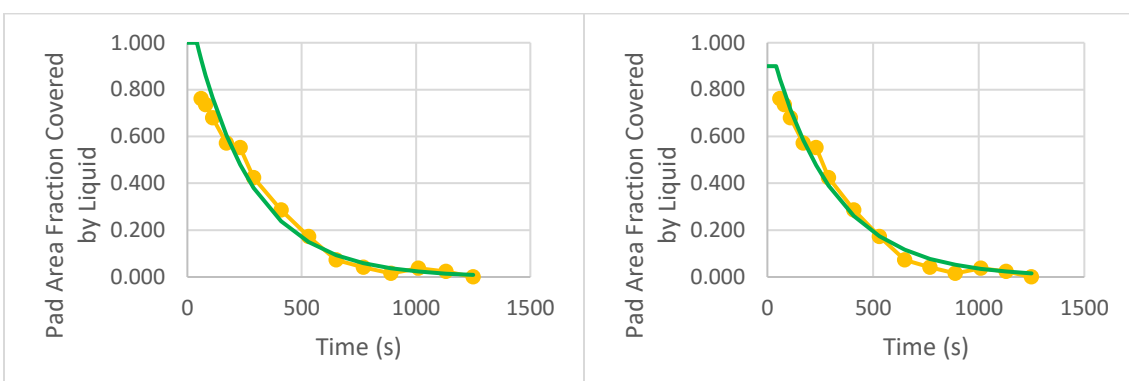


Figure 2. Liquid coverage of concrete pad as a function of time: (a) $f_{a,o} = 1$; (b) $f_{a,o} = 0.9$.

Equation 11 provides an estimate of the mass evaporated from t = 0, but the evaporation rate obtained from differentiating Equation 11 will be infinite at t = 0 (consistent with q" being infinite at t = 0). As discussed above, the evaporation rate is limited by the deposition rate for $t \le t_e$. Consequently, the time used to model the heat conduction rate from the concrete cannot

correspond to the start of the release (t = 0) to account for this (physical) limit. Define t_o as the initial time to be used in Fourier's Law model to account for this limitation; t_o is chosen so that the total deposition at t_e is equal to the total mass evolved by heat transfer at ($t_e - t_o$) and the deposition rate at t_e is equal to rate mass is evolved by heat transfer at ($t_e - t_o$). Considering the time when the deposition rate is equal to the evaporation rate (t_e), Equation 11 becomes

$$\begin{aligned} M_e(t_e) &= \frac{k\,\Delta T}{\Delta H_v}\int_{t_o}^{t_e}\frac{f_{a,o}A_p}{\sqrt{\pi\,\alpha\,(t\,-\,t_o)}}\;dt \\ &= \frac{k\,\Delta T}{\Delta H_v}\int_{0}^{t_e\,-\,t_o}\frac{f_{a,o}A_p}{\sqrt{\pi\,\alpha\,t}}\;dt \\ &= \frac{k\,\Delta T}{\Delta H_v}\left[2f_{a,o}A_p\sqrt{\frac{(t_e\,-\,t_o)}{\pi\,\alpha}}\right] = t_e\dot{M}_d(t_e) \end{aligned} \tag{1}$$

where $\dot{M}_d$ is the deposition rate (initially constant when the release rate is constant). Also, Equation 9 is related to the deposition rate by:

$$\dot{M}_d(t_e) = \frac{k\,\Delta T\,f_{a,o}A_p}{\Delta H_v\sqrt{\pi\,\alpha\,(t_e\,-\,t_o)}} \tag{14}$$

Equations 13 and 14 can be solved simultaneously to determine that $t_o = t_e/2$, and values for all of the parameters can be determined once $\dot{M}_d$ is found. (Values of t_e were less than 2 s for scenarios considered below.)

When the last puddle of liquid chlorine has evaporated, the total rainout from the release can then be determined. Using the area covered by liquid, Equation (13) becomes:

$$\begin{aligned} M_e(t) = \frac{k\,\Delta T}{\Delta H_v}\Bigg[&\int_{0}^{t_w\,-\,t_o}\frac{f_{a,o}A_p}{\sqrt{\pi\,\alpha\,t}}\;dt \\ &+\int_{t_w\,-\,t_o}^{t\,-\,t_o}\frac{f_{a,o}A_p e^{-(t+t_o-\,t_w)/\tau_w}}{\sqrt{\pi\,\alpha\,t}}\;dt\Bigg] \\ &= \frac{k\,\Delta T}{\Delta H_v}\left[2f_{a,o}A_p\sqrt{\frac{(t_w\,-\,t_o)}{\pi\,\alpha}}\right]\Bigg[1 \\ &+\frac{\sqrt{\pi}}{2}\left(\frac{\tau_w}{t_w\,-\,t_o}\right)^{1/2}e^{+(t_w-t_o)/\tau_w}\left(erf\left(\left(\frac{t\,-\,t_o}{\tau_w}\right)^{1/2}\right)\right. \\ &\left.-\,erf\left(\left(\frac{t_w\,-\,t_o}{\tau_w}\right)^{1/2}\right)\right)\Bigg] \end{aligned} \tag{15}$$

As discussed above, there are uncertainties in the evaluation of $f_{a,o}$, and this uncertainty influences the value for τ_w based on a curve fit of the data. In the fitting process, τ_w increases as $f_{a,o}$ decreases; these effects can be seen by considering the right hand side of Equation (15):

$$M_e(t) \propto f_{a,o} \left[1 + \frac{\sqrt{\pi}}{2} \left(\frac{\tau_w}{t_w - t_o} \right)^{1/2} e^{+(t_w - t_o)/\tau_w} \left(erf\left(\left(\frac{t - t_o}{\tau_w} \right)^{1/2} \right) - erf\left(\left(\frac{t_w - t_o}{\tau_w} \right)^{1/2} \right) \right) \right] \quad (16)$$

As $f_{a,o}$ decreases, the term inside the brackets increases because of the increase in τ_w. For $f_{a,o}$ ranging from 0.9 to 1.0, the right hand side of Equation (12) ranges from 2.40 to 2.50, respectively (roughly 5% change) evaluated for the time when the last puddle has evaporated.

Using generic properties for the concrete pad, the temperature difference between chlorine at its (local) boiling point and ambient temperature, and a heat of vaporization of 2.897×10^{-5} J/kg, the total mass evaporated (M_e) for Trial 6 is estimated to be 2938 kg. As discussed above, the total mass evaporated is also the total deposited or rained out ($M_d = M_e$). The initial mass in the vessel was 8391 kg, so the mass rained out represents approximately 35% of the mass released. Previous CCPS tests using chlorine that attempted to directly measure liquid rainout found the rainout to be roughly 17% of the released mass for a horizontal release at 1.22 m elevation (D.W. Johnson, and J.L. Woodward, "RELEASE-A model with Data to Predict Aerosol Rainout in Accidental Releases," AIChE CCPS, 1999).

With the total mass deposited (rained out), M_d, estimated above, the deposition rate can be determined based on the assumption that the deposition rate is proportional to the release rate. If the deposition ends at $t = t_d$, the mass deposited is given by

$$M_d(t) = \left(\frac{M_d}{M_r(t_d)} \right) M_r(t) \quad (17)$$

where $M_r(t_d)$ is evaluated as

$$M_r(t_d) = \dot{M}_x t_x + (M_x - M_h) \left[1 - exp\left(-\left(\frac{t_d - t_x}{\tau_x} \right) \right) \right] \quad (18)$$

The mass deposition rate ($\dot{M}_d$) is given by:

$$\begin{aligned} \dot{M}_d &= \left(\frac{M_d}{M_r(t_d)} \right) \dot{M}_x(t) && t \le t_x \\ &= \left(\frac{M_d}{M_r(t_d)} \right) \frac{(M_x - M_h)}{\tau_x} exp\left(-\left(\frac{t - t_x}{\tau_x} \right) \right) && t > t_x \end{aligned} \quad (19)$$

With the deposition rate determined, the evaporation rate can be calculated using

$$\dot{M}_e = \dot{M}_d \qquad t \le t_e$$
$$= \frac{k\,\Delta T\, f_{a,o} A_p}{\Delta H_v \sqrt{\pi\,\alpha\,(t - t_o)}} \qquad t_e < t \le t_w$$
$$= \frac{k\,\Delta T\, f_{a,o} A_p}{\Delta H_v \sqrt{\pi\,\alpha\,(t - t_o)}}\, exp\left(-\left(\frac{t - t_w}{\tau_w}\right)\right) \qquad t > t_w \tag{20}$$

5. *Airborne Chlorine Mass Rate for Trial 6*

The mass rate chlorine becomes airborne $\dot{M}_a$is estimated using

$$\dot{M}_a(t) = \dot{M}_r(t) - \dot{M}_d(t) + \dot{M}_e(t) \tag{21}$$

Note that the deposition occurs from the liquid phase while evaporation contributes to the vapor phase only so that the liquid fraction of the airborne aerosol is changed by these processes. Figure 3 summarizes the result for Trial 6. For this calculation, the mass release rate is taken to be zero when the calculated rate drops below 1 kg/s (at 63.4 s). (The mass release rate is modeled with an exponential decay, so it would continue long after its contribution was negligible without a criterion for it to stop.) The same approach to estimating the rainout rate and duration can be applied to Trials 1-7, provided the rainout percentage is assumed constant since the release rates are comparable across Trials 1-7. In Trial 6, the last puddle evaporated at 1250 s with a corresponding estimated evaporation rate of 0.042 kg/s, and this ending rate will be used in the analysis of the other trials.

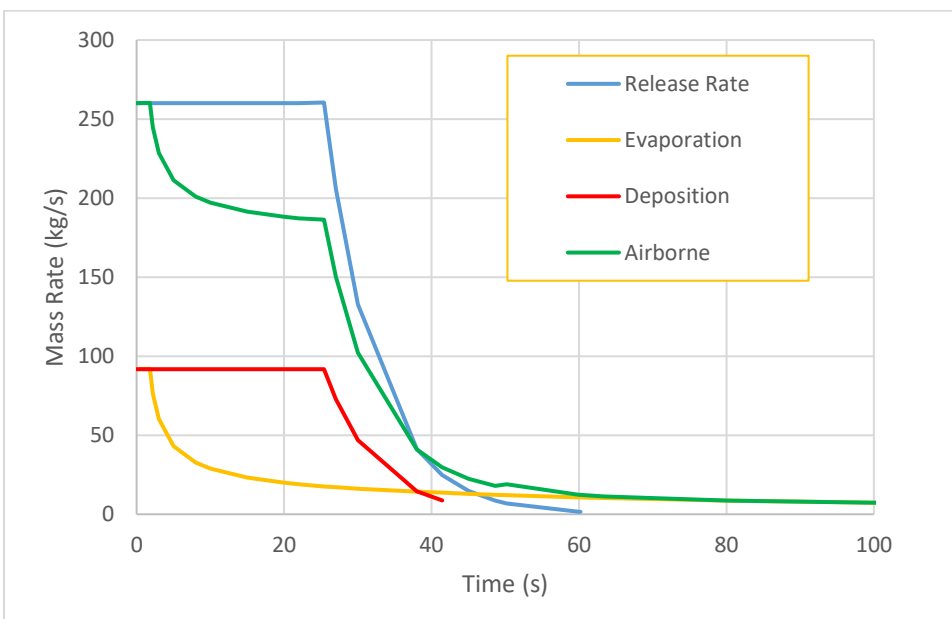


Figure 3. Instantaneous airborne mass rate as a function of time for Trial 6.

Figure 3 makes clear that the mass rate is consistently high for times less than t_x. At t_x, $M_r(t_x)$ = 6612 kg, $M_d(t_x)$ = 2333 kg, and $M_e(t_x)$ = 864, so the total mass airborne would be 5143 kg, so the average airborne mass rate would be 5143 kg/25.4 s = 202 kg/s. For times larger than t_x, the time varying airborne mass rate drops off rapidly. Note that the calculated (instantaneous) mass airborne rate is not monotonically decreasing at the time that deposition ends because the deposition rate is not continuous at t_d.

As an alternate approach, the average airborne rate can be calculated from the (total) cumulative airborne mass divided by the time over which that mass becomes airborne. Figure 4 shows the cumulative airborne mass and average airborne mass rate as a function of time. In addition to the total cumulative mass released, deposited, and evaporated, Table 2 includes average airborne mass rates for various times. The average vapor fraction in Table 2 is the total airborne vapor mass up to time t divided by the total airborne mass at the same time. The average vapor fraction is a strong function of the (adiabatic) flash fraction from storage conditions which was calculated for the (local) boiling point ignoring kinetic energy effects. The flash fraction was assumed constant until t_d and 1 thereafter (all mass released directly to the vapor phase). The final time in Table 2 of 63.4 s was chosen when the mass release rate drops below 1 kg/s, which is taken to be the time the (vapor only) jet has ended.

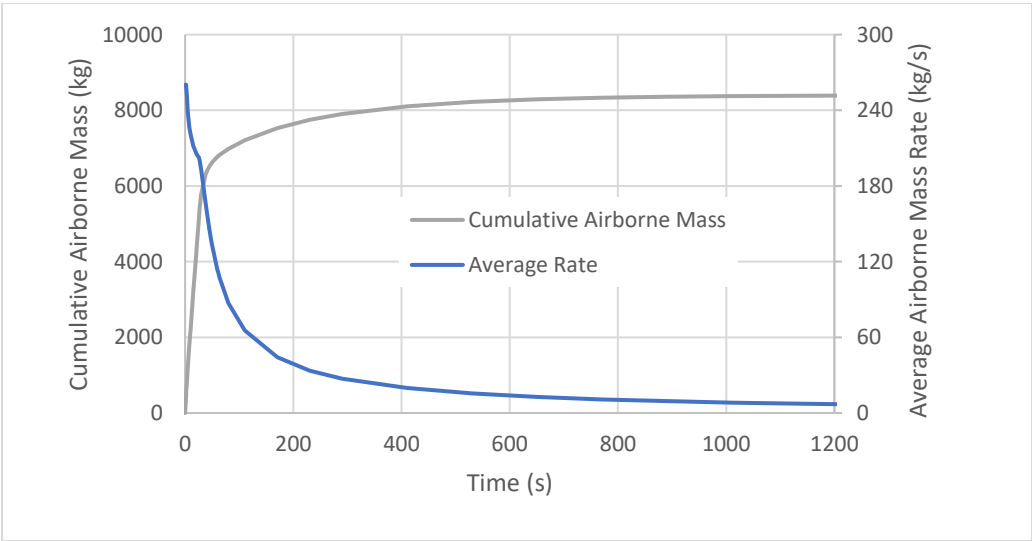


Figure 4. Cumulative airborne mass and average airborne rate as a function of time for Trial 6

Table 2. Cumulative mass fate and average airborne mass rate as a function of time for Trial 6.

Time, t (s)	Mass Released by t (kg)	Mass Deposited by t (kg)	Mass Airborne from Primary Release by t (kg)	Mass Evaporated by t (kg)	Average Vapor Fraction	Average Airborne Mass Rate (kg/s)
20	5200	1835	3365	763	0.401	206
25.4 (t_x)	6612	2334	4278	864	0.389	202
30	7484	2641	4843	942	0.385	193
48.6 (t_d)	8332	2938	5394	1205	0.400	136
60	8380	2938	5442	1335	0.416	113
63.4	8384	2938	5447	1371	0.420	108

6. Airborne Chlorine Mass Rate for Trials 1, 6, and 7

The approach developed to analyze Trial 6 was applied to Trials 1 and 7. To summarize the process,

1. The mass release parameters were determined as discussed above:
    a. The total mass released was determined from load cell data in conjunction with the liquid heel remaining after the release. (The heel was determined for Trials 7 and 8 to be the point when the change in mass readings was less than 1 kg from the average reading for at least 1 s.)
    b. The start of the release (t=0) was the last set of recorded values before they significantly changed. The initial average mass rate was calculated as the difference in mass between the beginning and end of the averaging time period divided by the averaging time period so that the derived values will match the mass remaining in the vessel. The length of the time period was limited to when the rate was no longer essentially constant.
    c. The parameters M_x, t_x, and τ_x were determined from the measured mass as a function of time so that the mass release rate was continuous at t_x (transition from continuous release rate to release rate decreasing with time at the end of the release).
    d. The parameters t_d (= $t_x + 3.4\tau_x$) and t_w (= $t_x + 2.35\tau_x$) from Trial 6 were assumed to apply to the other trials except Trial 7 where $t_d = t_x + 3.7\tau_x$.
2. The chlorine boiling point (used in the driving force for heat transfer to the concrete pad) was obtained at the reported ambient pressure at the time of the release using the vapor pressure correlation for chlorine from DIPPR. Average pad temperatures were found as discussed above.

3. The chlorine initial flash fraction was estimated assuming an isenthalpic flash to ambient temperature using the latent heat of vaporization correlation for chlorine from DIPPR and (mean) liquid heat capacity correlated from Chlorine Institute Pamphlet 72.
4. The initial fraction of pad area covered by the liquid and the rain out fraction were assumed constant for Trials 1-7 based on the analysis of Trial 6 discussed above.

The results for Trials 1 and 7 are shown in Figures 5 and 6 and Tables 3 and 4, respectively. This approach predicts that the last puddle of liquid evaporates at 380 s on Trial 1 and 1600 s on Trial 7. In Trial 1, there are several small puddles still visible at 380 s. In Trial 7, the liquid clearly deposited outside the concrete pad on the gravel surrounding the pad, and at 1600 s, the gravel is white indicating the presence of condensed and frozen water.

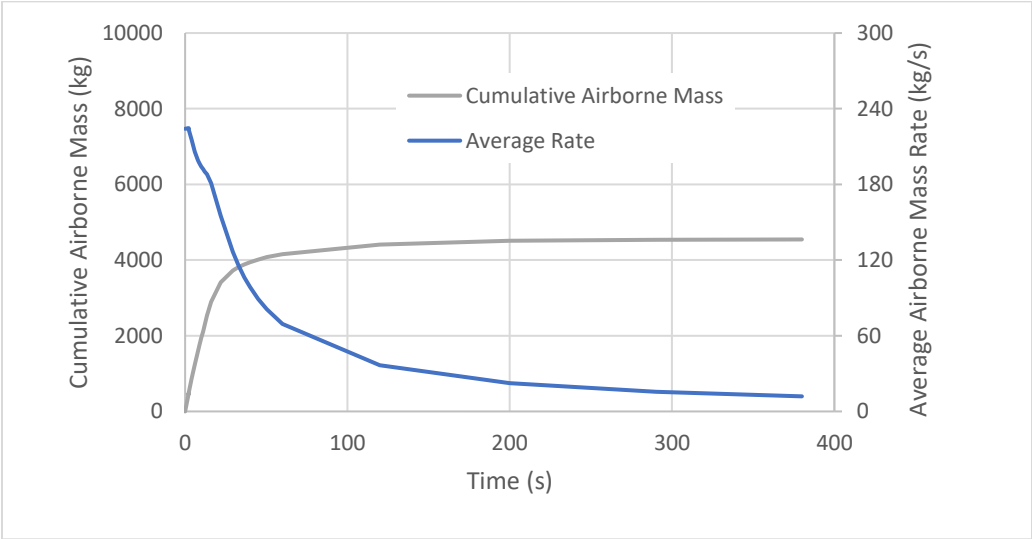


Figure 5. Cumulative airborne mass and average airborne rate as a function of time for Trial 1.

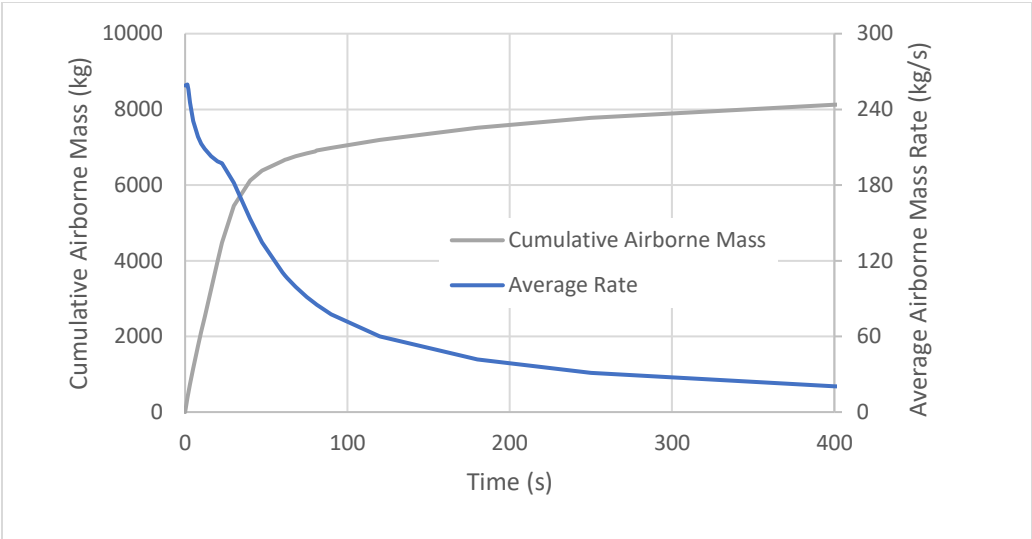


Figure 6. Cumulative airborne mass and average airborne rate as a function of time for Trial 7

Table 3. Cumulative mass fate and average airborne mass rate as a function of time for Trial 1.

Time, t (s)	Mass Released by t (kg)	Mass Deposited by t (kg)	Mass Airborne from Primary Release by t (kg)	Mass Evaporated by t (kg)	Average Vapor Fraction	Average Airborne Mass Rate (kg/s)
13.5 (t_x)	3021	1070	1951	583	0.434	188
20	3962	1403	2558	720	0.426	164
30	4411	1563	2848	890	0.440	125
36.6 (t_d)	4494	1591	2903	981	0.450	106
50.3	4545	1591	2954	1127	0.477	81.1
60	4545	1591	2954	1204	0.487	69.3

Table 4. Cumulative mass fate and average airborne mass rate as a function of time for Trial 7.

Time, t (s)	Mass Released by t (kg)	Mass Deposited by t (kg)	Mass Airborne from Primary Release by t (kg)	Mass Evaporated by t (kg)	Average Vapor Fraction	Average Airborne Mass Rate (kg/s)
20	5180	1926	3254	723	0.406	199
22.7 (t_x)	5897	2192	3705	772	0.399	197
30	7264	2701	4564	891	0.3923	182
60	8548	3175	5373	1265	0.412	111
61.6 (t_d)	8559	3175	5383	1281	0.413	108
81.1	8626	3175	5451	1462	0.436	85.2

Table 5 contains a set of inputs for the source specification necessary to run the atmospheric dispersion models for the JRII trials 1, 6 and 7. (All trials are planned to be modeled in the future.) The entries in Table 5 labeled "Primary release" are parameters which describe the release from primary containment as a jet and includes the portion of the liquid phase which rained out. In these entries, the release rate was estimated from experimental data, and the release duration was calculated to account for all of the mass released in a test. The entries labeled "Primary release modified for rainout" are parameters calculated by subtracting the mass rained out from the primary release mass, and the release duration was calculated to account for all of the mass released in a test that did not rain out. The entries labeled "Evaporated rainout" are parameters that account for the mass of chlorine that evaporates from the liquid that has rained out. The evaporation rate is averaged over (roughly) the duration of the "Primary release" source and assumed to apply until all of the rained out mass has evaporated. The area for the evaporated rainout is assumed to be the concrete pad area, but the liquid coverage of the concrete pad varied over time. Vapor densities were calculated assuming ideal gas behavior. As discussed above, all chlorine fluid properties are taken from the DIPPR database with the exception of liquid heat capacity which was based on data from Chlorine Institute Pamphlet 72. All parameters are reported after any depressurization process is complete.

Table 5. Averaged source emission rates and parameters.

	Trial 1	**Trial 6**	**Trial 7**
Primary release			
Discharge rate (kg/s)	224.	260.	259
Discharge period (s)	20.3	32.2	33.3
Temperature (ºC)	-37.3	-37.4	-37.4
Vapor fraction (ignoring KE effects)	0.171	0.172	0.172
Density (kg/m^3)	18.32	18.15	18.12
Velocity (m/s)	50.8	44.2	44.2
Area (m^2)	0.241	0.324	0.323
Primary release modified for rainout			
Discharge rate (kg/s)	145	168	162
Discharge period (s)	20.4	32.4	33.6
Temperature (ºC)	-37.3	-37.4	-37.4
Vapor fraction (ignoring KE effects)	0.264	0.266	0.274
Density (kg/m^3)	11.89	11.79	11.41
Velocity (m/s)	50.8	44.2	44.2
Area (m^2)	0.240	0.323	0.322
Evaporated rainout			
Discharge rate (kg/s)	43.2	34.0	34.0
Discharge period (s)	36.8	86.4	93.4
Temperature (ºC)	-37.3	-37.4	-37.4
Vapor fraction	1	1	1
Density (kg/m^3)	3.160	3.152	3.144
Area (m^2)	491	491	491

Conclusions

Sponsored by the U.S. Department of Homeland Security, the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense, and Transport Canada, the Jack Rabbit II tests were designed to release liquid chlorine at ambient temperature in quantities of 5 to 20 T for the purpose of quantifying the behavior and hazards of catastrophic chlorine releases at scales represented by rail and truck transport vessels.

There are ongoing efforts to analyze data from the test program. One aspect of this analysis involves comparison of selected tests with predictions using available atmospheric dispersion models. For this comparison between atmospheric dispersion models to be most meaningful, it was desired to have a common set of model inputs including meteorological parameters and source parameters. This paper presents representative source parameters that can be applied in many different atmospheric dispersion models.

Acknowledgements

This field test program was sponsored by the Chemical Security Analysis Center (CSAC) of the U.S. Department of Homeland Security (DHS), the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense, Transport Canada, and Defence Research and Development Canada (DRDC). In addition to the program's Dissemination and Near Source Working Group, we acknowledge the contribution of many people who planned and conducted the tests: DHS CSAC including Adolfo Negron and Shannon Fox; DTRA including Rick Fry; DPG including Damon Nicholson, Petr Serguievski, and Allison Hedrick; Chlorine Institute including Frank Reiner, Robyn Brooks, Therese Cirone, and Henry Ward; and the JR II Scientific Advisory Group (SAG) including Leo Stockham, Joe Chang, Steve Hanna, Allison Hedrick, Mike Sohn, and Thomas O. Spicer, III.

References

J.R. Couper, W.R. Penney, J.R. Fair, and S.M. Walas, "Chemical Process Equipment: Selection and Design," Elsevier, 2nd, 2005.

Spicer, T., and D. Miller, "Quantifying the Mass Discharge Rate of Flashing Two Phase Releases through Simple Holes to the Atmosphere," Process Safety Progress, 2018.

Spicer, T., A. Feuvrier, and S.B. Fox, "Transient Large-Scale Chlorine Releases in the Jack Rabbit II Field Tests: Rainout Source Data Analysis from Video Records," submitted to Journal of Loss Prevention in the Process Industries, 2018.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Integrating Human Factors Concepts into Improving Risk Management and Safety Performance

Phil Grossweiler*, Phil Emanuel, Paul Monaghan
M&H Energy Services
19450 Texas 249 Access Rd
Houston, TX 77070
*Presenter E-Mail: phil.grossweiler@mhes.com

Abstract

The international energy industry has made significant efforts over the last 10 years to improve risk management and safety performance. The industry continues to improve and increase emphasis on Occupational Safety and Process Safety programs in support of improving risk management.

Significant increases in work in areas of organizational development will help integrate human factors concepts into enterprise risk management frameworks and help improve safety and operational performance. Key elements of organizational development, including leadership and culture, require involvement across the entire organization.

The Society of Petroleum Engineers conducted several industry-wide summits and workshops to address human factors. The SPE Technical Report included in the list of references is one source for perspectives on future industry work on human factors. (Society of Petroleum Engineers - Technical Reports Committee 2014) Many organizations are working to integrate human factors. These include the National Academies, Chemical Safety Board, Ocean Energy Safety Institute, API, Center for Offshore Safety, military organizations, aviation industry, Chartered Institute of Ergonomics and Human Factors, and the Human Factors and Ergonomics Society. The range of activity considered for this analysis, while not a complete source of risk management activities, provides an thorough knowledge base of activities related to the application of human factors.

Table of Contents

Abstract 1
Introduction 3
Defining Human Factors and the Human Element 4
Risk Management and Human Factors – A Knowledge Base 5
General Industry Sources 5
The Society of Petroleum Engineers 5
Report: The Human Factor: Process Safety and Culture 5
Report: Assessing the Processes, Tools, and Value of Sharing & Learning from Offshore E&P Safety-Related Data 6
Report: Getting to Zero and Beyond: The Path Forward 6
Summit Paper: November 2012 6
National Academy of Science Engineering and Medicine/Gulf Research Program 7
Report: Strengthening the Safety Culture of the Offshore Oil and Gas Industry 7
Workshop: The Human Factors of Process Safety and Worker Empowerment in the Offshore Oil Industry 7
Summit Paper: Safer Offshore Energy Systems 8
Enterprise Risk Management Frameworks 9
API RP 75 - Framework for the Safety Management System 10
The Risk Matrix – A Key Tool 12
Extreme Operational Excellence 12
Barrier Management 15
Perspectives on Organizational Development 17
Leadership and Safety Culture 17
Path to Generative Performance – A Learning Organization. 19
Recommendations 20
Conclusions 21
References 22

Introduction

The perspectives presented in this paper reflect, to a great extent, the results of observing activities over the last decade to improve levels of safety in the oil and gas industry. Thought leaders and "power thinkers" across the industry continue to develop valuable ideas for a step change in improving performance. One new paradigm is *Getting to Zero Harm*. (Hinton, et al. 2018)

Getting to zero harm converges on two primary objectives:

- Nobody Gets Hurt
- The CEO never gets a phone call that "a major accident just happened." – an accident which destroys a major percentage of enterprise value for a larger corporation or bankrupts a smaller company.

These two objectives are not mutually exclusive. They reinforce each other. Addressing occupational safety, in general, helps ensure that nobody gets hurt. Effective management of process safety can prevent major accidents. The perspectives offered in this paper describe a framework in which application of human factors concepts contributes to both of these objectives.

Most companies have a well-developed Safety Management System (SMS). Continuous improvement is important. Periodic reviews of industry activities across the "Risk Management and Safety Space" by HSE leaders in individual companies help identify potential refinements and improvements to an existing company SMS.

As a result of the downturn in oil prices, attention to safety is sometimes reduced. Investments in safety are directly related to a company's bottom line. It is critical, even during industry downturns, to recognize that safety cannot be sacrificed by attempts to cut costs. The cost of recovering from the impact of accidents is simply too high.

General industry dialogues emphasize the need for closer communications between corporate and those "at the sharp end of the spear." This point emphasizes that the person on the front line must also accept ownership and responsibility for safety, especially within the realm of occupational safety. Whenever a serious accident or event occurs, inevitably some leader in the organization says, "We will put in place procedures to make sure it doesn't happen again!"

As Rex Tillerson put it in 2010:

> *"Written rules, standards and procedures, while important and necessary, are not enough…A culture of safety starts with leadership, because leadership drives culture and culture drives behavior. Leaders influence culture by setting expectations, building structure, teaching others and demonstrating stewardship…For a culture of safety to flourish, it must be embedded throughout the organization."*
>
> *(International Association of Oil & Gas Producers 2013)*

A key challenge in managing risk and safety performance is ensuring that safety leaders within the organization are able to identify potential risks for events which have not yet happened.

The paper extracts concepts from a broad range of industry activities related to risk management and safety. There are no "silver bullets." We must think in terms of range of "silver buckshot" from which to develop continuous improvements to safety management systems.

Defining Human Factors and the Human Element

According to IOGP Publication 368,

> *Human factors is the term used to describe the interaction of indidivuals with each other, with facilities and equipment, and with management systems. This interaction is influenced by both the working environment and the culture of the people involved. What may be a good system of work in one part of an organization, may be found to be less than ideal in a region where culturally driven attitudes to risk taking may be significantly different. Human factors analysis focuses on how these interactions contribute towards the creation of a safe workplace.*
>
> *(International Association of Oil & Gas Producers 2005)*

Human elements regarding facilities and equipment design and ergonomics are not included in this paper. This paper deals primarily with the interfaces between **management systems** and **people**, the two elements shown in the orange and green circles of Figure 1.

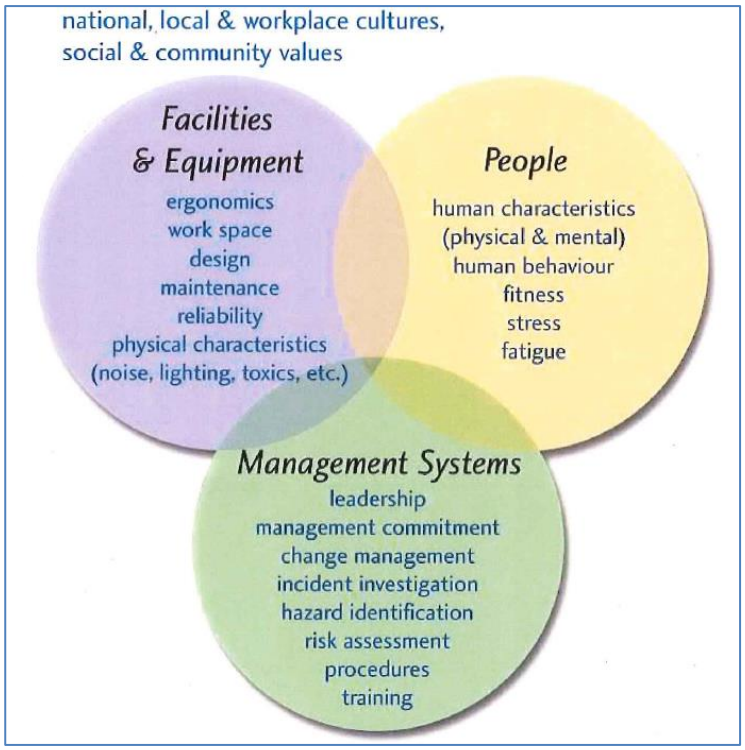


Figure 1: Culture and Working Environment (International Association of Oil & Gas Producers 2005)

Risk Management and Human Factors – A Knowledge Base

General Industry Sources

Table 1 lists a range of organizations and sources of information available for consideration in developing risk management systems.

Table 1

O&G Industry Standards & Practices & Other Studies	Standards & Risk Management Practices Outside O&G Industry

• IADC
• Health and Safety Executive – UK (HSE)
• Center for Chemical Process Safety (CCPS)
• DNV-GL
• ABS
• NORSOK
• OESI
• MKOPSC
• UK O&G Association
• IOGP
• Center for Offshore Safety
• Chemical Safety Board
• National Academies (NASEM)
• Society of Petroleum Engineers
	• ISO
	  ○ 17776 Guidelines on Tools and Techniques
	  ○ 31000 RM Principles & Guidelines
	  ○ 31010 RM – RA Techniques
	  ○ 45001 Occupational Health Safety Management Systems
	• Military
	• Aviation - CRM, High Reliability Organizations
	• Nuclear Industry
	• Insurance Underwriters
	• Financial Sector
	• Human Factors Societies

Many of the risk management and human factors concepts within these sources overlap and reinforce each other. A comparative reading of the various sources will provide valuable insights into improving an existing corporate safety management system.

The Society of Petroleum Engineers

Report: The Human Factor: Process Safety and Culture
(Society of Petroleum Engineers - Technical Reports Committee 2014)

This SPE report, based on input from 70 subject matter experts from throughout the international oil and gas industry, defines the scope of human factors and discusses safety culture, training and certification, operational control of work, decision making, and application of information technology (IT).

In civil aviation, a series of major accidents led to the introduction, mandatory requirement, and acceptance of human factors methodologies called Crew Resource Management (CRM). Similarly, the nuclear power industry identified and acted upon the concept of its safety culture after a small number of major incidents. The challenge is whether the E&P industry can achieve a similar breakthrough by confronting the human factor as an issue in process safety both onshore and offshore. The recommended changes include moving to an organizational culture in which process safety is as well managed as personal safety is currently managed.

Report: Assessing the Processes, Tools, and Value of Sharing & Learning from Offshore E&P Safety-Related Data
(Society of Petroleum Engineers - Technical Reports Committee 2016)

This SPE report provides guidance on an industry-wide safety management data sharing program. The overall objective of the effort is to eliminate or reduce risk of harm through industry sharing of data, including information on near misses.

Report: Getting to Zero and Beyond: The Path Forward
(Society of Petroleum Engineers - Technical Reports Committee 2018)

This SPE report identifies and evaluates elements that can aid the industry in removing obstacles to achieving zero harm. It explores current thinking and views; incorporates experiences and learnings from other industries that are mature in the application of human factors; and suggests the next steps that will enable the oil and gas industry to meet an expectation of zero harm.

Summit Paper: November 2012
(Hudson and Thorogood 2012)

This SPE report highlights the critical requirement for participation by individuals in achieving a successful safety culture. CEOs and company management alone cannot create the culture. **All persons on the front line have a responsibility for making "safety culture" happen.** See Figure 2 below.

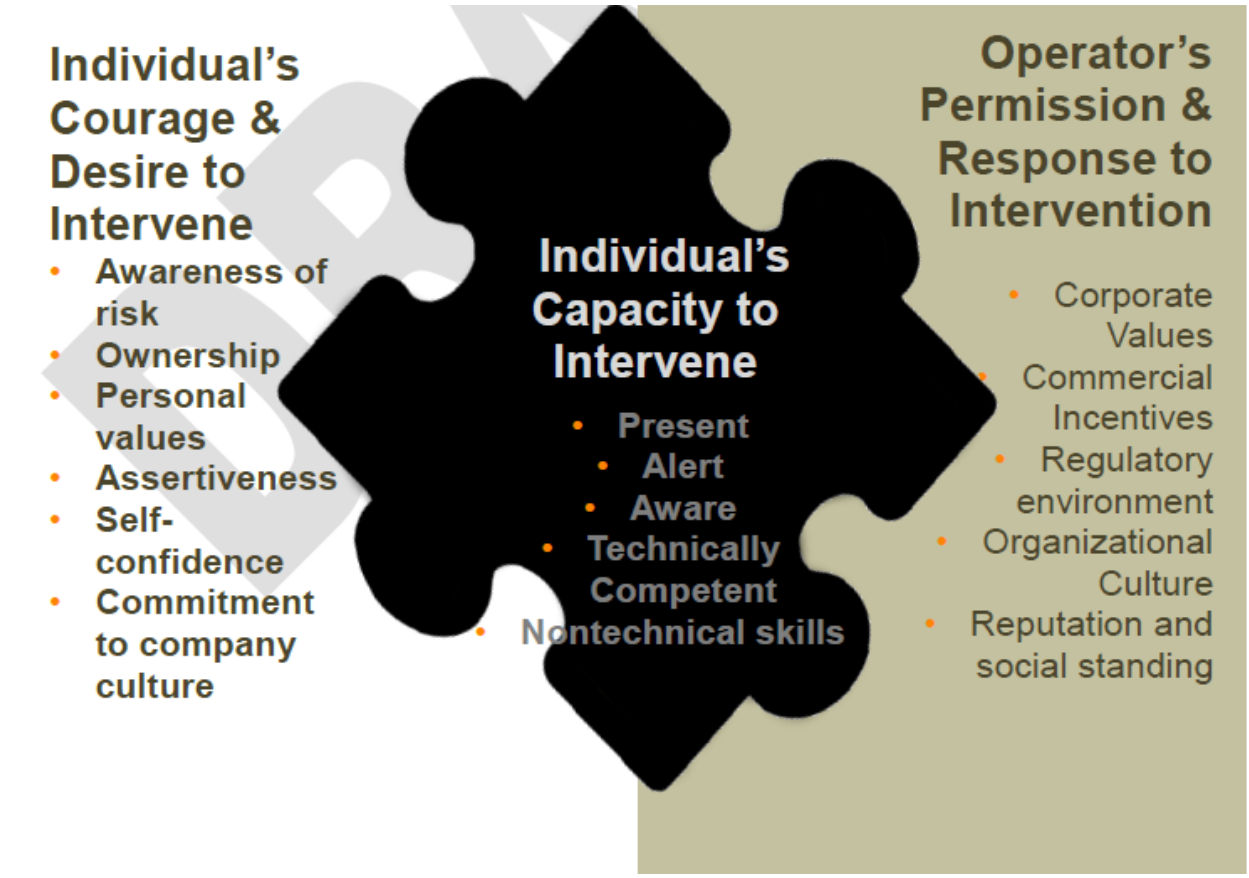


Figure 2: Human Intervention Model

National Academy of Science Engineering and Medicine/Gulf Research Program

Report: Strengthening the Safety Culture of the Offshore Oil and Gas Industry
(National Academies of Sciences, Engineering, and Medicine 2016)

This 240-page report issued in 2016 provided a detailed analysis of opportunities for achieving an effective safety culture within the industry. According to this report, critical success factors for an effective safety culture in the nuclear industry include:

- Management commitment to safety. Leadership safety values and actions, decision-making, and respectful working environment.
- Individual commitment to safety. Personal accountability, questioning attitude, and effective safety communication.
- Management systems. Continuous learning, problem identification and resolution, environment for raising concerns, and work processes.

Workshop: The Human Factors of Process Safety and Worker Empowerment in the Offshore Oil Industry
(National Academies of Sciences, Engineering, and Medicine 2018)

This January 2018 workshop, a product of the 30-year, $500 million Gulf Research Program, included 80 participants representing a broad cross-section of the domestic and international energy industry. Topics of discussion included:

- Differences between U.S. and international practices, both in regulatory frameworks and operating practices within the industry.
- Best practices and lessons learned from other high-risk, high-reliability industries.
- Differences resulting from union and nonunion work environments.
- Getting CEOs engaged.
- Perspectives from organizations outside the core oil and gas industry and especially the Chemical Safety Board.
- Defining the word, *empowerment*.

Professors Rhona Flin and Christiane Spitzmueller discussed the integration of organizational development and human factors concepts, as seen in Figure 3:

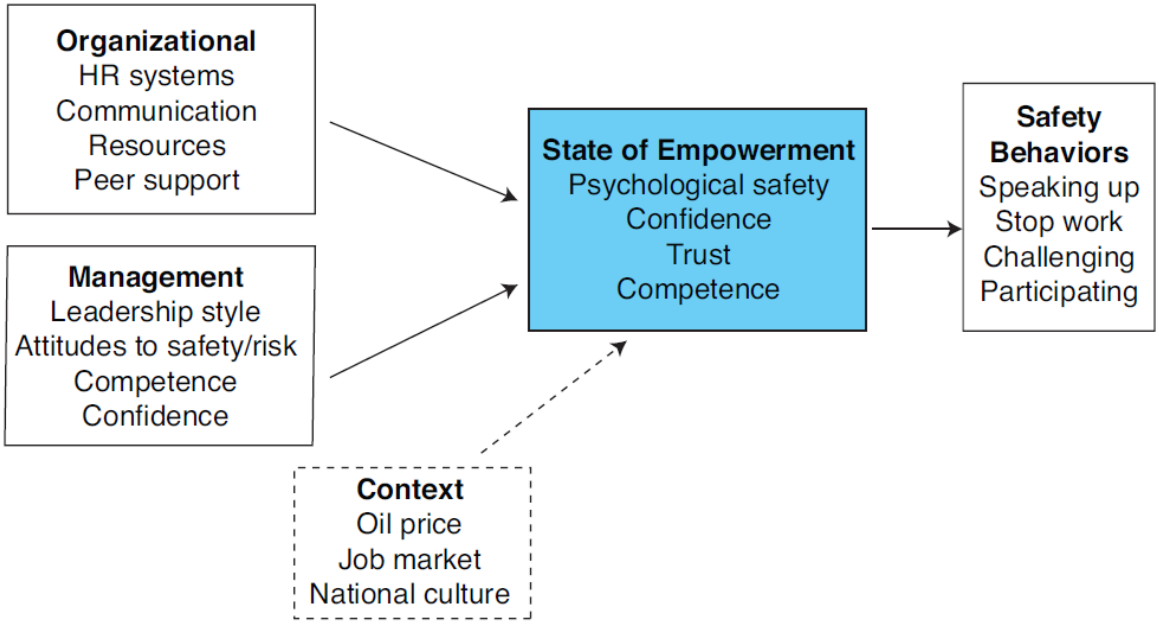


Figure 3: The state of empowerment links organization, management, and context to safety behaviors.

Bill Hoyle of the Chemical Safety Board emphasized another key point: When an audit report says everything is fine, "that's a bad report." You are getting no value from that. Reporting bad news is a good thing. People need to be trained to, "put bad news forward and push it up."

Andrew Imada, an Organizational Development Consultant and member of The National Academies Board on Human-Systems Integration, recommended a strong relationship between organizational safety culture, leadership, and voluntary safety performance. Voluntary performance is at the heart of empowerment. Also, empowerment requires a commitment to a safety culture that goes beyond compliance.

Summit Paper: Safer Offshore Energy Systems
(Society of Petroleum Engineers 2018)

This NASEM/SPE Summit engaged a broad set of industry experts to develop ideas on areas where the Gulf Research Program or jointly-funded research is needed to minimize and manage risks for both people and the environment by minimizing the possibility of a major incident. The scope included include both technical and human performance opportunities.

- Improving collaboration among industry, regulatory, and academic communities to advance understanding and communication about systemic risk.
- Fundamental scientific and technological research to spur innovation aimed at reducing or managing risks.
- Exploring how to create robust and resilient organizations that minimize major incidents with improved management of change, sim-ops management, decision support, and operational procedures that support safe work.

- Identifying educational or training programs to promote a skilled and safety-oriented workforce and to retain that workforce through economic cycles in the oil and gas industry.

The analyses and brainstorming activities were organized to span the full lifecycle of industry activities including: Pre-drilling, drilling, construction, and production phases of activity. The summit identified 144 opportunities to improve safety.

Enterprise Risk Management Frameworks

We operate in a high risk industry. Companies (and individuals) must consider their perspectives with regard to risk. Is it a risk averse/risk avoidance framework, or is it one of taking risks with appropriate risk management? The following figure provides a broad, qualitative perspective regarding taking or avoiding risk. A goal of zero risk is a recipe for negative returns.

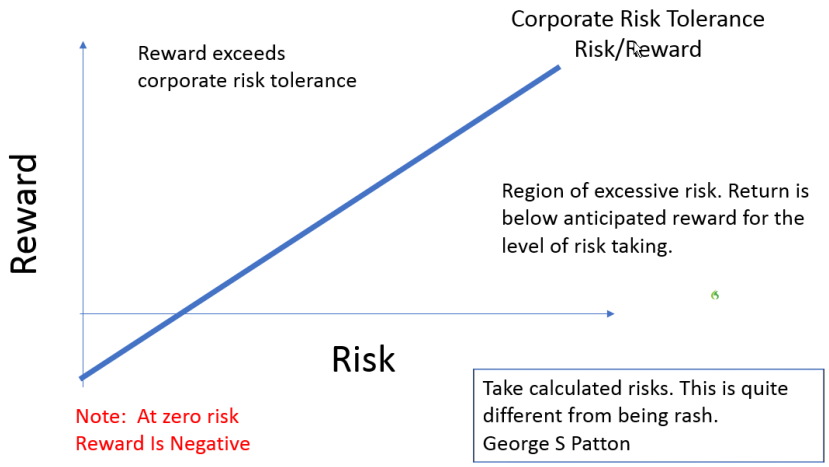


Figure 4: Strategic Positioning Risk/Reward

With the relationship between risk and reward in mind, companies can assess whether their projects or activities have sufficient reward to compensate for the risk exposure. Activities in the upper left region provide enough reward to justify taking the risk. Activities assessed in the lower right region should be avoided since the return is not enough to cover the risk exposure.

This framework should be considered from both a qualitative and quantitative perspective. The collective judgment of corporate leadership can provide an instinctual, qualitative perspective on whether to take or avoid risks. Quantitative tools can be used, when appropriate, for detailed evaluations of risks in any specific project or activity.

Thinking from the framework of "High Reliability Organizations" is critical. The objective is not to get to zero risk. The energy industry requires taking calculated risks, managed effectivly.

The industry is increasing emphasis on integrating knowledge and perspectives from outside the core oil and gas industry.

In an article published in Harvard Business Review, Nassim Taleb, author of the book, *The Black Swan*, discusses risk management issues relevant to the oil and gas industry and identifies additional ideas worth considering. "Black Swan events are almost impossible to predict. Instead

of perpetuating the illusion that we can anticipate the future, risk management should try to reduce the impact of the threats we don't understand." (Taleb, Goldstein and Spitznagel 2009)

He continues on to detail six mistakes executives make in risk management:

1. We think we can manage risk by predicting extreme events.
2. We are convinced that studying the past will help us manage risks.
3. We don't listen to advice about what we shouldn't do.
4. We assume that risk can be measured by standard deviation.
5. We don't appreciate that what is mathematically equivalent is not psychologically so.
6. We are taught that efficiency and maximizing shareholder value do not tolerate redundancy.

It is important to emphasize how to manage low probability, high impact events.

API RP 75 - Framework for the Safety Management System

API is updating Recommended Practice 75, *Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities*. The release of the updated RP 75 is scheduled for year-end 2018. The preamble for this update states:

> *This document is intended to describe a* ***performance-based management system*** *focusing on the purpose and expectations for each element of a safety and environmental management systems (SEMS). It is not intended to be prescriptive in defining how to achieve the purpose and expectations of each element; rather,* ***it allows flexibility appropriate to the size, scope, and risk of a company's assets and operations****.*

This revised RP 75 addresses the human element only in general terms. Applying and integrating the "human element" or "human factors" within the overall framework of the risk management system can be challenging. Where does the human element fit in? Generally everywhere. A keyword search of the term, *human,* within the draft update to API RP 75 shows that the term appears only a few times.

The following is a list of the required elements of an SMS in the updated RP75.

1. General
2. Safety & Environmental
3. Hazards Analysis
4. MOC
5. Operating Procedures
6. Safe Work Practices
7. Training
8. Mechanical Integrity
9. Pre-Startup Review
10. Emergency Response
11. Incident Investigation
12. Auditing
13. Records & Documentation
14. Stop Work Authority (SWA)
15. Ultimate Work Authority (UWA)
16. Employee Participation Program (EPP)
17. Reporting Unsafe Working Conditions

Guidance on human performance which impacts most of the elements within the SMS is included in the draft document under Section 3.2.4, *Human Performance*:

> *Achieving effective human performance results from the systematic application of knowledge and learnings to improve the interactions of individuals with each other, equipment, and systems. The SEMS influences human performance by incorporating the following concepts:*
>
> a. *Leadership Response: Leaders commit to responding to failures and successess in a way that improves human and team performance.*
>
> b. *Resilient Design: Systems are designed to account for the variability and error-likely situations that occur in the interactions of individuals with each other, equipment, and systems.*
>
> c. *Human Feedback: It is recognized that human input and adaptability enables effective HSSE performance and continual improvement in SEMS.*
>
> d. *Functionality: An effective SEMS considers human factors, the end user, the interfaces, the work, and the decision-making processes in the design, implementation, and maintenance of the management system.*

Within this high-level framework for a performance-based SMS as defined by API RP 75, organizations have significant flexibility regarding which potential standards or practices to use in developing an SMS. The following progression suggests one potential framework which relies heavily on IOGP and ISO standards. This framework also recommends expanding an SMS which meets the minimum regulatory requirements to an enterprise risk management framework with performance goals beyond compliance. *Note: Insert at right in figure below from IOGP.*

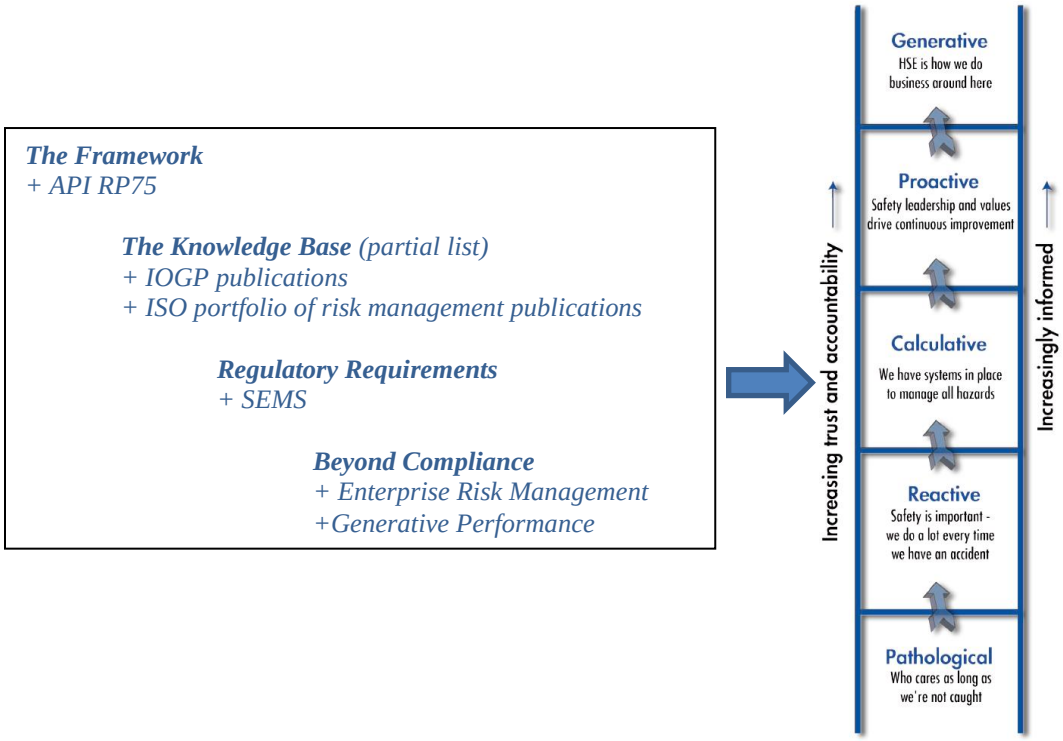


Figure 5 (International Association of Oil and Gas Producers 2010)

The Risk Matrix – A Key Tool

The paper, *Anatomy of the Risk Matrix*, (Van Scyoc and Hopkins 2012) provides an excellent framework for developing a risk matrix and is suggested as one of the best starting points for developing an overall assessment of corporate enterprise risk. This paper provides significant insights and perspectives on risk tolerance, the balance between intuitive and quantitative approaches, key pitfalls in developing and applying risk matrices, the level of granularity appropriate in a risk matrix based on the size of the corporation, and emphasis on analyzing risks with potential major impact on enterprise value.

Consequence					Increasing Probability			
					A	B	C	D
Severity Rating	People	Assets	Environment	Reputation	Has occurred in E&P industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero Damage	Zero effect	Zero impact				
1	Slight injury	Slight damage	Slight effect	Slight impact	Manage for Continued Improvement			
2	Minor injury	Minor damage	Minor effect	Limited impact				
3	Major injury	Local damage	Local effect	Considerable impact		Incorporate Risk Reducing Measures		
4	Single fatality	Major damage	Major effect	Major national impact				
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact			Fail to meet screening criteria	

Figure 6: Generic Risk Matrix based on ISO 17776

Rigorous application of this risk matrix provides the basis for:

- Identifying and prioritizing the hazards across the spectrum from risks to major enterprise value to less serious risks.
- Analyzing the impact of the hazards with and without mitigation.
- Selecting the critical safety activities for high priority treatment.
- Selecting and managing barriers to mitigate the risks including procedures, generally within the framework of a "bowtie."

Extreme Operational Excellence

Achieving compliance with procedures is one of the critical success factors in preventing accidents. How can an organization ensure compliance with procedures? High reliability organizations such as the nuclear submarine service have experienced proven success.

Trevor Kletz, author of the book, *What Went Wrong*, writes:

> *The 1988 explosion and fire on the Piper Alpha oil platform in the North Sea, which killed 163 people, was also caused by poor isolation. A pump relief valve was removed for overhaul and the open end blanked. Another shift, not knowing that the relief valve was missing, started up the pump. The blank was probably not tight, and light oil leaked past it and exploded in the confined processing area. The official report concluded "**that the operating staff had no commitment to working to the written procedure; and that the procedure was knowingly and flagrantly disregarded**." The loss of life was greater on Piper Alpha than on the other two incidents because oil platforms are very congested and escape is difficult.*
>
> *(Kletz 2009)*

Conclusions in the Piper Alpha Accident Report by Lord Cullen included: "**The operating staff had no commitment to working to the written procedure; and … the procedure was knowingly and flagrantly disregarded.**"

Problems with procedures are linked to numerous incidents and are frequently cited as one of the causes of major accidents. Ineffective management of procedures has not only contributed to disasters such as Bhopal, Piper Alpha, Exxon Valdez, and Bp Texas City, but also to most accidents which have resulted in fatalities and personal injuries. The main causes are too much reliance placed on procedures to control risk; a failure to follow safe working procedures; or the use of inadequate procedures.

Lessons from Bp Texas City (U.S. Chemical Safety and Hazard Investigation Board 2005):

- A work environment that encouraged operations personnel to deviate from procedure.
- Acceptance of procedural deviations during past startups.
- Failure to ensure the procedures remained up-to-date and accurate.
- Management did not ensure that unit operational problems were corrected over time, allowing operators to deviate from established procedures.
- The startup procedure lacked sufficient instructions for the Console Operator to safely and successfully start up the unit.

Risk management systems must clarify the difference between *empowering* and *engaging* all workers so that the organization is able to achieve operational discipline. Empowering workers does not mean companies should allow workers to choose which procedures to follow and which not to follow.

Multiple layers of protection are needed against human error. The following are just a few protections:

- Process engineering design
- Basic controls and alarms
- Operational excellence ownership/supervision
- Critical alarms and manual intervention
- Advanced controllers and automatic action (SIS or ESD)
- Physical protection (relief devices, dikes, or blast areas)
- Plant emergency response to community emergency response
- Procedures

Experience has proven that when people think of a production platform or process facility, they tend to focus on the equipment—the vessels, pumps, compressors, instrumentation, and controls. EPC firms, as well as the Owners, often fail to conisder the entire system, particularly the end users, the people who operate and maintain the facility. These people will have different competencies, training, and experiences, and will perform differently under various operating conditions, organizational structures, equipment configurations, and work scenarios.

The probability that the total system will perform correctly after it is commissioned is the probability that the hardware/software will perform as designed, times the probability that the operating environment will not degrade the system operation, times the probability that the end user will perform correctly.

By defining the total system this way, human performance is identified as a component of the system. By increasing the probability that operators and maintenance technicians can perform tasks effectively in the appropriate environment, the total system performance will increase significantly.

Of all the protections a company can employ, procedures are critical to operational excellence. Procedures, including work instructions, job aids, etc., are agreed safe and best ways of doing things. They usually consist of prerequisites, safety precautions, workflow sequences, action item series, consequences of deviation, and related information needed to carry out tasks safely. Procedures may include flowcharts, decision trees, step-by-step instructions, checklists, diagrams, and other types of job aids.

Key principles in procedure design:

- Risk assessment should clearly establish when procedures are an appropriate control measure. The results of the risk assessment should inform development of the procedure.
- In O&G, for a production platform or a process unit to be operated in a safe manner, a hazard analysis and the pre-startup review ensure that provisions made in final design and subsequent modifications are reflected in system operating limits. A major contributor to compliance with system operating limits is made by the development and use of operating and maintenance procedures.
- Consider the links between procedures and competency—they should support each other (e.g., on-the-job competency would include training on frequent, important, and critical procedures). Procedures do not replace competency. Procedures do not replace training.
- Have a system for managing procedures—job task analysis (e.g., how to decide which tasks need procedures based on frequency, importance, and difficulty of the task to be performed, how these procedures are developed, complied with, and reviewed/updated).
- Use a format, style, and level of detail appropriate to the user, task, and consequences of failure. Procedures should be fit for purpose. One size does not fit all. Support compliance with procedures through user involvement and by designing the task, job, environment, equipment, etc.

The exact strategy to reduce non-compliance will depend to a large extent on the reasons why procedures are not followed in the first place, for example:

- If not following a procedure or instruction has become the normal way of behaving within a facility, employees see little value in them. Consider explaining the reasons behind the procedure; change the procedure if it becomes inappropriate; or consider rationalizing work systems to reduce the number of unnecessary rules. If the rule is critical, then increase the probability of detection.
- If an instruction is impossible or extremely difficult to work in a particular situation (e.g., conflicting requirements or physically impossible to perform the activities in the specified manner), then improve job design, the human-machine interface, and the working conditions; implement a suitable reporting system; and provide more appropriate supervision.

The following will help ensure procedures more likely to be used:

- Ensure the "right" way to do the job requires less time and effort. Eliminate tendencies to take shortcuts.
- Use a procedure format that suits the task and the end user (e.g., checklist, flowchart, diagram, decision-aid, charts, photos).
- Involve end users in the development and implementation of the procedures (to help close the gap between "work as engineered" and "work as done").
- Design the task, job, environment, equipment, etc. to support the end user in following the procedures. Design the job so that the correct procedure is hard to avoid.
- Balance the level of detail in procedures with the experience and competence of the end user. Generally, procedures should be written for a "qualified" operator or technician.

As noted in the recent Gulf Research Program workshop summary, "Procedures have to be appropriate for the context in which they are being used, and employees need to know when they can and cannot follow them based on the situation." (National Academies of Sciences, Engineering, and Medicine 2018). Later in the report it is noted that it is important that employees, "should be empowered to slow down, shut down, stabilize, and get the right procedure before advancing" in any given situation.

Barrier Management

IOGP defines a *barrier* as, "A risk control that seeks to prevent unintended events from occurring, or prevent escalation of events into incidents with harmful consequences." (International Association of Oil and Gas Producers 2014)

During the recent updates to API RP 75 and within the Human Element Working Group there was significant debate and discussion as to whether the human element should be considered a barrier within an overall risk management system. The following comments and clarifications, based in part on IOGP Report 456, were discussed:

> *Human barriers rely on the actions of people capable of carrying out activities designed to respond and act to manage the potential cause or threat of an event. Human barriers include:*
>
> - *Operating in accordance with procedures*

- *Surveillance, operator rounds, and routine inspection*
- *Authorization of temporary or mobile equipment*
- *Acceptance of handover or restart of facilities and equipment*
- *Response to process alarm and upset conditions (e.g., outside safe operating envelope)*
- *Response to emergencies*

Human barriers require a set of individual and collective behaviors that ensure the barriers remain effective (e.g., not short-cutting procedures, honoring the full Management of Change process, and staying within the safe operating envelopes). Sometimes these behaviors are referred to as 'operating discipline.' Without these desired behaviors, resilience of human barriers will be very low. Strong, energetic and consistent leadership will always be required to maintain acceptable human barrier health.

(International Association of Oil and Gas Producers 2011)

For safety critical activities, a framework such as this is essential to reduce the possibility of major accidents to the lowest possible levels. In a recent white paper published in December 2016, the Chartered Institute of Ergonomics and Human Factors details rigorous ways to apply human factors in barrier management with emphasis on achieving resilience in the barriers. (Chartered Institute of Ergonomics & Human Factors n.d.) See the following figure:

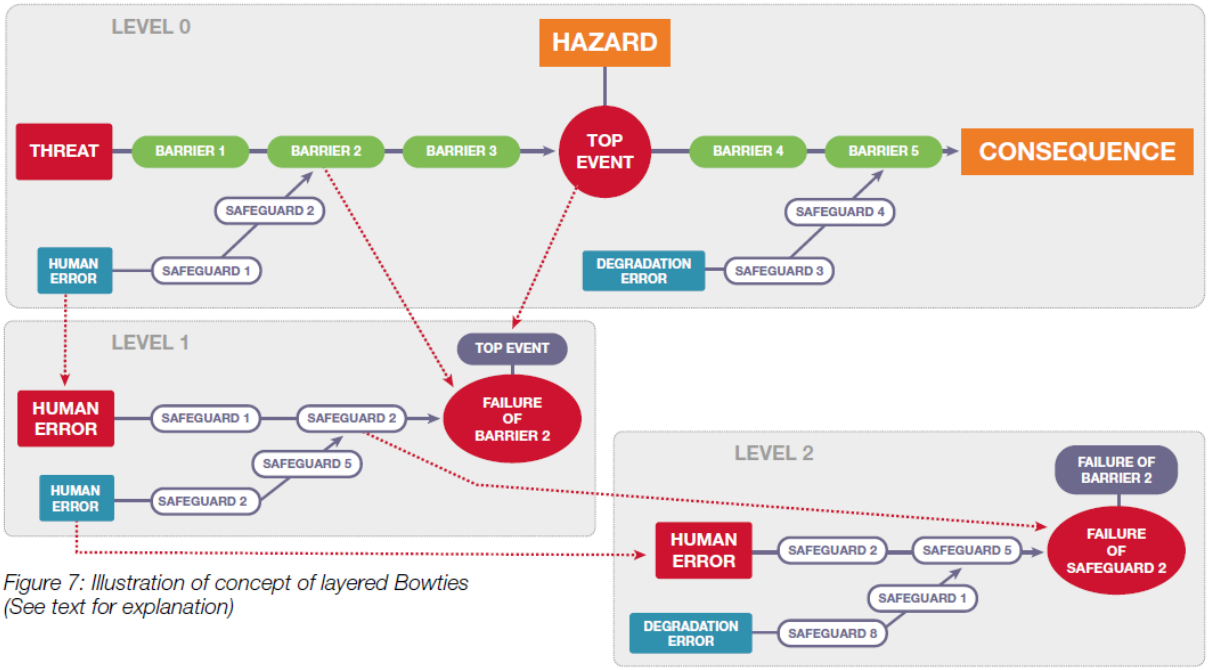


Figure 7: A Layered Bowtie - Integrating the Human Element into Barrier Management

HSE professionals and technical and operational managers are encouraged to use the concepts, guidelines, and detailed recommendations in this white paper as a basis for integrating the human element as one of the key barriers in a risk management system.

Perspectives on Organizational Development

Organizational development is a critical activity impacting all the key elements of a successful enterprise risk management structure. It is not simply a background activity to be "handled by human relations." Executive leadership should be directly involved in and lead activities in organizational development.

The "mental model" in Figure 8 depicts Organizational Development as an overarching activity essential to tie together the key elements of occupational safety, process safety, and human factors.

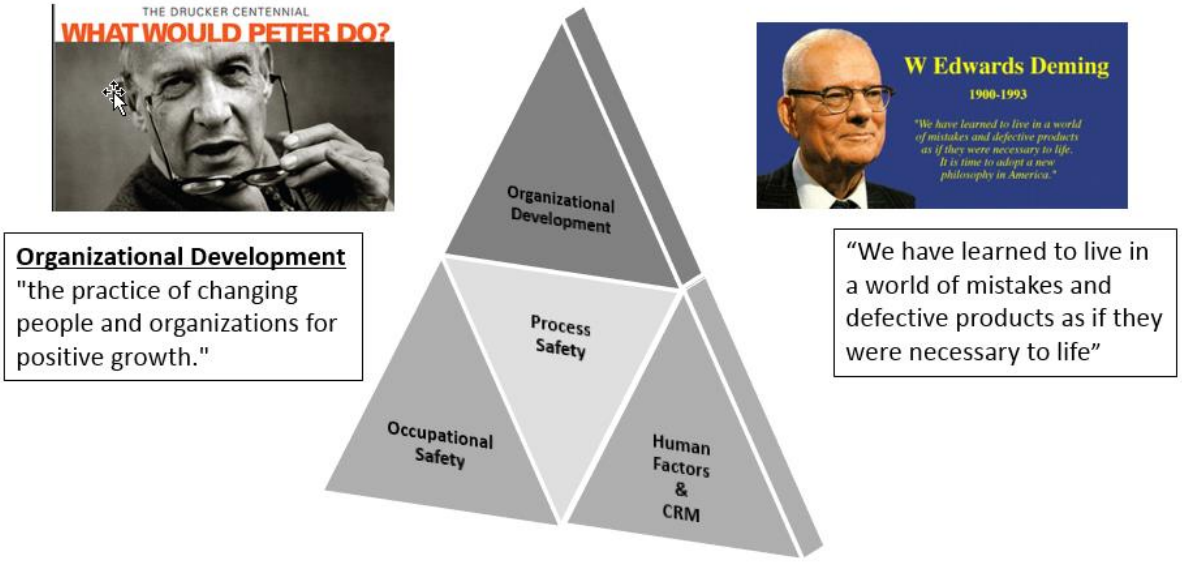


Figure 8: Expanding Risk and Safety to a Broader Framework of Organizational Development of High Reliability Organizations (Grossweiler 2015)

Two thought leaders with major impact and influence on organizational development concepts over the last several decades were Peter Drucker and Edward Deming.

Drucker noted that a company culture can prevent attempts to create or enforce a strategy that is incompatible with an existing culture. Culture must be driven by corporate leadership. It is a critical success factor for successful management of enterprise risk.

Deming was noted for advancing concepts for measuring performance as a key element in improving performance and a framework for continuous improvement in enterprise performance.

Leadership and Safety Culture

Leadership has many different definitions! It is not be necessary or possible to get a consensus definition of *leadership* or *safety culture*. Reading biographies of several famous leaders helps develop a broad perspective on leadership.

General Kelly, The Secretary, Department of Homeland Security gave two pieces of advice on leadership in a keynote address at the USCG Academy graduation in May 2017:

> ***Take care of your people.*** *Train them. Mentor them. Defend them. They will do anything you ask them to do. They'll show up to work on time. They will put their lives at risk, on the*

high seas interdicting drugs in tons, dealing with the most dangerous men on the planet, or they would jump out of a helicopter in the middle of the night into raging seas to save someone's life. All you have to do is lead them.

Tell the truth. *Tell the truth to your seniors even though it is uncomfortable, even though they may not want to hear it. They deserve that.*

(U.S. Department of Homeland Security 2017)

The point with regard to "truth" noted by some industry leaders, i.e. ***"An audit which does not find something which can be improved concerning actionable aspects is not a good audit."*** is worth emphasizing. Leaders expect and accept information critical to improving operations.

Achieving "safety culture" is also challenging. In some organizations, when the *"safety policeman/woman" is present (this could be an HSE safety representative), everyone acts in the right way and does the right thing. As soon as the safety policeman/woman leaves, performance returns to "business as usual."*

In the SPE Distinguished Lecturer Program, Kenneth E. Arnold outlined the following activities that help build a culture of safety:

From an organizational level there must be:

- *Mechanisms establishing structure and control – To specify what is needed to operate safely and check that it is being done.*
- *Actions establishing safety norms – To encourage people to act properly even when no one is looking or when it is not in their immediate best interest.*
-

From an individual perspective there must be:

- *Mechanisms establishing competency – Knowledge and ability of the structure, control, and behavioral norms.*
- *Actions establishing motivation – So a totally selfish person would act in accordance with behavioral norms.*

(Arnold n.d.)

"**Safety culture is doing the right thing, even when nobody is watching."**

Over the last decade, several sources, including IOGP, have introduced the characterization of performance within an organization along the progression of: Pathological, Reactive, Calculative, Proactive, and Generative Performance. Advancing enterprise performance on this path requires a strong contribution from organizational development.

IOGP 435 provides a framework within which a company can assess the overall quality and effectiveness of its risk management system. Organizations should strive to climb the ladder all the way up from *pathological* to *generative* performance.

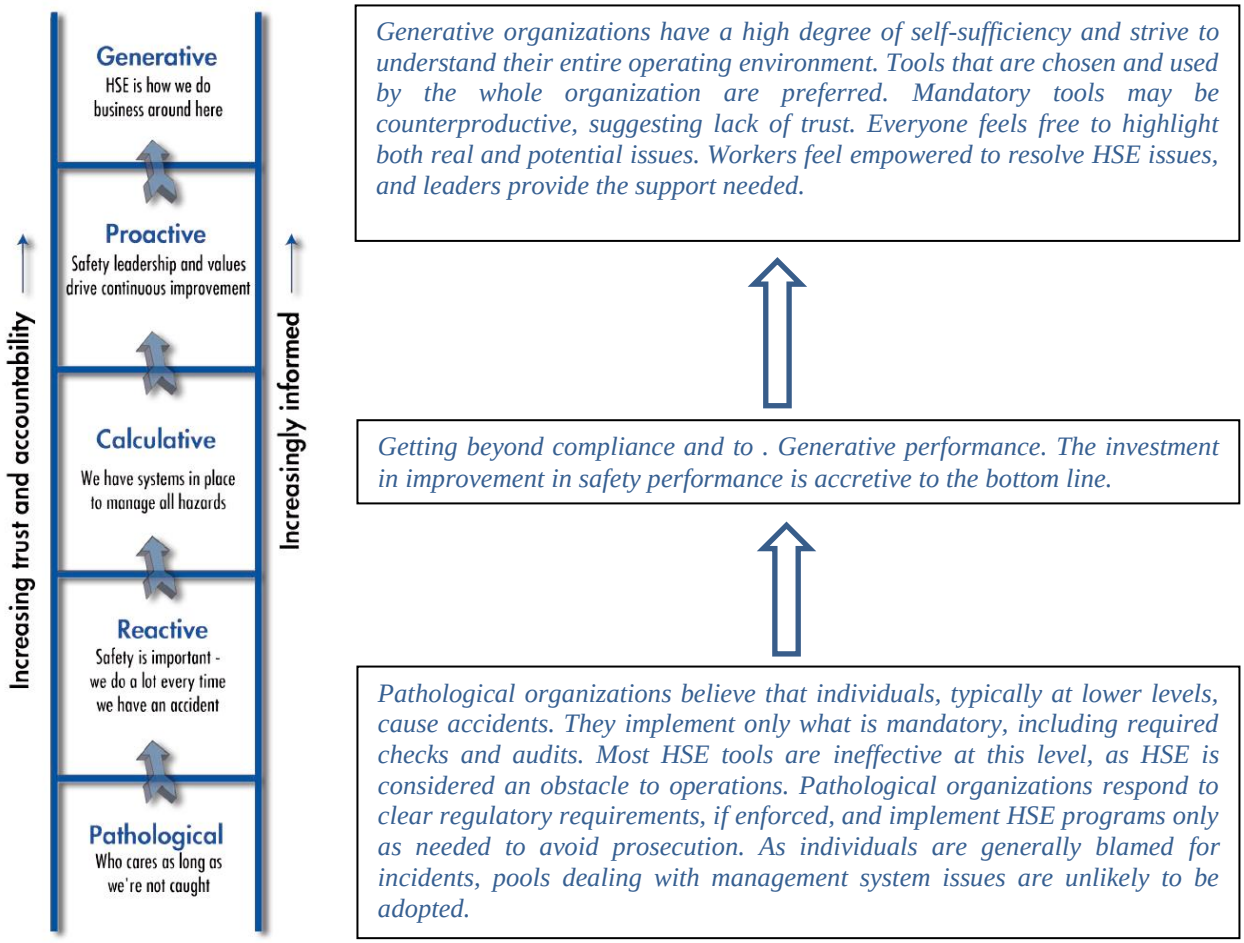


Figure 9 (International Association of Oil and Gas Producers 2010)

Path to Generative Performance – A Learning Organization.

The matrix in the table below was presented in the September 2015 SPE webinar. A framework such as this suggests approaches for a Learning Organization to ensure that persons at all levels throughout the organization have the appropriate background and perspective for managing risk and safety. Most organizations realize that appropriate training should be provided for front line workers. This framework outlines levels of education and training for everyone throughout the organization, including executive level management.

Organization Level	Retreats	Individual Coaching	Seminars and Symposia	Training in CRM Concepts and Implementation	Procedures	Simulators	Table Top Exercises	Support from CRM Consults	Periodic Audits
Executive / Senior Management	X		X						
Operating Management	X	X		X			X	X	
Senior Risk and HSE Professionals			X	X	X	X	X	X	
Front Line Operations				X	X	X	X	X	

Ref: (1) Guidance on CRM and Non-Technical Skills Training Programs – Energy Institute, London
(2) IOGP Publications Including 501 & 502
(3) Guidelines by Consulting Companies, CVAs, and Class Societies (Ex: ABS, DNV-GL, etc.)
(4) Book "Crew Resource Management" – Kanki et al

Figure 10: Potential Framework of Organizational Development and CRM Education and Training for a Learning Organization (Grossweiler 2015)

Activities at executive and senior management levels in a Learning Organization might include corporate retreats, industry seminars, and symposia. Emphasis would be on major enterprise risks, leadership development, and achieving commitment to corporate vision. Several leading business schools provide seminars on these topics.

Learning activities for operating management might include similar activities but with more specific training directly related to a persons current operational positions and responsibilities.

The HSE professionals continue to participate in industry sessions to maintain a "state of the art" competency of best practices in Occupational Safety and Process Safety.

Recommendations

Most companies already have safety management systems in place and should strive for continuous improvement. The approaches for continuous improvement established by Charles Deming in the 1990s are still relevant today.

Companies should strive for an appropriate balance between managing risks to personal safety and preventing major disasters. Within corporate risk management, companies should concentrate on the major risks. Personal safety in accordance with well-established corporate and industry guidelines should be the primary responsibility of all individuals throughout the organization.

Companies should set a goal of Beyond Compliance and Zero Harm for the organization. IOGP Report 435 provides a roadmap for categorizing and assessing an organization's level of performance across all elements of operations and risk management. Organizations performing at

the “Generative” level set performance targets beyond compliance. The SPE Technical Report, *Getting to Zero and Beyond*, reinforces this goal.

Continuing efforts to improve leadership or safety culture are important. However, a consensus on approaches to these concepts applicable to all companies across the industry is not possible or necessary. Ultimately, leadership is taking care of your people and safety culture is doing the right thing when no one is watching.

Conclusions

The discussions in this paper combine:

1. An overview of industry and regulatory activity over the last decade to improve risk management and safety performance, and
2. An outline of ideas for increasing emphasis on human factors to improve safety performance in the future.

The industry is strong in addressing occupational safety and process safety. The biggest improvements in managing risk can come from comprehensive approaches to applying organizational development concepts throughout the organization and especially at executive levels.

References

Arnold, Kenneth E. n.d. "Assuring an Adequate Safety Culture in Production Operations." *Society of Petroleum Engineers.* https://www.spe.org/dl/slides-graphics.php.

Chartered Institute of Ergonomics & Human Factors. n.d. "Human Factors in Barrier Management." (Chartered Institute of Ergonomics & Human Factors). https://www.ergonomics.org.uk/Public/Resources/Publications/Barrier_Management.aspx.

Grossweiler, Phil. 2015. "Human Factors & Crew Resource Management (CRM)." *Society of Petroleum Engineers Webinar.* Society of Petroleum Engineers, September 2.

Hinton, J. Jack, Andrew Dingee, Colette M. Glencross, Tony Zamora, Phil Grossweiler, John M. Karish, and Tom Knode. 2018. *Getting to Zero and Beyond: The Path Forward, Improving Safety in the Oil and Gas Industry.* SPE Technical Report, Society of Petroleum Engineers.

Hudson, Patrick, and John L. Thorogood. 2012. *The Human Factor, Process Safety and Culture.* Summit Paper, Houston: Society of Petroleum Engineers.

International Association of Oil & Gas Producers. 2005. "Human Factors - a means of improving HSE performance." (International Association of Oil & Gas Producers) 368. https://www.iogp.org/bookstore/product/human-factors-a-means-of-improving-hse-performance/.

International Association of Oil & Gas Producers. 2013. "Shaping safety culture through safety leadership." (International Association of Oil & Gas Producers). https://www.iogp.org/bookstore/product/shaping-safety-culture-through-safety-leadership/.

International Association of Oil and Gas Producers. 2010. "A guide to selecting appropriate tools to improve HSE culture." (International Association of Oil and Gas Producers) 435. https://www.iogp.org/bookstore/product/a-guide-to-selecting-appropriate-tools-to-improve-hse-culture/.

International Association of Oil and Gas Producers. 2014. "Operating Management System Framework for controlling risk and delivering high performance in the oil and gas industry." (International Association of Oil and Gas Producers) 510. https://www.iogp.org/bookstore/product/operating-management-system-framework-for-controlling-risk-and-delivering-high-performance-in-the-oil-and-gas-industry/.

International Association of Oil and Gas Producers. 2011. "Process safety - recommended practice on key performance indicators." (International Association of Oil and Gas Producers) 456. https://www.iogp.org/bookstore/product/process-safety-recommended-practice-on-key-performance-indicators/.

Kletz, Trevor. 2009. *What Went Wrong?* Butterworth-Heinemann.

National Academies of Sciences, Engineering, and Medicine. 2016. *Strengthening the Safety Culture of the Offshore Oil and Gas Industry.* Washington, DC: National Academies Press. doi:10.17226/23524.

National Academies of Sciences, Engineering, and Medicine. 2018. *The Human Factors of Process Safety and Worker Empowerment in the Offshore Oil Industry: Proceedings of a Workshop.* Washington, DC: The National Academies Press. doi:10.17226/25047.

Society of Petroleum Engineers - Technical Reports Committee. 2016. "Assessing the Processes, Tools, and Value of Sharing and Learning from Offshore E&P Safety Related Data." (Society of Petroleum Engineers). https://www.onepetro.org/general/SPE-182847-TR.

Society of Petroleum Engineers - Technical Reports Committee. 2018. "Getting to Zero and Beyond: The Path Forward." (Society of Petroleum Engineers). https://www.onepetro.org/general/SPE-191770-TR?sort=&start=0&q=&fromSearchResults=true&rows=10#.

Society of Petroleum Engineers - Technical Reports Committee. 2014. "The Human Factor: Process Safety and Culture." (Society of Petroleum Engineers). https://www.onepetro.org/general/SPE-170575-TR.

Society of Petroleum Engineers. 2018. *SPE Summit: Safer Offshore Energy Systems Summary Report.* Society of Petroleum Engineers. http://www.national-academies.org/cs/groups/gulfsite/documents/webpage/gulf_188531.pdf.

Taleb, Nassim N., Daniel G. Goldstein, and Mark W. Spitznagel. 2009. "The Six Mistakes Executives Make in Risk Management." *Harvard Business Review* (Harvard Business Publishing Corporation) 1-4. https://www.researchgate.net/publication/236302921/download.

U.S. Chemical Safety and Hazard Investigation Board. 2005. *Refinery Explosion and Fire.* Investigation Report, U.S. Chemical Safety and Hazard Investigation Board.

U.S. Department of Homeland Security. 2017. "Secretary Kelly Delivers Remarks at the USCG Academy Commencement." *U.S. Department of Homeland Security.* May 19. https://www.dhs.gov/news/2017/05/19/secretary-kelly-delivers-remarks-uscg-academy-commencement.

Van Scyoc, Karl, and Reese Hopkins. 2012. "Anatomy of the Risk Matrix." *15th International Symposium.* Mary Kay O'Connor Process Safety Center. http://psc.tamu.edu/wp-content/uploads/10A-Van-Scyoc-DNV.pdf.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Procedural Performance: Possible Costs of Time Pressure, Shift Change, and Task Complexity

S. Camille Peres[12], Ranjana K. Mehta[21], Wimberly S. Hoyle[1], Ashley Shortz[1]
[1] *Environmental and Occupational Health Department,*
[2] *Industrial and Systems Engineering Department,*
Texas A&M University, College Station, TX
Emails: peres@tamu.edu, rmehta@tamu.edu

Abstract

Procedural tasks, which typically involve performing a sequence of steps in a regular and consistent manner, are an inherent part of almost all high-risk industrial settings. Further, it is not uncommon for a need to arrive when these tasks need to be performed at an accelerated rate to meet a deadline or accommodate a mechanical state in the facility. Additionally, because these industries operate on 24-hour cycles, the workers performing these procedural tasks work shift work—often working 12-hour shifts and varying between day and night shifts. Extensive research has shown that changing between day and night (or vice versa) work shifts causes fatigue and can result in decrease performance. Finally, given the nature of these complex socio-technical systems, some of the procedural tasks are more complex than others. These three variables—time pressure, shift change, and task complexity—could of course individually have impacts on workers' performance with procedures as well as have combined impacts on performance. However, there is little objective research investigating workers' performance on procedural tasks in this domain.

It is conceivable that workers maybe able to sustain task performance for a period of time with a combination of these three variables with increased effort and focus. However, this task performance likely comes at a cost. For instance, Metha and her colleagues found that when stressed, participants were able to maintain a certain performance but it required a higher physiological load, which, if sustained can lead to fatigue.

This presentation will share the results of participants who completed 24 different procedural tasks (procedures) representing the 3 variables mentioned above. They completed 12 during a day shift and 12 during a night shift. For each of the 12 day/night shift, half required the participant to complete the procedure under time pressure and the other half were self-paced, and the procedures varied in their levels of complexity.

Participants' performance on the procedures at a step level (2-perfect, 1-some problems, 0-fail) were scored and their physiological responses (Heart Rate, Heart Rate Variability) were recorded.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Multi-level Failure, Causality and Hazard Insights via Knowledge Based Systems

Erzsébet Németh, Ian Cameron
School of Chemical Engineering
The University of Queensland,
Brisbane, Australia 4072

Email: itc@uq.edu.au

Keywords: Failure, causal graphs, hazard identification, diagnosis, knowledge based systems, intelligent systems

Abstract

Over many decades there has been a significant development of knowledge-based, intelligent design tools and their use in the design of process systems. Amongst such tools are "intelligent" piping and instrumentation (P&IDs) design environments, coupled to life cycle design environments. These tools can provide opportunities for the development of new, more efficient and re-usable approaches to hazard identification and diagnostic systems. They leverage modern information technology characteristics of such design environments. These considerations are part of a growing trend in industrial digitalization, as reflected in such initiatives as Industry 4.0 in Europe and driven by the Industrial Internet of Things (IIoT).

Within this larger industrial digitalization picture, this work discusses the principles, developments and application of a hazard identification methodology (BLHAZID) that exploits structured representations of the design in the form of ISO15926 data standards. The hazard identification methodology is based in knowledge representations of failure modes of equipment types that are found in many process designs and how those failures subsequently affect the system states and other components. The underlying causal models can be used at various levels of aggregation, model fidelity and component inclusion detail. The aggregation can span across the most detailed view at the smallest component level through subsystem level to plant level perspectives.

The ability to represent and then display failure causation and implications at different levels of granularity allows deeper insight into system failures, and the potential for real-time diagnostic deployment. The importance of failure and subsequent propagation prevention through the use of

safety instrumented systems and other barrier devices is possible. Outcomes can be visualized in informative ways.

The presentation will discuss these intelligent information technology approaches via some a case study, highlighting the advantages and challenges such approaches bring to hazard identification as well as highlighting other application areas such as real-time diagnosis, corporate knowledge capture of failures, operator training and accident investigation.

Motivation

In the following discussion, we highlight some of the motivations to consider computer aided developments driven by the significant focus on industrial digitalization. Increasing digital connectivity and the focus on system life cycle processes.

Challenges in failure, causality and hazard identification:

The hazard identification phase of risk management applied to complex process design systems is still a significant challenge in terms of detail, time, cost, quality of outcomes and efficient re-use of generated knowledge. Today, hazard identification tasks are almost exclusively performed by Hazard and Operability (HAZOP) studies that adopt a particular system representation and methodology. In some industries Failure Mode and Effects Analyses (FMEA) are also used. Both these approaches normally use diverse teams of participants applying a form of critical enquiry around the intended design. A primary source of information is represented in Piping and Instrumentation Diagrams (P&IDs). In the case of HAZOP studies, the basic approach has been accompanied by an ever-growing list of supporting documentation, and extended, rightly or wrongly, into other aspects of systems' analysis, such as non-fluid systems, maintenance, waste considerations, commissioning, emissions and the like.

In a comprehensive critique, Baybutt (2015) discussed a range of potential weaknesses using HAZOP around team issues, meaning and interpretation of design intent, basic issues related to parameters and guidewords as well as technical coverage, operability and specific hazard types. He also shows that many of these insights and concerns have been present for decades. Some things appear to have not changed.

In a recent review of hazard identification methodologies and tools, Cameron et al. (2017) also considered similar issues. The issues can be summarized around recurring challenges for the traditional HAZOP methodology as:

- lack of depth in analysis,
- lack of diversity and imagination within study teams
- lack of completeness in identifying scenarios
- lack of completeness in identifying initiating events
- dealing with the complexity of the process
- poor documentation and communication of outcomes
- loss of focus due to the duration of the studies
- confusion as to the propagation paths of deviation to initiating cause and to consequence
- repetitiveness of the studies
- inadequate assessment of the interactions amongst plant, people, procedures
- review of changes

Jarvis and Goddard (2016) recently did a study of 100 major losses over the 20 year period: 1996-2015, in order to understand the common causes of those losses. Major losses were classed as losses greater than $US50 million (capital plus business interruption), with no consideration of other consequential losses such as civil fines, environmental clean-up, personal injuries and reputational damage. Total losses for the period were in the order of $US25 billion.

The outcomes of this study in regard to the adequacy of Process Hazard Analysis (PHA)[1] were:

- 7% of mechanical integrity failure (MIF) were primarily associated with PHA inadequacies, which was one factor in Management System Failures (MSF) [2]
- 28% of non-mechanical integrity failures (NMIF) were associated with PHA activities, and,
- 48% of totalled MIF and NMIF were associated with PHA activities

These insights into current practice put pressure on maintaining very high quality PHA activities, and also raise questions concerning the long-term suitability of current practices in complex and highly interconnected socio-technical systems. This is especially a challenge around the present growth in systems' connectivity, embedded devices and life cycle perspectives driven by such developments as Industry 4.0 and IIoT. In the context of safety and risk we now briefly discuss some of the current drivers around smart systems.

Drivers from current industrial digitalization and the opportunities they afford:

For more than 25 years there has been a significant acceleration in industrial digitalization, driven primarily by information and communication technologies (ICT) and massive growth of internet technologies. Significant process and business performance is now driven by The Industrial Internet of Things (IIOT) which refers to:

> *"a network of physical objects, systems platforms and applications that contain embedded technology to communicate and share intelligence with each other, the external environment and with people".* (Accenture, 2018)

Key aspects to consider in the context of IIoT are:

- Investment levels in IIoT are predicted to reach $US123B in 2021 (i-scoop, 2018), 2018a).
- Massive sensor deployment and reduced costs – embedded and also wearable. There is predicted to be over 50 billion internet connected devices by 2020 from a base of 17 billion in 2016. (Morgan Stanley 2018a)
- Massive equipment embedding of micro-controller units (MCUs)
- Industrial IIoT adoption rising from about 8% of capital budget to 18%. IIoT is a key driver of market growth. (Morgan Stanley 2018b)

What does all this mean to the process industries and in particular to function and failure of complex systems? For industry, the main IIoT drivers as reported by Morgan Stanley are:

1. Improving operational efficiency (47%)
2. Improving productivity (31%)
3. Creating new business opportunities (29%)

---

[1] PHA in this study consisted of: HAZOP, LOPA and SIL activities.

[2] The 7 factors in the Management System Failures were: Inspection programs, Materials & Quality Assurance, Operations/Practices/Procedures, Control of Work, PHA and Management of Change, Available Safety Critical Devices.

4. Reducing downtime (28%)
5. Maximizing asset utilization (27%)
6. Reducing asset life cycle costs (18%)
7. Enhancing worker safety (14%)

Given that risk and safety are temporal in nature we need to consider the implications on the methodologies and the nature of the software platforms for safety and risk issues into the future. What was considered acceptable today will be under threat from tomorrow's developments. Transitions to life cycle, smart systems that are based on systems fundamentals will provide a range of benefits not easily achievable today, and fit more effectively into the current digital tools of IIoT.

In the next section we consider the specific area of function, failure, risk and the identification of hazard in complex designs. This is an area with a long and important history which has experienced numerous methodological developments over more than 60 years and more recently the development of software support platforms.

For major projects in the process industries, current practices are struggling to provide efficient and high quality outcomes as attested by recent studies and critiques already mentioned. It is also likely that good, viable solutions will involve an eco-system of integrated approaches: software platforms, knowledge based systems, re-use of prior knowledge, real-time gathering and processing of data and information to continually incorporate deeper and wider knowledge to enhance operational excellence. These will also provide easily accessible and usable corporate memory for future developments.

Function, failure and causation: the role of knowledge representation systems

Dealing with complex, highly interconnected systems subject to failure definitely requires "systems" approaches, conceptualizations and thinking. There are several important considerations to such approaches in the current era of rapid digitalization:

1. System conceptualizations that adequately represent the major elements and their interconnections. This involves not just the physical plant, but also procedural aspects and human factors, people issues.
2. The ability to exploit evolving digital representations and data interoperability standards such as ISO15926[3] that provide access to the evolving design in a neutral format.
3. An approach based on fundamental principles and formal concepts around function, capability, failure and causality, and their organized knowledge representation.
4. Approaches that have applicability across the whole life cycle of product and process, so that maximum benefit can be derived from the insights of designers, managers, operators and other associated staff and personnel.
5. The ability to incorporate learning from failures, to identify, capture and enhance knowledge of the system over time. This aids in capturing corporate memory.
6. The ability of the methodology to be adaptable to different scales of representation, such as:

[3] See the International Organization for Standardization (ISO): https://www.iso.org/search.html?q=15926

a. Access to multiple causal models of varying complexity and fidelity that can be applied as designs develop and mature
b. The ability to look at the system from highest level of detail at the individual component level to more aggregated views
c. The ability to exclude/include process equipment within any failure analysis
d. The ability to estimate system failure propagation time scales or track overall failure frequency or probability estimates.

There are numerous knowledge based system perspectives and conceptualizations that can be adopted to address function, failure and causation. Many had their origin in the 1980s when AI and expert systems were making some headway. An early AI based HAZOP system using the Prolog declarative language appeared in the 1980s (Cameron, 1986), and other work at Loughborough University in the UK has led to commercial realization in the form of the *hazid* software platform[4]. These approaches essentially took the HAZOP methodology at the time and applied structure and some aspects of artificial intelligence tools to aid users in performing their tasks.

Many of these approaches are highlighted in the recent review by Cameron et al. (2017), and the reader is referred to that for more information. What follows here, is a discussion around the conceptualization, development and application of a functional systems framework (FSF) that has formed the basis of our own research into looking at the issues around plant, people and procedures and their inter-relationships. It needs to be emphasised that this is one of many systems based approaches built on knowledge management and use.

The fundamental conceptualization is seen in Figure 1, with basic concepts drawn from fundamental system concepts of entities, properties, function, failure and causation (Bunge 1997). The framework provides a firm foundation to pursue systems related investigations.

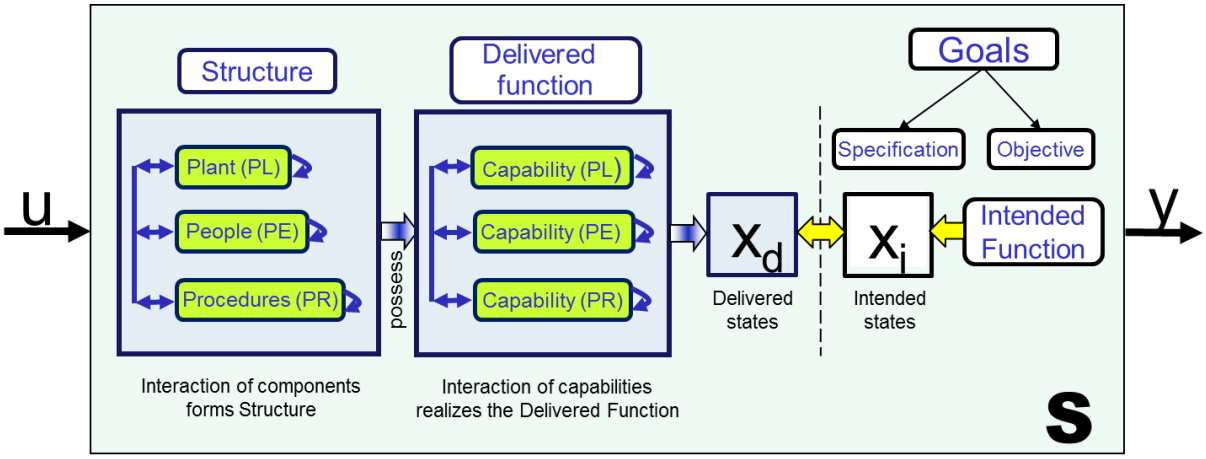


Figure 1 A functional systems framework (FSF)

[4] See: https://www.hazid.com/

The FSF pictures key components of plant, procedures and people, highlighting components capabilities, function and intended system goals. This has been discussed by Seligmann et al. (2012) in which he developed a blended hazard identification methodology that combined aspects of HAZOP with FMEA to generate deeper insights and better hazard coverage than either individual method. It was tested on a commercial design of a Benzene Saturation Unit.

The underlying causal model that considers the plant components (equipment) and the streams is seen in Figure 2. This considers that properties of both plant equipment and streams give rise to a set of system capabilities. It is those capabilities, acting together, that deliver the relevant system functions for a particular process structure, and these address design intentions as reflected in the intended states. Plant components and streams interact in complex ways. Loss of capabilities can lead to failures in components and hence impacts on stream properties and vice versa.

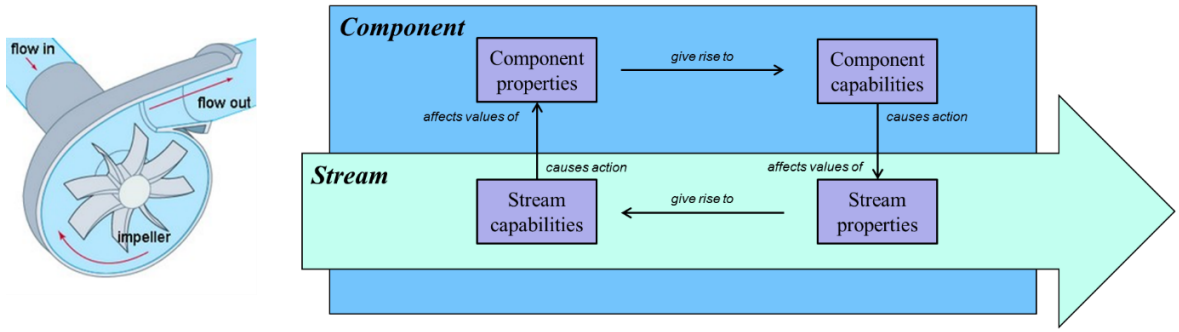


Figure 2 Causal model for failures and failure propagation

With reference to Figure 1, HAZOP considers 'intended function' in terms of the stream properties and looks at the difference between important 'intended' and 'delivered' states, typically expressed as stream values that can include such properties as pressure, flow, temperature, level and concentration. This leads to HAZOP 'deviations', which are then traced to causes and consequences. In a complementary manner, FMEA starts with failure modes with potential failure mode causes, then tracing through to system to identify impacts on function. This typical drives left to right in Figure 1, whilst HAZOP drives from right to left.

The original, overall strategy followed a general workflow which included:

- Efficient extraction of design information from P&IDs using a neutral format standard. In this case: ISO15926, that is now an agreed interoperability data standard between major CAD-CAPE software vendor systems.
- Structured decomposition of the topological information into interconnected subsystems that are amenable to investigation and analysis around failure, causes, implications and causal pathways.
- The ability to build, use, modify and extend knowledge based representations of plant component models that incorporate known failure modes. These can be built with various levels of detail and fidelity.
- The application of those models to the system design to illicit potential failure types, causes and implications across the system.
- Various forms and levels of visualization and representation of outcomes to understand implications for design thinking and operational performance.

The original implementation of this methodology as an experimental tool required the use of several information and knowledge representation and management systems that included:

- Formal description of equipment capability sets (see Figure 3)
- Use of failure modes (FM), failure mode causes (FMC) and failure implications (FMI).
- Development of causal descriptions that link component failures to stream failures and vice versa, leading to causal triplets: {cause, mode, implication}: <FMC><FM><FMI>.
- Development of causal models for common operational modes that incorporate: stream inputs and outputs, internal states, FMs and their interconnections. (see Figure 4).

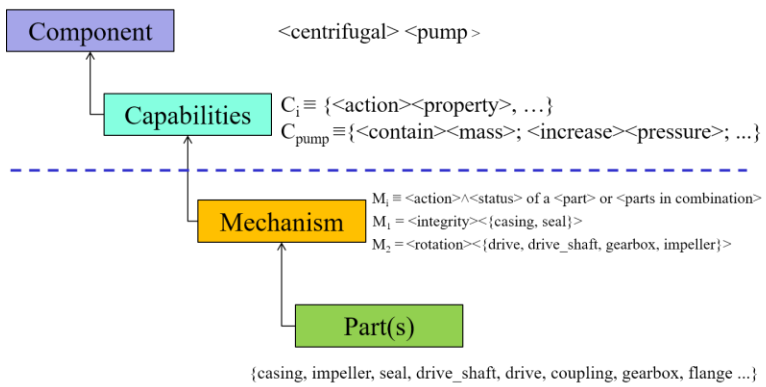


Figure 3 Component capabilities structure

Within the approach taken in this work there is the possibility of adopting multilevel perspectives that relate to:

- *Causal model fidelity*: providing simple to complex models of the causal relations for a component
- *System aggregation level*: providing high level views down to highly detailed views into the causal structures
- *Inclusion detail*: which provides the ability to include or exclude nominated components from the subsystems, such as every pipe segment in a subsystem

These levels of consideration are supplemented with the ability to consider a range of operational modes that can affect the failure modes of component. Other temporal factors related to causal interactions as well as failure frequency/probability can be considered.

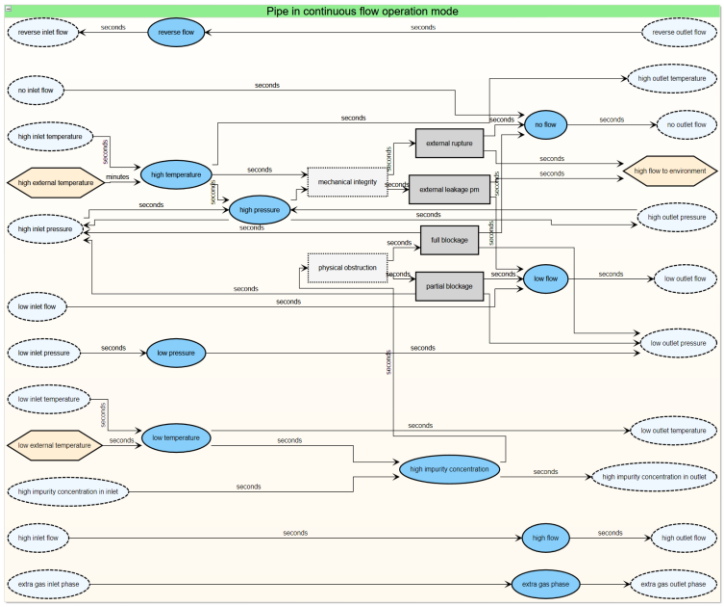


Figure 4 A causal model for a pipe segment

In the following section we discuss how these knowledge representations can be put to work when looking at a particular engineering design to understand failure propagation in the system.

Application and observations

The knowledge representation contained in approaches such as BLHAZID or similar methodologies can be used to consider a range of failure and hazard issues related to process plant. In this case we look at a bulk liquids storage and handling facility that is described in two separate, but linked P&IDs.

P&ID topology is imported via ISO15926 data exchange XML files and automatically analysed, decomposed into a series of interconnected subsystems that link inputs to internal subsystems and major mass and energy inventories and then to system outputs. Figure 5 shows the P&IDs and the first 3 levels of decomposition that is possible. These cover the overall system, the major subsystems and then further detail within a chosen subsystem. Disaggregation can proceed down to the finest level of every individual component in a Piping Network Segment.

Individual component types within a subsystem are automatically identified, and can be associated with models in a knowledge base (KB). The particular operational mode of the subsystems can be chosen, as well as the level of fidelity of model to be used as well as what specific components can be overlooked in the causality analysis. These overlooked items might be all pipe segments within a subsystem, where their failures modes are regarded as not significant.

Investigations can be performed on either, or both component failures (CF) in the form of failure modes (FM) in process equipment, or functional failures (FF) in the form of changes in stream properties. Search algorithms can then be used over the system topology to enumerate the possible causes and implications of a nominated failure. The outcomes of the search methodologies are shown as causal graphs. Other tabular outputs are also possible.

Figure 6a shows a situation where the issue of ‘no level’ in one of the main storage tanks (T-3) was investigated. The subsystem in which the initial failure occurs is highlighted by a yellow background and the specific failure by a yellow chevron shape. The live causal graph can be then traced through various intermediate failures to other functional or component failures, which are associated with other connected subsystems. In this case the two primary functional failures are related to ‘no inlet flow’ to T-3 and an ‘extra gas phase inlet flow’ which raises tank pressure, causing tank failure, and loss of containment.

The detail in Figure 6 is shown at a high level of aggregation. Finer details can be observed by opening other subsystem, as seen in Figure 7 where ‘component failures” in the main feedline subsystem can be seen. This involves numerous items of plant equipment. This methodology is using the causal model shown in Figure 2.

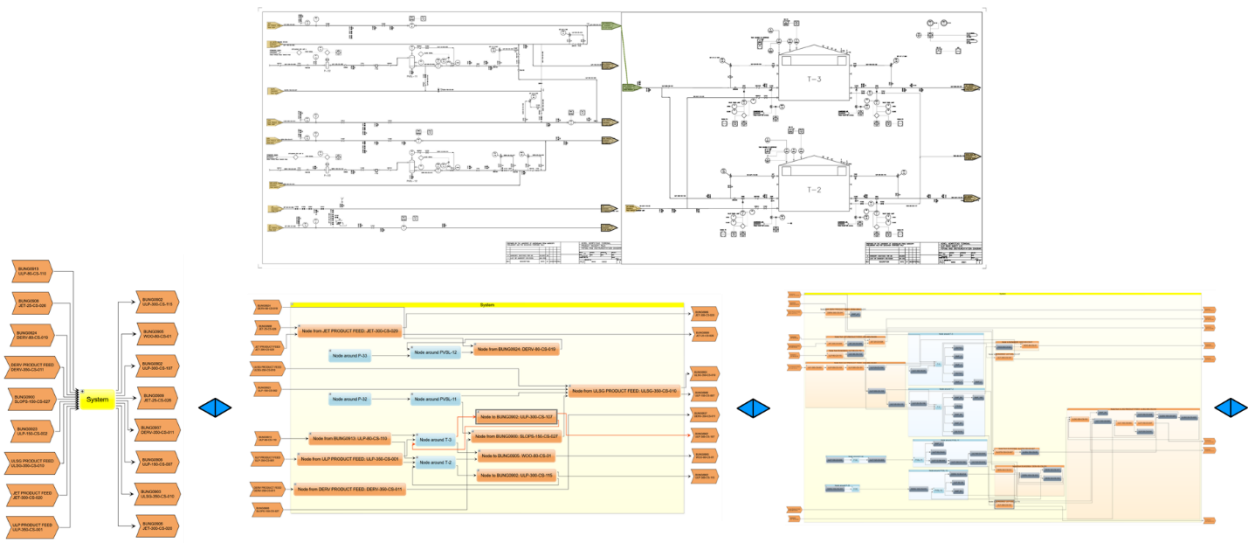


Figure 5 P&ID import and levels of system detail

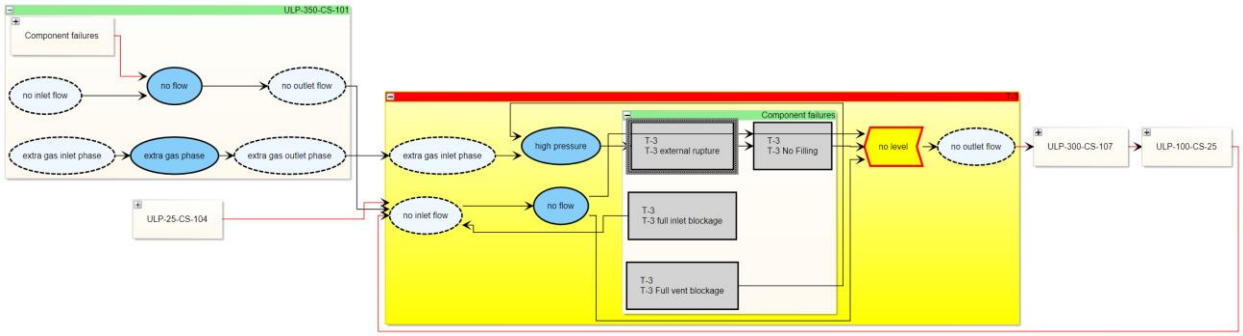


Figure 6a Possible causes of 'no level' (in subsystem T-3) storage tank

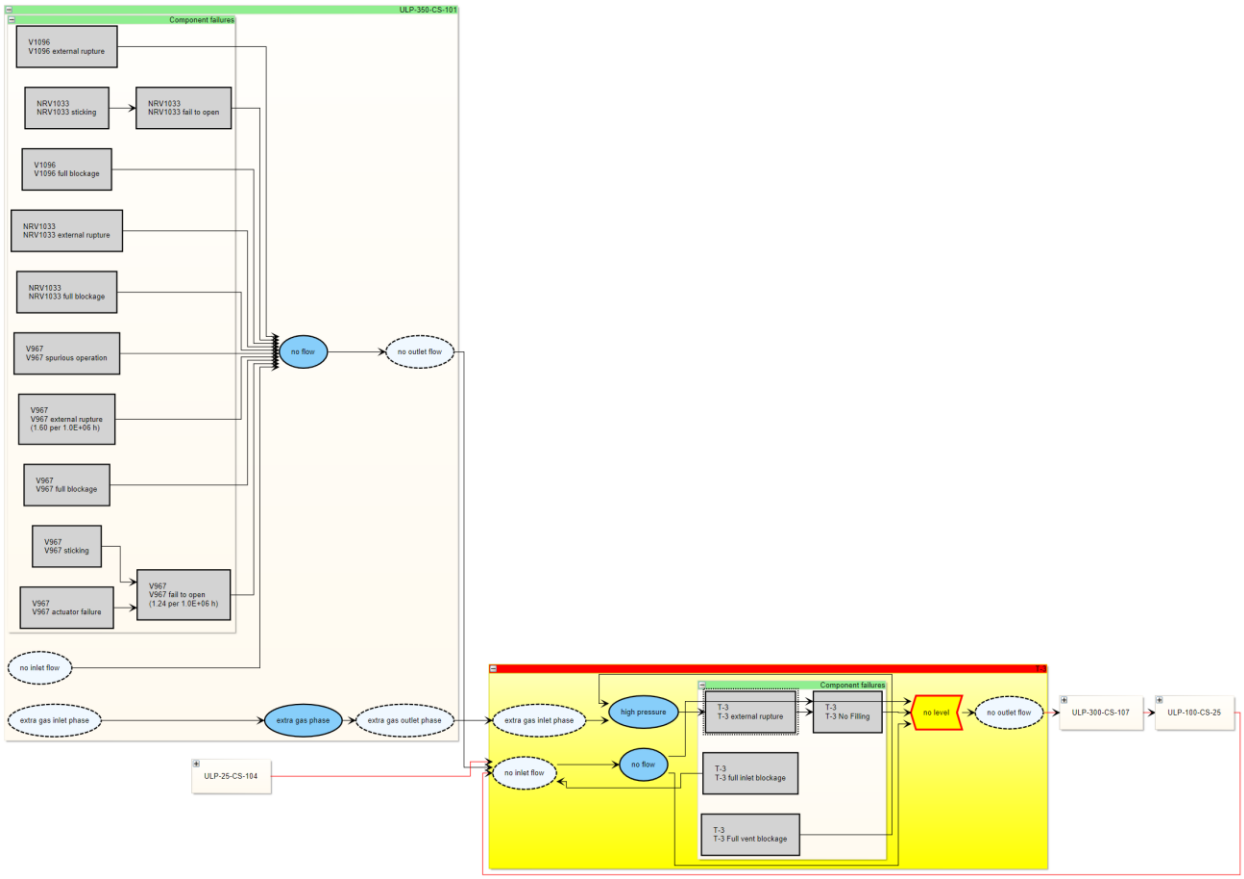


Figure 7 finer detail of component failures in feed subsystem that induce 'no flow' conditions to T-3

Besides the functional failures related to states within major equipment or streams be investigated but given the blended nature of the methodology failure modes in plant components can also be investigated to look at subsequent implications. Figure 8 shows the situation where a major inlet flow control valve (v1096) has a major failure (rupture). This generates several implications: high flow to the environment, no flow to the tank with potentially low level or no level in the tank. The inlet valve failure can also induce a reverse flow from the tank into the prior subsystem.

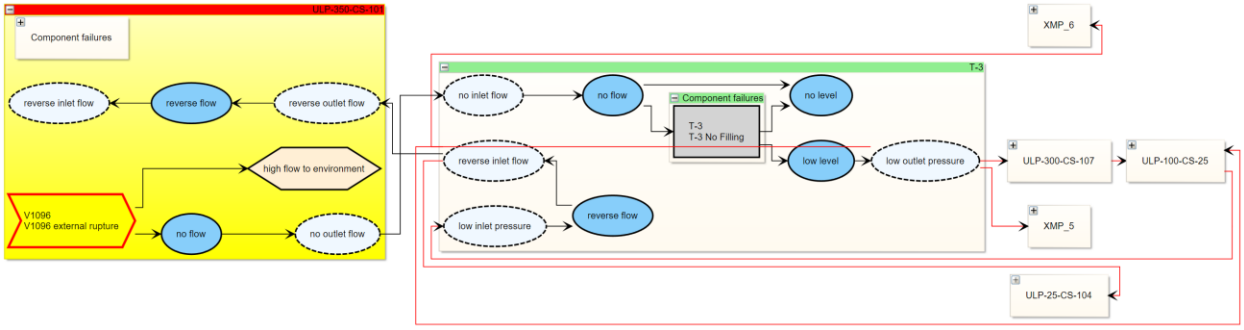


Figure 8 Implications of a major loss of containment through inlet feed control valve.

These rather straightforward examples illustrate the use of formal knowledge based systems that in this case span two P&IDs. More P&IDs can be handled, which potentially allows failure pathways to be tracked across significant sections of process plant.

The quality of the outcomes is clearly measured in terms of the underlying causal models, but the ability to trace causal links through the design can be very important in unravelling the behaviour of the design under numerous failure conditions. It can also be done over many interconnected P&IDs.

Using causal graphs is often a much easier means of visualization than equivalent tables, although these are also generated when the analyses are performed. Early experience with plant operators was encouraging, as they could see the nature of causation visually rather than textually, which required much more effort to interpret.

Higher fidelity models can be used to give more detail, and operational modes can be easily set to investigate what is often a difficult issue in more traditional techniques. Numerous other applications are possible.

Where to from here?

This paper has discussed the need for new approaches that can provide knowledge based tools for understanding failure implications in process designs. Given the growing complexity of information and interconnectedness of process systems, efficient investigation tools as part of risk management that deliver high quality and economically efficient outcomes are required.

Such knowledge based approaches should:

- Support human decision making across the whole life cycle from early conceptual design through detailed design and operations
- Adapt and grow as accumulated operational knowledge is integrated back into systems that can then easily exploit that knowledge in new situations.
- Provide advice in operational circumstances and also for new projects
- Are integrated with plant information systems, including real-time sensor data to provide pro-active functions that can help guide operators' decisions based on causal representations. This leads to real-time diagnostic tools, and the potential to build operator guidance systems off the outcomes of failure analyses.
- The ability to consider how barriers or lack of barriers affect failure propagation and the likelihood of such situations.

Whatever the approach to be taken in this era of IIoT and knowledge systems, it highly likely that the resultant systems will integrate numerous interoperable methodologies into real-time systems that continue to grow over the life cycle of the plant and product. It is also clear that the current digitalization emphasis of Industry x.0 (Schaeffer, 2017) or smart manufacturing will also include high fidelity quantitative modelling and simulation to complement the qualitative and semi-quantitative approaches.

References

Accenture (2015), Winning with the Industrial Internet of Things, How to accelerate the journey to productivity and growth. See: https://www.accenture.com/t20160909T042713Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdfla=en Accessed September 10.

Baybutt, P. (2015) A critique of the Hazard and Operability (HAZOP) study, Journal of Loss Prevention in the Process Industries, 33, 52-58

Bunge, M. (1977) Treatise on Basic Philosophy, Vol 3: Ontology I, The Furniture of the World, D. Reidel Publishing Company, Dordrecht, Holland

Cameron, I.T. (1986), Expert Systems for Hazard and Operability Studies, Proceedings of the Australian Institute of Petroleum Conference on Control and Prevention of Major Hazards, Brisbane, Australia, pg. 1-12, 1986

Cameron, I, Mannan, S, Nemeth, E., Park, S, Pasman, H, Rogers, W, and B. Seligmann (2017) Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better?, Process Safety and Environmental Protection 110, 53-70, August.

i-scoop (2018) See: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/ Accessed September 10.

Jarvis, R. (2015). An analysis of common causes of major losses in the onshore oil, gas and petrochemical industries. Retrieved from http://www.icheme.org/communities/special-interest-groups/safety%20and%20loss%20prevention/events/2015/large-losses-7-july.aspx#.W1kHDdIzY2w Accessed September 9, 2018

Jarvis, R. and A. Goddard (2016). An analysis of common causes of major losses in the onshore oil, gas and petrochemical industries: Implications for insurance risk engineering surveys, Lloyd's Market Association, Version 1.0, September.

Morgan Stanley 2018a, See https://www.morganstanley.com/ideas/microcontrollers-semiconductors-internet-of-things.html Accessed September 10

Morgan Stanley 2018b, See: https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics.html

Schaeffer, E. (2017) Industry X.0: Realizing Digital Value in Industrial Sectors, Redline Verlag, Munich, Germany.

Seligmann, B., et al. (2012) A blended hazard identification methodology to support process diagnosis, J. Loss Prevention in the Process Industries. 25, 746-759

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

An intelligent video fire detection approach based on object detection technology

Hao Wu*, Hao Xiong, Chengjiang Wang, Linhan Du
Jiajun Zhang, Jinsong Zhao
Beijing Key Laboratory of Industrial Big Data System and Application,
Tsinghua University, Beijing 100084, China
*Presenter E-mail: h-wu16@mails.tsinghua.edu.cn

Abstract

Fire that is one of the most serious accidents in chemical factories, may lead to considerable product losses, equipment damages and casualties. With the rapid development of computer vision technology, intelligent fire detection has been proposed and applied in various scenarios. This paper presents a new intelligent video fire detection approach based on object detection technology using convolutional neural networks (CNN). First, a CNN model is trained for the fire detection task which is framed as a regression problem to predict bounding boxes and associated probabilities. In the application phase, videos from surveillance cameras are detected frame by frame. Once fire appears in the current frame, the model will output the coordinates of the fire region. Simultaneously, the frame where the fire region is localized will be immediately sent to safety supervisors as a fire alarm. This will help detect fire at the early stage, prevent fire spreading and improve the emergency response.

1. Introduction

Fire that is one of the most serious accidents in chemical factories, may lead to considerable product losses, equipment damages and casualties. Fire detection at the early stage can effectively prevent the spread of fire and minimize the damage caused by fire. In indoor buildings, smoke detectors and flame detectors are widely used for fire alarm. However, traditional physical sensors have a number of limitations. For example, they require a close proximity to fire sources so that they cannot work for the outdoor scenes [1].

To overcome this problem, some convolutional neural network (CNN) based methods have been proposed and applied for fire detection in various scenarios. However, there are still some limitations during the practical application. Frizzi [2] and Zhang [3] utilized a slide window in

each frame to detect fire. The window size is fixed and usually less than the fire size, which may cause the network cannot learn the complete flame characteristics. Wang [4] and Maksymiv [5] used conventional hand-designed feature extractors to extract the region of interest (ROI), then detected fire in the ROI. However, these methods need to extract ROIs and compute patch images via the network for each frame. This will take a lot of time for the detection.

In this paper, we present a new intelligent video fire detection approach based on object detection technology. Object detection regards fire detection as a regression problem to predict bounding boxes and associated probabilities. This method does not use hand-designed features and the bounding boxes are not fixed so that the network can learn the complete flame characteristics. Each frame is only computed once through the network, which will reduce detection time and resource.

2. Method

Flowsheet

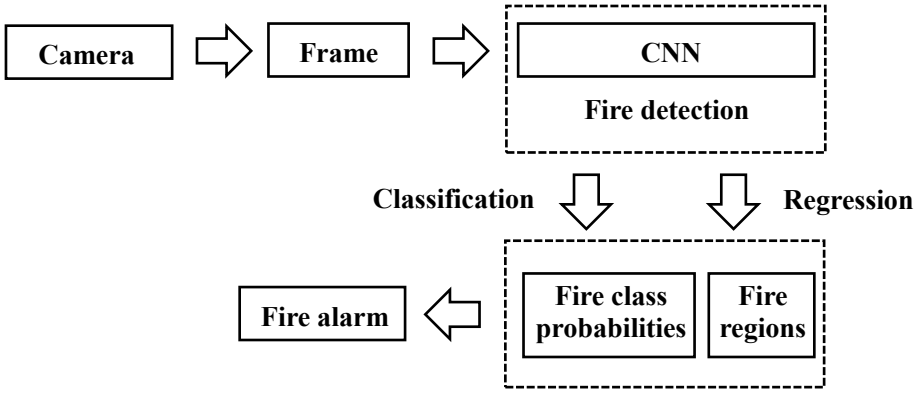


Fig. 1 Flowsheet of the proposed approach.

Fig. 1 shows the flowsheet of the proposed approach. In the application phase, videos from surveillance cameras are processed frame by frame through the trained fire detection model. Once fire appears in the current frame, the model will output the coordinates of the fire region. Simultaneously, the frame where the fire region is localized will be immediately sent to safety supervisors as a fire alarm.

YOLO (You only look one)

In our approach, the key is the fire detection model. There are two classes of method for the object detection task: two-stage and one-stage methods. Compared with two-stage method, one-stage method has faster computation speed. Considering real-time detection, we select YOLO [6, 7] as the fire detection method. YOLO frames object detection as a regression problem to spatially separated bounding boxes and associated class probabilities. YOLO is designed for multi-object detection, however, fire detection is a single-object detection.

Therefore, based on YOLO method, we developed our own method for video fire detection.

3. Experimental results

Fire image dataset

Fig. 2 Annotations of fire regions.

Images that contain fire regions, were collected from some fire image datasets built by previous researchers. Furthermore, via the internet, we augmented our dataset with images of chemical plant fire and other scenarios. The dataset contains 5075 images and the size of the images is not fixed. The proportion of the testing set is 20%, that is, 4060 images as the training set and 1015 images as the testing set. It is important to note that each image may contain several fire regions. Each fire region is annotated by a bounding box for describing its location (see Fig. 2).

Detection results

The fire detection method needs a CNN for prediction. The general function of CNN is a stack of convolutional layers, pooling layers and fully connected layers. Darknet was proposed as the base model of YOLO. For comparison, Darknet and Tiny Darknet were used for the fire detection task.

In the object detection domain, we need to define the true positives and the false positives. If $\mathrm{IOU} > 0.5$ between the predicted box and the ground truth box, the predicted box is true positive;

otherwise, it is false positive. The experiment was done on a computer server with a NVIDIA 1080 GPU. We augmented the testing set (1015 fire images) with 1000 no fire images. The details of the results are listed in Table 1 and Table 2. The accuracy reached 88% and 91% respectively. Compared with Tiny Darknet, Darknet has larger network size but better detection accuracy. Fig. 3 shows several instances of the detection results.

Table 1. Details of fire detection using Tiny Darknet.

		Actual Class	
Predicted Class	Size (63M)	Fire	No fire
	Fire	81.4%	5.1%
	No Fire	18.6%	94.9%

Table 2. Details of fire detection using Darknet.

		Actual Class	
Predicted Class	Size (193M)	Fire	No fire
	Fire	91.2%	9.2%
	No Fire	8.8%	90.8%

(a) No fire images.

(b) Fire images.

Fig. 3 Some instances detected by the trained network.

4. Conclusions

In this article, we present an intelligent video fire detection approach based on object detection technology. Compared with other CNN based classification approaches, our approach is based on YOLO method which predicts bounding boxes and associated probabilities directly. The performance of our approach can meet the needs of real-time fire detection on the precision and the speed.

In the future work, we will focus on reduce the false alarm by adding more negative images (no fire) into the training set. Moreover, a chemical factory may have hundreds of cameras, so developing a parallel fire detection system is also a vital problem for the practical application.

References

1. Shi, L., Long, F., Lin, C. H., & Zhao, Y. (2017). Video-Based Fire Detection with Saliency Detection and Convolutional Neural Networks. International Symposium on Neural Networks (pp.299-309). Springer, Cham.
2. Frizzi, S., Kaabi, R., Bouchouicha, M., Ginoux, J. M., Moreau, E., & Fnaiech, F. (2016). Convolutional neural network for video fire and smoke detection. Industrial Electronics Society, IECON 2016 -, Conference of the IEEE (pp.877-882). IEEE.
3. Zhang, Q., Xu, J., Xu, L., & Guo, H. (2016). Deep Convolutional Neural Networks for Forest Fire Detection. International Forum on Management, Education and Information Technology Application.
4. Wang, Z., Wang, Z., Zhang, H., & Guo, X. (2017). A Novel Fire Detection Approach Based on CNN-SVM Using Tensorflow. Intelligent Computing Methodologies.
5. Maksymiv, O., Rak, T., & Peleshko, D. (2017). Real-time fire detection method combining AdaBoost, LBP and convolutional neural network in video sequence. Experience of Designing and Application of Cad Systems in Microelectronics (pp.351-353). IEEE.
6. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. IEEE Conference on Computer Vision and Pattern Recognition (pp.779-788). IEEE Computer Society.
7. Redmon, J., & Farhadi, A. (2016). Yolo9000: better, faster, stronger. 6517-6525.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

A Refreshing Take: Analysing Accident Scenarios through Causal Network Topology Metrics

Benjamin J. Seligmann, Hans J. Pasman*, Sarah J. Domanti, Jesse T. Boadle, Adam C. Staples, Ashley Bels, Michael Small, Mistrel Fetzer Boegheim
College of Science and Engineering, James Cook University, Townsville City, QLD, Australia
Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University
Department of Mathematics and Statistics, University of Western Australia, Crawley, WA, Australia
Mineral Resources, CSIRO, Kensington, WA, Australia
*Presenter Email: hjpasman@gmail.com

Keywords: Incident Investigation, Metrics, Lagging Indicators, System Safety

Abstract

Accident causation investigation and even more hazard scenario identification are troubled by the complexity of interactions between three elements in a process facility: People, Plant and Procedures. Interactions are of various nature, such as physical change and information transfer, all influencing the process.

To facilitate investigation the digraph network was applied as the most flexible visual aid to describe a causal structure. Such structure consists of nodes and edges representing an event or condition in the accident scenario and a causal link respectively. Attributing the nodes and edges to the type of interaction, numbers of the same type can be counted, and so two metrics are developed:

- The *P3 Interaction Contribution* (PIC). This is the proportion of nodes and edges associated with an interaction between People, Plant and Procedures.
- The *Average Edge Weight*. This relates to the proportion of events in the scenario that are associated with the logical AND gate conjunction from its causes (incident nodes), where the event requires more than one simultaneous cause.

The technique was tried on four CSB accident descriptions. Interesting differences are seen. Also, in view of a paper accepted to be published in Safety Science the approach seems quite helpful in process hazard analysis.

1 Introduction

One of the most useful ways that lessons learned from past accidents can help support future sustainable operation is if those lessons are used to enhance an organization's ability to anticipate potential future accidents. Anticipating future accident scenarios ahead of time is what risk assessment is traditionally used for. But in the modern world, complexity in socio-technical process systems makes risk assessment difficult. This complexity is often linked to unforeseen, or difficult-to-identify scenarios which undermines anticipation efforts. Thus, the requirements to extract the best set of lessons learned from an accident investigation becomes even more critical, to support future risk assessment efforts.

This work seeks to demonstrate the use of two measures applicable to results of accident investigations, namely the accident investigation reports. Four accident reports previously generated by the US Chemical Safety Board were analysed. These are listed in Section 2.1. These measures are extracted from a *causal network* representation of the accidents, and are generally called *network metrics*. Network representations for modelling and analysing accident scenarios is a well-established practice, such as through the use of Fault Trees [1]. However, the directed graph or digraph network applied here allows feedback causation, not possible in Fault trees or Bayesian networks. A more recently established practice [2] is to study the topology of accident networks, through the extraction of various network metrics from that topology. The metrics applied here can be used to support accident investigators to reflect on the analysis they have performed and help them clarify whether they have extracted the most helpful or accurate set of lessons learned possible.

The first metric is called the *P3 Interaction Contribution* (PIC), a recently introduced metric for analysing accident in previous work [2]. The PIC is a relative measure of the contribution of so-called *P3 interactions*, or interactions between people, plant or procedures, to an accident scenario as a whole. This approach of categorizing process system components is well established [3, 4, 5]. The PIC can be an indication of how important causal links between fundamentally different component types can be to the generation and progression of an accident.

The second metric is the *Average Edge Weight* of the causal networks that represent the accident scenarios. This corresponds to the number of logical AND gates in the scenario. More edges participating in AND gates will show up as a lower overall *average edge weight* overall in the network. This is calculated by summing all the edge weights and dividing by the number of edges in the network. This metric is useful because more AND gates implies that more than one cause is required for the accident to progress, possibly implying that due to higher complexity it may be less likely to reoccur.

Either through using the PIC or the average edge weight measure, analysts currently investigating an accident can be lead to *question* whether the data they are collecting and the way they are writing the report is the most helpful or accurate for representing the accident. In this sense, then, using these network metrics alongside tradition accident analysis technique offers *a refreshing take* on generating lessons learned from past accidents, the purpose of which is to generate the best set of lessons learned possible to enhance the anticipation of future accidents, and thus the risk assessment efforts in an increasingly complex work.

This refreshing take is demonstrated by first describing a summary of the methodology used to generate the causal network diagrams and their metrics, in Section 2. Section 3 displays these results, with a short discussion given on them in Section 4. Section 5 summarizes the conclusions drawn and suggests avenues for future work.

2 Methodology

This section details the method used to extract and generate the networks from the CSB accident reports and calculate the two network metrics: the PIC and average edge weight.

2.1 Conversion of Accident Reports into weighted causal networks

The first step was to read the four accident investigation reports from the CSB website (www.csb.gov) that detailed the events surrounding the following four accidents:

- Barton Solvents [6]
- Valero Propane [7]
- ASCO [8]
- AL Solutions [9]

The text describing the accident events and how they were causally related, was then converted into a causal network. Each node of the network represents an *event* or a *condition* found in the relevant accident report. Figure 1 shows an example of the conversion process, using a section of text from the Valero Propane accident. The unique numerical identifiers assigned to each event are arbitrary.

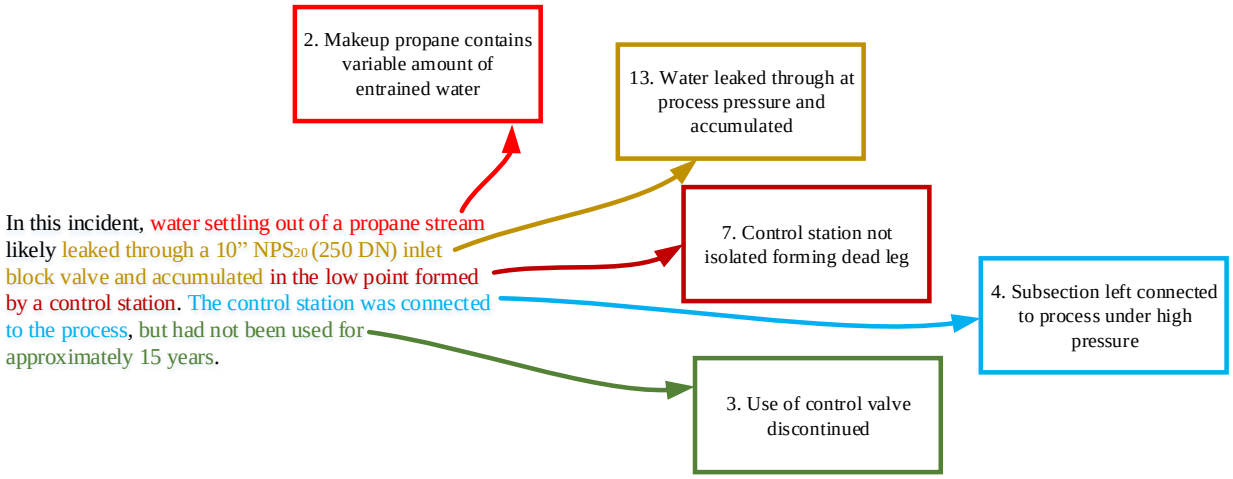


Figure 1 - Causal Network Event Extraction from Accident Reports

Based on the causal relationships extracted from the report, the numbered events were linked together. Weights were added to each edge based on whether the cause for a particular event was part of an AND gate or an OR gate, or a singular cause. Figure 2 shows how an OR gate is configured in the causal network used in this work.

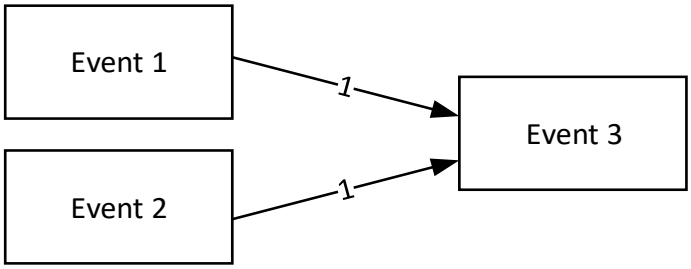


Figure 2 - OR gate configuration in a causal network

The events that comprise the list of causes in an OR gate with each have an edge weight of 1. This is to signify that they can each cause the latter event independently. If an event has only one cause, then the edge weight will likewise be 1.

Figure 3 shows two types of AND gates and how they are represented by part of a weighted causal network.

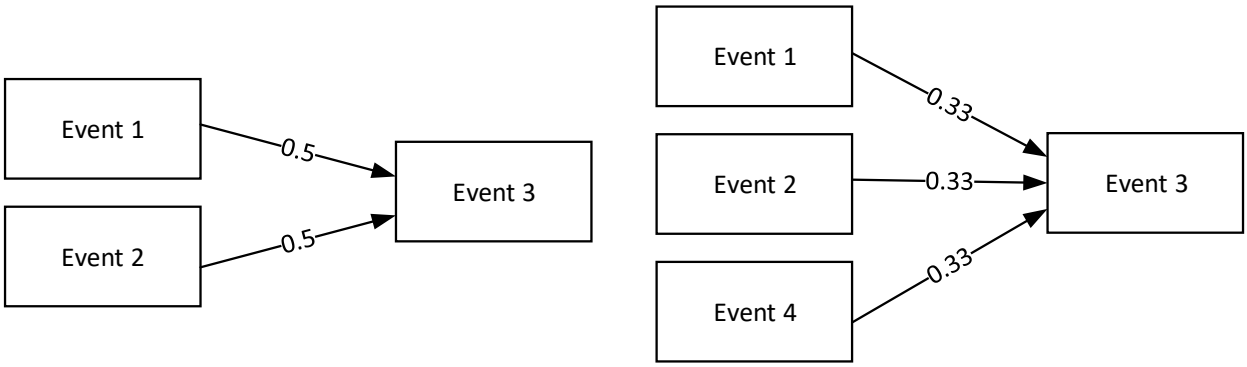


Figure 3 - AND gate configuration in causal network

The events that comprise the list of causes in an AND gate will have edge weights that sum to 1. Thus, a two-event AND gate will have two edge worth 0.5 each, and a three-event AND gate will have three edges worth 0.33 each (approximately 1).

2.2 Generating Network Diagrams

Once the weighted networks have been constructed as per the approach in Section 2.1, an *adjacency* matrix is constructed [5]. This matrix is a mathematical representation of the causal relationships between the events in a causal network. Figure 4 shows an example of how the example networks in Figure 2 and Figure 3 are represented as adjacency matrices.

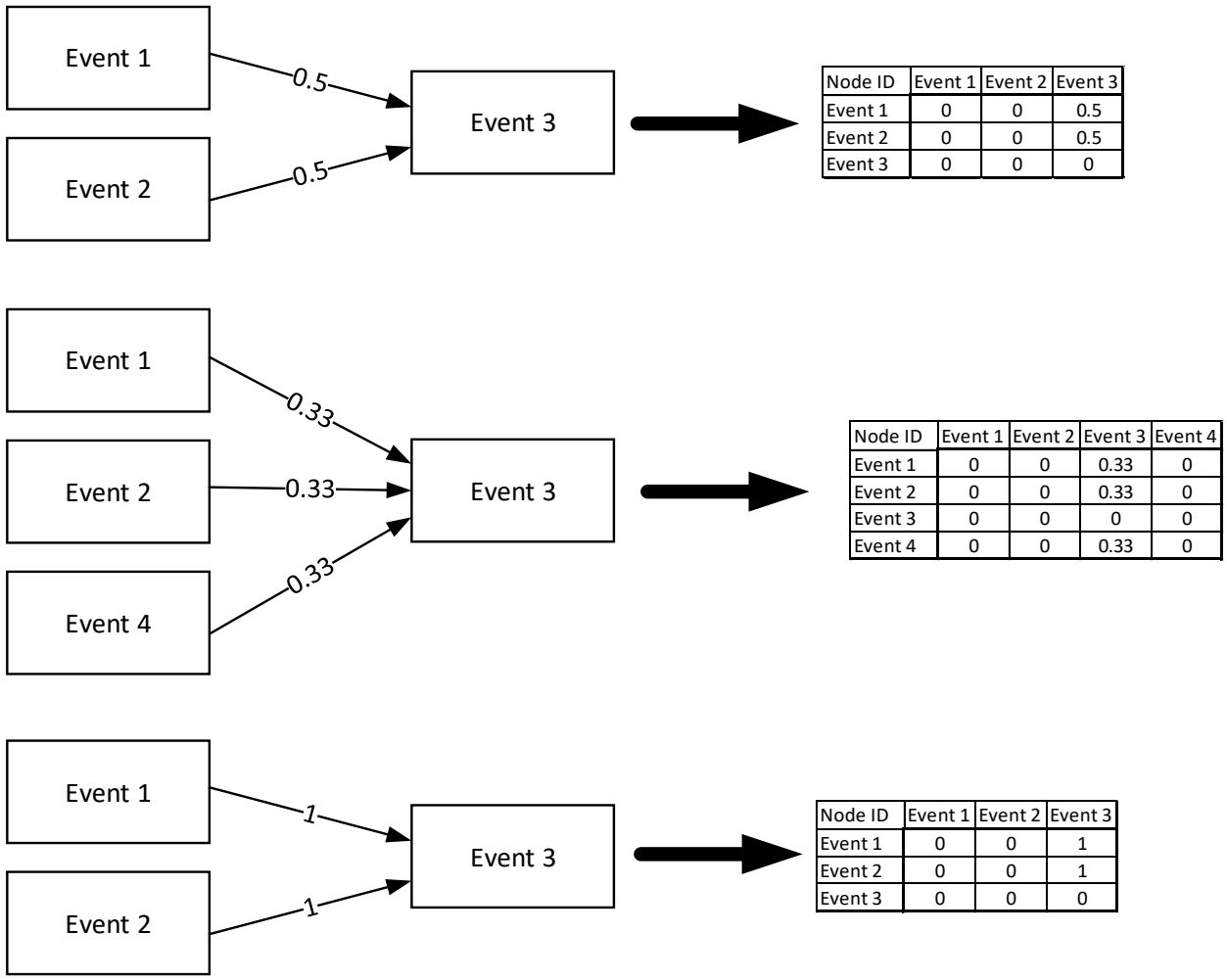


Figure 4 - Adjacency Matrices of Example Networks

These matrices are captured in MS Excel and are then imported into Matlab for network visualisation. Following the method detailed above, the causal networks that represent the four accident reports were generated and presented in Figure 5, Figure 6, Figure 7 and Figure 8.

2.3 Causal Network Metrics

The two network metrics applied to the accident networks in this work, as discussed in Section 1, are the P3 Interaction Contribution (PIC) and the Sum of Incoming Edges/Number of Edges.

2.3.1 P3 Interaction Contribution (PIC)

In previous work [2], the PIC metric was first introduced, with a summary included here. The PIC is a relative measure of the contribution of P3 interactions to an accident scenario as a whole. A P3 Interaction is counted as an association or a causal interaction between two different component types, from the following three categories: People, Plant and Procedures. P3 interactions can be found *within* an event description in a node, or *between* two different nodes, represented by an edge. There are four categories of P3 interaction: people-plant, people-procedure, plant-procedure and people-plant-procedure. The total number of P3 interactions were counted for each accident

network and divided by the sum of the number of nodes (N) and edges (E) for that network, according to Equation 1.

Equation 1 - PIC Calculation

$$PIC = \frac{P3\ Interaction\ Count}{Number\ of\ Nodes +\ Number\ of\ Edges}$$

2.3.2 Average Edge Weight

The average edge weight for a causal network will indicate the proportion of causal links that participate in AND gates. A higher number of AND gates in a particular accident scenario may indicate that the likelihood of that scenario to be lower than an accident with more AND gates. This is simply because *more* simultaneous events or conditions needed to occur for that accident to progress. The average edge weight is calculated according to Equation 2.

Equation 2 - Average Edge Weight

$$Average\ Edge\ Weight = \frac{Sum\ of\ edge\ weights\ over\ whole\ network}{Number\ of\ Edges}$$

3 Results

This section contains the results of the analysis. Firstly, event lists for each accident are contained in Table 1, Table 2, Table 3 and Table 4. The weight causal network for each accident is presented in Figure 5, Figure 6, Figure 7 and Figure 8. The P3 Interaction count for each network, with the distribution of all the types of interactions between components, is shown in Table 5 with a corresponding plot for the P3 interactions count for each accident shown in Figure 9. Table 6 contains a summary of the network metrics for each accident.

Table 1 - Events in Barton Solvents Accident Scenario

Node ID	Node Description
1	Three compartment tanker arrived to fill storage tank
2	Tank contained ignitable vapour-air mix in head space
3	No precautions in place to stop ignitable vapour-air mix in headspace
4	MSDS did not indicate that vapour-air mix could form within tank
5	MSDS did not list precautionary measures beyond normal grounding and bonding
6	Barton pumped naphtha from three separate compartments to tank, requiring pipe to be removed and position on tanker changed
7	Air pockets introduced to fill piping when compartments changed
8	Stop-start filling of naphtha tank accumulating static
9	No manway or access to facilitate cleaning
10	No records of tank ever being cleaned
11	Employees scooped sediment from similar tanks
12	Likelihood of presence of sediment and water in naphtha tank
13	Liquid gauging system float has loose linkage at tape/float junction

14	Turbulence and bubbling from stop/start pumping and air ingress
15	Rapid static charge accumulation
16	Slack in gauge tape created
17	Linkage separated
18	Non-conductive liquid static prevention precautions not in place
19	Tank filled to point of maximum expected surface voltage
20	Spark occurred
21	Spark ignited vapour-air mix
22	Naphtha tank exploded
23	Tank flew into the air and landed 130 feet away
24	Two more tanks ruptured and released their contents into the fire
25	Intense fire caused contents of other tanks to over-pressurize and ignite
26	Debris was launched into adjoining community

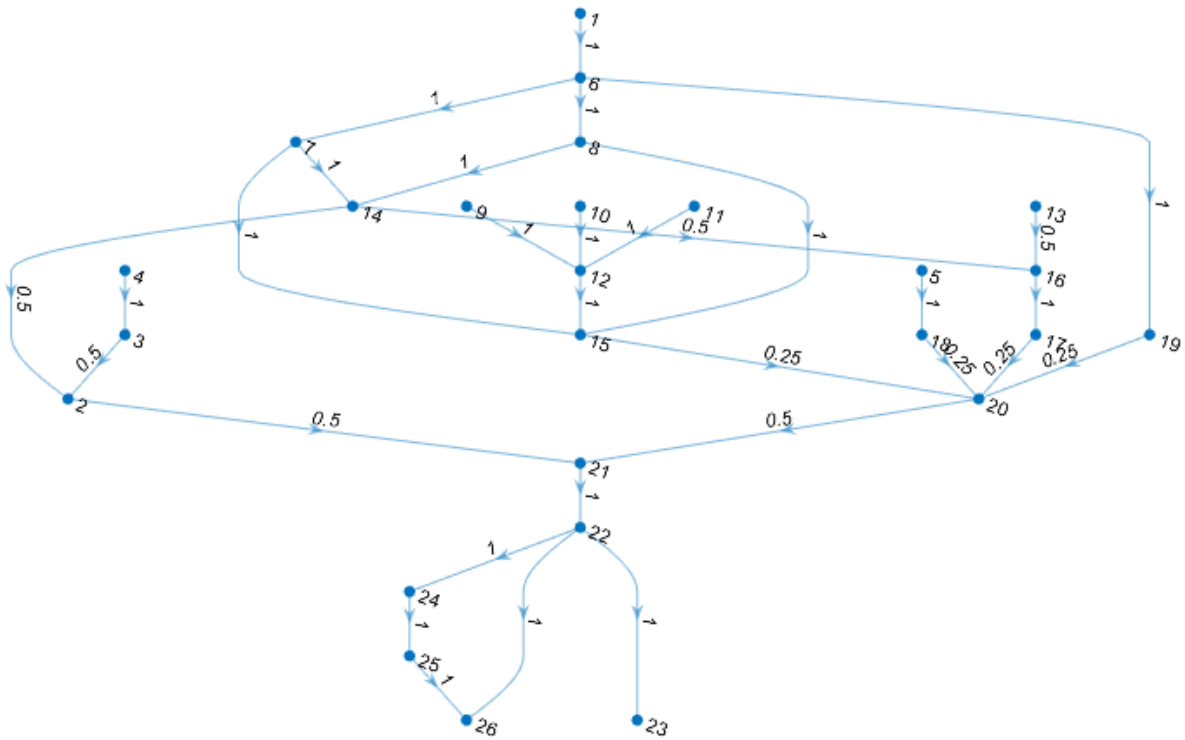


Figure 5 - Barton Solvents Causal Network

Table 2 - Events in Valero Propane Accident Scenario

Node ID	Node Description
1	Below freezing weather in morning
2	Makeup propane contains variable amount of entrained water
3	Use of control valve discontinued
4	Subsection left connected to process under high pressure
5	Block valves around control valve closed but subsection was not isolated with slip blinds
6	No formal process safety / change of management review conducted when control station removed from active service
7	Control station not isolated forming dead leg
8	American petroleum institute doesn't provide detailed guidance on freeze protection programs or sufficiently stress freeze protection of dead-legs
9	Freeze protection practices did not ensure process units systematically reviewed to identify and mitigate freezing hazards for dead legs
10	Control station not freeze-protected
11	Foreign object jammed block valve
12	Leak path created
13	Water leaked through at process pressure and accumulated
14	Water froze within pipe and expanded
15	Pipe elbow fractured along inner elbow
16	Air temperature rose
17	Highly pressurized propane released from fracture, since the ice sealing the fracture melted
18	High and shifting winds
19	Propane travelled downwind to boiler house or nearby fired heaters
20	Propane ignited and flashed back to leak source
21	Fire impinged on piping around No. 1 Extractor releasing additional propane
22	Rapidly expanding fire prevented access to manual isolation valves or local pump controls
23	API safety guidance does not address ROSOV use in process units handling large quantities of flammable materials
24	Valero closed ROSOV installation action item without verification
25	No remotely operable shut-off valves installed in PDA
26	Propane was unable to be isolated
27	API and Valero standards do not provide sufficient fireproofing guidance for pipe racks near high-pressure flammable units
28	Structural support was not fireproofed
29	Support column was impacted by high-pressure propane jet
30	Pipe rack collapsed
31	Multiple pipes failed discharging liquid petroleum products
32	Fire size/intensity rose significantly
33	Surrounding equipment damaged
34	Rapid spread of fire
35	Chlorine used as a biocide in adjacent cooling tower
36	PHA for system doesn't examine hazards of locating chlorine containers close to PDA unit
37	Three one-ton chlorine containers exposed to radiant heating from fire
38	All three containers vented varying amounts of chlorine when fusible plugs melted
39	2.5 tons of chlorine released
40	Butane storage sphere exposed to radiant heating
41	API-recommended practises do not require evaluation of adjacent process hazards in specifying location of deluge valves
42	Manual deluge valve located too close to PDA unit and could not be opened
43	Wind tended to move flames away from sphere
44	Near-miss - butane tank impinged with flame but did not fail. Minimal damage to tank
45	Plant personnel and contractors heard a 'pop' and saw propane cloud blowing from control station

46	Plant personnel directed workers in the area to evacuate
47	Fire alarm activated
48	Emergency response team arrived and approached fire
49	Winds hampered stationary fire water monitors
50	Operators noticed deteriorating situation
51	Evacuation ordered 15 minutes after ignition began
52	Main feeds and fuel gas supply isolated by emergency services
53	Chlorine and sulphuric acid leaks made entry too hazardous
54	Fire extinguished 52 hours after ignition
55	4 workers injured, 3 suffering serious burns
56	10 Valero employees and contractors treated for minor injuries
57	Total shutdown of McKee Refinery for two months
58	Refinery operated at reduced capacity for nearly a year
59	$50 million in direct losses due to fire
60	Significant quantities of gasoline lost in fire
61	Spot shortages of reformulated gasoline in Denver, Colorado in weeks following fire

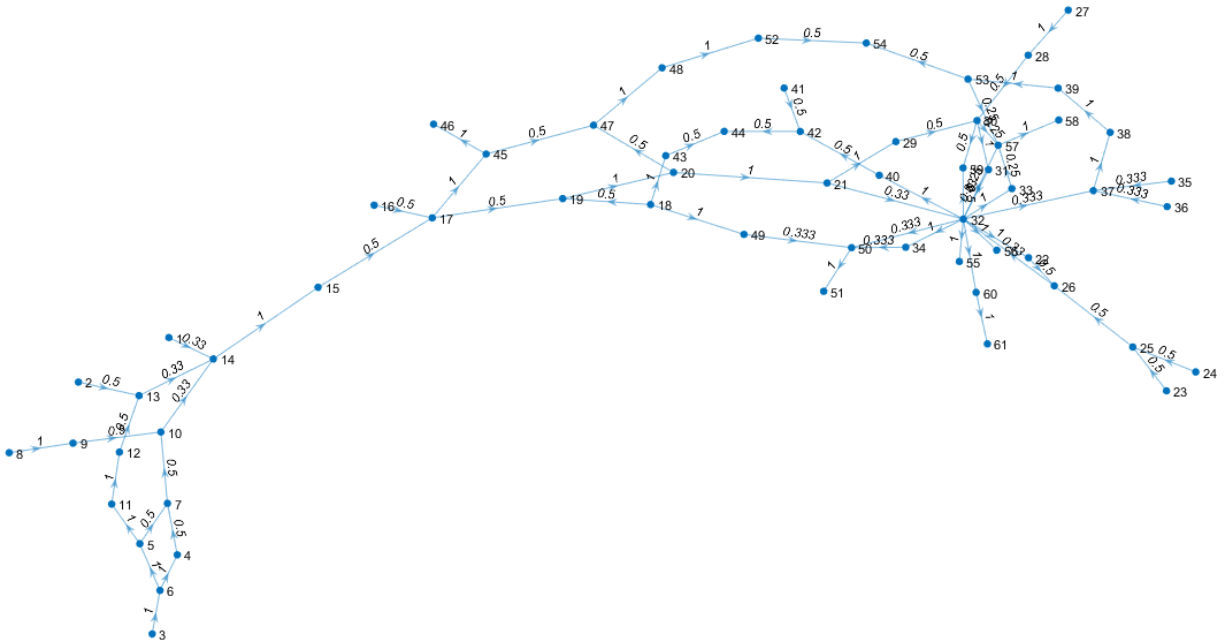


Figure 6 - Valero Propane Causal Network

Table 3 - Events in ASCO Accident Scenario

Node ID	Node Description
1	Workers shovelling snow south of shed where acetylene accumulated
2	Operator's manual did not address recycle water system
3	Operators had no written guidance on operation of recycle system or consequences on deviation from intended sequence
4	General procedures posted in generator room lacked guidance on appropriate sequence for adding water to the generator
5	Workers did not operate process consistently due to inadequate staff training / documentation
6	Generator was pressurized with acetylene gas before recycle water supply was established
7	City water supply valve closed prior to starting recycled water system
8	No source of pressurized water to prevent reverse flow of acetylene
9	1996 PHA didn't identify hazards created by decant water line drain in shed
10	Check valve in recycle water line did not use springs or guides to assist seating of plug
11	Plug is prone to misalignment
12	Check valve internals are prone to solid build-up such as scale
13	Check valve guide pin "hung up" on lower pipe nipple
14	Recycled Water "Found Closed" valve either open or leaked significantly in closed position
15	Acetylene was able to flow back through recycle water line
16	Acetylene leaked from the generator through to the shed through water recycle line
17	Heavy snowfall
18	Freeze Protection Practices in place: Decanted water line normally left open to protect from freezing
19	Lime shed had no ventilation
20	Shed contained a propane heater with a hot surface
21	Acetylene gas accumulated in lime shed through drain leak
22	Acetylene gas ignited upon contact with heater surface
23	Three workers were killed
24	One worker was seriously injured by the blast
25	Lime shed completely destroyed
26	Debris hurled up to 450 feet from the site
27	Two large holes were blown into the sides of adjacent building
28	Windows were shattered
29	Doors blown into building / knocked off their hinges/rails
30	PHA was not updated in 2001 as required
31	Conditions leading to explosion were unidentified

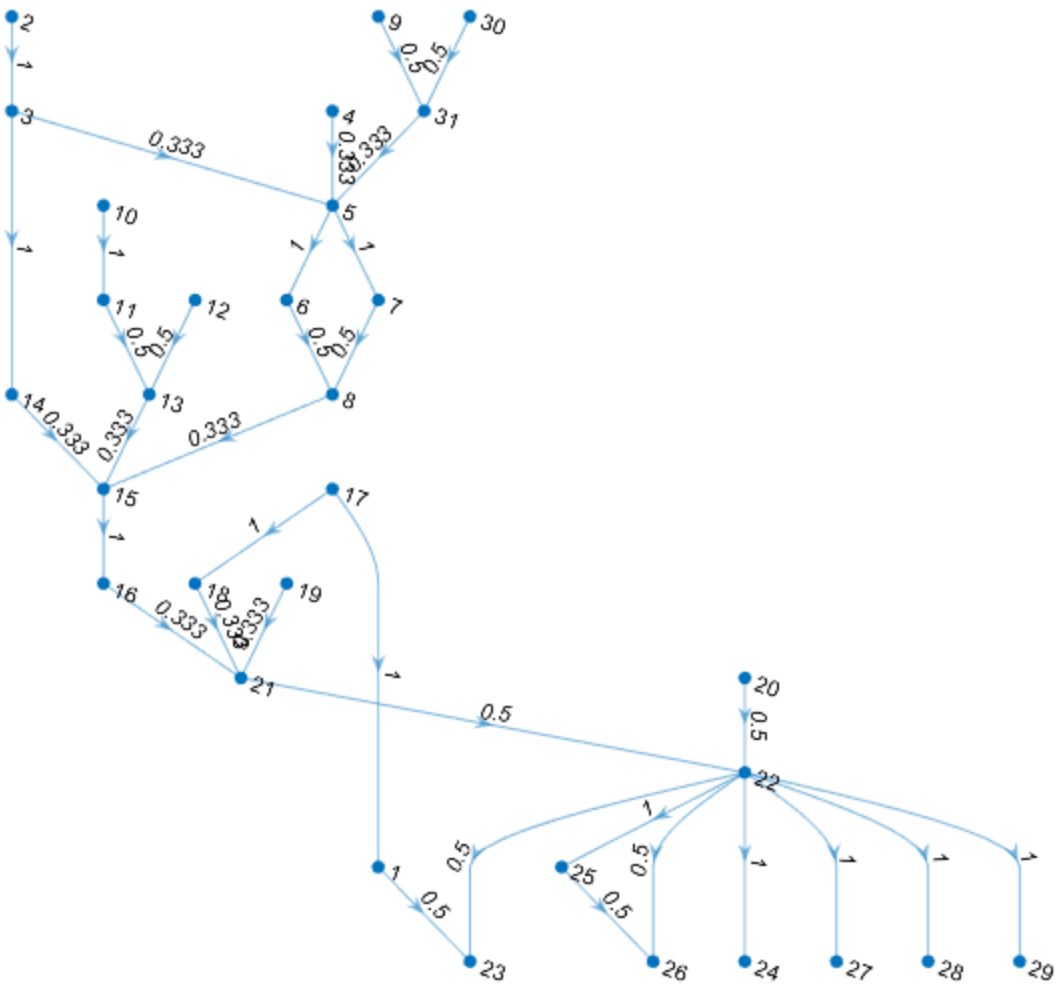


Figure 7 - ASCO Causal Network

Table 4 - Events in AL Solutions Accident Scenario

Node ID	Node Description
1	Weak safety management for handling titanium and zirconium safe storage and handling
2	Faulty blender identified
3	Insufficient temporary fix used
4	Metal blades continued scraping on metal casing
5	Spark occurred
6	Ignition of zirconium dust
7	Explosion
8	Lids not closed on equipment
9	Fire became airborne
10	Did not follow dust reduction recommendations or collection system, as recommended by standards
11	Mix of zirconium and titanium being milled (ground in to fine powders)
12	OSHA did not implement any combustible dust standard
13	Collection of dust on equipment
14	Fire spread

15	Water used for wash-down procedures
16	Hydrogen gas present in facility
17	Hydrogen gas caught fire
18	Barrels not in use left in production room instead of secondary storage facility
19	Barrels caught fire
20	Increased fire intensity
21	Operators at blender and presses died
22	Water deluge system activated
23	Insurance auditors commended facility and declared potential dust incidents are effectively controlled, not recommending a process hazards analysis.
24	Insurance auditors declared fire protection systems good process control
25	Damage caused throughout production area
26	Permanent shutdown
27	Electrical contractor received severe injuries
28	Electrical contractor in hydraulic room for maintenance
29	Management did not enforce lid closure on blender during operation
30	Housekeeping approach to dust control

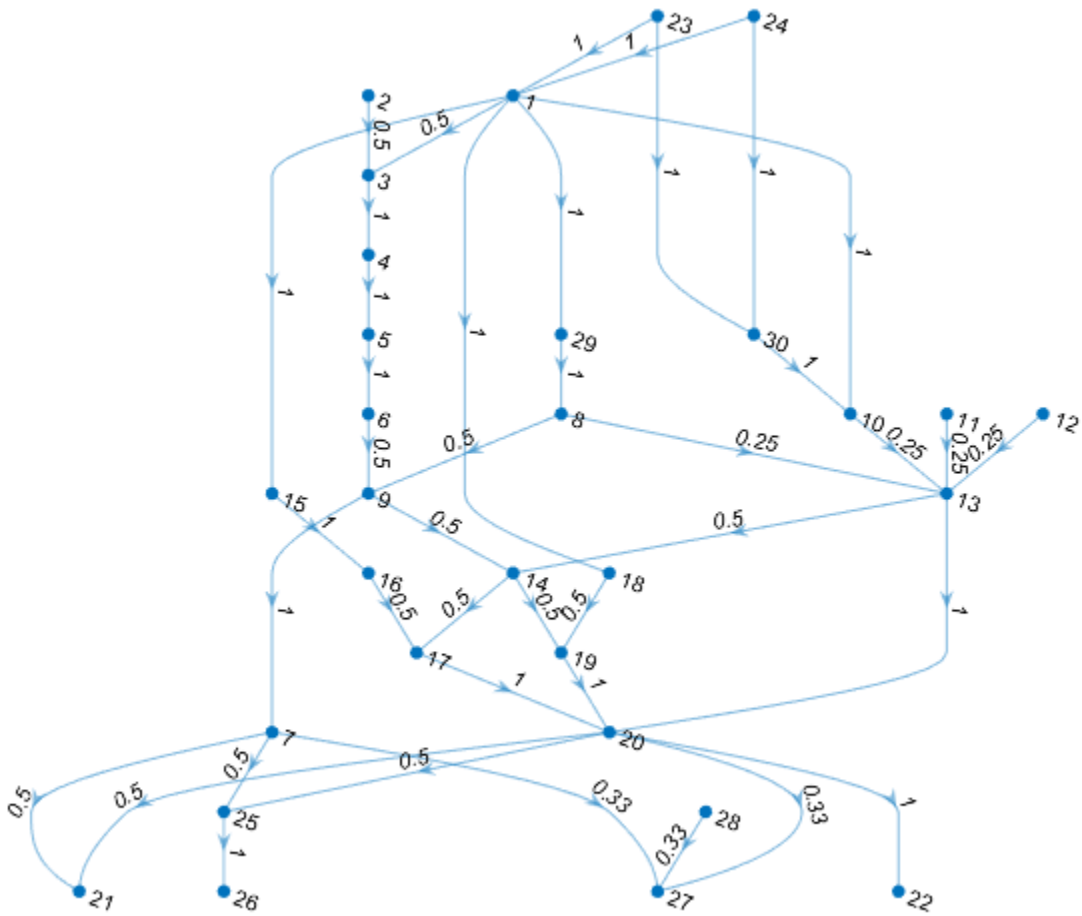


Figure 8 - AL Solutions Causal Network

Table 5 – P3 Interaction Count

Type of P3 Interaction	Barton Solvents			Valero Propane			ASCO			AL Solutions		
	Within	Between	TOTAL	Within	Between	TOTAL	Within	Between	TOTAL	Within	Between	TOTAL
People	0	0	0	2	0	2	2	0	2	0	0	0
Plant	11	0	11	27	0	27	13	0	13	13	0	13
Procedure	1	0	1	6	0	6	3	0	3	1	0	1
People-People	0	0	0	2	0	2	0	1	1	0	0	0
Plant-Plant	6	20	26	12	43	55	7	19	26	3	19	22
Procedure-Procedure	0	0	0	0	1	1	0	0	0	0	0	0
People-Plant	**4**	**6**	**10**	**10**	**20**	**30**	**3**	**5**	**8**	**8**	**9**	**17**
People-Procedure	**0**	**0**	**0**	**1**	**0**	**1**	**2**	**1**	**3**	**0**	**0**	**0**
Plant-Procedure	3	4	7	0	4	4	0	0	0	3	2	5
People-Plant-Procedure	1	1	2	1	5	6	1	8	9	2	11	13
P3 Count	**8**	**11**	**19**	**12**	**29**	**41**	**6**	**14**	**20**	**13**	**22**	**35**

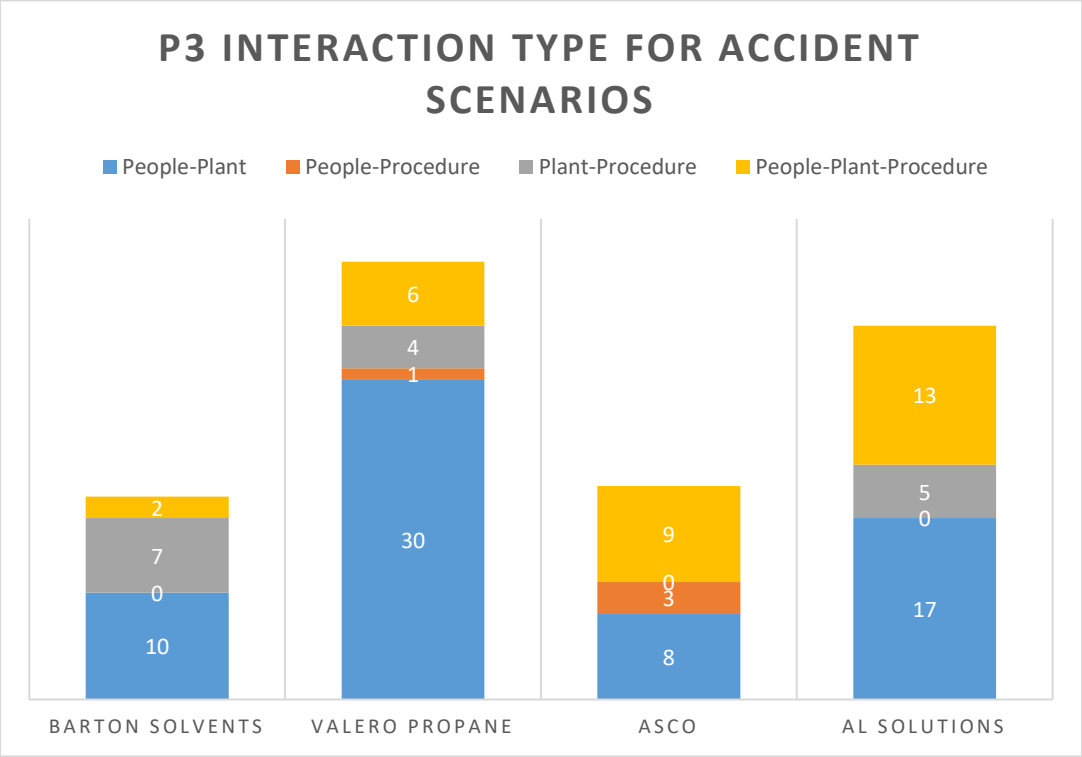


Figure 9 - P3 Interaction Type Plot

Table 6 - Network Metrics

Metrics	**Barton Solvents**	**Valero Propane**	**ASCO**	**AL Solutions**
Number of Nodes (N)	26	61	31	30
Number of Edges (E)	31	73	34	41
Sum of Edge Weights	25	49	22	29
Average Edge Weight	0.81	0.67	0.65	0.66
P3 Count	19	41	20	35
PIC	0.33	0.31	0.31	0.49

4 Discussion

Initial inspection of the networks in Figure 5, Figure 6, Figure 7 and Figure 8 reveals that they both have similarities and differences. Barton and ASCO have a series of initiating causes, focussing in on a few central events, which happen to be nodes 21 and 22 in both networks. AL Solutions and Valero have a more complex structure, and yet visual inspection reveals that they appear to be quite different from each other. In terms of the number of nodes and edges, Barton (26 N – 31 E), ASCO (31 N – 34 E) and AL Solutions (30 N – 41 E) are all similar sizes, shown in Table 6. Valero Propane is considerably bigger (61 N – 73 E). Thus, as is expected, Valero has the highest P3 count, but this is simply because it is a larger network. The PIC for Barton (0.33), Valero (0.31) and ASCO (0.31) are all similar, with AL solutions (0.49) having the largest. And yet the contribution of different types of P3 interactions for each scenario differs, as shown in Figure 9. Barton has the high average edge weight (0.81), where Valero (0.67), ASCO (0.65) and AL Solutions (0.66) are very similar.

A lower average edge weight indicates that Valero, ASCO and AL Solutions would potentially harder to identify ahead of time than Barton, during risk assessment, since more simultaneous events or conditions need to be in place for them to progress. Conversely, an accident with a high average edge weight may tend to be easier to identify but harder to stop, since on average there are more independent paths along which the accident can progress. This is the situation where there are more independent causes per node and/or more OR gates.

Thus, once the average edge weight useful questions that investigators could ask themselves could be:

- Did I expect that degree of AND gates in the scenario?
- If my average edge weight is very high, is the causal progression really that simple? Could there actually be other conditions hidden that I just haven't found yet, that contribute to the accident?
- If the average edge weight is very low, does that really mean this situation will be hard to identify in the future? If so, what can we embed in the lessons learned about new monitoring practices that could be implemented? Have we considered monitoring practices at all?

These kind of questions could push them to look further into the scenario until they are thoroughly satisfied that they have captured it accurately.

Similarly, the PIC for each scenario could help investigators ask the following kinds of questions:

- For ASCO, does the P3 interaction type distribution in Figure 9, suggest that perhaps the lessons learned should include recommendations that combine people-plant-procedure interactions, and people-plant interactions, in roughly equal measure?
- Since the PIC is almost 0.5 for AL Solutions, does that mean that the lessons learned should be related to P3 interactions at least half the time?
- For Valero Propane, does the lower PIC mean that P3 interactions are not that significant for the scenario as a whole? And does the high proportion of P3 interactions that a People-plant (Figure 9), and the high proportion of plant and plant-plant interactions in Table 5, mean that we don't have to strongly consider the impact of procedures at all?

The above hypothetical questions demonstrate that metrics like the PIC and the average edge weight, used during accident investigations, could be effective *reflective practice tools* to enhance the results. Using the metrics to form a series of checking questions, for example, could remove threats of complacency in the analyst's practice. One of the benefits of metrics based on topology of causal networks is that they are generic tools that can be used flexibly in many different circumstances to support accident investigation.

5 Conclusions and Future Work

This paper demonstrated the use of two causal network metrics applied to accidents previously investigation by the CSB. Then, intention was to show how the PIC and the average edge weight could be used to support reflective practice activities during the investigation activities themselves, with the goal of generating the best set of lessons learned possible.

Further explorations with the PIC and the average edge weight would be to calculate them for many accident reports that the CSB has produced, and see if there is a correlation, such as if a high PIC corresponds with a lower average edge weight, meaning more AND gates in the scenario. If so, then more P3 interactions would indicate that an accident scenario is harder to identify, but easier to arrest. Thus, the two metrics may be more deeply related than first thought.

We hope this paper is *a refreshing take* on the activity of accident investigation, spurring a renewed interest in how accident reports are written and investigations carried out, to maximise the benefits of them for identifying causal structures potentially leading to mishap and so enhancing risk assessment in a complex world.

6 References

1 Vesely W., Stamatelatos M., Dugan J., Fragola J., Minarick III J., Railsback J., Fault Tree Handbook with Aerospace Applications, Version 1.1, NASA, Washington, DC, 2002.

2 Benjamin J. Seligmann, Jiayi Zhao, Sophia G. Marmara, Tayla C. Corbett, Michael Small, Maureen Hassall, Jesse T. Boadle, The P3 Interaction Contribution: a network theory-based metric for quantitatively characterizing accident scenarios for the

comparison of hazard identification results in socio-technical process systems, Safety Science, accepted for publication 2018.

3 Seligmann B.J., Németh E., Hangos K.M., Cameron I.T., A blended hazard identification methodology to support process diagnosis. Journal of Loss Prevention in the Process Industries **25** (2012) 746–759.

4 Seligmann, B.J., A Functional Systems Framework and Blended Hazard Identification Methodology to Support Process Diagnosis, Ph.D. Dissertation, School of Chemical Engineering, University of Queensland, Australia, 2011.

5 Pasman, H.J., 2015. Risk Analysis and Control for Industrial Processes – Gas, Oil and Chemicals, A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events (Chapter 7). Butterworth Heinemann, Copyright 2015 Elsevier Inc., ISBN: 978-0-12-800057-1.

6 CSB, "Barton Solvents: Static Spark Ignites Explosion Inside Flammable Liquid Storage Tank," US Chemical Safety Board, Case Study 06/02/2008, 2008, Available: https://www.csb.gov/barton-solvents-explosions-and-fire/.

7 CSB, "LPG Fire at Valero-McKee Refinery," US Chemical Safety Board, Washington, DC, Report 09/07/2008, 2008, Available: http://www.csb.gov/valero-refinery-propane-fire/.

8 CSB, "Explosion at ASCO: Dangers of Flammable Gas Accumulation," Chemical Safety Board, Washington, DC, Safety Bulletin 25/01/2006, 2006, Available: http://www.csb.gov/acetylene-service-company-gas-explosion/.

9 CSB, "AL Solutions, Inc., New Cumberland, WV: Metal Dust Explosion and Fire," US Chemical Safety Board, Case Study 16/07/2014, 2014.

10 S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, "Complex networks: Structure and Dynamics," *Physics Reports,* **424** (4–5), (2006) 175-308.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Analytics and Artificial Intelligence: Deep Learning for Anomaly Detection - A case study from the financial sector with application to process safety

Arul Livingstone, Nnamdi Orakwue, Franz Hiebert
Cocolevio LLC
Austin, Tx

E-mail: franz@cocolevio.com

Abstract

This presentation reports on a case study from the financial sector with application to challenges in the field of process safety. Banks collect massive amounts of data from routine financial transactions. Some of the data is anomalous, is corrupt, or represents a signal that warrants follow-up attention from subject matter experts. Currently, review of such data is often a manual inspection which is time consuming, expensive, and limited to representative data sets. In this case study, we employ machine learning, deep learning to rapidly review historical data and tag anomalous data that represents a signal for follow-up attention. With this methodology, we are able to automate the manual process, quickly finding anomalies, dramatically reducing assessment time, expanding the range and volume of data that can be reviewed, and finding signals that previously would likely be missed. Benefits to the financial institution include major cost reductions and improvements in detection of fraud. Application of the machine learning/data assessment approach to process safety challenges may provide safety and cost-reduction benefits as well.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

A Hazard Identification Framework of Complex Systems

Mengxi Yu*, Noor Quddus, M. Sam Mannan
Mary Kay O'Connor Process Safety Center
Artie McFerrin Department of Chemical Engineering
Texas A&M University
College Station, Texas, USA
*Presenter E-mail: yuxxx433@tamu.edu

Abstract

A chemical process facility is a highly complex system. The interactions among a small group of the functions, such as process, equipment, human, organizational functions, could split, merge or couple leading to a complex non-linear system. The hazards brought by the tight coupling and nonlinear interaction of the functions are not so obvious to observers and may cause an unexpected incident without adequate prior indications.

A few number of socio-technical models have been developed in the recent years for complex systems, but their applications in the chemical industry are still limited. The objective of the current study is set to develop a framework to identify hazards present in a complex chemical process in terms of deviations of the functions. One of the socio-technical models, Functional Resonance Analysis Method (FRAM), has been used as a basic tool to understand the interaction of the functions that are involved in a chemical process. Process kinetics model, equipment reliability model, and human reliability model have been integrated on the basic structure of FRAM to develop the framework. Hazards corresponding to different interactions among the functions will be identified by stochastic simulation.

Keywords: hazard identification, socio-technical system

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Multi-Objective Stochastic Optimization for Preventive Maintenance Planning

Christopher K. Gordon*, M. Sam Mannan
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: ckagordon@tamu.edu

Abstract

Maintenance is an essential part of mechanical integrity programs and aims to prevent the occurrence of process safety incidents and costly unplanned shutdowns. Maintenance can increase the reliability of equipment in productive systems and effective preventive maintenance programs enable maintenance activities to be planned proactively. However, maintenance planning is subject to resource scarcity and is rendered nontrivial due to system complexity, reliability model nonlinearity, and parametric uncertainty.

Multi-objective stochastic mixed-integer nonlinear programming is well suited to addressing these challenges and is adopted here to optimize the time intervals in which to perform maintenance on different pieces of equipment. Following presentation of an optimal maintenance planning framework, a model is formulated and optimized accounting for: the effect of imperfect repair using an effective age model, equipment failure behavior using a Weibull reliability model, endogenous uncertainty in reliability model parameters, and the simultaneous need to satisfy the competing objectives of cost minimization and reliability maximization using the ε-constraint method. The results of the research consist of optimal maintenance plans, plots of resultant equipment and system reliability over time, and a Pareto frontier of optimal solutions from which the decision maker can select. The approach adopted here is illustrated with a case study and can be extended to improving the overall availability, effectiveness, and resilience of a variety of productive systems.

Introduction

Maintenance is used here to refer to actions taken to increase the overall availability of equipment in ageing productive systems. Maintenance actions such as repair, cleaning, testing, lubrication, and replacement are performed to improve mechanical integrity, aid in preventing process safety incidents, and avoid costly downtime due to unplanned shutdowns and slowdowns. Maintenance involves optimal resource allocation and the decisions of when, where and how to do maintenance are key.

Commonly adopted maintenance policies in industry include: (i) basing decisions on mean time to failure (MTTF) recommendations from original equipment manufacturers (OEM), (ii) scheduling maintenance at fixed intervals based on internal company data, (iii) corrective maintenance in which selected equipment are run to failure, (iv) condition-based monitoring and predictive maintenance, (v) risk-based inspection, and (vi) reliability-centered preventive maintenance.

Selection of the appropriate maintenance policy is in part informed by data availability, company culture, and the level of expertise available to create and provide support for developed solutions. It is noted here that the time horizon over which maintenance decisions are made influences maintenance policy selection. Planning is used here to denote high-level decisions taken over months or years and is distinguished from scheduling in which decisions are taken over hours, days, and weeks. A generic example of a maintenance plan is provided in Table 1 in which different equipment are tested (T) and replaced (R) over a five-year planning horizon.

Table 1. Generic maintenance plan

Equipment	**Y1**		**Y2**		**Y3**		**Y4**		**Y5**	
V-001		T		T		T		T		T
V-002	T		R		T		T		R	
⋮										
P-27	T	T	T	T	T	R	T	T	T	T
⋮										
C-11	T		T		R		T		T	

Regardless of the maintenance policy selected, certain factors affect optimal resource allocation:

1. Company resources are limited and need to be carefully allocated among operations; business improvement projects; and health, safety and environmental (HSE) projects. The portion of the budget allocated to maintenance is consequently finite and must be decided *a priori*.
2. There are monetary costs associated with maintenance actions and increasing maintenance expenditure leads to diminishing marginal gains in reliability. In other words, the objectives of minimizing cost and maximizing reliability are conflicting and maintenance planning is multi-objective in nature.
3. Productive systems are often composed of multiple degrading equipment whose complicated interactions impart system complexity.
4. Maintenance actions may be imperfect and do not necessarily restore equipment to either an ‘as good as new’ or an ‘as bad as old’ condition.
5. The functions used to rigorously estimate equipment and system reliability are nonlinear and their parameters are not known with absolute certainty.

It is the simultaneous consideration of these factors that distinguishes this research from other efforts in the academic literature on preventive maintenance. The interested reader is directed to a selected subset of the academic literature for context and background information [1-9].

This research employs techniques from the fields of stochastic programming (SP), multi-objective optimization (MOO), and mixed-integer nonlinear mathematical programming (MINLP) to formulate and solve a constrained maintenance planning model. The objectives considered here are cost minimization and reliability maximization. The key decision variables include: the expected number of repairs, the expected number of replacements, whether or not to do maintenance in a time interval, and the sequence of maintenance actions over the time horizon. The results of the research include an optimal maintenance planning framework, plots of equipment and system reliability over time, the expected maintenance budget, the number of spare parts to keep in inventory, and a Pareto front of optimal maintenance plans corresponding to different system reliability thresholds.

This paper proceeds with a description of the methodology used and formulates the maintenance planning model. A case study and preliminary results are subsequently presented to illustrate the multi-objective stochastic optimal maintenance planning approach.

Methodology

The maintenance model used here is data-driven and as such the first step of the methodology is obtaining equipment failure data. In the absence of detailed and complete maintenance and failure records, Monte Carlo methods are used to simulate the equipment failure data based on expert judgement and summary statistics such as the mean time to failure (MTTF). After data validation, maximum likelihood estimation (MLE), or as recourse, expert judgement, is used to determine the values of the reliability model parameters and their uncertainties.

Following estimation of the reliability model parameters, the optimization model is formulated. This formulated model includes the various considerations mentioned above and is a multi-period multi-objective stochastic mixed-integer nonlinear mathematical programming model. Optimization is then performed and an iterative procedure of examining and validating the results is carried out until they are deemed satisfactory. The final step of the methodology is visualization and assessment of the results. The present methodology has been formalized into the optimal maintenance planning framework shown in Figure 1.

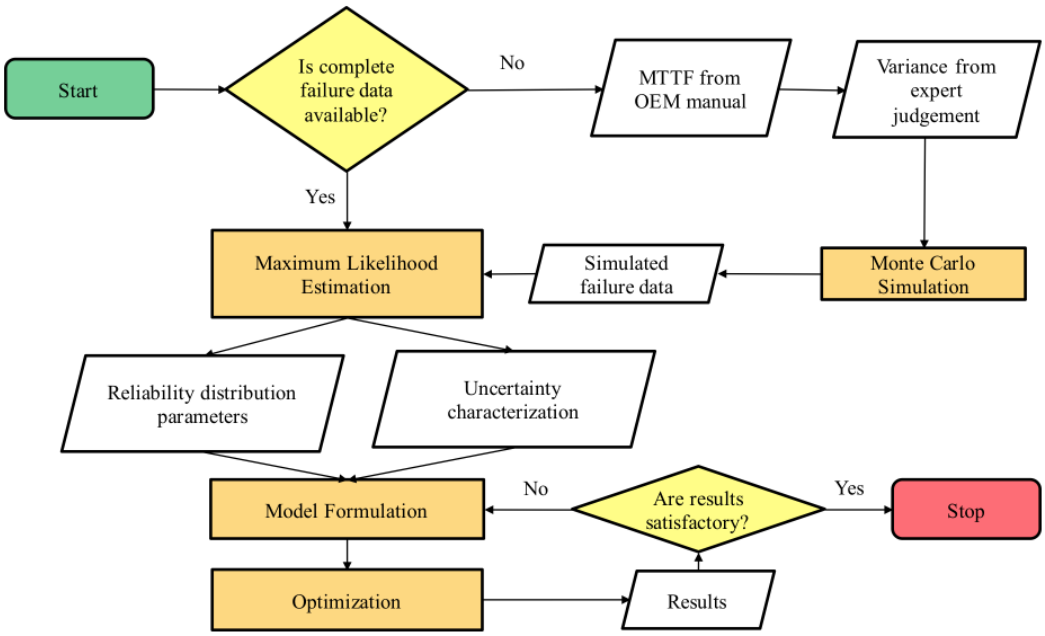


Figure 1. Optimal maintenance planning framework

Model formulation

Equipment are indexed by $i = 1, 2, \dots, I$. Maintenance actions are indexed by $k = 1, 2, \dots, K$, where k_1 is used to denote the absence of a maintenance action, k_2 is used to denote repair, and k_3 is used to denote replacement. Time intervals are indexed by $t = 1, 2, \dots, T$.

The decision variables used in the model are the Weibull scale parameter, τ, the effective age, age, the number replacements, n_{spares}, the number of repairs, $n_{repairs}$, and whether or not to perform a maintenance action in a time interval, m. These variables are bounded by (1-5).

$$age^L \leq age(i,t) \leq age^U \qquad \forall\, i \epsilon I, t \epsilon T \qquad (1)$$

$$0 \leq \tau_E(i) \leq \tau^U \qquad \forall\, i \epsilon I \qquad (2)$$

$$n_{spares}(i) \leq n^U_{spares} \qquad \forall\, i \epsilon I \qquad (3)$$

$$n_{repairs}(i) \leq n^U_{repairs} \qquad \forall\, i \epsilon I \qquad (4)$$

$$m(i,k,t) = \{0,1\} \qquad \forall\, i \epsilon I,\ k \epsilon K, t \epsilon T \qquad (5)$$

The first objective, (J1), is minimization of cost, Z. The cost considered here is a function of the maintenance actions, and is parameterized by the cost coefficients C_k and c_{spares}. The second objective, (J2), is the implicit maximization of system reliability, R_{sys}.

$$\min Z = \sum_i^I \sum_k^K \sum_t^T C_k m(i,k,t) + \sum_i^I \sum_t^T c_{spares} m(i,k_3,t) \qquad (J1)$$

$$\ln R_{sys}(t) \geq \ln \widetilde{R}(e) \qquad \forall\, t \epsilon T, e \epsilon \xi \qquad (J2)$$

The multi-objective method used here is the ε-constraint method with predefined reliability thresholds, $\widetilde{R}(e)$ where $e = 1,2, \dots, \xi$. A logarithmic transformation has been used here for consistency with other logarithmic transformations used in the model to reduce nonlinearity. It is noted as that (J2) is linear and convex. These objectives are optimized subject to scalar and vector equality and inequality constraints (6-18).

Constraint (6) enforces the performance of at most one type of maintenance action in each time interval.

$$\sum_k^K m(i,k,t) \leq 1 \qquad \forall\, i \epsilon I, t \epsilon T \qquad (6)$$

Constraints (7) and (8) determine the expected cumulative number of repairs, and expected number of replacements performed over the time horizon respectively.

$$n_{repairs}(i,t) = \sum_{t'}^{t} m(i,k_2,t') \qquad \forall\, i \epsilon\, I, t \epsilon\, T \qquad (7)$$

$$n_{spares}(i) = \sum_{t}^{T} m(i,k_3,t) \qquad \forall\, i \epsilon\, I \qquad (8)$$

An effective age model is used to capture the effect of the different maintenance actions on equipment condition and is shown in constraints (9) and (11-14). The increase in equipment age in the absence of maintenance is denoted t_d and is equivalent to the time discretization used. The imperfect maintenance factor, α_k, is used to account for maintenance actions that restore equipment to a condition between as-good-as new (AGAN) and as-bad-as-old (ABAO). It is noted here that the use of the effective age model in the context of optimization results in a nonconvex bilinear-integer-continuous (BIC) term shown in (10) which has been reformulated and replaced by (11-14).

$$age(i,t) = [age(i,t-1) + t_d] - \sum_{k}^{K} BIC(i,k,t) \qquad \forall\, i \epsilon\, I,\ t \in T \qquad (9)$$

$$BIC(i,k,t) = m(i,k,t)(1-\alpha_k)[age(i,t-1) + t_d] \qquad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad (10)$$

$$m(i,k,t)age^L \leq BIC(i,k,t) \qquad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad (11)$$

$$BIC(i,k,t) \leq m(i,k,t)age^U \quad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad (12)$$

$$[(1-\alpha_k)(age(i,t) + t_d)] - \big(1 - m(i,k,t)\big)age^U \leq BIC(i,k,t) \qquad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad (13)$$

$$BIC(i,k,t) \leq [(1-\alpha_k)(age(i,t) + t_d)] - \big(1 - m(i,k,t)\big)age^L \qquad \forall\, i \epsilon\, I,\ k \in K, t \in T \qquad (14)$$

The scale parameter is described here using a triangular distribution from which a corresponding discrete distribution is constructed. This discrete distribution consists of scale parameter realizations, τ, and realization probabilities, p, for different scenarios $\zeta = 1,2,\ldots,Z$. It has been assumed here that the number of repairs to date increases the lifetime of process equipment and that this corresponds mathematically to an increase in the probability of realizing higher-magnitude scale parameter scenarios. The constraints used to model the scale parameter and its decision-dependent uncertainty are summarized in (15) and (16).

$$p(\zeta,t) = f(n_{repairs}(i,t)) \qquad \forall\, i \epsilon\, I, t \in T \qquad (15)$$

$$\tau_E(i,t) = \sum_{\zeta}^{Z} p(\zeta,t)\tau(\zeta) \qquad \forall\, i \epsilon\, I, t \in T, \zeta \in Z \qquad (16)$$

A nonlinear Weibull model is used to describe the equipment reliability in (17) based upon the calculated effective age, the shape parameter, β, and the expected scale parameter, τ_E. This is followed finally by calculation of the system reliability in (18). It is noted that (18) has formulated for a series system, reformulated to reduce computational intractability, and can be adapted to other system configurations.

$$\ln\big(R(i,t)\big) = \left(\frac{1}{\tau_E(i)^{\beta(i)}}\right) \mathrm{age}(i,t)^{\beta(i)} \qquad \forall\, i \in I, t \in T \qquad (17)$$

$$\ln R_{sys}(t) = \sum_{i}^{I} \ln R(i,t) \qquad \forall\, t \in T \qquad (18)$$

The formulated model consists of (J1), (J2) and constraints (1-5), (6-9), (11-14), and (15-18).

Case study description

The system considered for the case study is presented in Figure 2 and consists of three identical centrifugal pumps in series. The parameters used for the case study are shown in Table 2.

Table 2. Model parameter values

Parameter		Value(s)
Equipment age lower bound, yr	age^L	0
Equipment age upper bound, yr	age^U	5
Time interval, yr	t_d	0.5
Scale parameter scenarios, yr	$\tau(\zeta)$	2.6, 3.0, 3.4
Scale parameter upper bound, yr	τ^U	3.6
Number of replacements upper bound	n^U_{spares}	10
Number of repairs upper bound	$n^U_{repairs}$	10
Normalized cost per repair	C_k	1
Normalized cost per replacement	c_{spares}	10
System reliability thresholds	$\widetilde{R_e}$	0.9, 0.95, 0.99, 0.995, 0.999
Imperfect maintenance factors	α_k	1, 0.1, 0
Shape parameter	$\beta(i)$	1.5, 1.5, 1.5

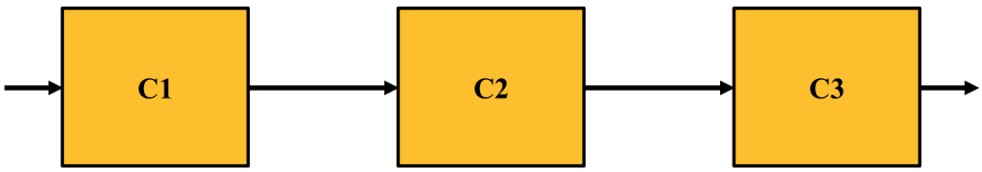


Figure 2. System

Results and discussion

Two sets of preliminary optimization results are provided here. The results consist of maintenance plans showing the optimal sequence of repairs (I) and replacements (P), plots of the corresponding equipment and system reliability against time, and a sensitivity analysis in the form of a Pareto front.

The first set of results corresponds to a maintenance policy in which a recommendation of a manufacturer to repair equipment once every three years is followed. The optimal maintenance plan corresponding to this policy is shown in Table 3 and was produced by adapting (7) and (8). It was observed that this policy rendered the model infeasible until the system reliability thresholds (J2) were relaxed. In less mathematical terms, this maintenance policy was inconsistent with the goal of maintaining system reliability above set thresholds over the entire time horizon. This is visualized in Figure 3, from which it can be observed that the equipment and system reliability profiles are below 90%, and by extension 99.5%, over the majority of the time horizon.

Table 3. Maintenance plan based on a manufacturer recommendation

Equipment	n_{spares}	**Y1**		**Y2**		**Y3**		**Y4**		**Y5**	
C1	0					I					
C2	0						I				
C3	0						I				

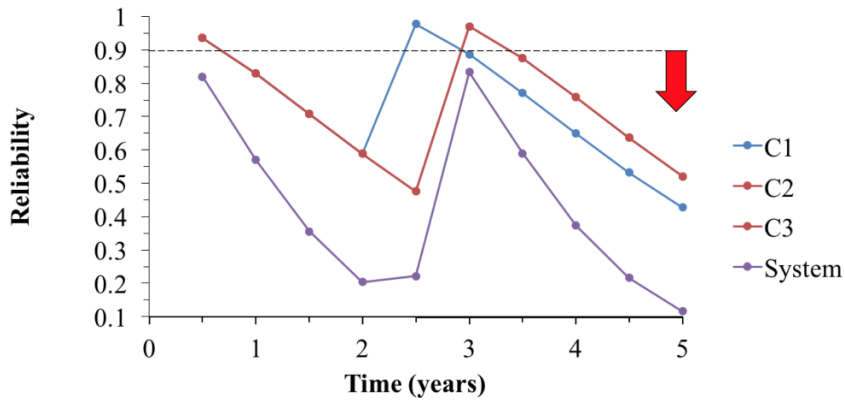


Figure 3. Equipment and system reliability based on a manufacturer recommendation

The second set of results corresponds to maintenance performed according to the methodology presented in this paper. The maintenance plan corresponding to a system reliability threshold of 99.5% is presented in Table 4.

Table 4. Maintenance plan based on present methodology

Equipment	n_{spares}	**Y1**		**Y2**		**Y3**		**Y4**		**Y5**	
C1	5	P	I	I	I	I	P	P	P	I	P
C2	4	I	I	P	P	P	I	I	I	P	I
C3	1	I	P	I	I	I	I	I	I	I	I

The equipment and system reliability profiles are visualized in Figure 4 and system reliability is seen to be maintained above the set threshold over the entire time horizon.

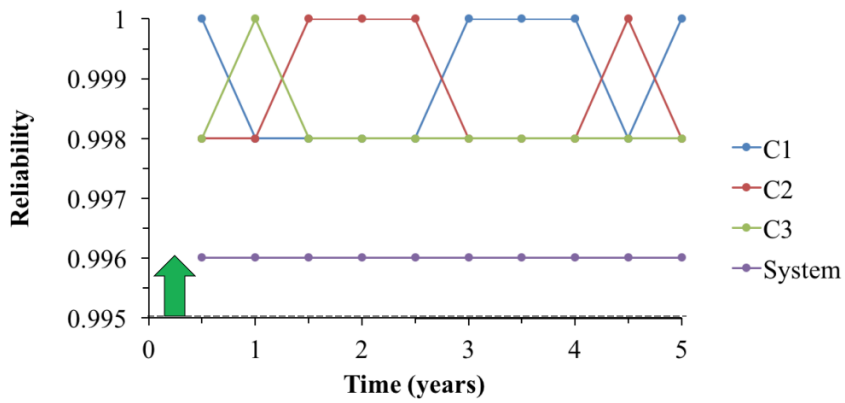


Figure 4. Equipment and system reliability based on the present methodology

Finally, it is noted that the results are dependent on the parameters used. The effect of changing the system reliability threshold is shown in Figure 5 in which each point corresponds to a different optimal maintenance plan and a trade-off between cost and reliability is observed.

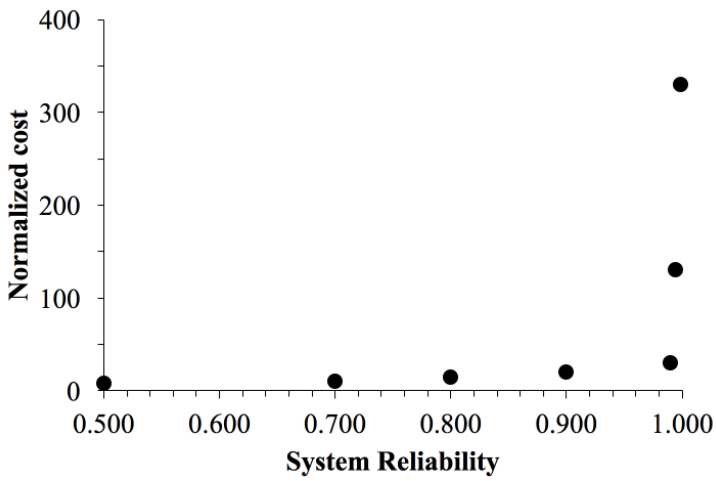


Figure 5. Pareto front of optimal maintenance plans

Conclusion

Maintenance planning is complicated by resource scarcity, system complexity, reliability nonlinearity and parametric uncertainty. This paper presents a maintenance optimization framework and employs multi-objective optimization under uncertainty to help guide resource allocation. Preliminary results show that application of the techniques adopted in this paper can result in improvements in equipment and system reliability as compared to implementation of a manufacturer recommendation.

The optimal maintenance planning framework and formulated model can be adapted to ageing productive systems in different industries inclusive of refining, chemical production, and manufacturing both onshore as well as offshore.

References

1. Chalabi, N.; Dahane, M.; Beldjilali, B.; Neki, A. Optimisation of preventive maintenance grouping strategy for multi-component series systems: Particle swarm based approach. Computers & Industrial Engineering 2016, 102, 440-451
2. Khatab, A.; Aghezzaf, E. Selective maintenance optimization when quality of imperfect maintenance actions are stochastic. Reliability Engineering & System Safety 2016, 150, 182-189
3. Manzini, R.; Accorsi, R.; Cennerazzo, T.; Ferrari, E.; Maranesi, F. The scheduling of maintenance. A resource-constraints mixed integer linear programming model. Computers & Industrial engineering 2015, 87, 561-568
4. Martón, I.; Martorell, P.; Mullor, R.; Snchez, A. I.; Martorell, S. Optimization of test and maintenance of ageing components consisting of multiple items and addressing effectiveness. Reliability Engineering and System Safety 2016, 153, 151-158
5. Moghaddam, K. S.; Usher, J. S. A new multi-objective optimization model for preventive maintenance and replacement scheduling of multi-component systems. Engineering Optimization 2011, 43, 701-719
6. Rajagopalan, S; Sahinidis, N. V.; Amaran, S.; Agarwal, A.; Bury, S. J.; Sharda, B.; Wassick, J. M. Risk analysis of turnaround reschedule planning in integrated chemical sites. Computers & Chemical Engineering 2017, 107, 381-394
7. Birge, John R., and F. Louveaux. Introduction to Stochastic Programming. Springer, 2011
8. Collette, Yann, and Patrick Siarry. Multiobjective Optimization: Principles and Case Studies. Springer, 2004
9. Floudas, Christodoulos A. Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications. Oxford University Press, 1995

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Fire Incidents at Ethylene Oxide Reactors in Ethylene Glycol Plant

Kevin S. H. Hsueh
Assistant Vice President, Nan Ya Plastics Corporation
No.2, Formosa Industrial Complex, Mailiao, Yunlin, Taiwan, ROC
Email: kevinhsueh@npc.com.tw

Keywords: Spool piece flange leakage, bolt deformation, oxidation reaction, spontaneous combustion, reactor inlet pipeline, emergency vent, compressor oil pump, power supply panel, ground fault relay, ACB, MCCB, ethylene oxide, ethylene glycol

Abstract

In September 26, 2012 NYPC Mailiao Ethylene Glycol (EG-4) plant reported a fire incident on the spool piece flanges of inlet pipeline of both two Ethylene Oxide (EO) reactors, R-1/R-2, which were founded 43 minutes later after Recycle Compressor tripped.

1. The deformed bolts were founded on the Inlet pipeline spool piece flanges of both R-1 and R-2 reactors, which were caused by unexpected extra high temperature, leaded to the leakage of ethylene mixed gas and spontaneous combustion.
2. The insufficient and invalidated emergency vent, following the Recycle Compressor trip, triggered the abnormal oxidation reaction of ethylene/oxygen mixed gas at the front-end of both two reactors, 180 seconds after compressor trip, which gave rise to the extra high temperature in the reactor inlet pipeline and reactor dome.
3. The 6 inches valve of emergency vent kept open 90 seconds following the compressor trip, but the pressure drop was only 1.5 Bar, less than safety criterion 3.0 Bar. It indicated an insufficient vent quantity and created a possible pocket of gas of explosive concentration.
4. Recycle Compressor was tripped by low oil pressure while its affiliate main and auxiliary oil

pumps losing its 380V power supply at the same time.

5. The ACB(air circuit breaker) of 380V power panel, MCC-100/200, was tripped by ground fault relay protection resulted in stopping of power supply for all its distributed seventeen equipment, which included not only the main and auxiliary oil pumps of Recycle Compressor but also the air cooler fan motors of CO_2 stripper condenser.
6. The stator winding damage of air cooler fan motor caused an unexpected trip of the upstream ACB of 380V power distribution panel for its improper setting of ground fault relay protection. Tripping the MCCB(molded case circuit breaker) of motor itself to be treated a satisfactory way for protection of power supply system.

Process Description

Ethylene Glycol plant consists of two water-cooled ethylene oxide reaction systems plus recovery facilities, glycol reaction, evaporation and purification facilities.

1. Basic chemistry

<u>Ethylene Oxide (EO) unit</u>

Ethylene is oxidized by oxygen in the presence of a sliver catalyst to make ethylene oxide.

$$C_2H_4 + 1/2\ O_2 \longrightarrow C_2H_4O$$

ΔH @ 25°C = -25,550 kcal/kg-mole of C_2H_4

In addition, carbon dioxide and water are formed as by-products

$$C_2H_4 + 3\ O_2 \longrightarrow 2\ CO_2 + 2\ H_2O$$

ΔH @ 25°C = -316,220 kcal/kg-mole of C_2H_4

<u>Ethylene Glycol unit</u>

The direct reaction of ethylene oxide and water is to form ethylene glycol. Other reactions take place since ethylene oxide also reacts with ethylene glycol and higher homologues.

$$C_2H_4O + H_2O \longrightarrow MEG$$

$$C_2H_4O + MEG \longrightarrow DEG$$

$$C_2H_4O + DEG \longrightarrow TEG$$

2. EO reactor unit description

Ethylene and oxygen enter from battery limits and are mixed with cycle gas. The gas mixture from the Gas-Gas Exchanger flows downward through the tube of two EO Reactors where a partial conversion of ethylene to ethylene oxide occurs over a solid catalyst. The heat of reaction is removed by boiling water in the shell of the Reactor and producing steam. The ethylene oxide is scrubbed from the Gas-Gas Exchanger shell side exit gas using EO lean cycle water, and EO rich cycle water is sent to the Ethylene Oxide Stripping and Reabsorption Section. A major portion of the lean (scrubbed) cycle gas is sent through the CO_2 contactor section to remove CO_2 made in the EO Reactors. EO reactor unit scheme is shown in figure 1. The Recycle Compressor provides the head necessary to circulate the large flow of cycle gas through the reactors and scrubber.

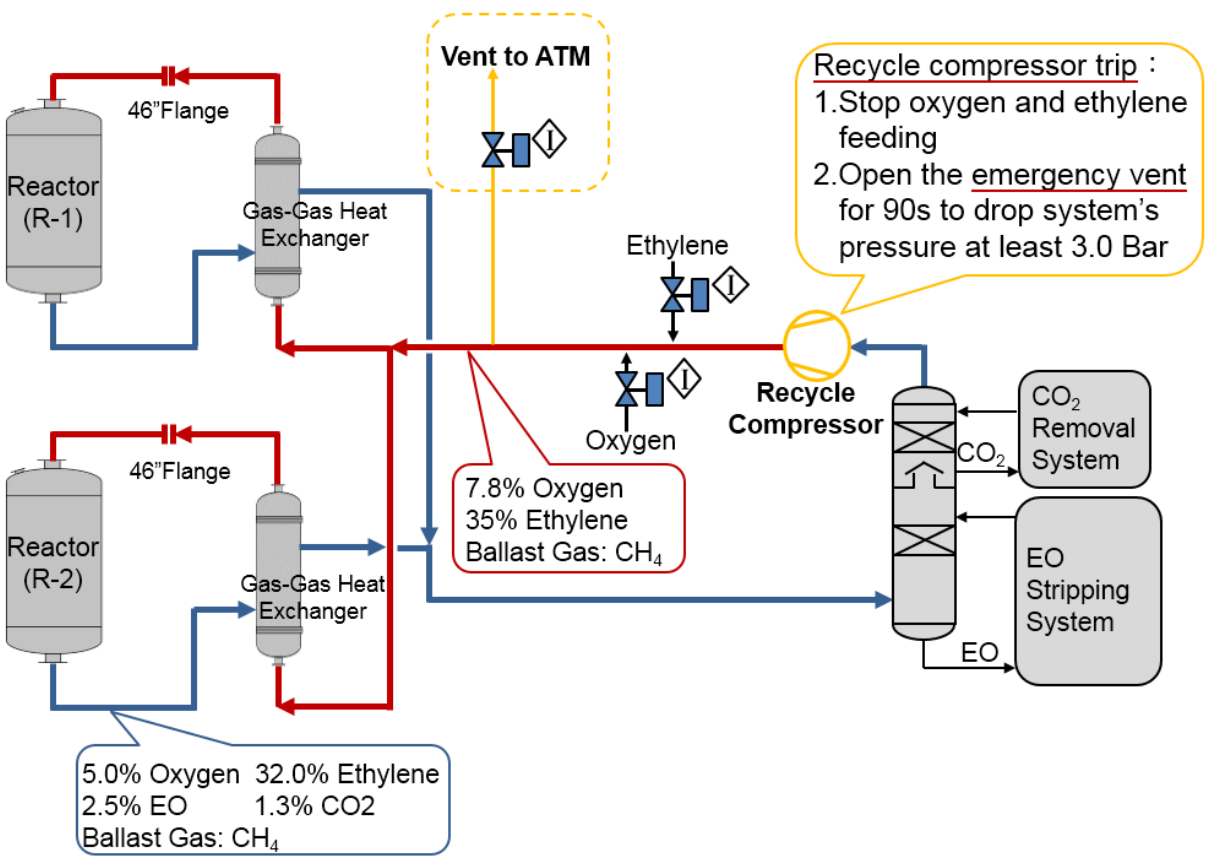


Figure 1. EO reactor unit Scheme

3. Emergency Vent Design

The Recycle Compressor may fail as a result of failure. Even though the automatic feed shutdown system has functioned correctly, there is the possibility that a pocket of gas of explosive concentration may have formed in the cycle gas pipe in the vicinity of the oxygen feed point.

To ensure that gas does not reach the Gas-Gas Exchanger or Reactors, the vent valve downstream of the oxygen feed station will open immediately. This will vent gas away from Reactors. Venting will be continuing for 90 seconds.

4. Reactor Inlet Pipeline Design

The 46 inches top outlet pipeline of Gas-Gas exchanger (the other word is inlet pipeline of Reactor) must be removed while perform the internal inspection based on the local government rule. In order to perform the crane job easier that the pipeline was designed with a spool piece on the Gas-Gas Exchanger side.

5. Power Supply Scheme

(1) High voltage: 13.2KV
Recycle Compressor motor power (13.2KV) is supplied from 3.3KV feeder LINE #1, and the system's power supply scheme is shown in figure 2.

(2) Middle/Low voltage: 3.3KV/380V

A. Pump/fan motors are supplied from 3.3KV feeder LINE #2 and divided into two groups.

B. The 380V power of main and auxiliary oil pumps of Recycle Compressor comes from the MCC-100/200 panel, same as CO_2 stripper air cooler fans.

C. Power Panel Protection Trip Design:

ACB (Air Circuit Breaker):

Grounding Fault Relay (0.3s)
Over Current delay
Short Circuit delay

MCCB (Molded Case Circuit Breaker):

Rated Current Protection (10s)
Short Circuit delay

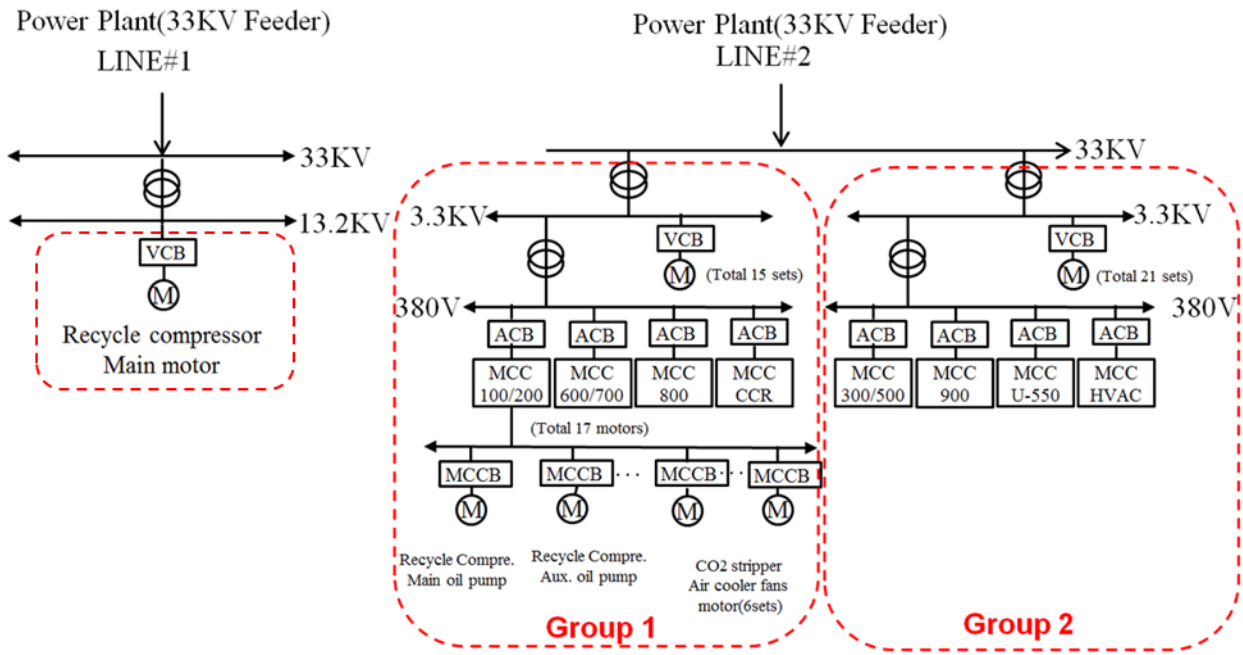


Figure 2. Power Supply Scheme

Description of Event

In September 26, 2012 NYPC Mailiao Ethylene Glycol (EG-4) plant reported fire incidents on the spool piece flanges of inlet pipeline of both two Ethylene Oxide (EO) reactors, R-1/R-2, which were founded 43 minutes later after Recycle Compressor tripped. Events sequence shown as figure 3 and line-up during pipeline flange fire shown as figure 4.

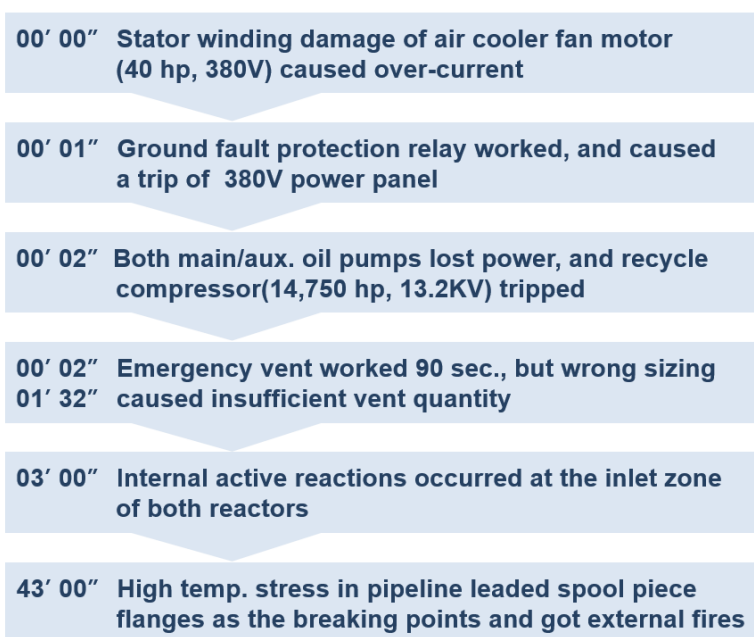


Figure 3. Events Sequence

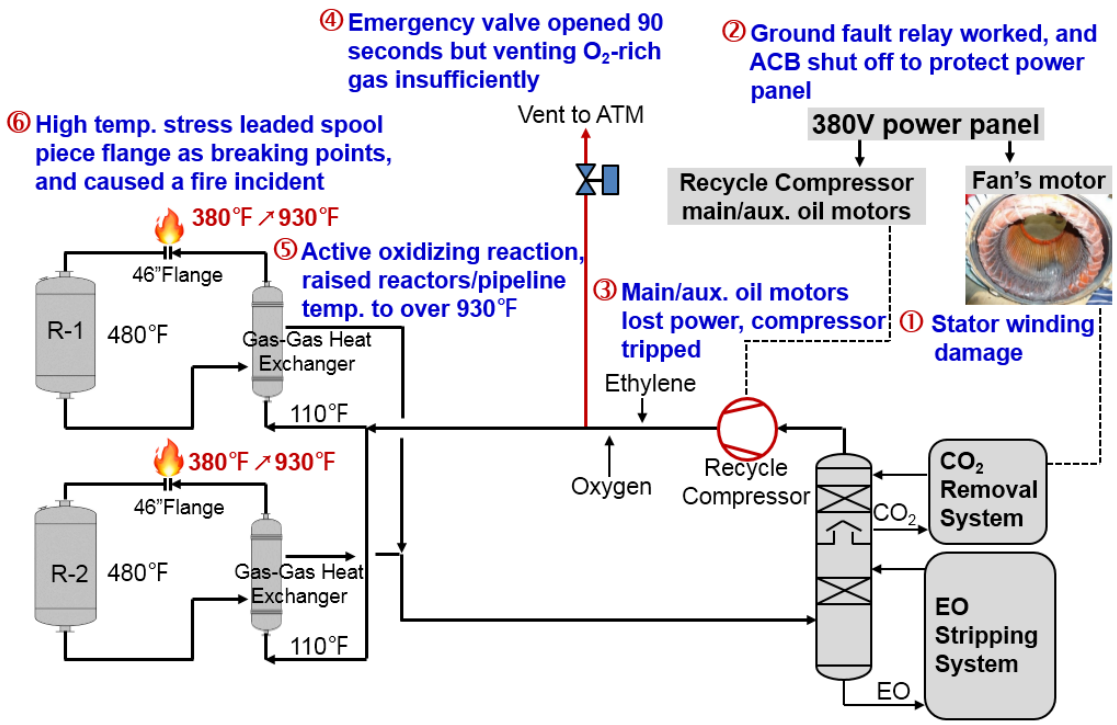


Figure 4. Line-Up during Pipeline Flange Fire

Root Cause Investigation

1. Bolt Deformation

The bolt deformation on the Inlet pipeline spool piece flanges of both R-1 and R-2 reactors, caused by unexpected extra high temperature(>930°F), leaded to the leakage of ethylene mixed gas and spontaneous combustion.

(1) According to Table 1, the strength of bolting materials will reduce to 34% at 950°F.

(2) Unequal thermal expansion across the pipeline at 930°F causes higher stress on spool piece flange, which simulation result is shown in figure 5.

ASME B31.3

Nominal Composition	Spec. No.	Type/ Grade	Min. Temp., °F (6)	Specified Min. Strength, ksi Tensile	Specified Min. Strength, ksi Yield	Min. Temp. to 100	200	300	400	500	600	700	800	850	900	950	1,000	1,050	1,100	1,150
Ni–Cr–Mo	A320	L43	−150	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	...	...	...	...	...	...	...	...
Cr–Mo	A320	L7	−150	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	...	...	...	...	...	...	...	...
Cr–Mo	A320	L7A	−150	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	...	...	...	...	...	...	...	...
Cr–Mo	A320	L7B	−150	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	...	...	...	...	...	...	...	...
Cr–Mo	A320	L7C	−150	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	...	...	...	...	...	...	...	...
Cr–Mo	A193	B7	−55	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	21.0	17.0	12.5	8.5	4.5	2.4	...	...
Cr–Mo–V	A193	B16	−20	125	105	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	23.5	20.5	16.0	11.0	6.3	2.8	1.2
...	A354	BD	−20	150	130	30.0	30.0	30.0	30.0	30.0	30.0	30.0	...	...	...	...	...	...	...	...

Table 1.Strength of Bolts in Different Temperature

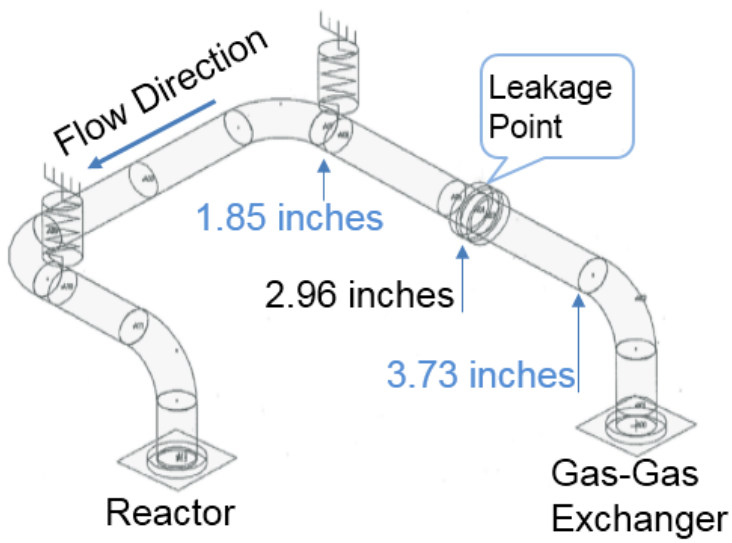


Figure 5. Simulation of heat expansion of pipeline at 930°F

Action

(1) Eliminate the spool piece design of the reactor inlet pipeline to strengthen its high temperature endurance, shown as figure 6. Use the bigger crane to lift up the whole pipeline to perform the internal inspection during overhaul

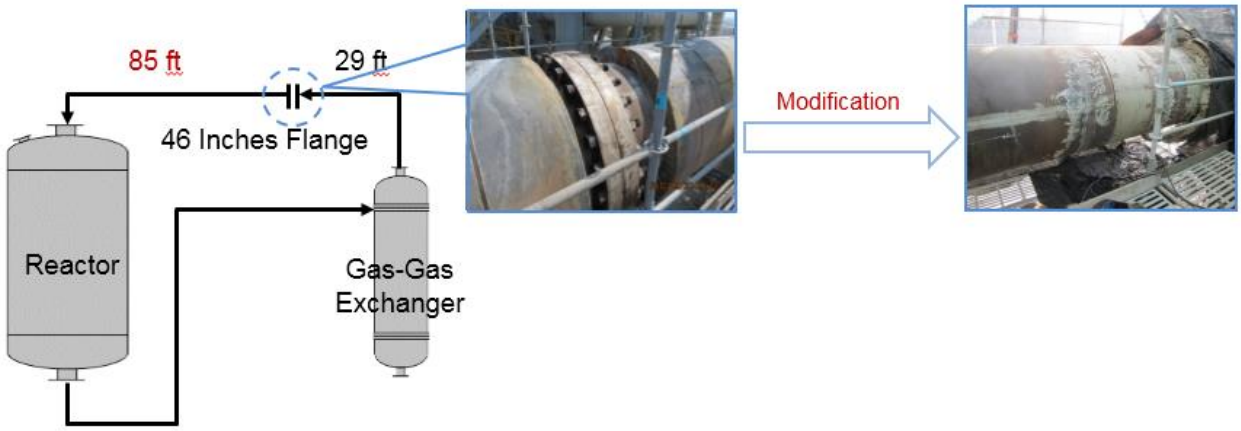


Figure 6. Eliminate the spool piece design of the reactor inlet pipeline

(2) Cr-Mo alloy bolts of inlet flange of reactors are replaced by Cr-Mo-V alloy bolts to improve its high temp. stress endurance. Strength of bolts in different temperature shown as figure 7.

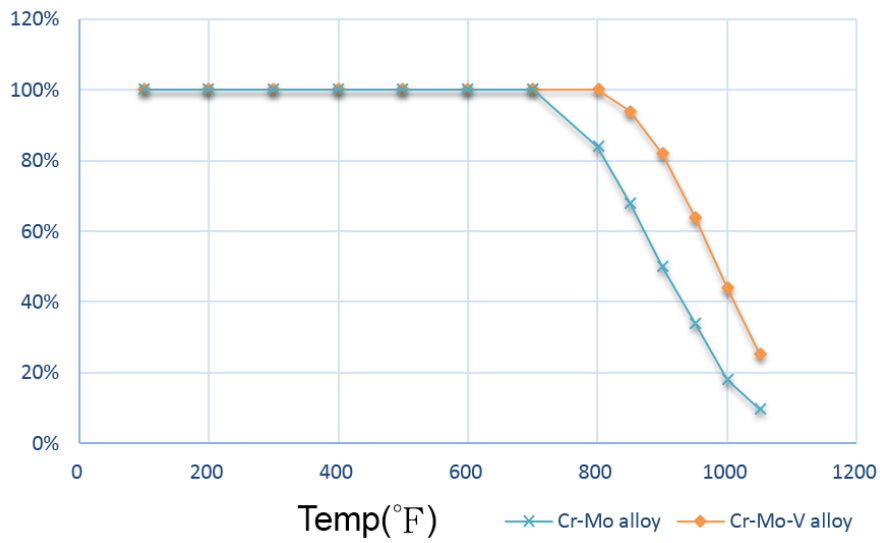


Figure 7. Strength of bolts in different temp. with Cr-Mo and Cr-MO-V alloy

(3) One of HAZOP and MOC team member must be proficient at material science to evaluate and recognize the impact correctly and properly.

2. Insufficient Emergency Vent

The insufficient emergency vent, following the Recycle Compressor trip, triggered the abnormal oxidation reaction of ethylene/oxygen mixed gas at the front ends of both two reactors, 180 seconds after compressor trip, and leaded the temperature to above 930°F in the reactor inlet pipeline and reactor dome.

The six inches valve of emergency vent kept open 90 seconds following the compressor trip, but the pressure reduce was only 1.5 Bar, less than the safety criterion 3.0 Bar, that indicated an insufficient vent quantity and created a possible pocket of gas of explosive concentration. On the other hand, PHA failed to confirm whether or not the amount of emergency discharge reached safety limitation.

<u>Action</u>

(1) Emergency vent valve and line size is replaced from 6 to 8 inches, and interlock logic is modified to take into account not only venting time (90 seconds) but also process pressure drop (>3.0 Bar), the modification shown as figure 8.

(2) All the safeguards, included emergency vents and pressure relief valves, must be reviewed not only the mechanical function but also its discharge quantification.

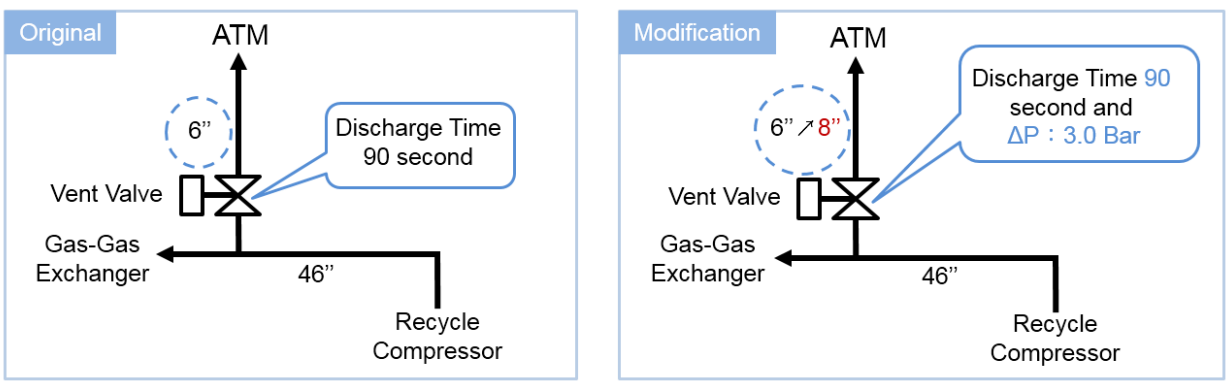


Figure 8. Emergency Vent and Interlock Modification

3. Recycle Compressor Tripped by losing power of oil pumps

Recycle Compressor was tripped by low oil pressure while its affiliate main and auxiliary oil pumps losing 380V power supply at the same time.

Action

(1) The main oil pump and auxiliary oil pump of Recycle Compressor comed from the MCC-100/200 panel which was belonging to middle/low voltage GROUP #1 originally. In order to reduce the risk that the auxiliary oil pump is modified to relocate to another MCC-300/500 panel, belonging to middle/low voltage GROUP #2, to reduce the risk of losing both oil pumps at the same time. The modification is shown in figure 8.

(2) Other affiliated oil pumps and blowers of major equipment, such as incinerator…etc., are also modified to be supplied from different power supply panels.

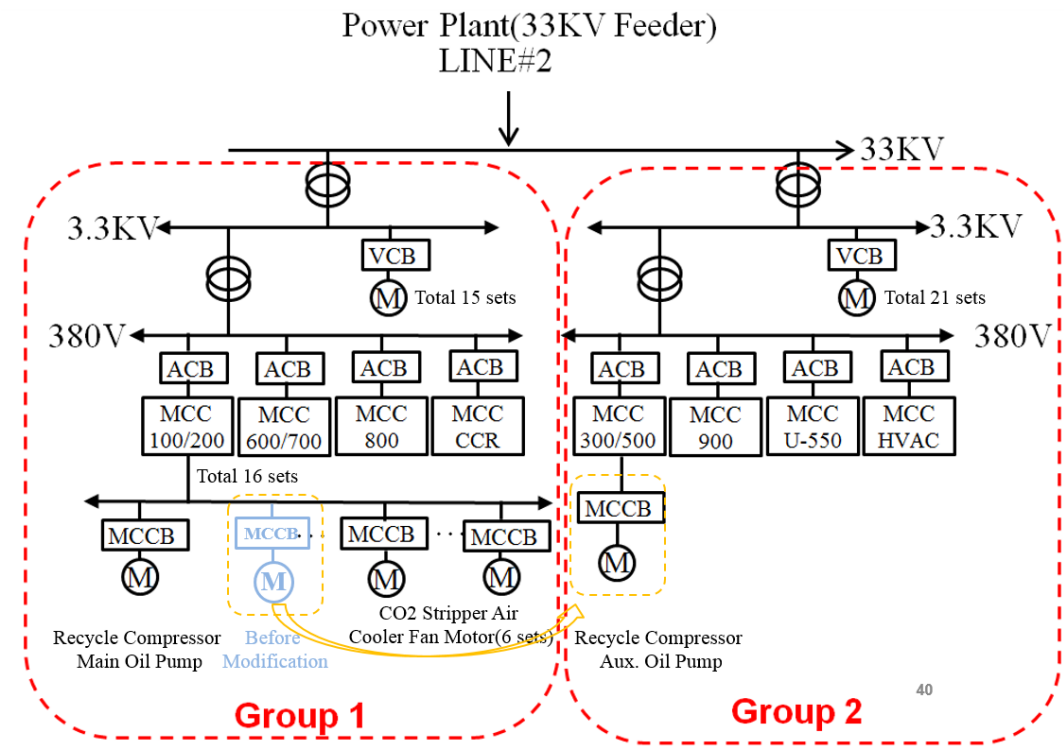


Figure 8. Power Supply Scheme Modification

4. Power Supply Panel Tripped by the Improper Ground Fault Trip Setting

The ACB(air circuit breaker) of 380V power panel, MCC-100/200, was tripped by ground fault relay protection resulted in the losing power for all its distributed seventeen equipment, which included not only the recycle compressor's main and auxiliary oil pumps but also the CO_2 stripper condenser air cooler fan motors.

The stator winding damage of air cooler fan motor was expected to be protected by its own MCCB. However, it tripped the upstream 380V power supply panel for the improper protection setting of ground fault relay of ACB.

(1)The insulation and ground resistance tests of fan motor were performed three months before the incident. Its insulation resistance >100MΩ@500V and ground resistance 0.12Ω showed that the motor was at good condition.

(2)The failed motor is analysis by TUV that the root cause is insulation failure between layers of stator which could be the manufacture defect or maintenance non-conformity. The insulation failure result is shown in figure 9.

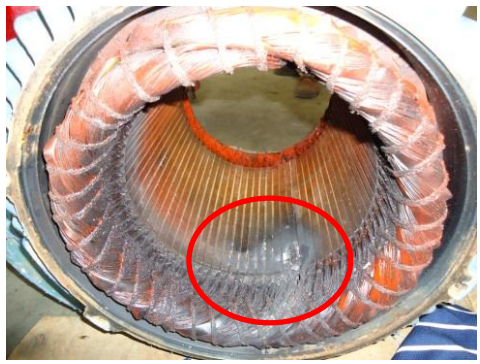


Figure 9. Insulation failure between layers of stator

<u>Action</u>

Because of the motor can be protected by its own MCCB with rated current protection and short circuit delay, that Protection Trip Design of ACB is modified to delete the ground fault relay.

ACB Protection Setting Modification

ACB (Air Circuit Breaker):

~~Ground fault relay (0.3s)~~ (deleted)
Over current delay
Short circuit delay

MCCB (Molded Case Circuit Breaker):

Rated current protection (10s)
Short circuit delay

Conclusions

1. The spool piece for the potential oxidation pipeline must to be eliminated to strengthen its high temperature endurance.
2. Emergency vent must be validated and confirmed.
3. Separated power supply scheme must be considered for the main and auxiliary oil pumps of major compressor.
4. The coordination of protection settings between ACB of power supply panel and MCCB of downstream terminal motors must be reviewed.
5. PHA group to assign a member specialized in materials to recognize the impact of process deviation.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

After the HAZOP
A Practical View of Process Hazards

Gregg M. Kiihne
BASF Corporation
Freeport, TX 77541
Email: gregg.kiihne@basf.com

Abstract

Much focus within process safety and process safety education is on the basic engineering phase where the principles of process safety and inherently safer design can be incorporated into the process design. The culmination or capstone of these process safety-related activities is typically the HAZOP study, where the study team carefully reviews the process design and declares at the end that acceptable levels of risk are achieved (once Corrective Actions are implemented). Experience has shown, however, that incident-causing errors may be introduced into the design during many different stages in the project lifecycle including detailed design, construction, maintenance and even during normal operation; all of which are *After the HAZOP*. This paper examines a number of process safety incidents to demonstrate how such errors can creep into the design and provides a few key principles that engineers can use to limit such errors and the resulting incidents.

Introduction

Throughout the lifecycle of a chemical manufacturing facility there are many stages and many opportunities to influence the safety of the facility (See Figure 1), but none has the potential to influence – positively or negatively – the inherent safety of the plant as the development of the process chemistry. The hazards introduced in this stage must be safely managed for the entire operating life of the facility. But through the intelligent and often clever development of the chemical synthesis route and processing steps, the hazards that are removed at this stage will no longer need to be managed.

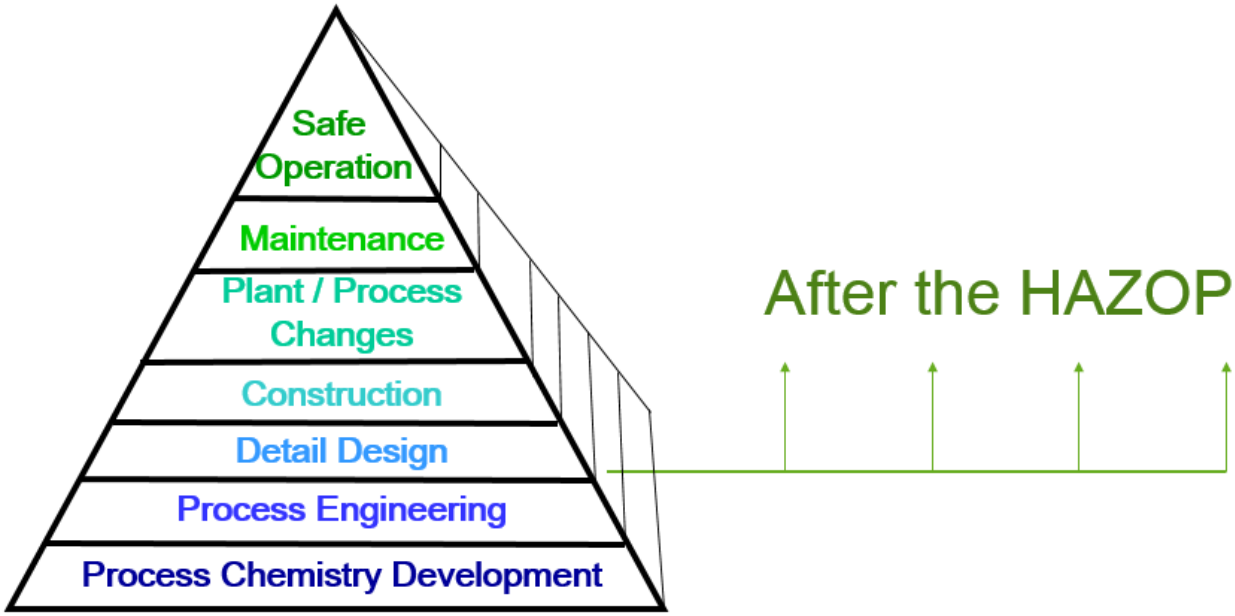


Figure 1: Stages of the Project / Plant Lifecycle

The process (design) engineering step that follows is the typical task of chemical engineers in industry; taking the lab scale chemical process and scaling it up to an industrial scale manufacturing facility. However, this role is typically limited to equipment design from a chemical process perspective. There are typically multiple design reviews throughout the process engineering stage, and the cap stone review, especially from the perspective of process safety is the process hazard analysis, often carried out as a Hazard and Operability (HAZOP) study. Because of the thorough, rigorous nature of a HAZOP study, it can be quite tempting for the project team to think that their work is done with regards to process safety. Experience has shown however that there are many opportunities for new hazards to be introduced in later stages of the plant life cycle.

In the detail design stage of the project, the chemical engineers hand over the process design to the other disciplines, who then create the blueprints from which the plant is built; blueprints for the foundations, the structures, the processing equipment and instrumentation. In the construction phase, the construction engineers and the fabrication teams make those blueprints become reality in concrete, steel and wires; making progress…but also making opportunities for new hazards to become reality.

Once the plant is commissioned and started-up, engineers cannot leave ‘good enough’ alone, so they optimize, increase the throughput, decrease the energy consumption…all good things, but also opportunities to introduce new hazards into the process and plant. As it does to all of us, time and the elements take their toll on the equipment and instrumentation, so they must undergo routine maintenance to keep system performance and integrity within the specified bounds. Maintenance also means putting people close to the equipment and potentially the process chemicals; an opportunity for the hazards of the process to be manifest in an incident.

Finally, if all goes well, the process operates smoothly more than 98% of the time. Yet even during these times of relatively smooth operation, because there are routine interactions between people and the process, there are still opportunities for something to go wrong.

Detail Design

Many years ago, the propylene purification section of a Naphtha cracker was largely destroyed by a fire after a section of piping split (see Figure 2) releasing several tons of a propylene lights stream to atmosphere. The feed to the Propylene purification column was named "Water-free Propylene" because it had already undergone an initial de-watering step. The specification for this stream, however, allowed up to 3 ppm of water in the propylene. At first glance, that seems like a trivial amount of water, but with a throughput of roughly 100 million lbs/yr, the total amount of water entering the column was roughly 300 lbs.

The line in which the rupture occurred was a 4-inch diameter line used for the start-up of the system, then blocked in at the valve labeled as normally closed (NC) during normal operation. During normal operation, water – being denser than propylene – would settle and accumulate in the blocked-in start-up line. Over the course of one year of operation, enough water could potentially collect to fill roughly 50 feet of 4-inch piping.

Believing this system to contain only propylene and traces of lighter organics, the detail designers did not anticipate any freeze potential in the system, and since the overhead system operated close to ambient temperature, no insulation was specified for the system.

After several years of operation, a particularly cold stretch of winter hit, and ambient temperatures were below freezing for many hours off and on over the course of several weeks. It was determined following the incident that sufficient water had accumulated in the dead leg to freeze during those cold stretches. During the third freeze cycle, the freezing water caused the pipe to split. When the ice thawed, the water escaped through the crack, followed by propylene and "light-ends."

Here, the use of the term "water-free propylene" for a stream that could and did indeed contain water, misled the design team into making a poor choice for the design of the start-up line. The take-away from this incident is that it is important to consider cumulative effects, especially for high volume or high-throughput systems, and to avoid dead legs in piping systems whenever possible (unless important to the design).

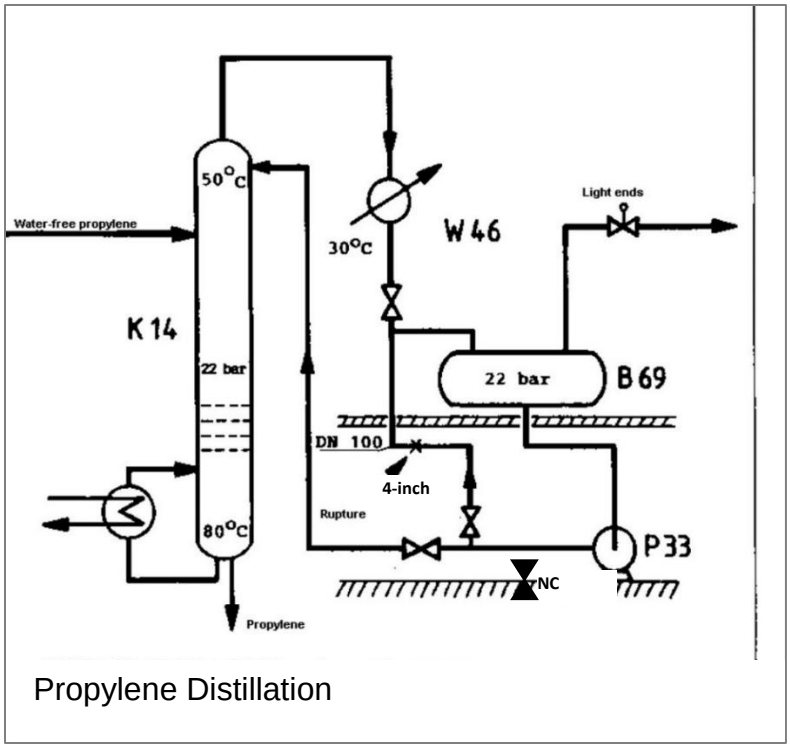


Figure 2: A Propylene Purification System

Construction

A particular project was implementing as part of the design a medium pressure, superheated steam line. As the project was running short of engineering funds, the designed included instructions to field-support the steam line. The construction team identified a convenient location for supporting the line and added a cross-beam which was about 4 inches beyond a condensate drop on the steam header. What the construction team did not fully understand is that a superheated steam line can "grow" several inches or even feet due to thermal expansion of the steel piping from ambient start-up temperature to operating temperatures. As the steam head approached operating temperatures, due to the improper supporting of the steam header, the growth of the header caused the condensate header to impinge on the cross-beam which eventually sheared off the smaller pipe, allowing a jet of medium pressure steam to escape, deflecting the pipe like a jet engine.

Field routing / design of piping, instrumentation and other components often leads to sub-optimal performance and/or the introduction of new hazards into the system.

Plant or Process Changes

During the debottlenecking of an overseas syngas plant, the process engineer determined that the existing relief device might not have sufficient capacity for the largest relief scenario. The existing plant had 2 x 100% relief valves installed, with one always in operation and the other valved-out to allow for inspection, testing and maintenance, see Figure 3. In order to provide enough relief capacity, the two existing relief valves and associated piping would need to be

replaced with the next larger sized valve. A cheaper option was identified, in which a third relief valve, the same size as the two existing valves, could be added in parallel. In future operation, two of the three valves would be in operation and one would be valved-out. For convenience, the set-point of all three valves was kept the same so that the maintenance and operations teams would not have to keep up with the various set-points.

During a high-pressure excursion following start-up of the new system, the two operational relief valves both opened in an effort to relieve the excess pressure. However, since there was far more relief capacity than needed for this scenario, the two valves started 'fighting' each other leading to chattering of the relief valves. This led to such severe vibration in the newly installed PSV inlet piping that the weld connection to the Syngas header cracked, leading to a significant jet fire.

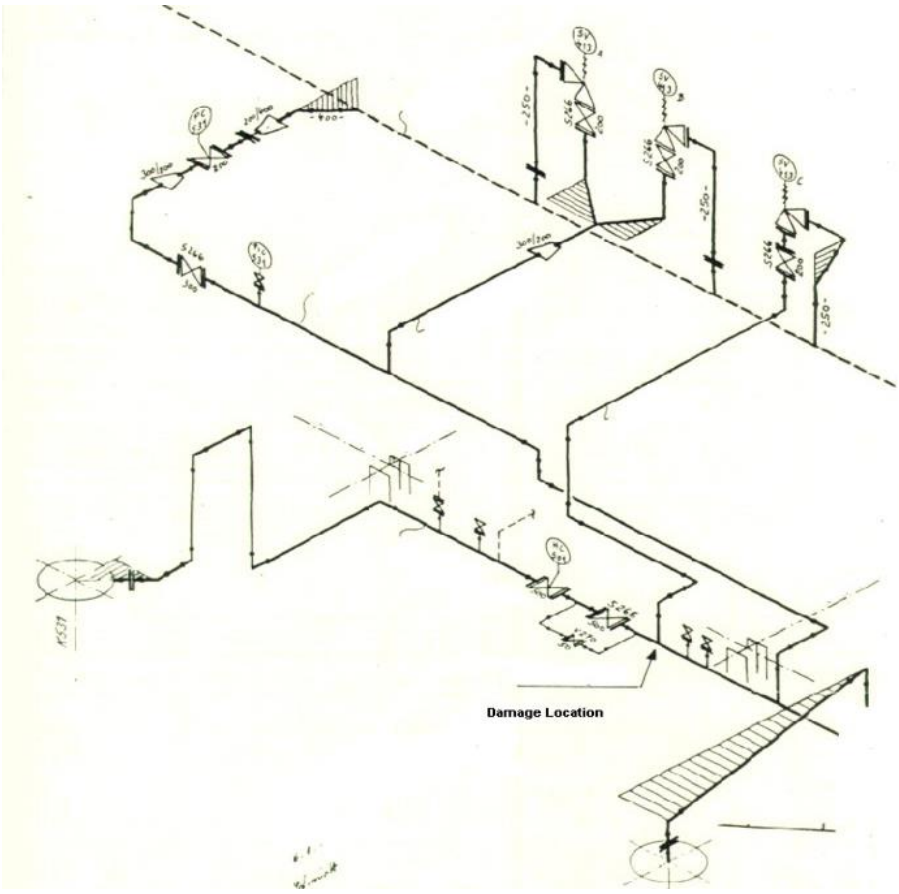


Figure 3: A Syngas header with additional relief capacity.

Due to the need to cover a variety of scenarios, relief devices will always have some level of over-design with regards to capacity. However, the installation of too much capacity can increase the likelihood and severity of relief device chatter. In addition, installing two relief devices on the same system with the same set-pressure is a recipe for disaster. In fact, API 520 recommends a setpoint offset of approx. 5% when using multiple valves.

Maintenance

During a proactive mechanical integrity thickness check, a pipeline was found to have several spots of thinning in one area. Once the replacement piping spools were fabricated, the line was taken out of service and cleared for line cutting activities. The contractor selected for the job was experienced with the type of work, the company and the work location. In order to remove the almost 200 feet of piping to be replaced, the line had to be cut several times at roughly 20-foot intervals. The piping contractor was walked through the job and made several cuts on the first day. Following a 3-day weekend, the contractor resumed work and made several more successful cuts on the line. On the third cut of that day, the contractor mistakenly cut the neighboring active pipeline full of flammable organic liquid. A significant fire immediately resulted, damaging a large portion of the pipeway and many of the pipelines.

We learn from this incident that in crucial communications, we must never assume that we have been understood. In addition, when administrative systems are used to manage hazards that can have catastrophic results – such as for hot work or confined space entry – the measures taken must be sufficiently robust and taken deadly serious by all parties involved.

Normal Operation

Even under so called normal operation, process-related incidents can occur. In one plant, a water system was circulated by a centrifugal pump. An installed spare was provided to improve the reliability of this important stream. During a storm near the plant, the plant experienced a momentary power 'blip'. Most of the electric motors in the plant continued to operate, but a few of the motors tripped as a result of the power blip. In an effort to maintain/regain normal operation of the plant, an operator was quickly sent to each of the motors that had tripped in order to restart each one.

When the operator reached the water pumps, he inadvertently started the offline pump, which had been blocked in, but not yet drained of water or locked out as the storm had disrupted maintenance activities. The operator confirmed that the pump started running then rushed to restart the next pump. He did not take time however to confirm the flow of water or the correct discharge pressure of the pump. Several minutes later, the pump ruptured, tearing the motor from the base and causing significant damage to the surrounding piping and equipment, see Figure 4.

It can be tempting to rush through certain jobs, especially when we have performed them many times before or are under time pressure. Yet it is at these times when we are more likely to make a mistake…and fail to recognize it. Multi-tasking and rushing greatly increase the likelihood of error. How do you ensure complete engagement of mind and body when performing important tasks? Do you ensure that appropriate safeguards are installed to help catch errors? A simple flowmeter on the pump discharge could have prevented such an incident.

Figure 4: Damage caused by a running blocked-in water pump

Conclusion

Process safety starts during chemical process development and is also strongly influenced throughout the process design engineering phase, but it does not end with the HAZOP. Constant vigilance is needed throughout the project / plant lifecycle to identify and manage new and developing hazards. Successful process safety is a team effort throughout the life of the facility.

Notice of Redaction:

At his request, Ravi Sharma's presentation (pages 437-457 of these Proceedings), has been redacted. Please refer to his related article published at:

https://doi.org/10.1016/j.engfailanal.2019.104192

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Systems-focussed risk and process safety education

Ian Cameron, Paul Lant, Maureen Hassall
School of Chemical Engineering
The University of Queensland, Brisbane, Australia 4072
Email: itc@uq.edu.au

Keywords: Education, risk, process safety, systems thinking, professional practice, industry engagement

Abstract

Risk management and safety are at the core of performance in the process and manufacturing industries. Global studies by major consultancies show that mature risk management drives performance. That maturity considers a multifaceted risk perspective. Given the complexity of risk and process safety situations in industry a strong systems focus provides an effective means for establishing learning designs and driving student outcomes.

This paper describes the design principles, implementation, learning activities of two compulsory, integrated units in risk management and process safety within the School of Chemical Engineering at The University of Queensland. Two courses, one in the 4th year of the Bachelor's degree, and another in the 5th year of our Integrated Masters program were designed on the educational basis of the Knowing, Acting, Being (K-A-B) schema.

This curriculum model considers the key knowledge domains in each course, their interlinking, as well as active learning strategies to exercise the knowledge areas within a socio-technical systems approach. The 'Being' aspect focusses on the personal transformation in thinking, professional attitudes and dispositions of students. It aims at preparing students for professional practice.

Course design was done in conjunction with industry personnel, who continue to be involved throughout the course delivery, using live industry projects, and site visits to major hazard facilities. Learning activities are coupled to individual and group assessments that include significant industry case studies, consulting projects and professional standard reporting. Oral assessments or defence are used to get deeper insight into student learning.

The transformation and expansion of previous UQ risk and safety courses that are fully immersed in socio-technical systems has provided an extensive, solid educational framework that informs, challenges and equips student engineers for entry to professional practice.

Introduction and Educational drivers

We all know that process safety is paramount. Getting it wrong affects lives, damages the environment, sinks companies and stains many corporate reputations. You do not have to look any further than national or international news reports on major fires, explosions or toxic releases to realize the necessity of high quality education and practice to help address such disasters. In every case, a series of complex systems related failures combine to produce major disasters that affect people, societies, businesses, reputation, the environment and other important risk receptors.

For higher education, effective course design and delivery, to develop understandings of the fundamental principles and practices that lead to managing risks and ensuring process safety are both non-trivial and sadly rare.

Interest in this area of engineering higher education is however a key requirement of many global accreditation practices. Such professional accreditation bodies often have clear requirements and statements around risk and safety. For example, Engineers Australia (2018), emphasize the following Intended Learning Outcomes (ILOs) for engineering graduates:

ILO1. "Appreciates the principles of safety engineering, risk management and the health and safety responsibilities of the professional engineer, including legislative requirements applicable to the engineering discipline" [s1.6(b)]

ILO2. "Identifies, quantifies, mitigates and manages technical, health, environmental, safety and other contextual risks associated with engineering application in the designated engineering discipline"[s2.1(h)]

ILO3. "Executes and leads a whole systems design cycle approach including tasks such as: identifying assessing and managing technical, health and safety risks integral to the design process" [s2.3(c)]

ILO4. "Understands the need for 'due-diligence' in certification, compliance and risk management processes" [s3.1(b)]

Similar statements of required competences can be found in ABET[1], AIChE[2], IChemE[3] or EUR-ACE[4] documents and accreditation practices.

---

[1] ABET states under General Criterion 3: "(c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability", http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2018-2019/#GC2

[2] Outline of Guidelines for PEVs and Programs (31 Oct 2017). See: https://www.aiche.org/sites/default/files/docs/pages/pevprogram-guidelines-v2_10-31-17.pdf

One recurring theme that underpins such competences is that of a *systems* approach. It is the case that system conceptualizations with deep system thinking and quality decision making are needed as learners synthesize and analyze complex engineered systems. Those systems are not simply the interconnected plant items but are also concerned with human interactions often guided by procedural requirements in both normal and abnormal circumstances.

In this contribution, we focus on two key courses within the School of Chemical Engineering at The University of Queensland that specifically address risk and process safety education: one course at the undergraduate level and the other at masters level. The School has a long history back to the 1970s of providing formal courses that address process safety and risk.

The first course, CHEE4002: *Impact and Risk in the Process Industries*, is a compulsory course in the first semester of the final (4th) year of the Bachelor degree in Chemical Engineering. It has a large cohort of approximately 200 students from all chemical engineering options that include chemical and also chemical/biological, metallurgical, environmental, materials degree options.

CHEE4002 course details are considered in an accompanying paper in this symposium authored by Lillburne, Lant and Hassall (2018).

The second course, CHEE7112: *Integrated Safety Design and Management*, is a compulsory course in the first semester of the final (5th) year of the combined Bachelor/Masters degree. In contrast to CHEE4002, the cohort has approximately 30 students, again drawn from the various chemical engineering programs within the School.

In the next section we consider some curriculum design principles that can guide the development and effective delivery of learning, driven by a 'systems' perspective. The design principles also consider effective andragogy and assessment techniques that help provide evidence of learning.

Following the background concepts we show how we have taken these principles and created two courses that seek to develop knowledge, skills and professional attitudes in our graduates that prepare them well for entry into professional practice.

Curriculum and course design considerations

Systems thinking for risk and process safety

Any reading of major reports arising from official inquiries or commissions into significant disasters clearly spells out the system-based nature of the events and their connections. The BP *Deepwater Horizon* accident report (BP, 2010) stated factors behind the disaster to be:

---

[3] See Appendix A2.6 on Process Safety, and 3.3 on advanced masters qualifications: http://www.icheme.org/~/media/Documents/icheme/Membership/Accreditation/Accreditation%20guidance%20V20%20Final%2011%20Aug%202017.pdf

[4] See EUR-ACE under the European Network for Accreditation of Engineering Education (ENAEE), http://www.enaee.eu/accredited-engineering-courses-html/engineering-schools/accredited-engineering-programs/

"*A complex and interlinked series of mechanical failures, human judgments, engineering design, operational implementation and team interfaces came together to allow the initiation and escalation of the accident.*"

Figure 1 gives an overview of the two key elements within a systems perspective. That perspective sees the real world as made up of *elements* or *parts* with *capabilities.* Along with their *interconnections* this provides the *functions* to ultimately fulfil *intended goals.* We briefly discuss those system concepts and will later show how they are considered within risk and safety education.

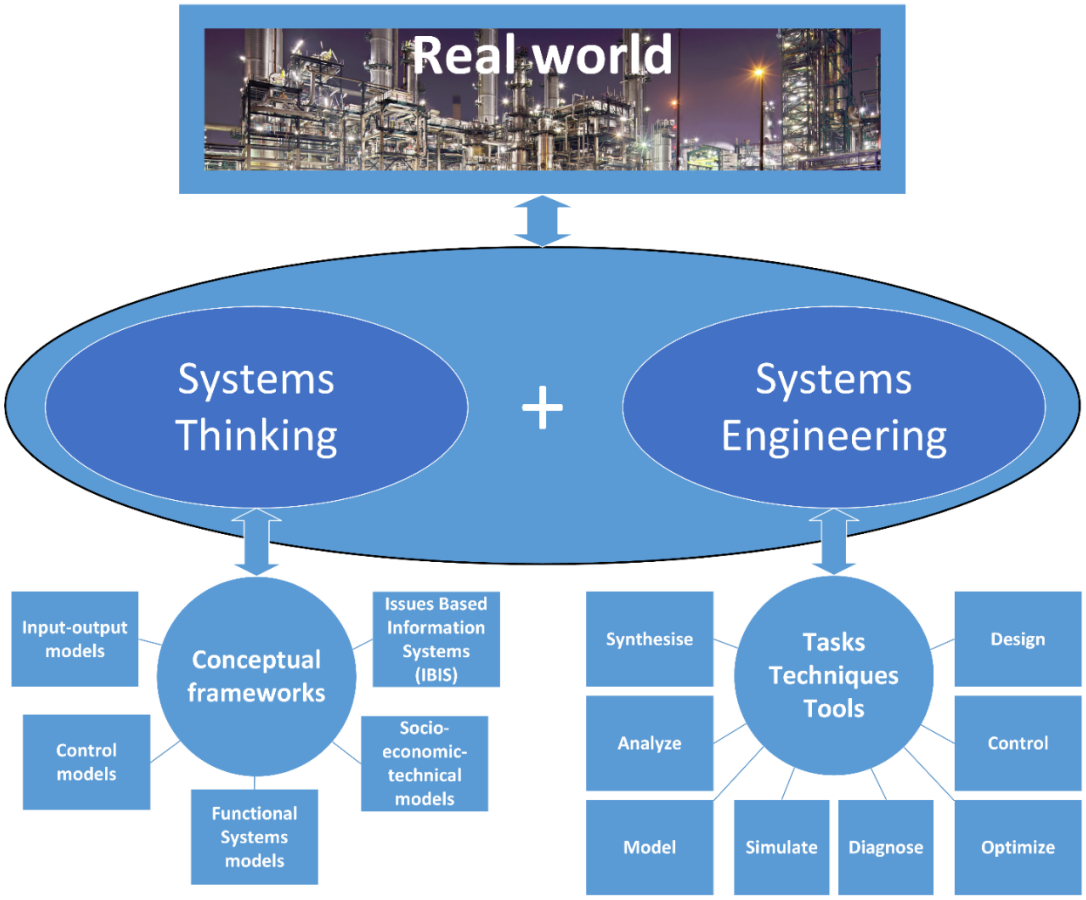


Figure 1 Representative components of a systems perspective

- *Key Aspect 1: Systems thinking*: exercises the skills and mental activity that forms and arranges in our mind ideas about the system. This allows us to address a wide range of outcomes. In doing so, we can employ a number of helpful conceptualizations that aid and organize our thinking. It helps address the issues around complexity.

  These conceptualizations can include:

  - *Input-output models*: considering system inputs and outputs, typical of process systems representations.

- *Control models*: considering inputs (manipulated variables), disturbances (unmeasured and measured) and outputs (controlled variables), often incorporating feedback and/or feedforward aspects or embedded control models.
- *Functional systems models*: these explicitly incorporate design intent into the models, as well as operational modes, system tasks, methods and constraints. They introduce concepts of capability, function and failure.
- *Socio-technical-economic models*: these consider the wider setting of engineered systems by introducing consideration of engineered designs, human factors as well as procedural aspects, all this set within a company culture and a much wider social and environmental setting.

A final social sciences conceptualization framework known as *Issues-Based Information Systems* or IBIS becomes important in risk and safety education. It provides a formal structure that captures the interrelations amongst issues, positions and arguments that are behind the various decisions made as learning activities such as projects are performed. This helps shape students' critical thinking and decision making.

- *Key Aspect 2: Systems engineering*: which consists of Tasks, Techniques and Tools applied in addressing risk and safety issues. Those tasks range from system synthesis and analysis, through modelling, diagnosis, optimization and design. To carry out tasks, a range of techniques can be deployed that often make use of numerous digital tools.

Systems concepts and practices are vital ingredients in learning design, as we now discuss.

Educational design principles

In considering the educational importance of risk and safety, key graduate outcomes can be formulated across three main areas:

- the knowledge areas that are to be acquired,
- the capabilities to take up knowledge and use it in familiar, new and challenging situations, and
- the professional attitudes, dispositions and personal skills required and developed

These three areas of *Knowing*, *Acting* and *Being*, form a schema (Barnett & Coate, 2005) as seen in Figure 2. This schema or variants of it[5] can be used for the design of learning units and curricula.

[5] Other concepts such as the *Episteme, Techne, Phronesis/Praxis* (Knowledge, Technique/tools, Practical wisdom/conduct) nexus can help drive course designs for intended learning outcomes. These issues are Aristotelian in origin.

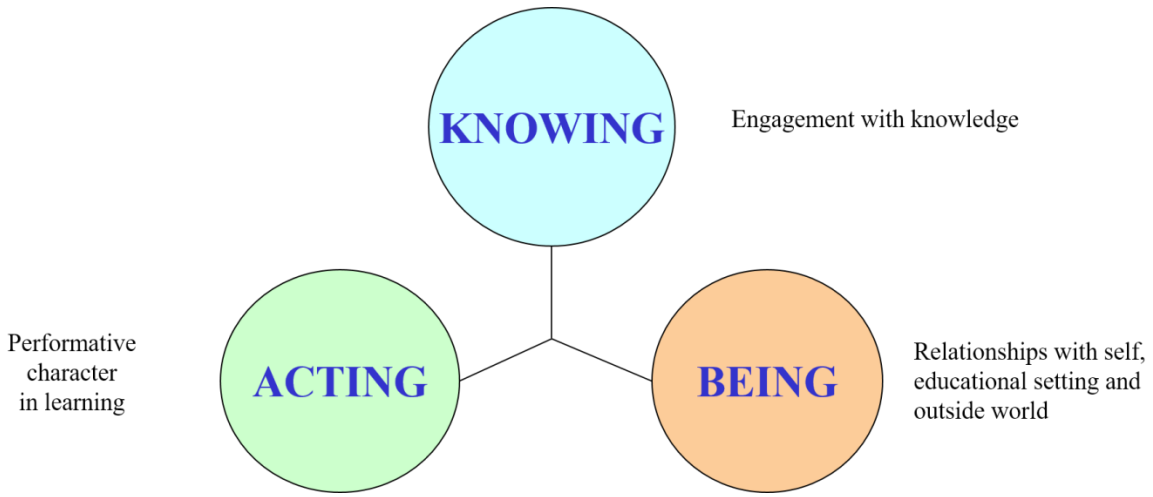


Figure 2 The Knowing-Acting-Being (K-A-B) schema for learning and design of curricula

In considering the K-A-B schema, we can identify that the 4 previously mentioned professional engineering accreditation requirements from Engineers Australia primarily relate to *Knowing* (*ILO1*), *Acting* (*ILO2*, *ILO3*) and *Being* (*ILO4*). Other accreditation jurisdictions are similar.

This schema can then help drive course design and also help in considering the interaction across years and courses. Those 3 focus areas of curriculum learning outcomes must be accompanied by a range of learning activities and student responsibilities. In the following section we discuss a set of interconnected course aspects that can guide learning activity choices.

Andragogy and learning activities

Andragogy describes a learning environment that incorporates a significant move towards self-directed learning. This learning model is essential for those moving into early-stage professional practice. It contrasts with the concept of pedagogy which is primarily teacher driven learning.

To help focus attention on learning designs that incorporate effective components to promote learning, Figure 3 captures some key considerations in addressing the theory-practice nexus.

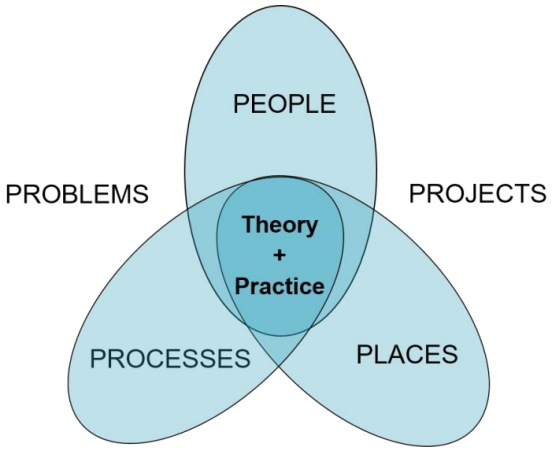


Figure 3 Dimensions of creative learning environments (5Ps model)

The concern in course and curriculum design and delivery is not just knowledge acquisition but also the development of competences in applying knowledge, skills and methodologies to complex risk and safety situations. We are very interested in the development of personal, professional attitudes and dispositions regarding risk and safety.

The dimensions of importance for educational design are:

1. *People*: what people will students meet and engage with during learning activities?
2. *Places*: what places and spaces will the students use and/or visit that will enhance their learning and drive the development of professional skills and attitudes?
3. *Processes:* what learning approaches and activities are best suited to drive ILOs? What should be the individual and team responsibilities within the course? And importantly, what range of assessment techniques should be adopted to provide proof of learning?
4. *Problems:* what types and complexity of problems should student confront in developing application abilities
5. *Projects:* what type and complexity of projects should be adopted to exercise a range of systems models that help address complex designs and operational scenarios?

Innovative course design comes from clever, engaging and interesting ways that students traverse the learning journey guided by these 5P dimensions. The following section illustrates some applications of these engagement dimensions.

Design and deployment of systems-focussed education in UQ risk and safety courses

In this section we discuss two current courses within the School of Chemical Engineering that provide education to 4th and 5th year students. The goals of these courses are presented, the various systems perspectives are laid out, and the use and importance of the chosen learning activities are described. The two courses are:

- CHEE4002 Impact and Risk in the Process Industries
- CHEE7112 Integrated Safety Design and Management

We now discuss the details of these courses, and emphasize important educational design features from both.

CHEE4002 Impact and Risk in the Process Industries

The intention of this course is to develop 5 learning themes:

1. Understanding risks and their impacts – from technical, human, social, and environmental perspectives.
2. Professional engineering practice and risk – values, ethics, behaviour, accountabilities and obligations
3. Modern risk management approaches and tools
4. Humans and risk
5. Sustainability and risk

The course is based on a broad view of industrial risk management concepts shown in Figure 4.

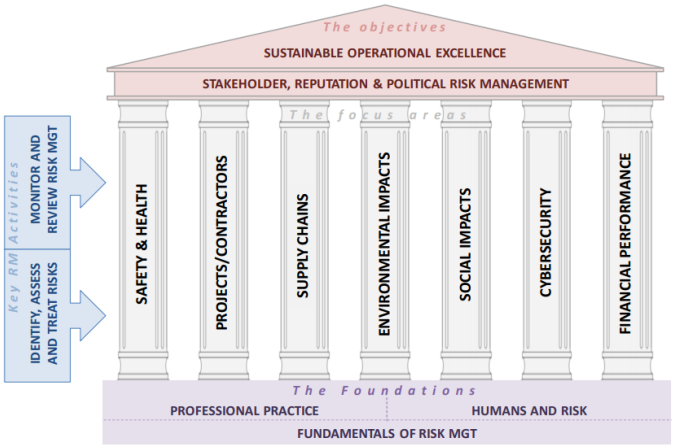


Figure 4 Scope of risk management considerations in CHEE4002

Figure 5 gives a structured map of key elements within the course. This shows the major system models that drive learning and importantly the student activities and assessments (Hassall & Lant, 2017).

Similar to CHEE7112 this course makes significant use of case studies, because:

1. They help build knowledge around the complexity of socio-technical systems,
2. They encourage systems thinking to unravel the role of "agents" and interconnectivity,
3. They utilize "story telling" which engages learners in their educational journey, and,
4. They emphasize the need for them to develop professional skills and attitudes

An important point is the assessment strategy. The strategies and assessment types help drive an "active learning" approach, with team-based case studies and projects accompanied by individual accountability in several assessment tasks and oral examination.

The course is "fit-for-purpose" for our Bachelor graduates and is very well regarded by the professional accrediting bodies – both Engineers Australia and IChemE as excellent preparation for entry into professional practice.

The reader is encouraged to look at the accompanying paper by Lillburne, Lant and Hassall in this symposium proceedings which details more in-depth information.

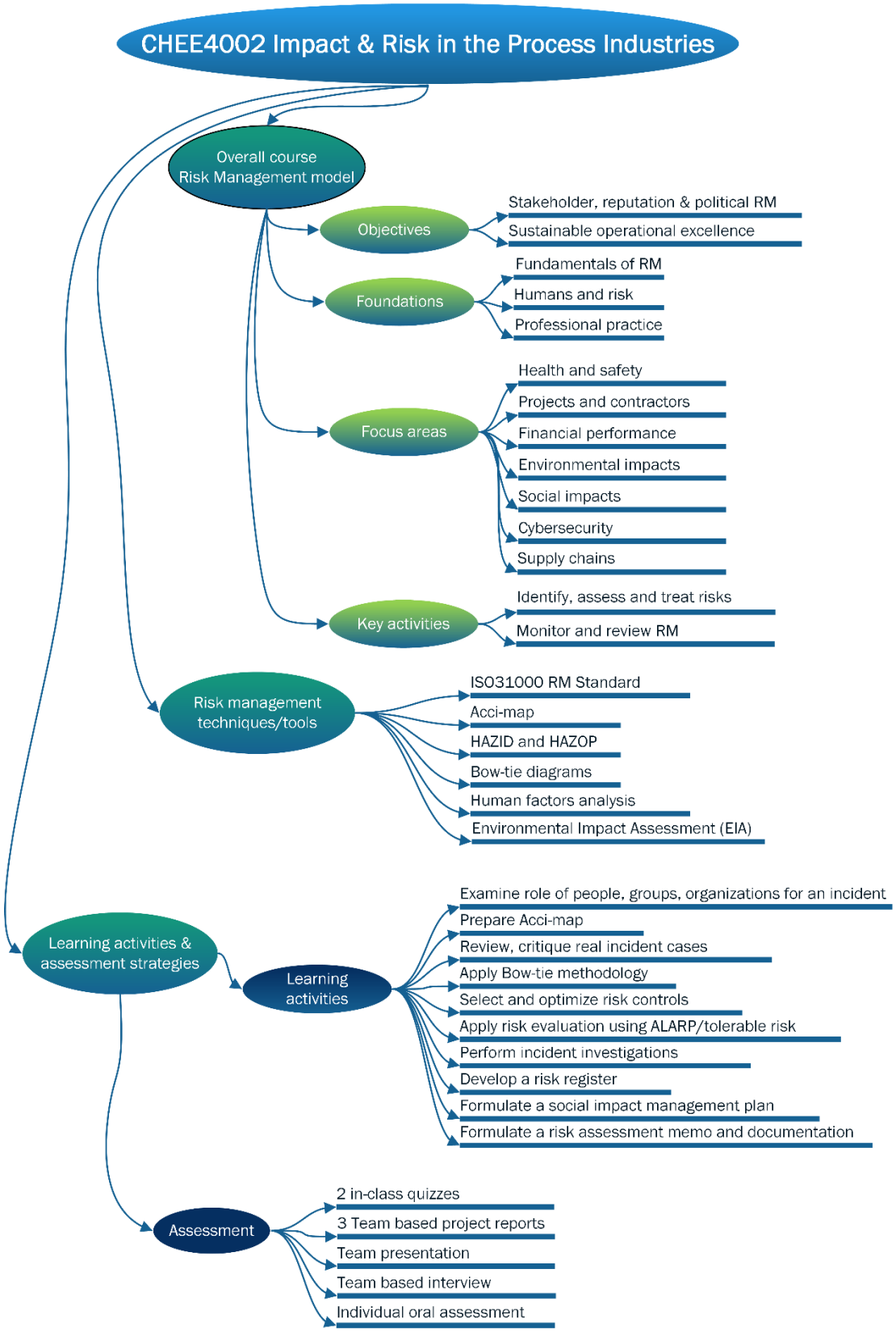


Figure 5 Structural components of CHEE4002 Impact & Risk in the Process Industries

CHEE7112 Integrated Safety Design and Management

The intention of CHEE7112 is to build upon prior learning in CHEE4002. The aims include:

1. Discern and evaluate existing and emerging system models that underpin approaches to dealing with risk and safe operation in complex industrial designs.
2. Develop and investigate Acci-Map representations to enhance insights around complex system failures and interactions.
3. Analyse complex industrial systems to determine best actions in design to address risks through inherently safer design principles
4. Critique and perform LOPA studies so as to assess risk levels and risk reduction strategies related to process plant
5. Analyse and specify the need for safety instrumented systems (SIS) for specific industrial case studies.
6. Evaluate the interaction of humans within complex engineered systems in order to enhance system resilience.
7. Investigate, analyse and design strategies for operator actions in industrial applications using cognitive work analysis (CWA) and strategy development and assessment

The overall structure of CHEE7112 is shown in Figure 6. The approach has the following characteristics:

1. A very strong systems fundamentals emphasis around formal system theory and deployment that deals with function and failure
2. In-depth considerations of qualitative and quantitative risk and safety issues
3. Application of a range of system models to complex process circumstances and critical examination of their applicability
4. Working on real industry projects or major system failures as consulting teams with time, financial and confidentiality accountability to the industry client.
5. Engagement with a wide range of professionals from senior process engineers, safety and operational risk experts, senior industry risk managers to heads of government regulatory agencies.

Having established the intended learning outcomes of this course the embedding of systems concepts, systems thinking and its use will be discussed as well as use of the 5Ps learning model.

The embedding of systems concepts, thinking and use into courses

The use of systems to help guide thinking and learning activities is paramount in the design of the two courses. Figures 5 and 6 show the range of system-based ideas used within each course as well as the assessment strategies and types. We now look at the importance of those learning design ideas, as summarized in Figure 3.

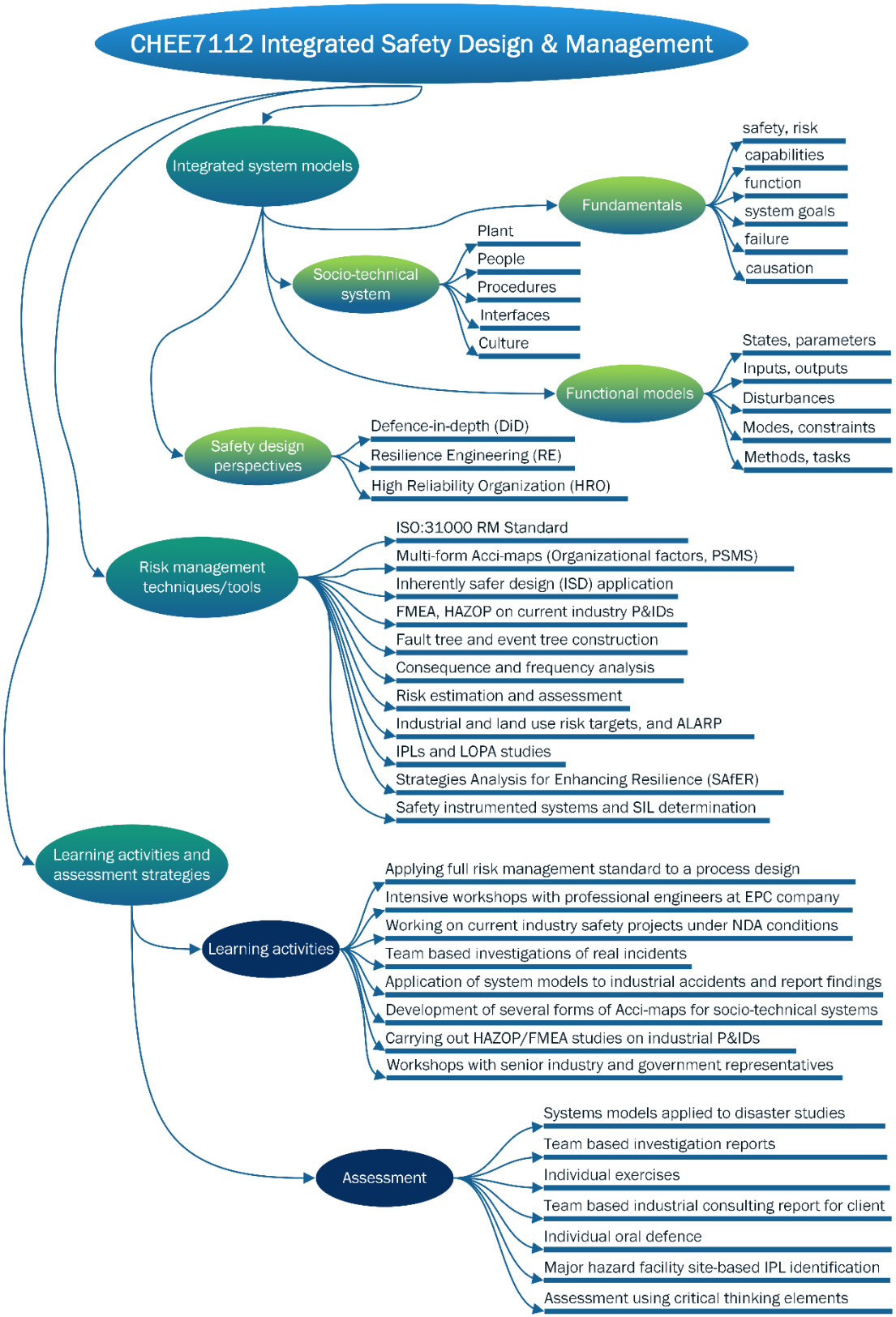


Figure 6 Structural components of CHEE7112 Integrated Safety Design and Management

Systems perspective and thinking

Ideas here include:

- Introducing students to system models that have the ability to capture the key components of the real world. They help direct and organize deep thinking and understanding of complex engineered systems
- A range of system conceptualizations that move from the simplest input-output models to socio-technical models that capture a much wider range of 'actors', viz. plant, people, procedures, management, culture and societal/environmental settings.
- Application of these models to a significant number of case-studies and industry projects, where insights, decision making and critical thinking can be developed

People

This involves interactions with:

- Academics
  - Engaging with existing and recent knowledge developments in the field
  - Seeing a diversity of views and expert discipline areas (Engineering, Psychology, …)
- Tutors
  - Personalized engagement in knowledge and application
- Senior industry and government personnel
  - The vital role of process safety and risk leadership
  - Exposure to professional attitudes and dispositions
  - Deep knowledge and practice is shared
  - Organizational cultures articulated and how they shape thinking and behaviours
  - Theory and practice seen together in work situations
  - Grasping the challenge of government responsibilities in a wider social context
  - Role and importance of high quality auditing
- Industry and EPC senior engineers/staff and operators
  - The role of engineers in assuring safety-in-design as a regulatory requirement
  - Importance of multi-disciplinary teams and thinking around complex designs
  - The role of time and cost to deliver high quality solutions to clients/company
  - Exposure to professional practice, techniques and tools
  - The importance of life cycle information systems and decision making documentation

Places

This involves taking student engineers into places with key affordances:

- Corporate offices: which provide opportunities to engage students with practising engineers, managers and consultants
- Collaboration areas: that facilitate student teamwork, proto-typing ideas and displaying thinking

- Virtual spaces: such as 3D walkthrough, observation and interrogation of plant such as our BP Refinery VR environment
- Industry places: where student teams can see the process plant under study, appreciate equipment scale, engage with engineers, senior managers, see a range of control stations and speak with operators around the situations and decisions to be made when abnormal conditions occur

Processes

This involves a wide range of learning activity and assessment models:

- Learning activities, can include:
  - Pre-recorded presentations on theory or fundamental concepts
  - Workshops where theory and practice meet in a specific risk or safety situation
  - Video presentations/sessions on many risk/safety topics, sourced globally
  - Case studies, drawn from a wide range of industries (Oil-gas, minerals, food, bio, …)
  - Industry sponsored projects
  - Debates around contentious topics such as land use planning for major hazard facilities
  - Visiting speakers that challenge student thinking and deal with issues such as ethical dilemmas.
- Assessment should be aligned to the intended learning outcomes, and these courses use a range of approaches that include:
  - Individual, focussed exercises for understanding and skill development
  - Team-based case studies and industry projects with substantial feedback
  - Team-based presentations to class and industry clients
  - Team oral assessments
  - Individual oral defence around theory and practice issues
- Formal critical thinking elements and project assessment rubrics

Finally we set out some ideas around the Problems and Projects aspect of our learning environments.

Problems

These can be classed as questions raised for discussion and/or solution. Most are focussed on individual knowledge, application and skill development. In these risk and safety courses they might typically be:

- An exercise to classify process system variables into: states, inputs, disturbances and outputs. This understanding can then be used for more complex team activities.
- An estimate of the physical effects from a specific loss of containment situation giving rise to a fire (thermal radiation), explosion (overpressure/duration) or toxic release (concentration).
- The application of ISD principles to a set of reaction pathways for a specific chemical compound.

  These types of problems are to drive student learning and help assess their individual capabilities

Projects

These activities are focussed on providing collaborative, team-based learning that requires significant research, deep investigation and insights around process design and human factors considerations, operational and management issues. They require careful planning, execution and professional reporting that is constrained by time and cost. In CHEE7112 the active learning strategy is driven primarily through projects: some on available case studies but other specifically sourced from major operating companies. Typical projects around risk and process safety have been:

- Addressing design, control and operational improvements for a naphtha separation unit.
- Examination of ship-to-shore fuel transfers for a major flammables fuel terminal.
- Study of facility design and operations, including key human factors for LPG export
- Design and operational investigation for new bulk liquids terminal for land use planning requirements
- Study of the design and operations of a catalytic polymerization unit
- Incident review of an isomerization unit for design, control and operator performance improvement.

These are projects that bring together complex chemical and physical processes, large DCS data sets, process engineering information and documentation including PFDs, P&IDs, SoPs, emergency response plans, along with actual control performance and operator screen designs. It provides a realistic immersion into real-world risk and process safety situations.

Summary and conclusions

Systems perspectives in risk and safety studies are absolutely essential. Higher education will fail our graduate engineers if they cannot grasp the complexities and the required integrity of engineered systems with considerations of process safety management and the vital role of human-centred design considerations. We believe that exposure to, and use of, various 'systems' perspective will better prepare our graduates for entry into professional practice.

We have set out some of the important systems-based concepts that form the foundation of two compulsory risk and safety courses in Chemical Engineering at The University of Queensland. Response from students has been extremely encouraging, that these courses help inform their knowledge around risk and safety issues, as well as developing basic skills in risk management practice.
Other evidence suggests that students recognize the importance of growing their professional attitudes, dispositions and skills around risk and safety via these learning pathways

Our experience with industry collaboration, EPC companies and government agencies has been excellent in terms of ready access to facilities, staff and challenging projects that add significant reality to the learning journey. As well, we have established excellent working relationships with other academic discipline areas such as psychology, philosophy and business that adds significant value to the student experience.

We continue to review, explore and focus on providing excellent learning design and pathways for our graduates. For us, the journey is never really finished!

References

ABET (2018), *Criteria for Accrediting Engineering Programs, 2018-2019*, see: http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2018-2019/#GC2 Accessed July 27.

AIChE (2017), *Outline of Guidelines for PEVs and Programs, PEV and Program Guidance Subcommittee*, See: https://www.aiche.org/sites/default/files/docs/pages/pevprogram-guidelines-v2_10-31-17.pdf Accessed July 27.

Barnett, R and K. Coate (2005), *Engaging the Curriculum in Higher Education*, Open University Press.

BP (2010), *Deepwater Horizon* Accident Investigation Report, September 8. (see page 31). https://www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report.pdf Accessed July 31.

ENAEE (2018), Standards and Guidelines for Accreditation of Engineering Programmes, See: http://www.enaee.eu/accredited-engineering-courses-html/engineering-schools/accredited-engineering-programs/ Accessed July 27.

Engineers Australia (2018), *Stage 1 Competency Standard for Professional Engineer*, see: https://www.engineersaustralia.org.au/sites/default/files/resource-files/2017-03/Stage%201%20Competency%20Standards.pdf, Accessed August 31.

Hassall, M. E. and P. Lant (2017). *Teaching Risk: a New Approach*, The Chemical Engineer, The Institute of Chemical Engineers.

IChemE (2017), *Accreditation of chemical engineering programmes: A guide for higher education providers and assessors.* See: http://www.icheme.org/~/media/Documents/icheme/Membership/Accreditation/Accreditation%20guidance%20V20%20Final%2011%20Aug%202017.pdf Accessed July 27.

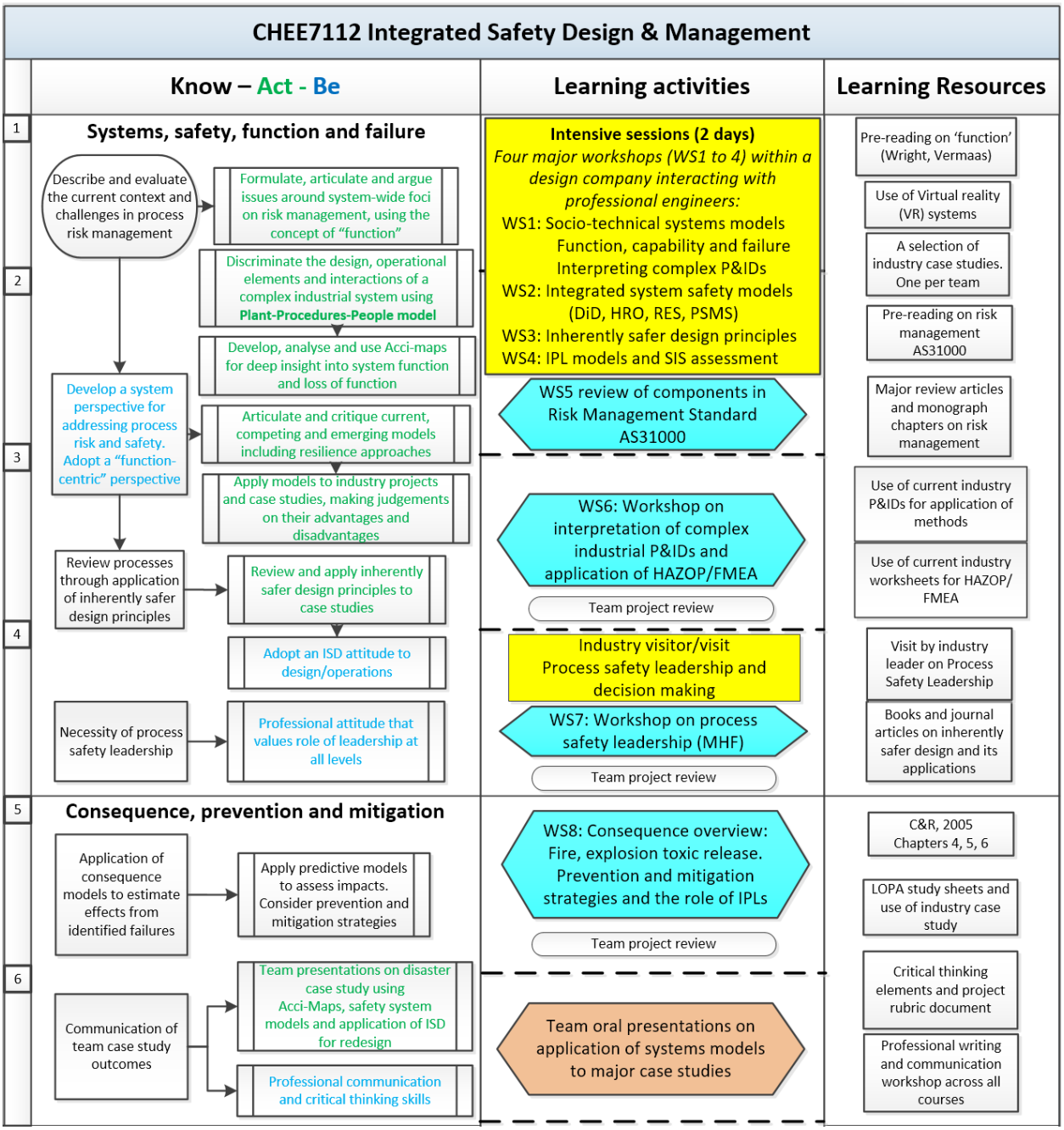
Lillburne, C., P. Lant and M. Hassall (2018), *Flipping the assessment model: Teaching and assessing 'things that matter'*, MKOPSC International Symposium, Texas A&M University, College Station, Texas, USA.

Werner, Kunz and Rittel, Horst (1970), *Issues as Elements of Information Systems*, Working paper No. 131, Studiengruppe für Systemforschung, Heidelberg, Germany, July 1970 or see full entry at: https://en.wikipedia.org/wiki/Issue-based_information_system Accessed July 27.

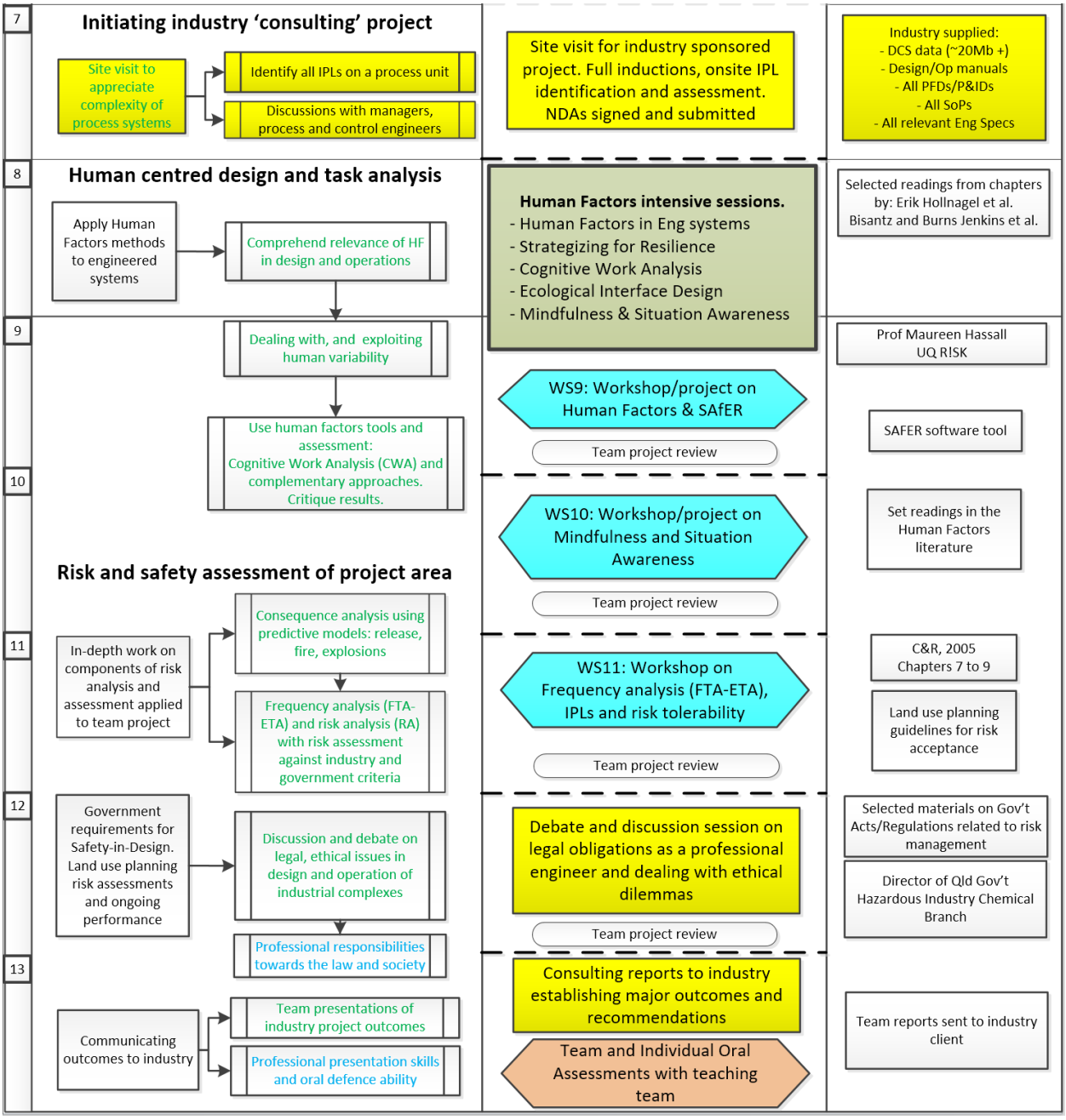
APPENDIX: The learning pathways for CHEE7112

This shows the intended learning pathways design or pathway over a 13 week seminar, summarising the K-A-B elements, learning activities and some of the many resources available to students.

First half of semester:



Second half of semester:



Other information on these courses is openly available on The University of Queensland website at:

For CHEE4002: https://my.uq.edu.au/programs-courses/course.html?course_code=CHEE4002

For CHEE7112: https://my.uq.edu.au/programs-courses/course.html?course_code=CHEE7112

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Improving the Quality of Undergraduate and Company Interactions in Process Safety

Trish Kerin
IChemE Safety Centre
Email: tkerin@icheme.org

Key words: Commitment, Integration with Operations, Process Safety Information

Abstract

There are many different elements an undergraduate student needs to learn to become an engineer. These range from basic chemistry to fundamental engineering principles and process safety. But a key aspect of the education is interaction with facilities and future employers. This interaction can be achieved via a number of ways, with the most intensive being intern employment ranging to the least intensive consisting of facility tours. As part of a project to improve the overall process safety education for engineering undergraduates, the IChemE Safety Centre has been exploring specific guidance to help focus the interactions regarding process safety to achieve greater value from them. This includes aspects like establishing a criteria for what students should be seeking information on as well as what companies should be seeking to provide. This paper will explore this criteria and challenge companies and academics to apply this with students.

Introduction

Studying engineering at university is an intensive program, and one of the longest bachelor's degrees. During this time of between four and five years studying, there needs to be opportunities for the students to interact with industry and gain valuable experience in the workplace. This is because the academic setting and the industry setting are significantly different and they typically work on different priorities and timelines. In the past in Australia, at the end of year three, students would seek work experience for approximately 12 weeks usually over the summer period. Given by this stage they have some engineering fundamentals, they can contribute effectively to the organisation, but also learn a great deal about the industrial environment. When they return to complete the fourth and or fifth year, they do so with some experience, which can enhance their experience as they have learnt to translate their academic information into industrial applications.

What is the problem?

Sadly, over time, these experiences have become less prevalent, with students struggling to find the work placement. Anecdotal information from a university suggested approximately only 60% of their students were achieving placements. There may be several reasons for this, and this paper is not intended to discuss these reasons, other than to suggest that the opportunities offered by companies have decreased, making it more difficult. It is then important for companies to recognise that they have a place in providing these opportunities to have a chance of getting better rounded and experienced graduates to employ. It is now possible for students to graduate and enter the workforce having never seen a process plant.

While the lack of experience leading into the final years of education is a challenge for the engineering development of the student, it also results in reduced opportunities for students to experience process safety in an operational sense.

Without any operational experience while a student, there is a chance that when they enter the industry as a graduate they do not understand the importance of operational process safety. For example, if their first experience of a permit to work system is when they have been stopped from doing a task and sent to get approvals, this can set a tone that safety systems just "get in the way of doing the job". While this may be an oversimplification, the smallest issues can shape a person's perspective and create a culture that may not be optimal.

When interaction does occur, it is often less structured. A student may receive a tour of a facility where they are shown the different units and have a chance to ask questions. This shows what a facility looks like but does not explain how it operates from the people perspective. Or during placement a student may be given a project to work on, varying from an actual engineering task involving working with others, to a mundane task of processing and filing paper work. Obviously the more the task focuses on engineering work the better the experience will be for all the parties.

A possible solution

There are multiple aspects to the possible solution. First, more opportunities for placement activities is required, however that is not the point of this paper. There also exists other opportunities for students to interact with industry facilities to gain some degree of experience, such as detailed site tours. Again, it would be useful to see more of this occur, but that is not the point of this paper. This paper focuses on how to improve any interaction that does occur by providing a structure that highlights the place process safety plays in an organisation. Process safety in any high hazard organisation should be an integral way of doing business. This means that a great deal can be learnt about an operation by asking about process safety. This is because the discussion will venture into elements of operational control, allowing the knowledge transfer about the process as well as the safety.

It should be noted that the responsibility for a positive interaction between student and industry rests with both parties. Students have an obligation to seek information and ask questions and industry needs to have a will to show students different aspects and answer the questions asked. It is important to understand that the first interaction between students and a particular facility is likely to be the site induction. This is a great opportunity to show case some of the process safety processes at a facility as well as an opportunity to ask questions.

What are the key topics?

There are several areas that the student and industry should engage in. As discusses above, several of these can be introduced in a facility induction, but others require more targeted questions. Considering the key element is to show and learn about operational process safety in an industrial setting focuses the questions to the types of interactions. Such interactions include:

- Discussion on key hazards at the facility
- Discussion of the controls implemented to manage these hazards
- Understanding the role of the student during their time at the facility – is it is tour or an internship, as well as what activities the student will undertake and understanding the role of the supervisor at the facility
- Understanding the emergency response requirements and the student's role in these
- Use of the permit to work system
- Use of the management of change system
- How the incident reporting and investigation process works
- How the safety management system is structured and their role within in it
- How safety is measured on the site with respect to metrics or indicators
- How integrity of equipment is maintained
- Operational parameters

What should students be asking and what should industry be sharing?

Each of the items listed above have a different perspective depending on whether it is the student asking or the industry sharing. Table 1 highlights key considerations from each perspective. This is not an exhaustive list, but some initial ideas on interaction.

Topic	**Industry**	**Student**
Key hazards	Site hazards should be presented as part of any induction, however for engineering students, extra information should be shared, such as how they hazards were assessed and how decision were made on their management.	The student should seek out information on the site hazards, such as chemical properties, so they are informed and able to ask about specific details of the properties and how it is managed.
Controls	The philosophy behind the selected and rejected controls should be discussed. This would include how they are maintained to ensure they function as intended. This detail may be found in the	This follows on from the hazards, for example if a hazard is flammable gas, how is the atmosphere monitored, where are gas detectors located and how do they function. If there are reaction hazards, how is the

	Process Hazards Analysis or Safety Case Report.	reaction started, how can the reaction be controlled or terminated?
Role clarification	It should be clear to the student what role they have in the current interaction and therefore what obligations they have with that position. It should also be clear how that role fits in with the rest of the organisation.	Students should seek to understand how the role that are fulfilling impacts on the safety of the facility (or not) and how it interacts with others in the organisation.
Emergency response	In addition to basic induction information on what to do in an emergency, students should also be taught about why specific scenarios for emergency planning were selected and how the process is developed.	Students should ask about how the emergency response plans are developed and how the hazards and controls feed into the plans. They should also ensure they are fully aware of their role in an emergency and be able to exercise that role confidently, even if it is just to muster.
Permit to work system	Students should be introduced to the facility permit to work system and its requirements, especially if they will need to be a permit holder at some point.	Students should ask about when a permit is required and how the process is managed, including what isolations and risk assessments are required and who has authority to approve a permit.
Management of change	Students should be introduced to the facility management of change system and its requirements, especially if they will need to be involved in a change at some point. This should include the requirements for management of change to be closed out.	Students should ask about when a management of change is required and how the process is managed, including what risk assessments are required and who has authority to approve the change. This should include the requirements for management of change to be closed out.
Incident reporting and investigation	Students should be informed of the need to report incidents and how to do as, as well as an overview of	Students should seek to understand the different incident classifications and in particular how process

	what the investigation process involves. This should be a standard part of any induction.	safety events are managed. They should also look to understand more about the investigation process works and if possible sit in on some investigations during internships.
Safety management system (SMS)	An induction should cover the overarching aspects of the SMS including the policy and how it is structured.	Students should ask about how different elements of the SMS fit together and what their role is in supporting the SMS during internships.
Metrics or indicators	The facility should inform students that that do measure performance via a variety of means including lead and lag indicators. It can also be helpful explain how the indicators are calculated and reported.	Students should ask about which indicators they have can an impact on and how.
Integrity management	Integrity management is a critical part of process safety but is often not mentioned in inductions. Information on the integrity philosophy should be shared with the students when they are on an internship so they understand how the plant is kept functioning safety.	Students should ask about how the integrity management is managed and what sort of preventative maintenance in undertaken, as well as how this is scheduled and monitored.
Operational parameters	This is an area not typically covered in inductions. The operational philosophy should be shared, including how the operational envelop is defined and monitored, and what the escalation levels are.	Students should ask about how the operational parameters are defined and monitored, as well as what occurs when they are exceeded. This is both from a response perspective as well as an investigation perspective.

Table 1: Key considerations

Further work

This paper outlines topic areas for conversation led both by students and industry. This information needs to be further defined into useful examples of the interactions and the information. The IChemE Safety Centre will continue to develop this concept and produce a

detailed resource aimed at students and one aimed at industry to help them focus their interactions to get better process safety outcomes. It is anticipated these resources will be published in 2019.

Conclusion

A fundamental part of an engineering education is a positive interaction with industry to show application of the topics studies. Without this interaction, the learning can sometimes be too theoretical. Industry do need to offer more opportunities for workplace interaction with students, but we also need to ensure that we can get the most value from any interaction that occurs. Simply increasing the number of interactions but having them low value will do very little to enhance the education of our future engineers. We need both industry and students willing to seek out high value interactions to maximise learnings and better develop our future generations of engineers to achieve improved process safety outcomes in the future.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

High Surface Area Oxidation – Development of an Improved Open Cup ARC Vessel and Validation

Brenton L. Drake*, Steve Horsch, Travis Scholtz, Jeff Kelly
The Dow Chemical Company
Freeport TX 77541
*Presenter Email: bdrake1@dow.com

Abstract

Easily oxidized, low volatility organic liquids absorbed/dispersed on inorganic solid materials such as insulation, absorbents, and molecular sieves can result in spontaneous ignition incidents. This is due to increased rates of oxidation of the organic when it is spread out over the very high surface area inherent in these types of solid materials. Similarly, high surface area organic solids that are either self-reactive or oxidizable may self-heat when accumulated in a pile of sufficient size, resulting in thermal runaways, gas generation, and/or fire. Understanding and quantifying this behavior is critical to identifying hazards and developing appropriate mitigative measures. Previously, an Open Cup Accelerating Rate Calorimeter technique was developed at Dow using an open, stainless steel container, purged with air heated to testing temperatures to maintain adiabaticity. This method has been used for many years to understand the reaction kinetics of "auto-oxidation" reactions and high surface area runaway reactions. While the method has been shown to be reliable and able to accurately predict large scale hazards, the exposure of the gaseous decomposition and oxidation products of the reactions is destructive to the ARC calorimeter. The open-cup system vents directly into the ARC, resulting in accelerated corrosion or potentially exposing the internals to fire. A new ARC container design has been developed that has been demonstrated to produce comparable results and removes the concerns associated with damaging the equipment. The new design of the Open Cup ARC test cell, validation, and discussion of the data application will be included in this article.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Thermal Analysis and Characterization of Polystyrene Initiated by Benzoyl Peroxide

Xin-Miao Liang, Hui-Chun Jiang, Jiang-Lai Fang, Min-Hua, Xu-Hai Pan*, Jun-Cheng Jiang
College of Safety Science and Engineering, Nanjing Tech University
Nanjing, Jiangsu, 210009, China
*Presenter E-mail: xuhaipan@njtech.edu.cn

Abstract

Based on the complexity of the polystyrene polymerization mechanism initiated by benzoyl peroxide (BPO), the thermal risk of the reaction process was estimated using thermal analysis and characterization. The polymerization process was thermally analysed using an adiabatic rate calorimeter and differential scanning calorimeter. The results demonstrated that the onset reaction temperature, adiabatic temperature rise, and maximum temperature of the synthesis reaction of BPO-initiated polymerization were lower than those of thermos initiated polymerization. Moreover, nuclear magnetic resonance imaging, gel permeation chromatography, and Fourier transform infrared spectrometry were used to characterize the polymerization products obtained under the two initiation conditions. The polystyrene obtained using the two initiation methods had the same hydrogen structure; however, their molecular weight and distribution uniformity differed considerably, and the BPO-initiated process was discovered to include the effects of the thermos initiated process. Moreover, the free radicals produced by BPO decomposition participated in the chain reaction of polystyrene polymerization, accelerated instantaneous grain growth, and promoted the formation of short-chain polystyrene. In summary, the BPO-initiated polymerization process exhibited the desired thermal safety characteristics and has potential for practical use.

Keywords: Polymerization mechanism, Thermal risk, Polymerization products, BPO-initiated, Thermo initiated, Characterization, Polystyrene.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Potential for Hydrogen DDT with Ambient Vaporizers

J. Kelly Thomas*, Jihui Geng, Oscar Rodriquez
Baker Engineering and Risk Consultants, Inc. (BakerRisk®)
3330 Oakwell Court, Suite 100, San Antonio, TX 78218-3024

Simon Jallais, Elena Vyazmina
Air Liquide R&D
1 Chemin de la Porte des Loges - Les Loges-en-Josas, 78354 JOUY-EN JOSAS

Derek Miller
Air Products
7201 Hamilton Boulevard, Allentown, PA 18195-1501

Bill Lindberg, Richard Pawulski
Air Liquide Large Industries U.S.
9811 Katy Freeway, Suite 100, Houston TX 77024
*Presenter E-mail: KThomas@BakerRisk.com

Abstract

The ignition of a hydrogen-air mixture that has engulfed a typical set of ambient vaporizers (i.e., an array of finned tubes) may result in a deflagration-to-detonation transition (DDT). Simplified curve-based vapor cloud explosion (VCE) blast load prediction methods, such as the Baker-Strehlow-Tang (BST) method, would predict a DDT given that typical ambient vaporizers would be rated as medium or high congestion and hydrogen is a high reactivity fuel (i.e., high laminar burning velocity). Computational fluid dynamic (CFD) analysis of a single vaporizer of typical construction was carried out using the FLACS code to evaluate the potential for a DDT with a vaporizer engulfed by a hydrogen-air mixture at the worst-case concentration. This analysis showed that while significant flame acceleration occurs within the vaporizer, as expected, a DDT is not predicted. However, the analysis did indicate that a DDT may occur for two or more closely spaced vaporizers. This is relevant since multiple vaporizers are frequently present at industrial installations and are typically placed closely together to limit the required area. Spacing adjacent vaporizers further apart could preclude a DDT. However, specification of the spacing to preclude a DDT would require refined CFD analysis and/or testing, neither of which has been performed at this time.

This paper also discusses the application of simplified VCE blast load methods to ambient vaporizers engulfed in a flammable hydrogen-air cloud in order to illustrate the impact of a DDT.

Introduction

Vaporizers are employed on industrial sites to convert cryogenic liquids (e.g., hydrogen, nitrogen, etc.) into vapor for use in a process. The vaporizers of interest are finned tubes. Typically, a vaporizer consists of a number of vertically oriented finned tubes placed in close proximity in order to limit the vaporizer footprint. The vaporizer dimensions and the number and size of the finned tubes employed in a vaporizer depends on its service (i.e., gas vaporized, required flow rate, etc.) Multiple vaporizers are frequently utilized, with individual vaporizers typically separated by no more than several feet in order to limit the footprint of the vaporizer set.

An accidental hydrogen release could potentially interact with or engulf a vaporizer or set of vaporizers; a release could occur either from the liquid hydrogen supply or from downstream pressurized gas. The vaporizer structure (i.e., array of finned tubes) represents a congested volume, which could trigger a vapor cloud explosion (VCE) if filled with a flammable gas and subsequently ignited. If a hydrogen release near a congested volume is credible for a given operation, then a hydrogen VCE should be considered as a credible event when performing explosion consequence and risk assessments [1]. An approach to predict the resulting VCE blast loads is therefore needed in order to carry out such assessments at industrial sites employing vaporizers.

A typical vaporizer represents significant congestion level in terms of area blockage ratio (ABR), volume blockage ratio (VBR) or surface area to volume ratio (SA/V) due to the arrangement of finned tubes. The congestion level for a typical vaporizer would be classified as either medium or high under the Baker-Strehlow-Tang (BST) VCE blast load prediction method [2]. The BST method predicts a deflagration-to-detonation transition (DDT) at medium or high congestion levels for a high reactivity fuel (e.g., hydrogen) [3], and hence a vaporizer hydrogen-air VCE would be treated as a detonation. The prediction of a DDT for a medium congestion level with a high reactivity fuel under the BST method is based on testing performed by BakerRisk with ethylene and lean hydrogen mixtures [4, 5, 6]. The test rig used in these tests had dimensions of 48 feet (14.6 m) by 12 feet (3.7 m) by 6 feet (1.8 m) tall rig. The congestion employed in these tests was formed by a uniform array of 2-inch (5 cm) vertical pipes (pitch-to-diameter ratio of 4.1, area and volume blockage ratios of 23% and 4.2%, respectively); this would be classified as medium with the context of the BST method. Hydrogen-air mixtures were ignited at the rig center near grade level. Deflagrations resulted for hydrogen concentrations of 18% or less, a very fast deflagration was achieved at a concentration of 20%, and a DDT occurred with a concentration of 22%. Others have observed similar behaviour in hydrogen VCE tests. For example, Shirvill and Roberts [7] tested hydrogen in a congested 3 m by 3 m by 2 m high rig with congestion formed by 1-inch (2.54 cm) diameter pipes. A vertical array was placed in the bottom half of the rig, and a horizontal array in the top half. The mixture was ignited by a spark near the rig center. A near-stoichiometric H_2-air mixture underwent DDT near the edge of the rig.

If the flammable hydrogen-air mixture was restricted to the congested volume associated with a vaporizer or vaporizer set, the assumption of whether the VCE progressed as a high-speed

deflagration or a detonation would have little impact on the VCE blast loads at moderate distances from the vaporizer (i.e., at most building locations). However, a detonation wave, once triggered by a DDT, can propagate through the remaining (i.e., unburned) flammable cloud [8, 9]. It is recognized that the detonation wave may fail before the edge of a flammable hydrogen-air cloud (i.e., at a higher concentration than the lower flammability limit), if the flammable cloud is too thin, or the concentration gradients are too large. A DDT that triggers a sustained detonation can therefore dramatically increase the VCE explosion energy for a hydrogen-air cloud which is much larger than a vaporizer, which would be the case for most postulated design-basis hydrogen release scenarios.

The lateral dimensions of a typical vaporizer (i.e., several meters) are less than rig length employed in the BakerRisk hydrogen DDT tests (i.e., 15 m). Hence, although the congestion level associated with a typical vaporizer is more severe than that of this test rig, it is possible that a DDT may not occur due to the decreased congested volume dimensions. Of course, the use of multiple closely spaced vaporizers increases the effective dimensions of the congested volume. A DDT evaluation for a typical vaporizer and vaporizer set was therefore carried out using the FLACS computational fluid dynamics (CFD) code. In order to illustrate the impact of whether or not a DDT occurs, a VCE blast load assessment was performed using the BST method for a hydrogen-air cloud resulting from a moderate liquid hydrogen release.

Effect on DDT on Predicted Blast Load

A ½-inch release of liquid hydrogen at a pressure and temperature of 150 psig and -410°F, respectively, was considered for the purposes of illustration. The postulated release was assessed using SafeSite$_{3G}$©, BakerRisk's consequence assessment and facility siting code. A Pasquill stability class B and a wind speed of 2 m/s was assumed for the dispersion. Figure 1 shows the upper flammability limit (UFL), lower flammability limit (LFL) and LFL/2 contours on a vertical cut plane through the center of the resulting hydrogen-air cloud. The corresponding flammable cloud volume is 130,000 ft^3. It should be clearly noted that larger releases and more severe weather conditions giving larger flammable cloud volumes are likely credible and would typically be considered in a risk analysis; that is, this flammable cloud volume should be viewed as moderate within the context of this illustration.

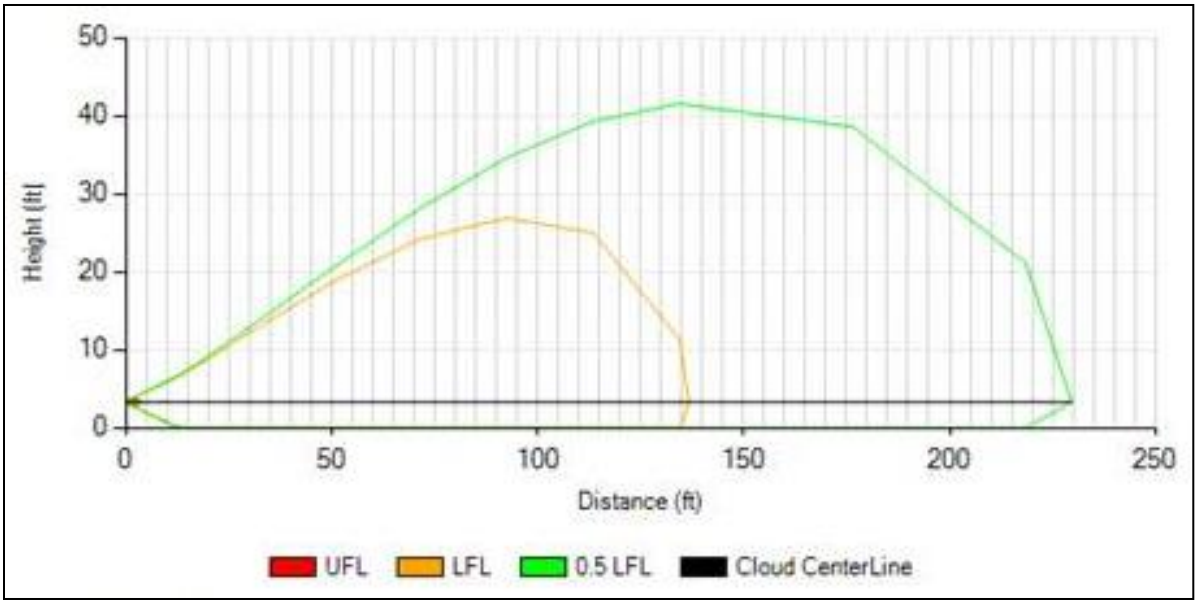


Figure 1. Flammable Hydrogen-Air Cloud for Example Release Scenario

For the purposes of the illustrative blast load evaluation, consider the flammable cloud and vaporizer arrangement shown in Figure 2. The flammable cloud is much larger than the vaporizer and engulfs it, with the vaporizer being the only congested volume within the flammable cloud. The ignition location is near the center of the flammable cloud and well outside the vaporizer. A low flame velocity flash fire (i.e., combustion without the generation of significant overpressure) would propagate out from the ignition location until the flame reached the vaporizer, at which point the flame would accelerate within the vaporizer due to the congestion presented by the finned tube array. If a DDT did not occur, then the flame would decelerate rapidly as it left the vaporizer (i.e., due to the absence of congestion outside the vaporizer), and the remainder of the flammable cloud would be consumed as a flash fire. However, if a DDT occurred within the vaporizer, then the resulting detonation wave would propagate outward from the vaporizer and consume the remaining flammable cloud (i.e., through the portion of the cloud capable of supporting a detonation, down to the leanest hydrogen concentration that supports detonation propagation).

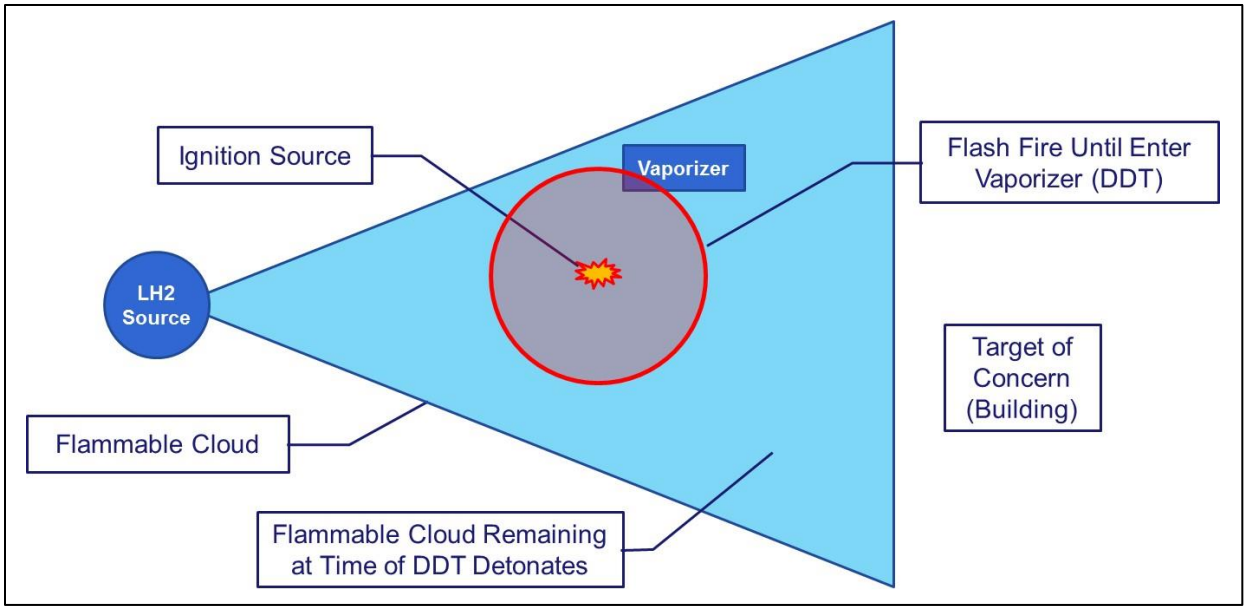


Figure 2. Illustrative Flammable Hydrogen-Air Cloud and Vaporizer Arrangement

A single vaporizer with lateral dimensions of 5 feet by 6 feet is considered for the purposes of the VCE blast load evaluation, with the flammable cloud within the vaporizer extending to a height of 9 feet (i.e., only fills a portion of the vaporizer). The volume of the congested volume filled with a hydrogen air mixture would therefore be 270 ft^3 (7.6 m^3). A flammable cloud with a length of 100 feet, a width of 50 feet, and a height of 10 feet is assumed, which gives a flammable volume of 50,000 ft^3 (1,400 m^3). This flammable cloud volume is roughly 40% that from the release scenario discussed above (i.e., this should be viewed as a relatively small cloud within the context of a typical facility explosion consequence assessment or risk analysis).

VCE blast loads (pressure and duration) were predicted using the BST method assuming a very high-speed deflagration (flame speed of Mach 1) of the flammable volume within the vaporizer (i.e., 270 ft^3) and the detonation of one-half of the flammable cloud volume (i.e., 50,000 ft^3); only one-half of the flammable cloud volume was assumed to detonate to account for a portion of the cloud being consumed as a flash fire and a portion of the cloud not participating in the detonation (i.e., due to failure of the detonation wave). The predicted VCE blast loads are shown in Figure 3. At a standoff distance greater than 100 feet (30 m), the detonation gives about 7 times the pressure and three times the duration of the deflagration, with larger blast pressure differences closer in to the vaporizer.

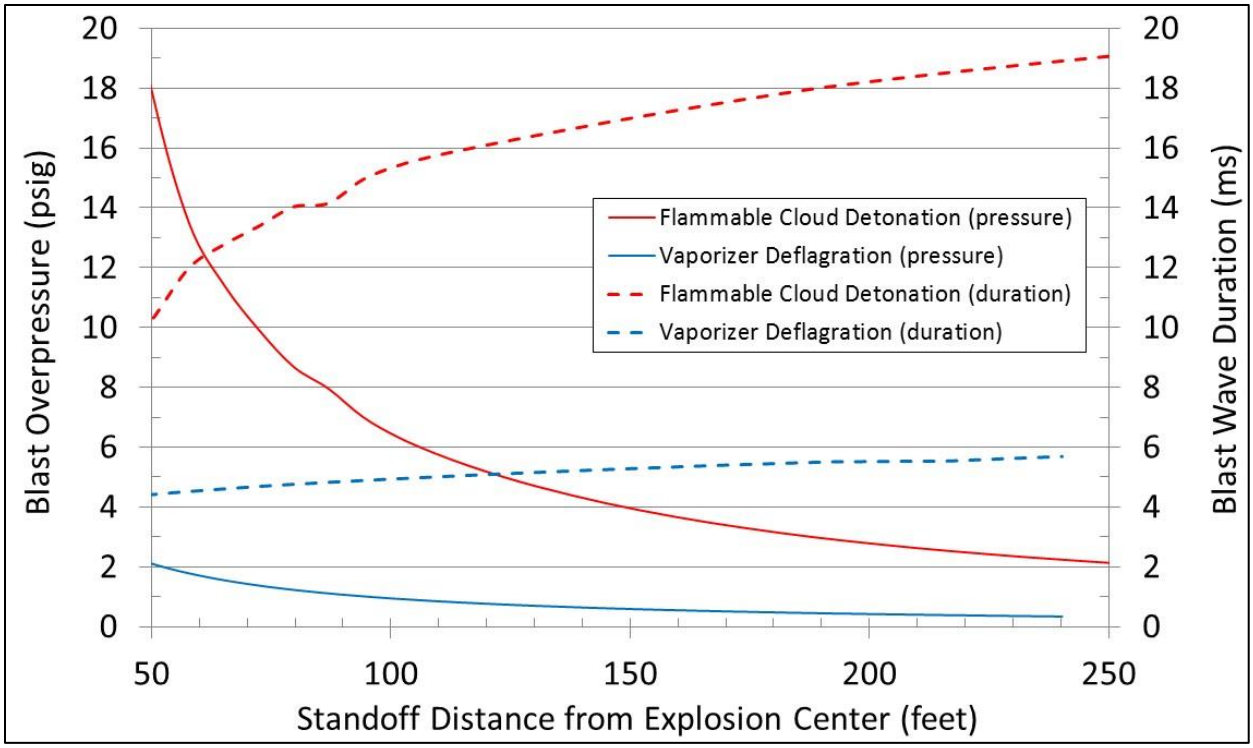


Figure 3. Blast Loads for Deflagration and Detonation of Illustrative Flammable Cloud

The resulting damage to a building can be considered to put the difference in the predicted blast loads for a deflagration and a detonation in context. The building considered for this purpose is a typical reinforced load-bearing CMU building, with the damage level predicted using BakerRisk's BEAST analysis tool [10]. Major damage and/or collapse is predicted for the detonation at a standoff distance of 150 feet, whereas only minor damage (cosmetic) is predicted for the deflagration.

This comparison illustrates the significant impact of determining whether a deflagration or a detonation occurs during a VCE involving a flammable hydrogen-air cloud engulfing an ambient vaporizer on the predicted blast loads and resulting building damage. The flammable cloud considered in this illustration is comparatively small. Larger differences between the predicted deflagration and detonation blast loads and building damage would result for a larger flammable cloud.

Vaporizer Selected for Evaluation

A "typical" vaporizer was selected for this evaluation based on field observations from range of refining and chemical processing sites. The vaporizer finned tubes have an outer diameter (OD) of 1.22 inches (3.1 cm), a fin width of 7 inches (18 cm), and a tube spacing of 12 inches (30 cm); the resulting element spacing (tip-to-tip distance) is 5.0 inches (12.7 cm). An 8×8 array was considered, giving lateral vaporizer dimensions of approximately 2.5 m. A vaporizer height of 7 m was assumed. A section of the vaporizer layout drawing is provided as Figure 4. Schematics of the vaporizer elements and element array, including key dimensions, are shown in Figure 5 and Figure 6, respectively. Example photos of a vaporizer with these design parameters are shown in Figure 7, with a close-up photo of the elements provided as Figure 8. A vaporizer based on a 6×6 array with same fin size and outer dimensions (i.e., larger tube spacing) was also evaluated in this work.

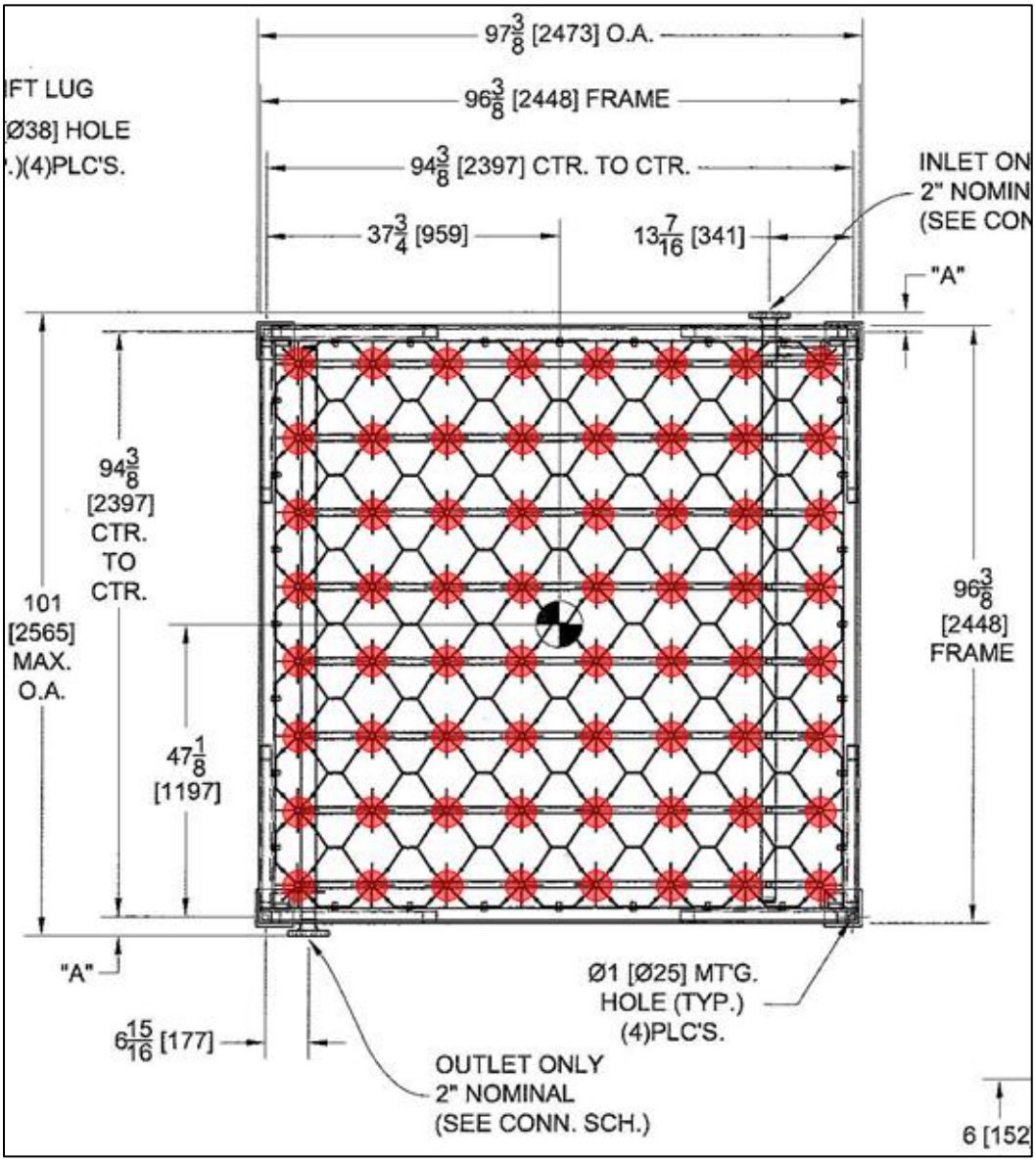


Figure 4. Vaporizer Cross Section

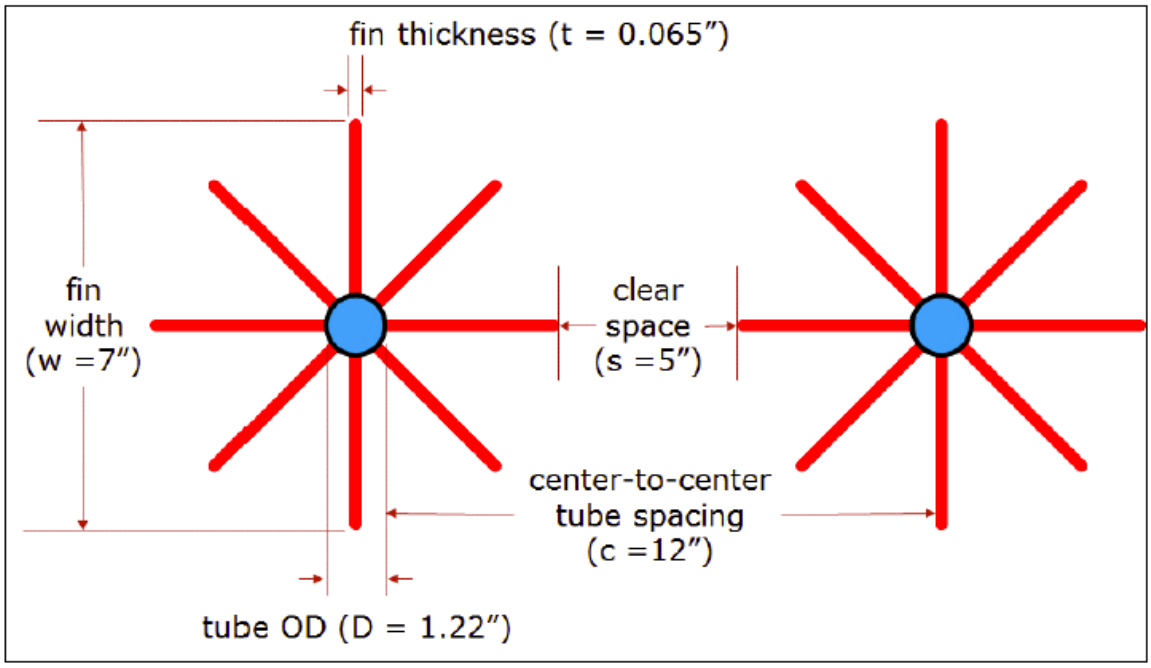


Figure 5. Vaporizer Element Schematic

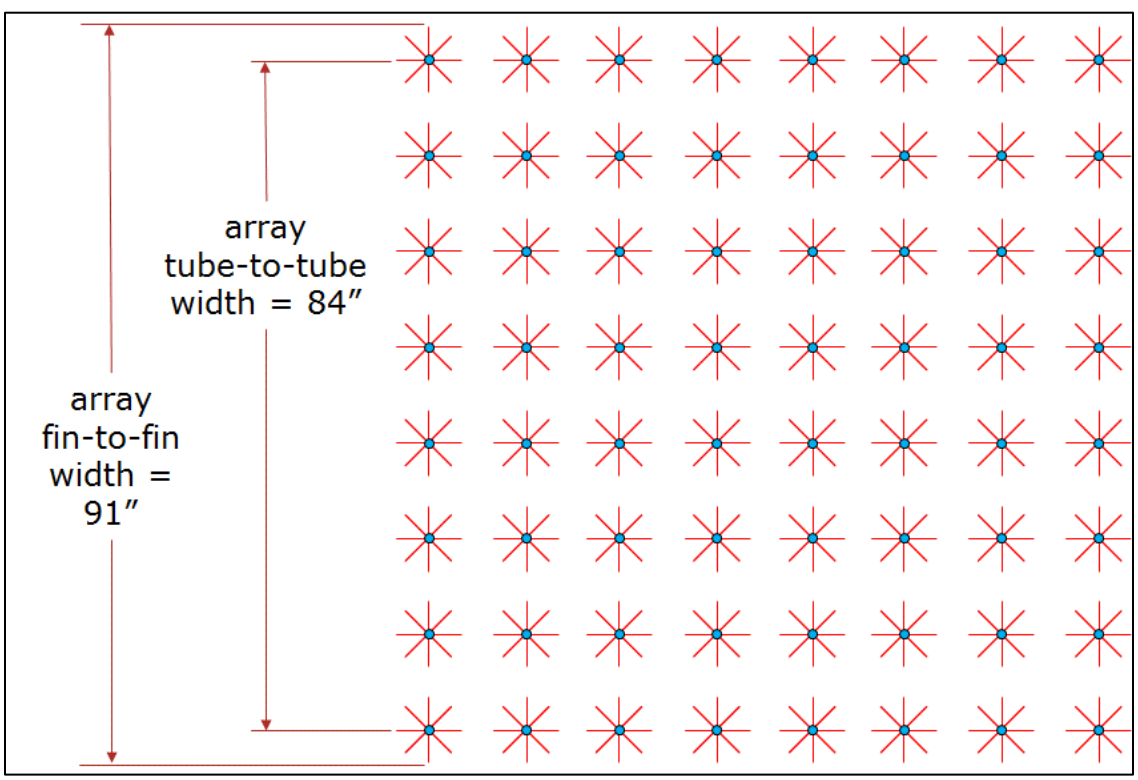


Figure 6. Vaporizer Element Array Schematic

Figure 7. Vaporizer Photographs

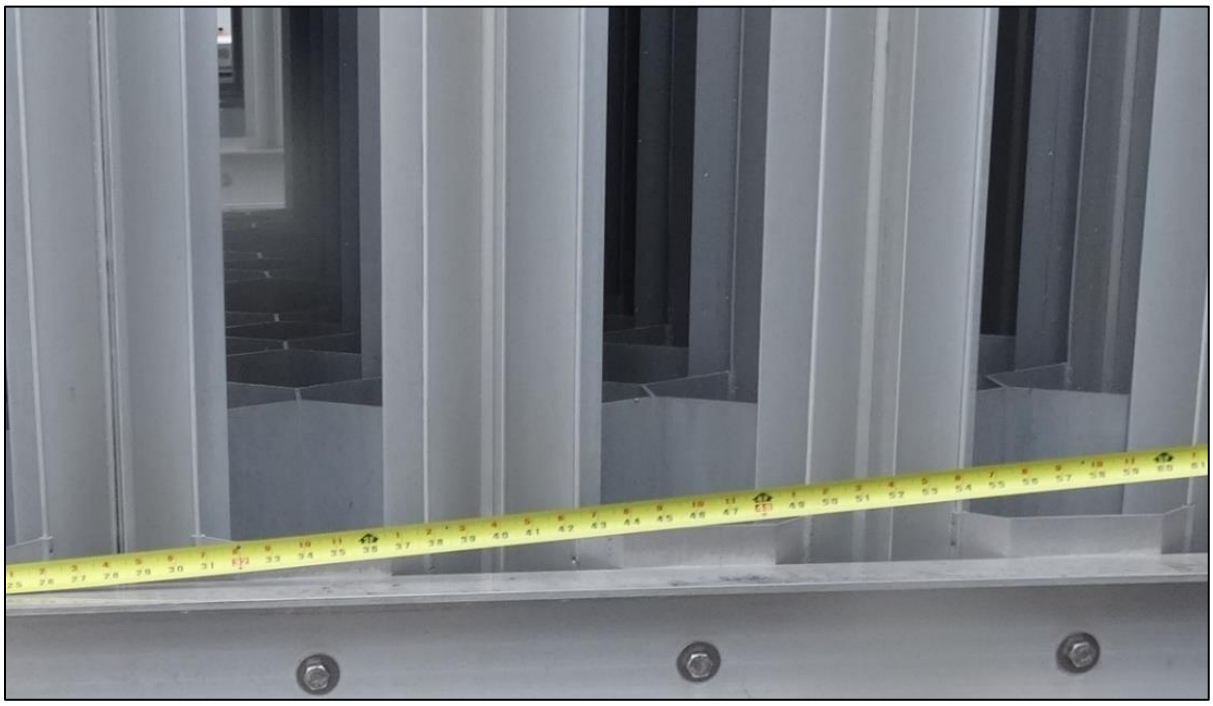


Figure 8. Photograph of Vaporizer Elements

Vaporizers are often employed in sets, with multiple vaporizers located adjacent to one another. Both a single and two-vaporizer set were evaluated in this work. A separation distance of 3 feet (1 m) was assumed, which is typical of that seen in actual installations. A separation distance of zero (i.e., a "double width" vaporizer) was also evaluated. An attempt was made to evaluate greater separation distances, but, as discussed in the results section, issues associated with the current version of FLACS precluded obtaining reliable results for vaporizer sets separated by larger distances.

FLACS Simulations

The FLACS (Flame Acceleration Simulator) CFD code was used to perform an assessment of whether a DDT would occur within a single vaporizer or a set of two adjacent vaporizers. FLACS is commonly used in industry for CFD-based dispersion and VCE simulations. FLACS solves conservation equations for mass, momentum, enthalpy, turbulence and species/combustion on a 3D Cartesian grid. Obstacles such as structural supports and pipes are represented as area porosities on control volume (CV) faces and volume porosities within a CV, with the porosity defined as the fraction of the area/volume that is available for fluid flow. The resulting porosity model is used to calculate flow resistance and turbulence source terms from objects smaller than the computational grid (i.e., subgrid), as well as the flame speed enhancement arising from flame folding.

As assessment of whether a DDT is predicted can be made using FLACS based on a combination of the dimensionless pressure gradient and normalized flame speed. The use of the dimensionless pressure gradient for this purpose was originally suggested by GexCon [11]. BakerRisk has developed both dimensionless pressure gradient and normalized flame speed criteria for FLACS assessments based on comparisons with VCE tests yielding both deflagrations and detonations.

The vaporizer design evaluated was described in the previous section. Figure 9 shows the FLACS geometry created for the simulation of a two vaporizer set. Figure 10 shows the vaporizer set engulfed in the flammable cloud along with the ignition point location. The flammable cloud was extended 2.5 m beyond the vaporizers in the short-axis direction and above the vaporizers, 5 m beyond the vaporizer nearest to the ignition source, and 0.5 m from the rear of the vaporizer opposite the ignition source. The flammable cloud was taken to be a hydrogen-air mixture at a uniform stoichiometric mixture; it should be noted that the worst-case hydrogen concentration (i.e., that most prone to a DDT) is slightly hyperstoichiometric. The ignition source was placed 1 m (3.3 ft) outside the vaporizers near grade level, such that a developed flame would propagate into the nearest vaporizer. Figure 11 shows the monitor points placed within the FLACS model to record the predicted blast pressure, pressure gradient and gas temperature history. Flame speeds were determined based on the gas temperature history (i.e., flame arrival times at monitor points).

The computational mesh was created following the guidelines in the FLACS user's manual [12], which states that, for unconfined gas clouds, that there should be a minimum of 13 grid cells across the cloud. For the smallest dimension of the vaporizer (2.5 m), this requires a computational cell size of 19 cm (i.e., 250 cm / 13). A sensitivity study was performed using a computational cell size of 15 cm, and similar results were obtained.

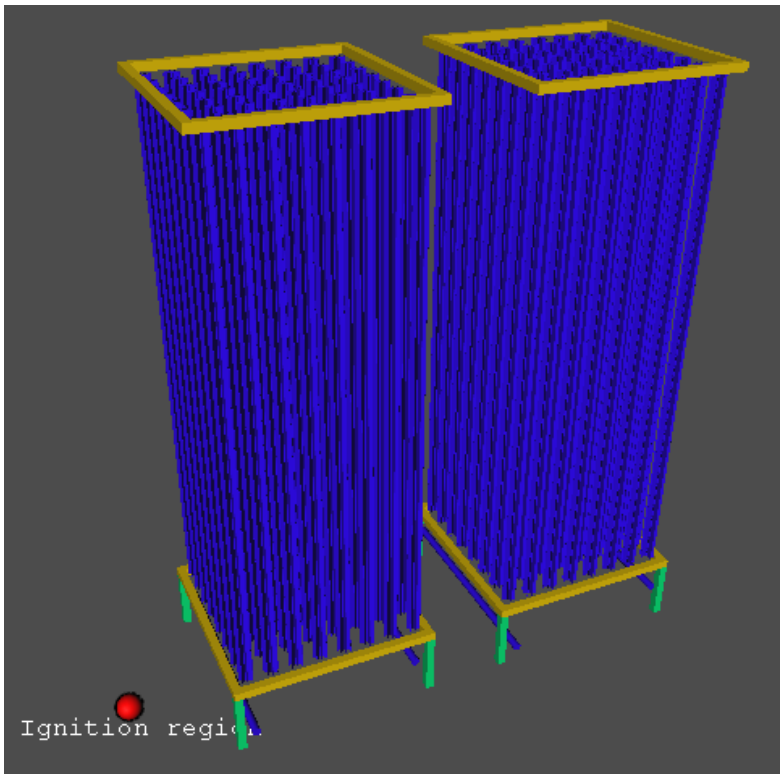


Figure 9. FLACS Solid Model of Vaporizer Pair (8×8 Array)

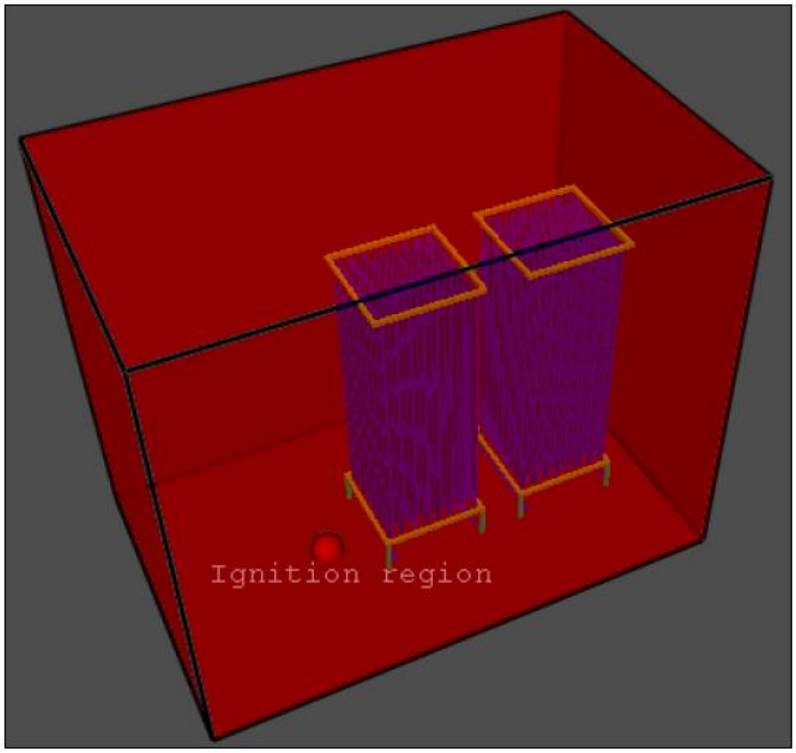


Figure 10. FLACS Model with Flammable Cloud and Ignition Point
(8×8 Array, 3-foot Separation Distance)

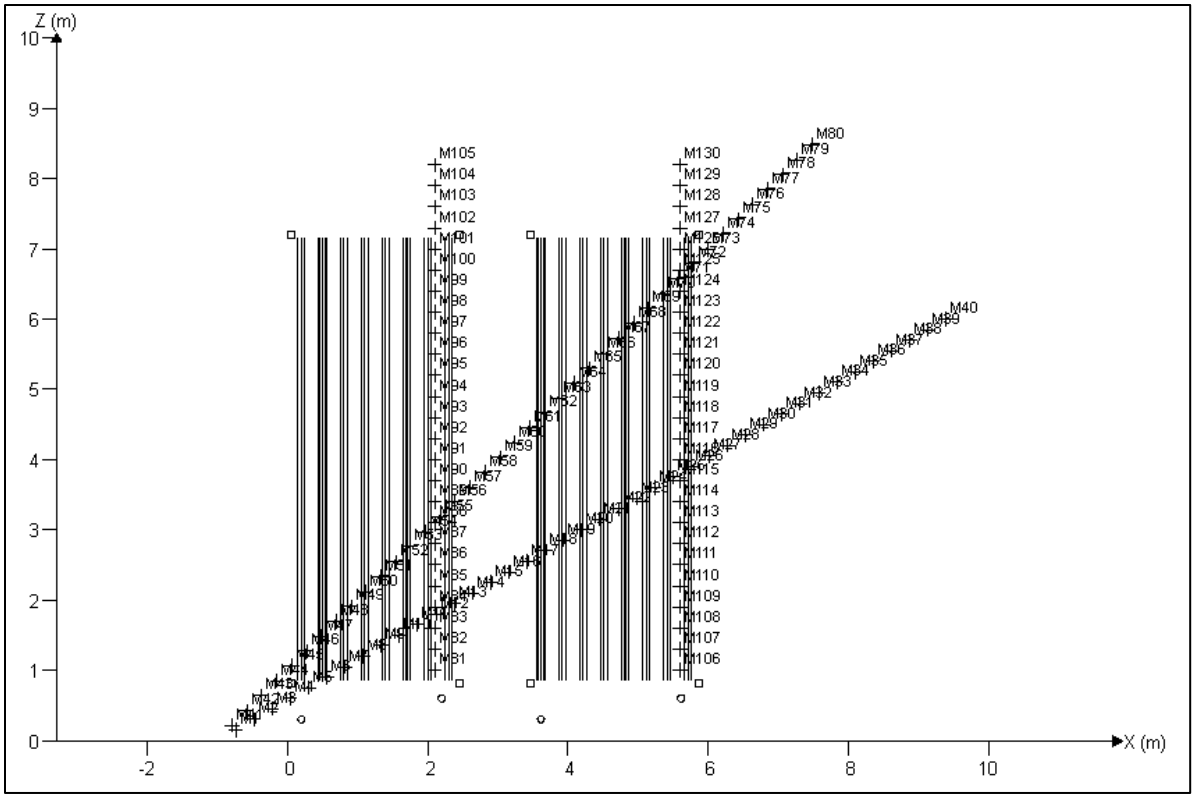


Figure 11. Target Distribution within FLACS Model

Results and Discussion

The predicted maximum dimensionless pressure gradient contour for two vaporizers with a 3-foot (1 m) separation distance between the two vaporizers is shown in Figure 12. The maximum dimensionless pressure gradient exceeds 3 over a large portion of the upper section of the second vaporizer. Dimensionless pressure gradient and normalized flame speed values along a 45-degree target line (see Figure 11) are shown in Figure 13. A DDT would be predicted based on the combination of the dimensionless pressure gradient and normalized flame speed along this target line just inside the second vaporizer. The dimensionless pressure gradient and normalized flame speed values along a 45-degree target for a set of vaporizers with no separation distance (i.e., a "double wide" vaporizer) are shown in Figure 14; a DDT would once again be predicted along this target line just inside the second vaporizer.

Analyses were also performed at lean (23%H_2, 0.71 ER) and rich (35%H_2, 1.28 ER) fuel concentrations. Both 8×8 and 6×6 vaporizer arrays were evaluated, assuming no separation distance between two adjacent vaporizers. The results are shown in Table 1. For the 8×8 array set, DDTs were predicted for all three fuel concentrations examined, with the flame travel distance required for a DDT decreasing slightly with the rich fuel concentration. For the 6×6 array, a DDT was not predicted for the lean fuel concentration, and the flame travel distance required for a DDT decreasing slightly with the rich fuel concentration.

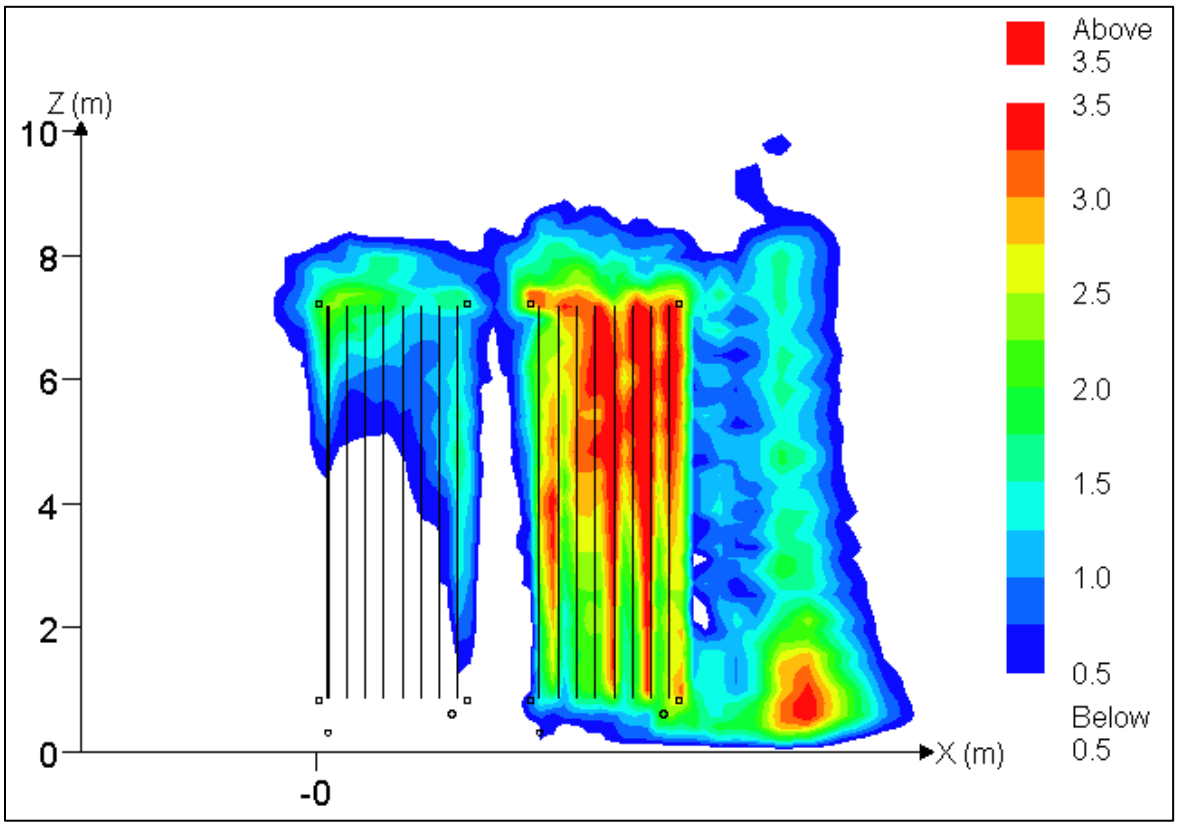


Figure 12. Maximum Dimensionless Pressure Gradient Contour (1 m separation distance)

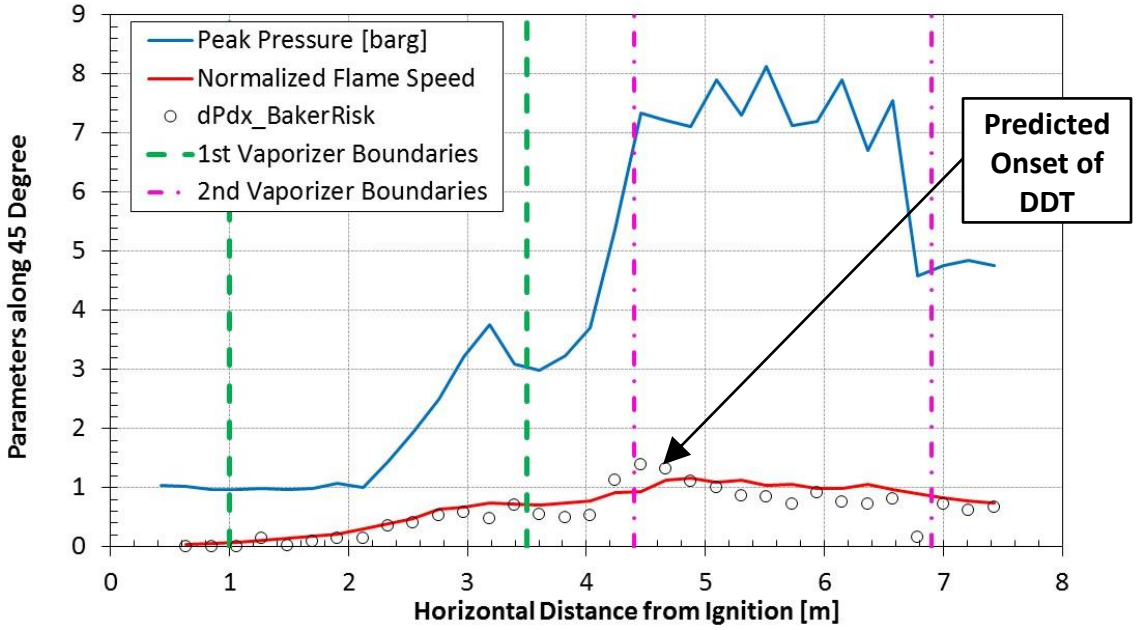


Figure 13. Maximum Dimensionless Pressure Gradient and Normalized Flame Speed (45-degree target line, 1 m separation distance between vaporizers)

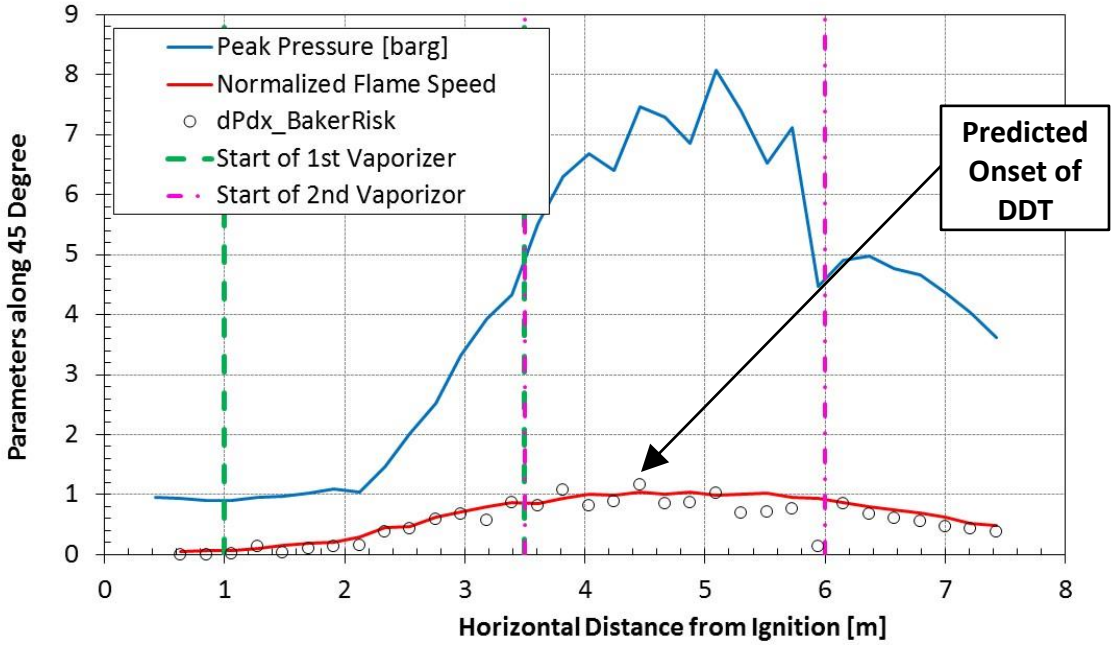


Figure 14. Maximum Dimensionless Pressure Gradient and Normalized Flame Speed (45-degree target line, no separation between vaporizers)

Table 1. Horizontal Distance for DDT with Adjoined Vaporizer Arrays

Vaporizer Array (two adjacent vaporizers)	Separation Distance (feet)	DDT Location (m) for Specified Hydrogen Concentration (equivalence ratio / % hydrogen)		
		0.7 (23%)	1 (30%)	1.3 (35%)
8×8	0	3.5 m	3.5 m	3.2 m
6×6	0	-	3.5 m	3.2 m

Issues with the ability of FLACS to accurately predict flame acceleration in a second congested volume (i.e., where two adjacent congested volumes are separated by some distance) has been reported in the literature [13], where the underlying issue was identified to be the turbulent length scale assigned by FLACS; it was determined that this issue would impact FLACS simulations where the second congested volume was separated by one to times the size of the congested volumes (i.e., by approximately 8 feet or more for the vaporizers considered in this work). A potential approach (i.e., "data dump technique") was identified [13], but this approach was not deemed to be applicable to the current analysis. Furthermore, the data dump technique was "only a suggestion for others working in this area" rather than an approach which had been thoroughly tested or which was ready for incorporation into FLACS. The FLACS developer (i.e., GexCon) is aware of this issue and is actively working to resolve it. A joint industry project (MEASURE) may develop information which could help address this issue.

Conclusions and Recommendations for Future Work

The results of this analysis indicate that a DDT would not occur for a single vaporizer of the type evaluated, even for worst-case hydrogen-air mixtures. It should be noted that this analysis implicitly assumes that a single vaporizer would be located well away from other congested volumes. A single vaporizer with significantly larger dimensions and/or tighter element spacing could potentially result in the prediction of a DDT.

A DDT would be expected based on the results of this analysis for a pair of closely-spaced (i.e., 3 foot separation distance) 8×8 vaporizers for all hydrogen concentrations evaluated (i.e., 23%H_2 to 35%H_2). The DDT was predicted to occur approximately ½ meter inside the second vaporizer (i.e., shortly after the flame enters the second vaporizer). As discussed earlier, a detonation, once triggered by a DDT within a vaporizer, could propagate through a significant portion of the remaining flammable cloud, which could extend well beyond the vaporizer set. A DDT would not be expected for smaller vaporizers at lean hydrogen concentrations (e.g., a 6×6 array at 23%H_2). It should be recognized that a flammable hydrogen-air cloud engulfing a set of vaporizers from an actual release may not trigger a DDT due to the hydrogen concentration at the vaporizer set (i.e., may be too lean or too rich).

It is recommended that this CFD analysis be revisited when a version of FLACS is released that addresses the issues associated with predicting the flame acceleration in a second congested volume. As discussed earlier, this is a known issue that is currently being addressed by the code developer. The extended CFD analysis should include an evaluation of the impact of vaporizer design parameters (array size, element spacing, etc.), as well as vaporizer separation distance. Air Liquide has performed additional analyses which indicate the effect of the hydrogen-air mixture temperature is relevant, with lower temperatures expected to give slightly less flame acceleration and decrease the potential for a DDT.

It is also recommended that explosion tests be performed with hydrogen-air mixtures engulfing both single vaporizers and vaporizer sets in order to provide definitive benchmark data. Benchmark data for this type of congested volume is important to validate the CFD predictions, particularly for establishing the separation distance required to preclude a DDT. Such tests could include the effect of an actual release versus a premixed hydrogen-air cloud.

References

1 Thomas, J.K., C.D. Eastwood and M.L. Goodrich (2015) "Are Unconfined Hydrogen Vapor Cloud Explosions Credible?" Process Safety Progress, 34(1): 36-43

2 Baker, Q.A. et al. (2010) Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE and Flash Fire Hazards, Second Edition, Center for Chemical Process Safety (CCPS) & John Wiley and Sons, New York, NY.

3 Pierorazio, A.J., J.K. Thomas, Q.A. Baker and D.E. Ketchum (2005) "An Update to the Baker-Strehlow-Tang Vapor Cloud Explosion Prediction Methodology Flame Speed Table," Process Safety Progress, 24(1): 59-65.

4 Thomas, J.K., A.J. Pierorazio, M. Goodrich, M. Kolbe, Q.A. Baker and D.E. Ketchum (2003) "Deflagration to Detonation Transition in Unconfined Vapor Cloud Explosions," Center for Chemical Process Safety (CCPS) 18th Annual International Conference & Workshop, Scottsdale, AZ, 23-25 September 2003.

5 Thomas, J.K., R.J. Duran and M.L. Goodrich (2010) "Deflagration to Detonation Transition in a Lean Hydrogen-Air Unconfined Vapor Cloud Explosion," Mary Kay O'Connor Process Safety International Symposium," College Station, TX, October 27, 2010.

6 Thomas, J.K. and D.R. Malik (2017) "Ammonia and Hydrogen Vapor Cloud Explosion Testing (A Tale of Two Gases)," 62nd Annual Safety in Ammonia Plants and Related Facilities Symposium, New York, September 10-14, 2017.

7 Royle, M, Shirvill, LC and Roberts, TA, "Vapour Cloud Explosion from the Ignition of Methane/Hydrogen/Air Mixtures in Congested Region. http://ukelg.ps.ic.ac.uk/40GC1.pdf.

8 Thomas, J.K., M.L. Goodrich and R.J. Duran (2013) "Propagation of a Vapor Cloud Detonation from a Congested Area into an Uncongested Area: Demonstration Test and Impact on Blast Load Prediction," Process Safety Progress, 32(2): 199-206.

9 Duran, R.J., M.L. Goodrich and J.K. Thomas (2012) "Propagation of a Vapor Cloud Detonation from a Congested into an Uncongested Area," Chem. Eng. Trans., Vol. 26.

10 BEAST (building assessment tool developed by BakerRisk for the Explosion Research Cooperative Joint Industry Program).

11 Middha, P. and O.R. Hansen (2008) "Predicting Deflagration to Detonation Transition in Hydrogen Explosions," Process Safety Progress, 27)3): 192-204.

12 Gexcon AS, "FLACS Version 10.5 User's Manual," 5/27/16.

13 Ma, G., J. Li and M. Abdel-Jawad (2014) "Accuracy Improvement in Evaluation of Gas Explosion Overpressures in Congestions with Safety Gaps," J. Loss Prev. in the Process Ind., 32: 358-66.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Heat transfer modeling of high expansion foam application for vapor risk mitigation of Liquefied Natural Gas (LNG) spills

Pratik Krishnan, Bin Zhang, Salma Akhter, M. Sam Mannan
Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, United States
Emails: pratik@tamu.edu, drsalma@tamu.edu

Abstract

The consumption of natural gas is expected to increase significantly over the next few decades due to much less carbon dioxide emission per unit of energy, when compared to other sources like oil or coal. This has also been facilitated by availability of a large number of reserves and improvements in fracking technologies. Liquefaction of natural gas enables ease of storage and transportation because of a high ratio of liquid to vapor density, especially over long distances when constructing pipelines is economically infeasible. While presenting many advantages, there are several safety concerns involved in the handling of LNG. A spill of cryogenic LNG can absorb heat from the surroundings and form a vapor cloud which has the potential to ignite and presents an asphyxiation hazard. In addition, this vapor cloud can migrate downwind near ground level because of a density greater than air. The National Fire Protection Association suggests application of high expansion foam to mitigate LNG vapor risk. Foam blocks the effects of convection and radiation on an LNG pool and warms rising LNG vapors. Understanding the heat transfer mechanisms between the applied foam and LNG is important to quantify its mitigation effect and determine the amount of foam to be applied for effective vapor risk mitigation. This work aims to address some of the gaps observed in previous efforts towards heat transfer modeling of foam applied on LNG spills.

Keywords: Liquefied Natural Gas (LNG); vapor cloud; high expansion foam; mitigation; heat transfer

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Experimental and Computational Study of the Dispersion and Combustion of Wheat Starch and Carbon-Black Particles During the Standard 20L Sphere Test

José Serrano*, Paula Pico, Mariangel Ami, Andrés Pinilla, David Torrado, Carlos Murillo, Felipe Muñoz, Olivier Dufaud, Nathalie Bardin-Monnier
Department of Chemical Engineering, Universidad de los Andes
Carrera 1 # 18a-12 Bogota, Colombi
Laboratorie Réactions et Génie des Procédés, Université de Lorrain
UMR 7274, Nancy, France
(571) 339-4949 Ext. 1841.
*Presenter: Email: jdj.serrano10@uniandes.edu.co

Keywords*:* CFD, 20L Sphere, Flammable Dust, Starch, Pyrolysis, Combustion.

Abstract

The 20L sphere is one of the standard devices accepted as an international normativity used for dust explosivity characterization. One concern about the effectiveness and reliability of this test is related to the particle size variation due to particles agglomeration and de-agglomeration. These phenomena are determined by the turbulent regime of the dust cloud during the dispersion. This variable must be considered since it determines the uncertainty level of the ignitability and severity parameters of dust combustion. In this context, this study describes the influence of the cloud turbulence on the dust segregation and fragmentation through an experimental and computational study. The behavior of the gas-solid mixture evidenced with the standard rebound nozzle was compared with that observed with six new nozzle geometries. Thereafter, the variations of the Particle Size Distribution (PSD) that occur during the dispersion within the 20L sphere were analyzed for two different powders: carbon-black and micrometric wheat starch. This description is performed with the implementation of two complementary approaches. On the one hand, an experimental approach characterizes the turbulence levels with Particle Image Velocimetry (PIV) tests that are complemented by the description of the PSD variations with granulometric analyses. On the other hand, a computational approach described the dispersion process with CFD-DEM simulations developed in STAR-CCM+ v11.04.010. The simulation results established that the homogeneity assumption is not satisfied with the nozzles compared in this study. Nonetheless, the particles segregation levels can be reduced using nozzles that generate a better dust distribution in the gas-solid injections. Subsequently, an additional first-approach CFD model was established to study the behavior of the combustion step when a starch/air mixture. This model considers the gas-

phase reactions of the combustible gases that are produced from the devolatilization of Wheat starch (CO, CH4, C2H4, C2H6, C2H2 and H2) and allowed to establish the approximate fraction of the particle mass that devolatilizes, as well as to confirm that the modelling of the pyrolysis stage is essential for the correct prediction of the maximum rate of pressure rise.

Nomenclature

CFD – Computational Fluid Dynamics
RANS – Reynolds-Averaged Navier-Stokes
LES – Large Eddy Simulation
IDDES – Improved Delayed Detached Eddy Simulation
DEM – Discrete Element Method
TKE – Turbulent Kinetic Energy
t_v - Ignition Delay Time
N_i – Nozzle i
P_{max} – Maximum average pressure
$\left(\frac{dP}{dt}\right)_{max}$ – Maximum rate of pressure rise
K_{st} – Deflagration index
V – Volume of the testing vessel
m_p – Mass particle
v_p – Particle velocity vector
F_s – Particle surface forces
F_b – Particle body forces
I_p – Particle moment of inertia
ω_p – Particle angular velocity vector
M_b – Particle drag torque
M_c – Particle total moment from contact forces
CFL – Courant–Friedrichs–Lewy number
Δt – Simulation time-step
u – Maximum flow velocity
Δx – Minimum cell size
V_{rms} – Root-mean-square velocity
V_{rms}^0 – Initial Root-mean-square velocity
t – Testing time
t_0 – Initial testing time
n – Fitting parameter
v_i' – Velocity fluctuation of particle i at a given direction
v_i – Velocity of particle i at a given direction
$\bar{v}$ – Average velocity
N – Number of particles present in the sample
ω – Vorticity vector
v – Velocity vector
ρ – Fluid density
ν – Fluid kinematic viscosity
P – Local pressure

1. INTRODUCCTION

1.1. General context and background

In the past few years, the use of dusts, particularly flammable dusts, has become more prominent in certain chemical industries, such as food production, pharmaceuticals, chemical manufacturing, wood processing, and even Oil & Gas industries [1]. Dusts are present in a great variety of processes stablished by these industries such as the transport of materials on rotatory-screw conveyors, milling, grinding, shredding, pulverization, storage, polishing, filtering, among others [2]-[3]. However, dust explosions represent a hazard to these industries in terms of considerable financial losses, damage to physical facilities and often serious injuries to personnel or even fatalities [4], [5].

The first known reported and comprehensive study on the matter was the analysis performed by Count Morozzo of an explosion of flour inside a warehouse in Turin, in the year 1795 [6]–[8]. Fast forwarding to more recent examples, a study of the US Chemical Safety and Hazard Investigation Board (CSB) concluded that, between 1980 and 2005, a total of 281 major dust explosion accidents occurred, resulting in the death of 119 workers, the injury of 718, and the destruction of entire industrial facilities [1], [9], [10]. Similarly, between 1979-1989, The United Kingdom Health and Safety Executive reported 303 incidents; between 1965-1985, The Federal Republic of Germany reported 426 incidents [7] and currently The Chemical Safety Board of the United States reported 50 incidents between 2008-2012 [11]. As a result of the high number of accidents/incidents regarding the use of particulate materials, several efforts have been made to propose, characterize and improve the active and passive security systems of the equipment and the overall process [3].

One of these efforts is related to the correct characterization of the most commonly used dusts in chemical process plants in terms of its explosivity characteristics. These characteristics can be divided in two main categories. The first one aims at determining how likely a certain dust is to explode and can be estimated through the calculation of the Minimum Explosible Concentration (MEC), the Minimum Ignition Energy (MIE), the Limiting Oxygen Concentration (LOC), the Minimum Auto-ignition Temperature (AIT), among others. The second category stablishes the severity level of a potential explosion with the maximum explosion pressure (P_{max}) and the maximum rate of pressure rise ($[dP/dt]_{max}$) [1], [12],[13].

The parameters mentioned above can be measured by several standard tests that are based on the dispersion of a known dust mass with air at different operating conditions. Some of the most widely used tests are the 20L Sphere (ASTM E2019-03, ASTM E2931-13 and ASTM E1515-14) [14]–[17] , the Hartmann Tube (ASTM E2019-03) [15] , the BAM Oven, and the Godbert-Greenwald furnace (ASTM E1491-06) [18] . In spite of the fact that the 20L Sphere is currently recognized internationally as a valid and rigorous testing equipment to determine explosivity parameters, recent theoretical, experimental and computational studies have regarded some of its assumptions as highly questionable [1], [7], [12], [19]–[27]. In particular, these studies have agreed that certain operating parameters, such as the geometry of the disperser, the agglomeration and/or de-agglomeration of the dust particles throughout the test, as well as the levels of turbulence have a high influence in the homogeneity of the dust cloud in the dispersion and combustion step, and therefore, could lead to the mis-estimation of the design parameters of the security systems [1], [7], [26], [27], [12], [19]–[25].

1.2. Theoretical Framework: 20L Sphere Standard Test (particle dispersion and combustion)

The 20L standard test was originally designed by Siwek in 1988 to characterize some explosivity parameters of combustible dusts and gases, and became the standard device after replacing the 1 m^3 tube, given that it requires a dust sample with 50 times lower mass [24]. The main parts and components of the geometry are shown in **Fig. 1**.

This geometry can be divided in two main parts. The first part consists of a stainless-steel spherical chamber that occupies a total volume of 20L. This chamber is covered by a cooling jacket system specially designed to dissipate the excess heat produced by the combustion reactions. The interior of the 20L chamber contains an ignition system with two pyrotechnic ignitors that are located at the center of the sphere and that provide an energy spark of 5kJ each. The second part consists of a 0.6L reservoir or canister (where the dust particles are initially stored), a quick action valve and a nozzle that works as a connection between this dust reservoir and the spherical chamber.

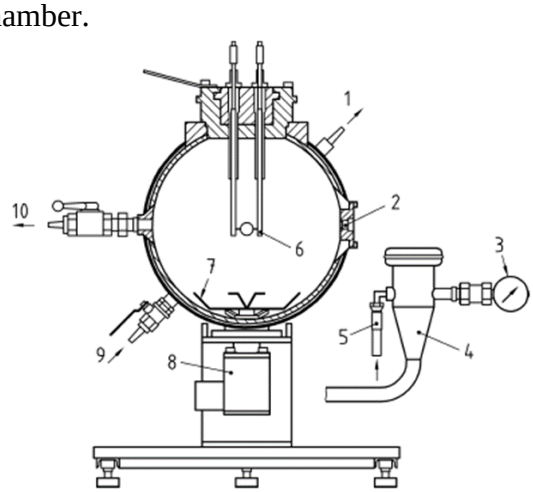


Fig. 1. 20L explosion sphere. **1.** Water Outlet **2.** Pressure sensors **3.** Manometer **4.** Canister (injection chamber) **5.** Air inlet **6.** Igniters **7.** Dispersing nozzle **8.** Quick-action valve **9.** Water inlet **10.** Product outlet [14].

The standard experimental procedure initiates with the de-pressuring of the dispersion chamber (sphere) to a set value of 0.4 bar and the addition of a weighted sample of the studied dust into the canister. Following these activities, the pressure of the canister is increased to a value of 20 bar by allowing the entrance of the dispersion gas, which is usually air unless limiting oxygen tests are performed, in which case its composition can be altered. The next step of the test consist of opening the quick-action valve to let the dust particles pass through the nozzle openings into the 20L sphere by the action of the pressure gradient [28]. Finally, after a given amount of time, the two ignitors have an energy discharge and the combustion process initiates. This time is known as Ignition Delay Time (tv) and is one of the most relevant operating parameters in the development of the test. The determination of an appropriate tv is highly crucial given that this parameter has a noteworthy influence on the turbulence levels reached within the reaction chamber and on the kinetic behavior of the pyrolysis/oxidation reactions. However, several studies on the matter have concluded that an appropriate tv would be approximately 60 ± 5 ms given that, at this point of the process, the concentration of dust particles is somehow homogeneous and the degree of turbulence is high [28].

During the entire process, the mean pressure of the dispersion chamber is increasing at a high rate given the effects of the gas entering the system and the over-pressure wave generated by the combustion reactions. The measurement of these two parameters is the basis for the definition of the deflagration index or K_{st}. This parameter is used to classify dusts materials according to their potential risk of explosion regardless of the volume of the vessel where the test was carried out. **Eq. (1**) shows the mathematical definition of deflagration index [14].

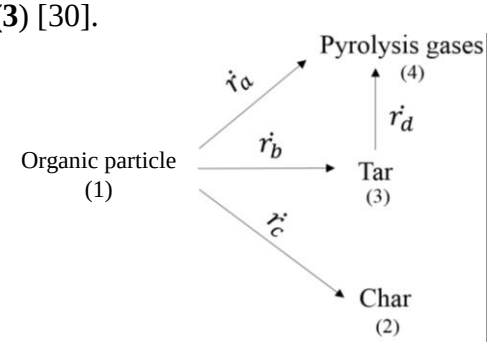
$$K_{st} = \left(\frac{dP}{dt}\right)_{max} * V^{1/3} \qquad \text{Eq. (1)}$$

Table 1 shows the risk level classification according to standard values of K_{st}.

Table 1. Risk level ranges from deflagration index

Risk Level	K_{st} (bar*m/s)	Severity
St 0	0	None
St 1	0-200	Weak
St 2	**200-300**	**Strong**
St 3	**>300**	**Very Strong**

Most authors agree that the procedure described previously for characterizing dust materials through the standard 20L sphere test can be divided in two main stages: (i) Particle dispersion and (ii) Combustion. For organic particles, the second main stage can be further divided in three main sub-stages: particle heating, particle devolatilization (pyrolysis) and gas oxidation [3], [29]. Some authors have stated that particles of an average diameter lower than 30μm would undergo heating and pyrolysis processes at a sufficiently rapid rate to consider these sub-stages as negligible. However, other authors have demonstrated that, depending on factors such as particle internal and external heat transfer, particle diameter, and the pyrolysis reactions themselves, the pyrolysis sub-step of the process could be the rate-controlling process and should not be discarded [9], [30]. The general reaction pathway for pyrolysis is shown in **Eq. (2)**-**Eq. (3)** [30].



Eq. (2)

$$k_j = A_j \exp(E_j/RT) \qquad \text{Eq. (3)}$$

1.3. State of the art

One of the most important contributions to the improvement of the 20L sphere standard test was developed by Dahoe in 2001, when he discovered that the turbulence levels reached inside the dispersion/combustion chamber are influenced by the Ignition Delay Time, and that these levels also differ from those found inside the 1 m^3 tank at the same dispersion time [24]. From these findings, other authors started questioning how the difference in turbulence levels could affect the results of the test. In particular, Van der Wel showed that the values of the deflagration index measured with the 20L sphere differed significantly with those measured with the 1 m^3 tank for the same dust sample [31]. He attributed this inconsistency to the difference of the turbulence fields that occur in the two geometries.

Other studies have focused their attention on the evaluation of the influence of the nozzle type on the turbulence levels reached and the concentration homogeneity. These authors include Murillo [28], Dahoe [24] and Mercer [7], who separately analyzed different nozzle geometries and concluded that this factor is indeed one of the parameters that could be modified in order to obtain higher levels of homogeneity and therefore, more accurate and reliable test results.

As for other parameters, such as the particle size distribution, the studies made by Callè [32], Cashdollar [33] and Soundararajan [34] have led to conclude that, in the micrometric range, the reduction of the particle size tends to have a positive effect on the explosion severity, particularly on the maximum pressure reached. On the other hand, in the nanometric scale, this trend is not maintained as the reduction of the particle size only influences the MIT and MIE [35].

Besides the experimental studies mentioned above, there have been some efforts to use certain computational tools to study the validity and improvement of the standard test. As an example, Di Benedetto [1] used Computational Fluid Dynamics (CFD) to show that the turbulence levels suffer a decay over time and that the ignition points (at the geometrical center of the sphere) have higher turbulence levels than the remaining parts of the domain. Other studies have analyzed the influence of particle properties, nozzle geometry and initial agglomeration shape in the turbulence levels reached [21], [33]. While most of the CFD studies limit their reach to the dispersion stages, Skjold [36], Salamonowicz [37] and Redlinger [38] have used commercial software, such as FLUENT and FLACS, and simplified chemical reaction mechanisms to successfully simulate the combustion stage and obtain some relevant information.

Considering the previous remarks, this study will be focused on applying experimental and computational tools in order to study how the behavior of the discrete phase (particles) during the dispersion stage is influenced by the geometry of the disperser and by the dust material (Wheat starch and Carbon-black), and how this affects the validity of the assumptions of the standard test. Additionally, this study contains an initial attempt at simulating the combustion stage with a detailed kinetic combustion mechanism and at determining the fraction of the particles that devolatilize into the combustion gases.

2. METHODOLOGY

The upcoming section addresses in detail the methodology followed for the experimental and CFD approaches to analyze the dispersion and combustion stages of the 20L Sphere.

2.1. Experimental approach

To evaluate the dispersion stage and the most relevant variables, the 20L Sphere was modified by the installation of visualization windows through the axis center and two piezoelectric transducers on the equatorial plane at the wall of the dispersion chamber to monitor the pressure profile. Moreover, the dust dispersion dynamics and agglomeration phenomena were analyzed experimentally by Particle Image Velocimetry (PIV) and Granulometric analysis techniques using the standard rebound nozzle geometry.

The first technique allows the study of the variation of the velocity field at the center of the 20L Sphere, in a region of $3 \times 3\ cm$, by the determination of the average motion of small groups of particles contained within small regions, known as interrogation spots [39]. In addition, the assembly used includes a high-speed camera Phantom V91 (**Table 2**) placed in front of a visualization window, a laser focus at the center of the sphere to illuminate the particles and the MATLAB ® tool, PIVLab® to process the images captured. Furthermore, the measures of Carbon-black were performed neglecting additional light sources, as the black body optical properties of this dust.

Table 2. Phantom V91 technical specifications

Specifications	Value
Resolution	$480 \times 480\ px$
Exposure	$150\ \mu s$
Area	$(2.95 \times 2.80)\ cm$
Framerate	$6410\ fps$
Time interval	$156\ \mu s$

The Granulometric Analysis was used for the measurement of the variation of the PSD using a laser diffraction method to study the de-agglomeration/agglomeration phenomena. The equipment handled was a HELOS-VARIO/KR (Sympatec) with an optic system composed by

a laser emission and detection device. For the measurements, the dispersion chamber was located between the sensor and the detection unit.

Furthermore, the dust materials used in this research are the micrometric Wheat starch and Carbon-black, because of the widely industrial use, the extensive dust dispersion studies, and the well know explosibility parameters [27], [40]. One of the more important variables which characterizes the dust materials is the particle size distribution in a cumulative distribution function, as shows the **Fig. 2**.

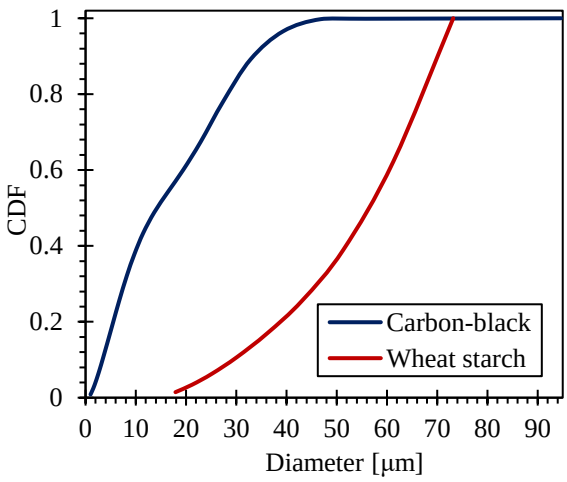
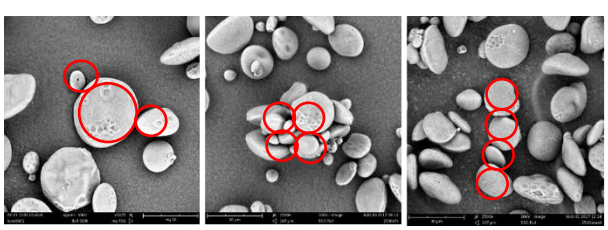


Fig. 2. Average particle size distribution (PSD) of the Carbon-black and Wheat starch dust samples

On the other hand, microscopy technique was used to study the agglomerate shapes of the dust materials. **Fig. 3** shows the most common configurations of Wheat starch, which were adjusted to easier shapes; like triangular, cube and line assemblies. Moreover, the most common agglomeration shape of the Carbon-black was a line configuration, comparable to **Fig. 3c.**



(a) **(b)** **(c)**

Fig. 3 Most common agglomerate shapes in Wheat starch samples **(a)** Triangular **(b)** Cube **(c)** Line

2.2. CFD modelling

Given that this study is focused on both, the dispersion and combustion stages of the standard test, two separate CFD sets of simulations were established with the aim of testing different variables and performing various analyses.

The dispersion stages were studied through two different dust materials and seven disperser geometries. The two selected materials were micrometric Wheat-starch and Carbon-black. The seven dispersers included the standard nozzle, a symmetric nozzle proposed by Murillo [28] and five nozzles proposed by this study. **Fig. 4** contains a schematic representation of these nozzles.

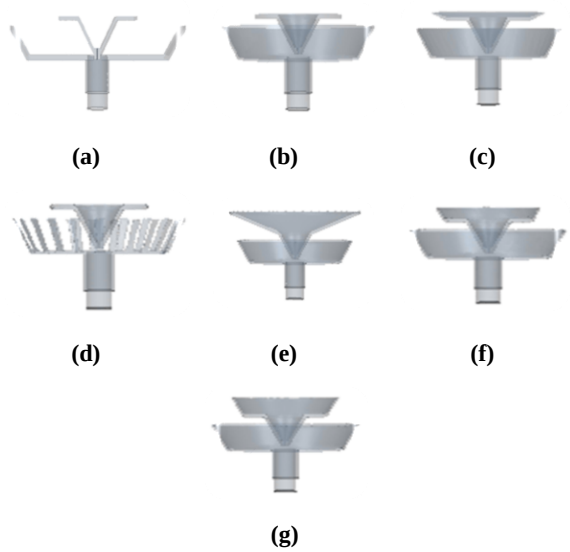


Fig. 4. Disperser geometries used. **(a)** Standard (N1). **(b)** Symmetric (N2). **(c)** N3. **(d)** N4. **(e)** N5. **(f)** N6. **(g)** N7.

As will be meticulously explained in the following sub-sections, the physical model selected to simulate the dispersed phase (DEM) requires the establishment of an initial shape for the particle agglomerations. Considering the microscope images of Wheat starch shown in **Fig. 3**, three initial shapes were selected: line, cube and triangle (see **Fig. 5**).

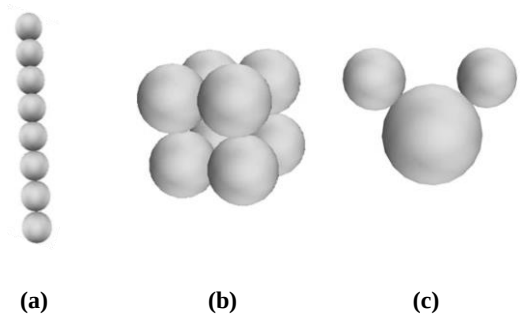


Fig. 5. Initial agglomeration shapes considered for the dispersion simulations. **(a)** Line. **(b)** Cube. **(c)** Triangle

Considering that it is highly desirable to find the combined effect of these variables, the simulations of Wheat starch were run with each of three initial agglomeration shapes and the standard and symmetric nozzles. In contrast, the simulations for Carbon-black were run with the line shape and the seven nozzles.

The CFD model constructed for the combustion stage considered only the standard disperser and used only the pyrolysis gases of Wheat starch. The use of this method was performed as a first approximation and simplification of the complex process of organic particles combustion [41]. In addition, the generation of tar and char, described in Section 1.2, is neglected because of the significant increase of the gas formation rates and the considering of complete devolatilization at high temperatures, as upstream of the flame [29], [41].

Furthermore, the pyrolysis gases mixture composition of Wheat starch sample was established from an adjustment of the study of flash pyrolysis reactor by Bozier [42], taking into account the variation of compositions at different reactor temperatures and the typical flame temperature of this dust combustion [29]. The gas mixture compounds loaded on CFD simulations were $H_2, CH_4, CO, C_2H_4, C_2H_6$, C_2H_2[42].

Additionally, taking into consideration the PSD of Wheat starch (**Fig. 2**) was on average greater than $30\,\mu m$, therefore the devolatilization would become a rate-controlling step of combustion process [29]. Consequently, this study proposes the study of this restriction using a proportional constant (k_c), which correlates the equivalent ratio between the solid mass of the organic dust (m_o) and the mass of pyrolyzed gases (m_p), as shown in **Eq. (4)**. This simplification was made considering the complexity of measuring and lack of data about the pyrolysis kinetics of Wheat starch at conditions of 20L Sphere standard test.

$$\frac{m_p}{m_o} = k_c \qquad \text{Eq. (4)}$$

Moreover, the value of k_c can be interpreted as the percentage of solid mass converted to pyrolyzed gases, which according to the work done by Zhang, et al. [43], this variable could value 0.86 for corn starch, which is comparable with Wheat starch used in this study. However, the conditions at the 20L Sphere standard test could affect the prediction of k_c [43] and the state of the sample at measurement. For that reason, this study evaluated the combustion of a pyrolyzed gas mixture at different k_c (taking the value reported by Zhang, et al. [43] as the middle point, the upper bound of the variable and a proportional lower bound), of a mass of 10 g of Wheat starch, which correspond to a fuel-equivalence ratio $(F/A) = 1$ [29], as shown the **Table 3**. Furthermore, there were made several test to validate the behavior of the combustion dynamics at the most relevant value of k_c and different (F/A), in order to compare with the experimental data found by Dufaud, et al.[29].

Table 3. Simulated cases to evaluation of k_c at combustion of pyrolyzed gases

Cases	(F/A)	k_c
1	1	1.00
2	1	0.86
3	1	0.60

On the other hand, the kinetics parameters of the combustion reactions were taken from the optimized mechanism of methane-air combustion based on GRI-Mech 3.0 with 30 species [44]. This mechanism was selected because it involves all the pyrolysis gases of the Wheat starch and the contrast of the combustion behavior prediction between the complete mechanism of 53 species, don't present a significant difference [44].

2.1.1. Spatial discretization

The discretization of the geometry was made by the finite-volume method. A polyhedral mesh was selected due to the generation of more neighboring cells and optimal directions for the flow when compared to other models, such as tetrahedral [20], [45].Additionally, previous CFD studies used the polyhedral mesh for different applications and obtained good agreement with experimental data [20], [27], [46]. Moreover, the surface remesher was used for the re-triangulation of the surface to allow cell refinement over certain volume regions [45], in order to model accurately the fluid behavior in the most complex zones (nozzle and ignitors) of the geometry and avoiding divergence, as shown in **Fig. 6**.

Furthermore, the prism layer model was added because of the important source of vorticity at the walls of the geometry, in order to improve the prediction of the flow and turbulence across the boundary layer [45]. The resultant mesh was around 820,000 cells with an average cell quality of 0.738.

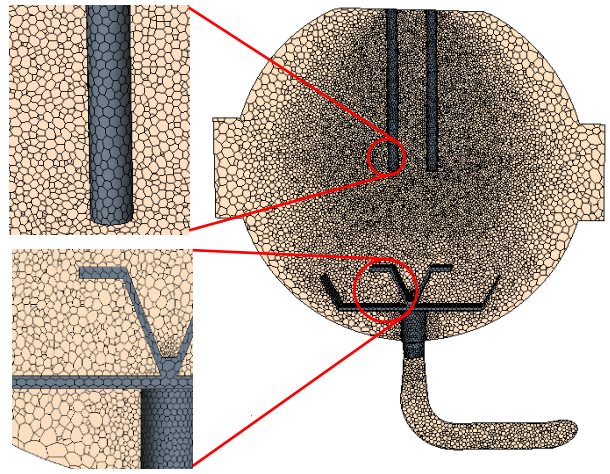


Fig. 6. Mesh of the 20L Sphere and refinements on the ignitors and nozzle near zones.

2.1.2. Boundary and initial conditions

The initial and boundary conditions loaded on the simulations were in agreement with the experimental settings and the international standard ASTM E1226 [14], however the cooling jacket was simulated as a thermal boundary at constant temperature, as shown in **Table 4**.

Table 4. Initial and boundary conditions

Condition	Value
Initial pressure [bar]	20 (Canister), 0.4 (Sphere)
Initial temperature [K]	300
Boundary solid type	No-slip wall
Thermal boundary [K]	Adiabatic (Canister), 300 (Sphere)

2.1.3. Physical models' selection

The physical models that describe the overall system of the 20L Sphere were selected considering the accuracy and suitability of the model for this application, as well as computational power and time requirements.

Considering that the dispersion stage of the process is a phenomenon of a two-phase nature, a Eulerian-Lagrangian problem formulation was selected as the general approach. Broadly speaking, the Eulerian representation of a fluid

flow considers the fluid properties (such as velocity, pressure, and density) as field functions of time and position within a specific control volume, which makes this approach very suitable to model 'continuous' flow phases, such as the gas phase present in the 20L Sphere. On the other hand, the Lagrangian approach is focused on describing and tracking the motion of each individual particle in order to determine the fluid flow properties. The consideration of each particle as an individual entity indicates that the Lagrangian model is highly appropriate to describe the combustible dust particles of this study [47], [48].

The upcoming paragraphs contain the specificities of the approaches followed for the Eulerian (gas) and Lagrangian (dust particle) phases.

(i) Gas-phase modelling: The fundamental constitutive equations of a continuous flow were resolved through the the Reynolds-Averaged Navier-Stokes (RANS) approximation, coupled with the standard k-ϵ turbulence model to calculate the Reynolds-stress tensor. In spite of the fact that previous studies on the matter of the 20L Sphere have mainly used a combined LES-RANS (IDDES) approach with a k-ω SST turbulence model [20], [27], [49], [50], as will be seen in the forthcoming section, at the later stages of the dispersion step, the fluid domain can be considered isotropic, which makes the flow appropriate to be described by RANS [51]. Additionally, it can be stated that the k-ϵ turbulence model is very well-fitted for high Reynolds applications, provides a good balance between accuracy and computational time and has been successfully used for CFD modelling of the combustion stages in the context of the 20L Sphere standard test [36], [37]. The k-ϵ turbulence model was configured with an upwind second-order convection scheme

(ii) Particle modelling: The behavior of this phase was modelled through the Discrete Element Method (DEM), an extension of general Lagrangian approach. As opposed to the general model, DEM tracks the motion of the entire set of particles contained within the system, and is able to account for the interactions between particles [45]. These characteristics of DEM are particularly useful for this application given that one of the main objectives of this study is to analyze the process of particle agglomeration/de-agglomeration during the dispersion stage, which is a phenomenon highly influenced by particle-particle interaction forces. Several studies have previously used DEM to model different particulate materials inside closed systems with very accurate results [52], [53].

The general equations of motion of the particles are derived from the classical mechanics' equation of conservation of linear and angular momentum (**Eq. (5)**-**Eq. (6)**) [45].

$$m_p \frac{d\boldsymbol{v_p}}{dt} = \boldsymbol{F_s} + \boldsymbol{F_b} \qquad \text{Eq. (5)}$$

$$\boldsymbol{I}_p \frac{d\boldsymbol{\omega_p}}{dt} = \boldsymbol{M_b} + \boldsymbol{M_c} \qquad \text{Eq. (6)}$$

The term of the surface forces represents the overall momentum transfer from the gas (continuous phase) to the particles. This force term was considered as the sum of the contributions of the drag force and the pressure gradient force. The drag coefficient was estimated through the Schiller-Nauman correlation given that the agglomerates were assumed to be comprised of completely spherical particles.

On the other hand, the body forces were assumed to be the sum of the gravity forces and the interparticle contact forces. These contact forces were calculated through the Hertz-Mindlin no-slip contact model, which is a

variation of the standard non-linear spring-dashpot model [54]

As for the combustion step of the standard test, the transport equations related to each one of the chemical species involved were resolved through the Complex Chemistry transport model. This model is well-fitted for this particular application given that it is a highly rigorous approach that integrates all the source terms of the transport equations over time and considers that the reactions are limited by their actual kinetics and not by the rate in which the species and heat are mixed into the flame zone by the turbulence [45]. The solver selected for the time integration of the source terms was CVODE.

Additional to the models mentioned previously, it is relevant to highlight that both main stages of the standard test (dispersion and combustion) are unsteady phenomena. Taking this into account, an Implicit Unsteady method, coupled with a second order discretization scheme, was selected. The time-step was set for all simulation aiming for a Courant number of 1 as this ensures that the flow travels only one cell each time-step.

$$CFL = \frac{u\,\Delta t}{\Delta x} \qquad \text{Eq. (7)}$$

3. RESULTS AND DISCUSSION

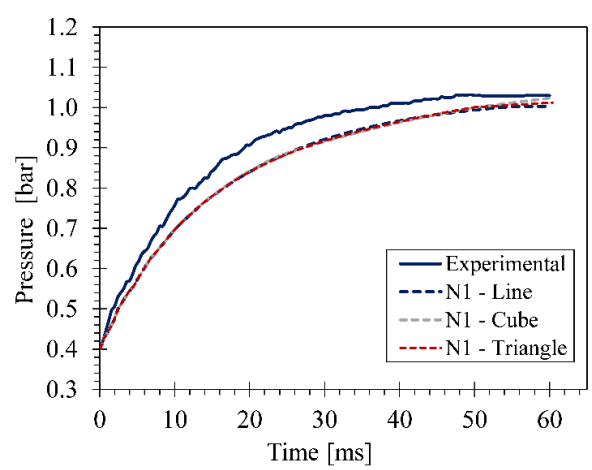
This section contains the main results of this study and a detailed discussion of the implications of the data acquired through experimental and CFD means. These results are divided in two main sub-sections: (i) Analysis of the dispersion stage of wheat starch and Carbon-black, and (ii) First approach to the modelling of the combustion stage of the 20L standard test.

3.1. Evaluation of the effect of turbulence on the agglomeration/de-agglomeration of the particles and the overall dispersion step of the test

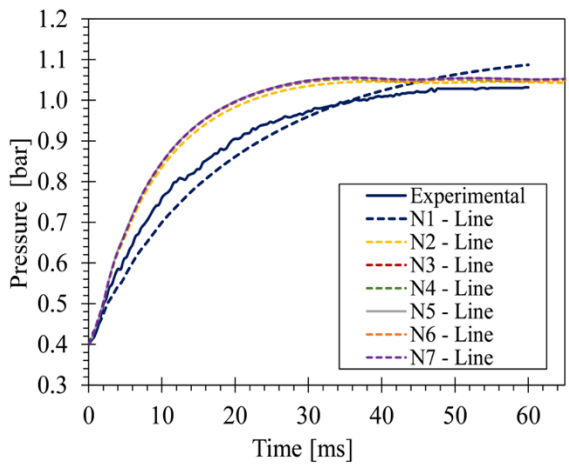
As it was mentioned previously, this sub-section has the main objective of evaluating certain phenomena that occur during the dispersion stage and how these could potentially affect the subsequent pyrolysis/combustion stage, which affects the reliability of the assumptions of the standard test.

3.1.1. CFD validation and effect of the disperser on the pressure profile

The validation of the CFD model stablished for this part of the analysis was performed through the comparison of the average pressure profile of the sphere region obtained by CFD and the pressure obtained experimentally by two transducers located at the equatorial plane of the sphere. This variable was selected for validation purposes over temperature or particle velocity as the maximum pressure and maximum rate of pressure rise are the fundamental variables that determine the explosive potential of a certain dust material [36]. **Fig. 7** contains the experimental and CFD pressure profiles for the three initial particle shapes of Wheat Starch and the seven nozzles for Carbon-black.



(a)



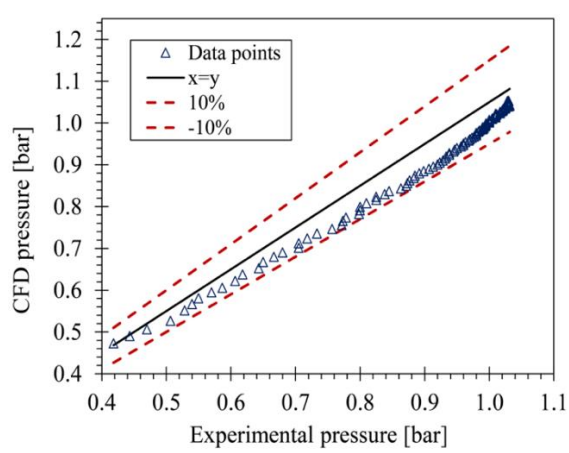
(b)

Fig. 7. Comparison of the sphere pressure profile obtained experimentally and by CFD for **(a)** Wheat starch and **(b)** Carbon-black

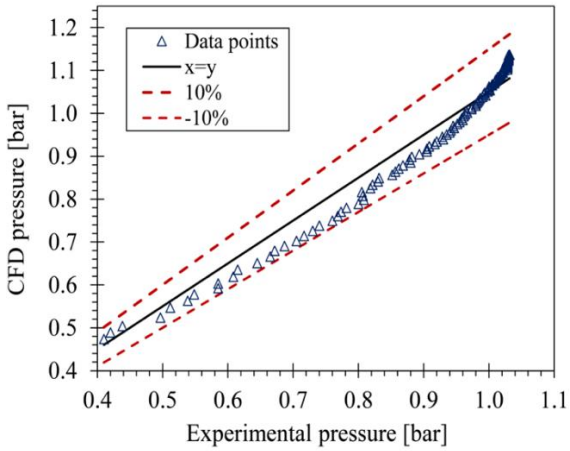
From **Fig. 7** it can first be stated that both, the experimental and CFD results are congruent with previous experimental and theoretical studies as the sphere undergoes a very rapid pressure increase up to 20ms, followed by a more gradual increase until the system reaches the desirable pressure of 1 bar at approximately 60ms (standard Ignition Delay Time) [28], [55]. This can be explained by the fact that, at the very beginning of the test, the pressure gradient between the sphere and the canister is high, which directly translates into a high driving force that induces a high rate of mass, momentum, and energy transfer. As the pressure of the sphere increases (and the pressure of the canister decreases), the driving force is lowered and therefore, the rate of pressure rise within the sphere also decreases.

Fig. 7 also suggests that the CFD model constructed for both materials provides a very accurate prediction of the sphere pressure given that the deviations from the experimental points (for the standard nozzle) do not overcome 8.6% for Wheat Starch and 5.5% for Carbon-black (with an average error of around 5.03% for Wheat Starch and 3.76% for Carbon-black). To better highlight the quality of the prediction achieved, the experimentally-measured pressure values were plotted against their CFD counterparts to obtain **Fig. 8**. It is important to mention that **Fig. 8** only contains the pressure values obtained every 0.5ms in order to have the same number of experimental and CFD points (the low time-step selected for the simulations results in a significantly higher number of CFD points). However, it should be noted that the intermediate values have the same tendency and deviation and that 0.5ms intervals can correctly represent the entire data set.

Fig. 8 shows that the CFD model tends to under-predict the pressure values for both materials. This behavior is consistent with previous CFD studies [20] and can mainly be explained by the selected physical models of agglomeration/de-agglomeration and the set-up parameters (such as Poisson's ratio, Young's modulus, Tensile strength, among others) used for Wheat starch and carbon-black. Additionally, from **Fig. 7** and **Fig. 8** it can be noted that the highest errors are found at intermediate times (from around 10ms to 40ms), which would suggest that the assumptions of the CFD model (refer to section 2.2) are more appropriate for very high and/or very low velocities and turbulence levels (beginning of the test and end of the dispersion stage, respectively).



(a)



(b)

Fig. 8. Pressure profile obtained experimentally vs. CFD with the standard dispersion nozzle. **(a)** Wheat Starch and **(b)** Carbon-black

On the other hand, **Fig. 7(a)** implies that the initial agglomeration shape does not have a considerable influence on the behavior of the sphere pressure with time. This result is interesting given that, as will be thoroughly analyzed in the upcoming sub-sections, the initial shape of the particles is very much an influential parameter on the degree of de-agglomeration reached at the end of the dispersion stage and on the validity of the assumption that the particle concentration is homogeneous throughout the domain of the sphere.

To finalize this sub-section, it is relevant to highlight that the pressure profile obtained for the standard nozzle differs from the one obtained with the remaining six nozzles (**Fig. 8(b)**). As can be expected, this behavior is attributed to the geometrical differences between the nozzles and the turbulence levels reached in each case. **Fig. 9** shows the average CFD Turbulent Kinetic Energy (TKE) for Carbon-black. As can be seen in **Fig. 9**, a significantly lower TKE peak is obtained with the standard nozzle, which influences directly the average sphere pressure and explains the pressure behavior found in **Fig. 7(b)**.

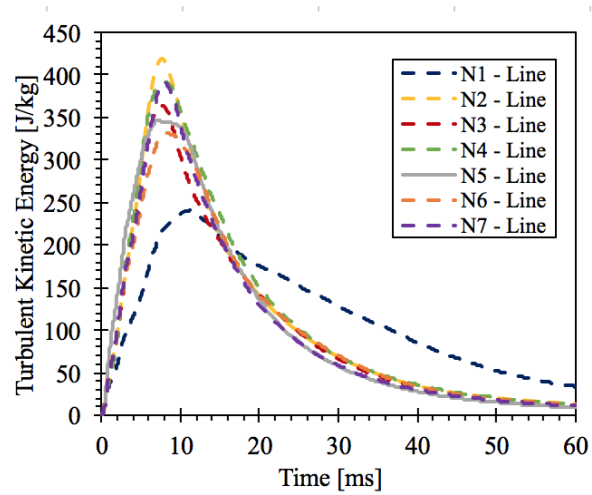


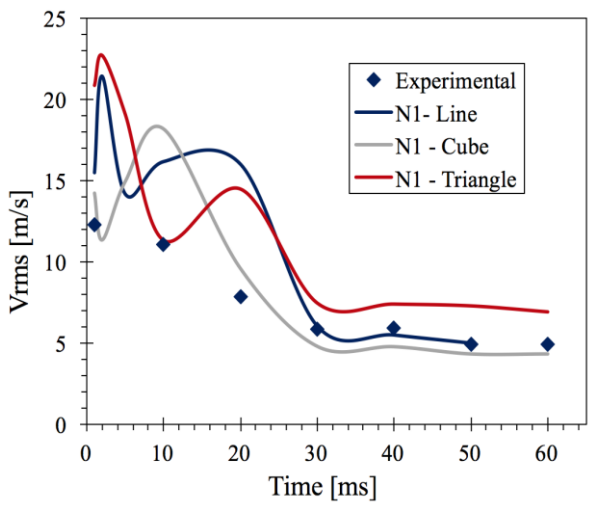
Fig. 9. Average CFD Turbulent Kinetic Energy profile for Carbon-black

3.1.2. Analysis of particle velocity at the ignition zone

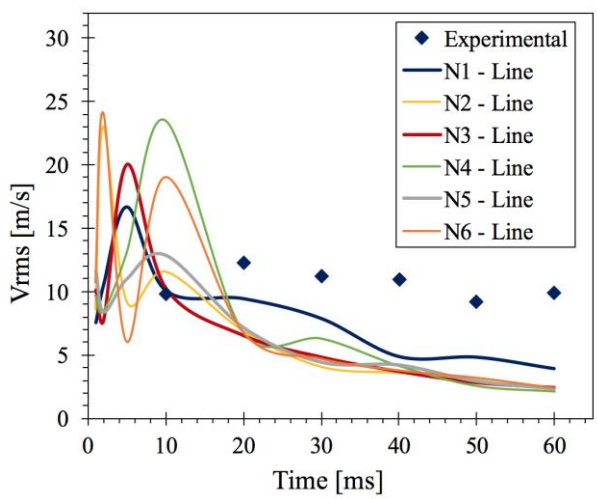
As it was mentioned on the Methodology section, a PIV analysis was performed at the center of the sphere to obtain the particle velocities at the x and y plane coordinates and compare then with those obtained by CFD. Considering the considerable number of particles present within the system, the two component velocities of each particle were averaged by the total number of particles through the definition of the root-mean-square velocity. **Fig. 10** shows the V_{rms} magnitude obtained experimentally and by each of the CFD simulations.

$$V_{rms} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(v'_{xi}\right)^2 + \frac{1}{N}\sum_{i=1}^{N}\left(v'_{yi}\right)^2} \qquad \text{Eq. (8)}$$

$$v_i{}' = v_i - \bar{v} \qquad \text{Eq. (9)}$$



(a)



(b)

Fig. 10. Root-mean-square velocity at the center of the sphere for **(a)** Wheat starch and **(b)** Carbon-black. The experimental measurements were taken with the standard nozzle (N1).

The results shown in **Fig. 10** indicate that the dispersion process can be divided into two main sub-stages. The first one (from 0 to ~30 ms for Wheat-starch and from 0 to ~20 ms for Carbon-black) includes a highly fluctuating particle flow and a high degree of velocity decay that coincides with the high degree of TKE decay of **Fig. 9**. Considering only this sub-stage, it can be stated that the lowest V_{rms} values, as well as the slowest rate of V_{rms} decrease are obtained with the standard nozzle and Carbon-black particles. This result is consistent with both, the TKE and pressure CFD profiles shown previously.

The second sub-stage (from ~30 to ~60ms for Wheat-starch and from ~20 to ~60ms for Carbon-black) shows a much smoother V_{rms} decrease over time and a less prominent difference between the V_{rms} values for the different nozzles, initial agglomeration shape and particle materials. This result is in agreement with previous studies [56], [57] as these state that 60ms is the testing time where the turbulence reaches constant levels over time and the flow becomes approximately isotropic (the three velocity components are equal in magnitude).

As it was suggested by Dahoe et al. [24], [25], the decreasing behavior of the V_{rms} and TKE over time can be explained by the three main mechanisms that induce turbulence in the system. The first mechanism is the baroclinic contribution to the change of vorticity within a velocity field (last term of **Eq. (10)**).

$$\frac{D\boldsymbol{\omega}}{Dt} = (\boldsymbol{\omega}\cdot\boldsymbol{\nabla})\boldsymbol{v} - \boldsymbol{\omega}(\boldsymbol{\nabla}\cdot\boldsymbol{v}) + \nu\boldsymbol{\nabla}^2\boldsymbol{\omega} + \frac{\boldsymbol{\nabla}\rho \times \boldsymbol{\nabla}P}{\rho^2} \qquad \text{Eq. (10)}$$

At the very beginning of the test, the particles are flowing through a cylindrical channel that connects the canister to the sphere. Consequently, the pressure and density gradients are expected not to have the same direction and to have a significant magnitude, producing high vorticity, velocity, and turbulence levels. However, as the particles start entering and dispersing inside the sphere domain, the pressure gradients decrease and the contributions from the baroclinic effects become insignificant [24], [25].

The other two sources are the turbulence that arises from the flow interaction with the wall friction [58] and the shear turbulence. These two remain present all throughout the entirety

of the test but their contribution to the turbulence levels is not significant. Subsequently, considering that the baroclinic effect has the highest influence on the turbulence levels reached, the decline on the TKE and velocity can be attributed to the decline on the baroclinic contribution to the vorticity.

On the other hand, the decaying nature of the V_{rms} for Carbon-black shown in **Fig. 10 (b)** was fitted to the inverse power-law equation proposed by Dahoe et al. [24] (Eq. (11)) from 20ms to 120ms. This time range was selected for the fitting given that the equation proposed by Dahoe is mostly used when the rapid decay that follows the TKE peak has already been surpassed. **Table 5** shows the parameter fitted by the application of the standard least square method and the average deviation between the CFD and the fitted V_{rms} values.

$$\left(\frac{V_{rms}}{V_{rms}^{0}}\right) = \left(\frac{t}{t_0}\right)^{n} \qquad \text{Eq. (11)}$$

Table 5. Fitting parameter of the equation proposed by Dahoe et al. [24] for Carbon-black

Nozzle	Parameter n	R^2
N1	-0.8250	0.3783
N2	-0.9338	0.0613
N3	-0.9932	0.0567
N4	-0.9463	0.2365
N5	-1.0244	0.0545
N6	-0.9814	0.0630

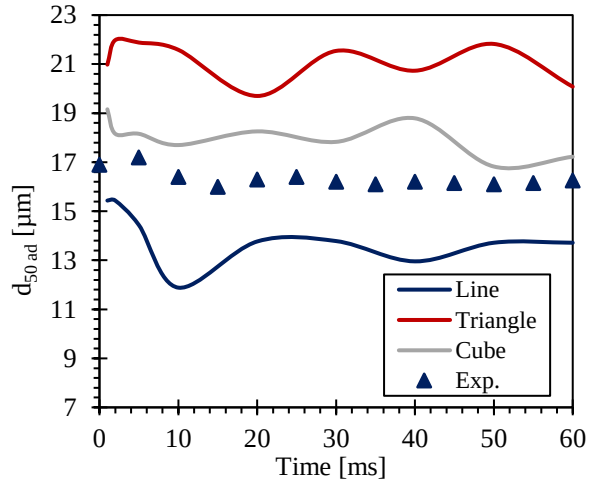
The comparison between the magnitudes of the R^2 for each nozzle (**Table 5**) and the V_{rms} values (**Fig. 10 (b))** indicate that the data set predicted by CFD can be fitted very well to the decaying function proposed by Dahoe et al. [24], [25] and, therefore, that the CFD results are in complete agreement to the data of that particular study. In addition, **Table 5** shows that the obtained fitting parameter n does not differ significantly for the six nozzles being studied. This suggests that, from around 20ms to the selected Ignition Delay Time, the rate of decay of the V_{rms} is not strongly influenced by the geometry of the nozzle.

3.1.3. Evaluation of the agglomeration/de-agglomeration process

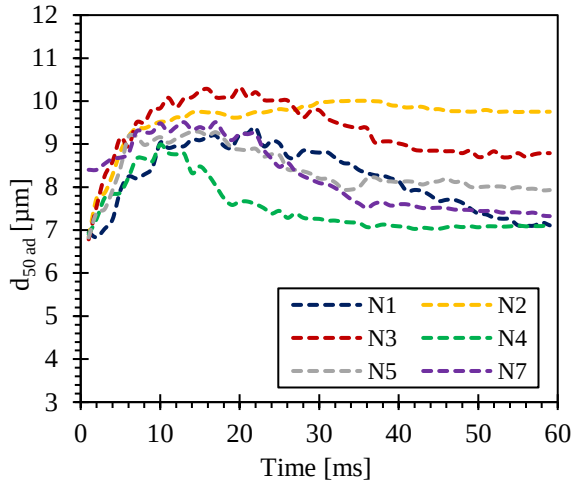
The agglomeration and de-agglomeration phenomena of dust particles was studied in a quantitative approach by the determination of the mean diameter after dispersion (d_{50ad}), as shown in **Fig. 11**, and bear in mind the mean diameter before dispersion (d_{50bd}), which are 14.5 and 56.5 μm for Carbon-black and Wheat starch respectively.

Fig. 11(a) exhibit a slightly de-agglomeration of the Wheat starch at the center of the sphere along the dispersion, which suggest that the overriding stage is at the beginning of the injection process, with a reduction of 68% of the mean diameter of the particles. This behavior is according to the high-pressure gradients when the particles moves through the canister exit to the nozzle. That assumption is in accordance with Weiler, et al. [59] who found that the disintegration of micron sized agglomerates occurs mainly by shear stress induced by vortices, which are generated by the baroclinic effect near the nozzle area [1]. Moreover, the velocity gradient in this section generates rotary stresses which promote the de-agglomeration, making the connection duct as

the overriding region of this phenomena, as well as Kalejiaye, et al [12] found.



(a)



(b)

Fig. 11 Mean diameter during dispersion of **(a)** Wheat starch and **(b)** Carbon-black particles. The experimental and CFD data of Wheat starch were taken at the center of the sphere with standard nozzle (N1)

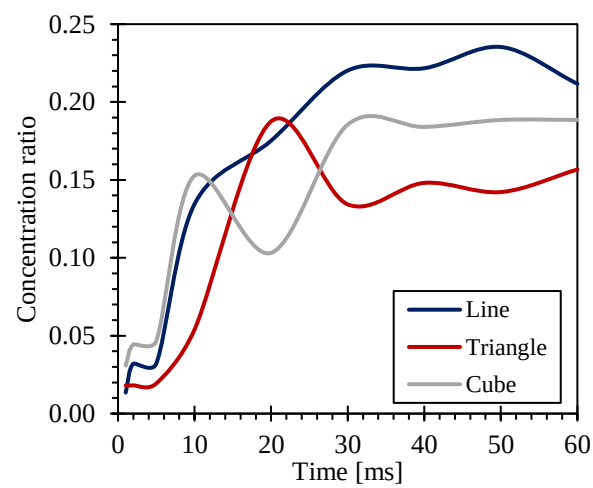
Therefore, the line agglomerate shape had a higher de-agglomeration, as shown in **Fig. 11(a)**, since this configuration has more surface area available for turbulent stresses transfer than other configurations. Additionally, the results of the mean diameter of Carbon-black **(Fig. 11(b))** on the sphere show a de-agglomeration of more than 45% since the beginning of the dispersion process. Nonetheless, the Carbon-black particles have a slightly agglomeration stage until 20 ms. This behavior is in agreement with the smaller particle size which promotes the effects of cohesive forces and the generation of agglomerates during collisions [60].

On the other hand, (**Fig. 11(b)),** indicates that the nozzle variation marginally affects the de-agglomeration of Carbon-black particles, where the nozzles 1 and 4 had the higher values. The previous statement is explained by the lower velocity decay, which hinders the effects of cohesive forces and agglomeration, as found by Sanchirico, et al. [19].

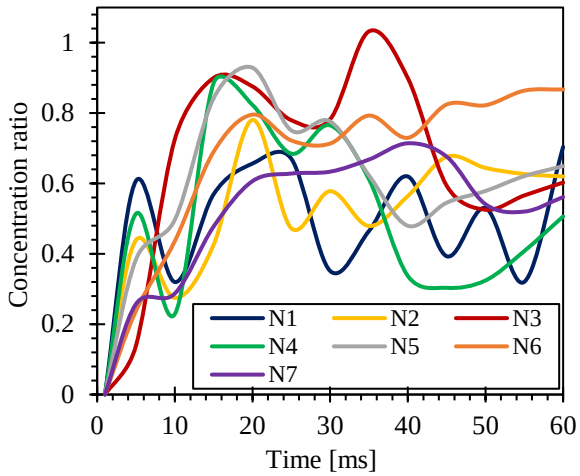
3.1.4. Evaluation of the homogeneity of particle concentration

The evaluation of the homogeneity of the dust cloud is related with the concern about the Minimum Explosive Concentration (MEC). As mentioned earlier, this variable is calculated from the dust nominal concentration, which assumes a homogeneous dispersion of the dust along the sphere. Therefore, the dimensionless concentration **Eq. (12**) is used as a homogeneity degree of the dust cloud.

$$C_{ratio} = \frac{C_{ignition}}{C_{nominal}} \qquad \text{Eq. (12)}$$



(a)



(b)

Fig. 12 Concentration ratio in the ignition zone of **(a)** Wheat starch and **(b)** Carbon-black.

The results shown in **Fig. 12** indicate that the real concentration is lower than the nominal concentration for all the different nozzle and agglomerates at the ignition time. Moreover, the line shape of wheat starch agglomerate exhibits a better homogeneity (**Fig. 12(a)**), and this behavior can be explained by the higher de-agglomeration (**Fig. 11(a)**) that benefits the increase of the dispersibility of the dust.

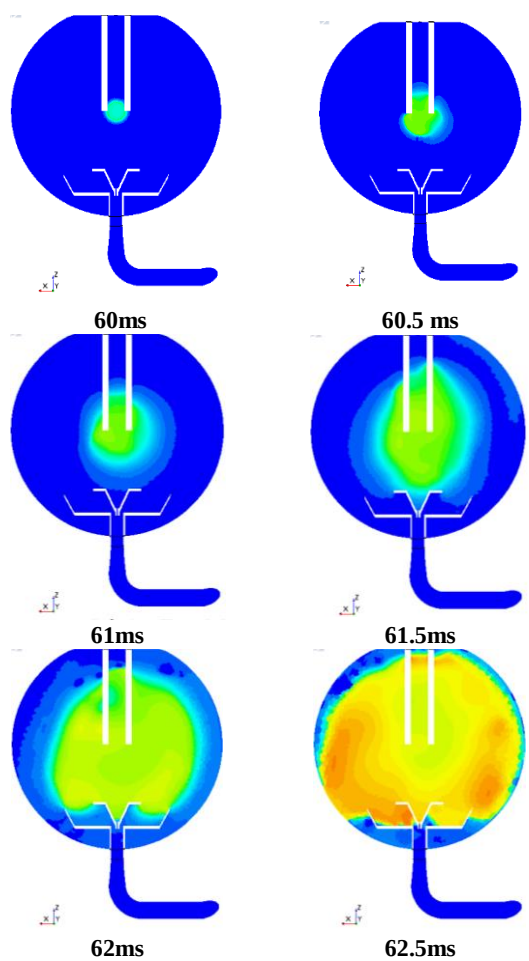
Additionally, the outlines of the concentration ratio of carbon black for the different nozzle types (**Fig. 12b**) suggest a similar behavior along the dispersion stage, with greater fluctuations at the earlier times (< 30 ms) and no significance difference at the ignition time. Nevertheless, nozzle 6 develops a slightly better homogeneity, followed by nozzle 1.

Furthermore, the results in **Fig. 12** show that the homogeneity of the Carbon-black dust cloud is better than the Wheat starch one. It can be described by the lower particle diameter of carbon black, which decreases the drag force per particle [27] and enhances the displacement of more particles to the center of the sphere, where the velocity fields are lower [28].

3.2. First approach to pyrolysis and fuel combustion

3.2.1. Model validation

Prior to the application of the CFD model established for the combustion stage of the standard test, an initial simulation was run to evaluate the validity of the reactions kinetic model, the thermodynamic data of the species involved and the overall CFD model, as well as analyze the general behavior of the flame and its propagation rate. The validation simulation was run with a gas equivalence ratio of 1.5 and it was compared to the equivalent experimental data taken by Dufaud et al. [29]. **Fig. 13** shows the evolution of the flame front at an Ignition Delay Time of 60 ms.



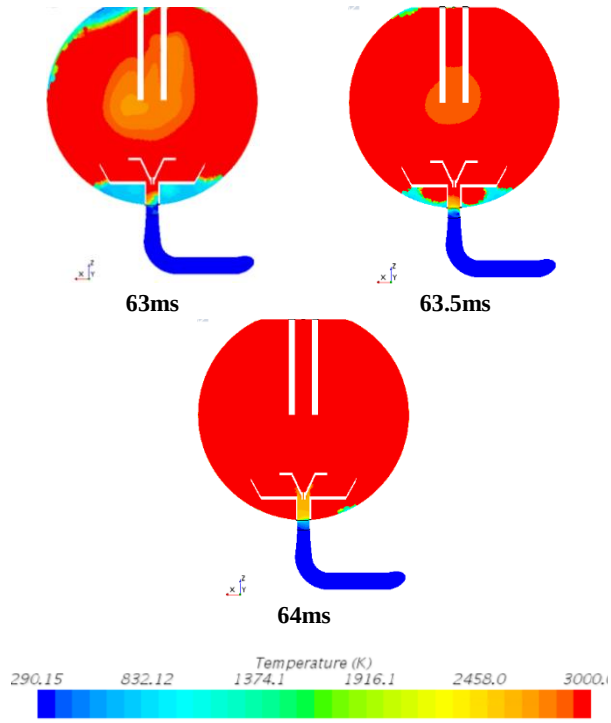


Fig. 13. Evolution of the flame front for the validation case

As can be seen in **Fig. 13**, the time passed from the beginning of the reaction to a state of total flame propagation within the system does not exceed the value of 4ms. This indicates that the environment in which the pyrolysis gases are present at 60 ms is highly reactive. Besides the conditions of temperature, pressure and fuel composition, the reaction rates are aided by the levels of turbulence that the system reaches after a dispersion time of 60 ms. From **Fig. 13** it can also be noted that the flame front is not perfectly spherical and, at certain times, has a preferred direction. This can be explained by the fact that the solid ignitors act as obstacles to the general flow and that, despite that at the Ignition Delay Time the system is close to being isotropic (refer to sub-section 3.1.2), there are still certain velocity gradients that direct the flame to a particular direction.

The selected variable to compare the CFD model to the literature experimental value was the maximum rate of pressure rise as this parameter is fundamental to the calculation of the deflagration index. **Table 6** shows the CFD and literature values and the deviation between the two.

Table 6. Comparison between the validation simulation and the data of Dufaud et al. [29]

CFD $\left(\frac{dP}{dt}\right)_{max}$ [bar/s]	Dufaud et al. $\left(\frac{dP}{dt}\right)_{max}$ [bar/s]	%Error
1721	2050	16%

As can be seen in **Table 6**, the proposed model fits well to the literature data. However, it should be noted that the chemical reaction model selected is highly rigorous and that the combustion reaction path considers several main and secondary equations. Consequently, it can be suggested that the deviation to the literature data is attributed to the calculation of the fuel equivalence ratio and, therefore, the concentrations of each of the initial chemical species. This remark will be further discussed in the following sub-section.

3.2.2 Evaluation of explosibility parameters and k_c to wheat starch combustion

The evaluation of explosibility parameters of Wheat starch at different values of k_c (reported on **Table 3**) were simulated in order to find the better fit with experimental values reported by Dufaud, et al. [29] at a $(F/A) = 1$. The $(dP/dt)_{max}$ was the chosen variable for the comparison because the relevance for the design of safety equipment [38]. Therefore, **Fig. 14** indicates a significantly difference (one order of magnitude) between the CFD and experimental data of the combustion of starch dust, validating the impact and the predominance of the pyrolysis step during a dust explosion [29], [41].

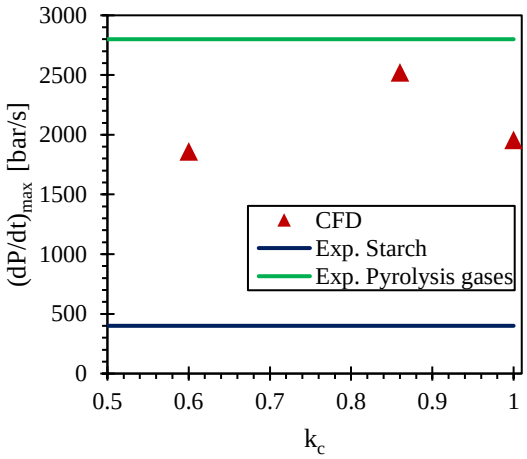


Fig. 14. $(dP/dt)_{max}$ behavior at different values of k_c at (F/A) equal to 1. The experimental data of pyrolysis gases and starch were taken from Dufaud, et al [29].

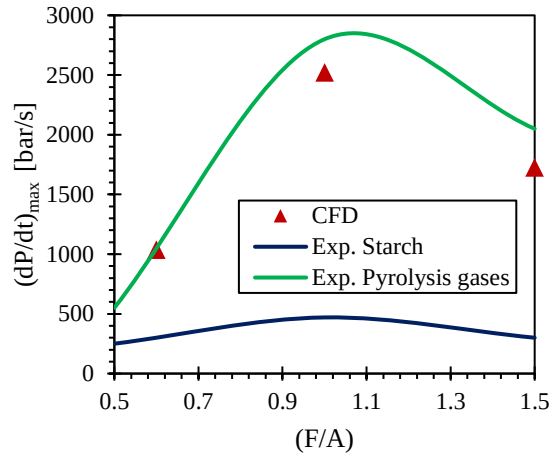


Fig. 15. $(dP/dt)_{max}$ behavior at different values of (F/A) at constant k_c equal to 0.83. The experimental data of pyrolysis gases and starch were taken from Dufaud, et al [29].

Additionally, it could be seen that, when an evaluation of a value lower than 0.3 for k_c, the value of $(dP/dt)_{max}$ simulated would be in the same order of magnitude of the experimental data. Nevertheless, a lower value of the k_c suggest that the combustion of wheat starch generates more tar and char than pyrolysis gases, which is contradictory at conditions of combustion inside the 20L Sphere test [29].

In the other hand, the performance of the CFD results reveals an inaccuracy since the maximum value of $(dP/dt)_{max}$ was reached at $k_c \neq 1$. That indicates that the stoichiometric F(dust)/A had some errors, because a generation of an excess of fuel at this point, as shown **Fig. 14**. Moreover, the results obtained in this study suggest the calculation of stoichiometric concentration of Wheat starch dust with a k_c close to 0.86.

Furthermore, regarding to the estimation of $k_c = 0.86$ as a close value to the stoichiometric relation between dust mass and air into the combustion inside the 20L Sphere test, there were made several test to validate the behavior at different (F/A) and compared with the experimental data found by Dufaud, et al. [29].

Fig. 15 shows that the general behavior of the CFD results are in agreement with the experimental data reported by Dufaud, et al [29]. Nonetheless, the discrepancy between the starch dust data and CFD are significantly, confirming the predominance and rate-limiting step of pyrolysis during explosions of organic dust [29], [41]. Moreover, the CFD data had better agreement with the experimental data of pyrolysis gases combustion, because of the lack on the CFD simulations of the influence of solid particles on turbulence during dispersion stage and the absence of the interference of the solid particles on heat transfer upstream the flame front [29], [40], [61], [62].

Furthermore, the disagreement between CFD data and pyrolysis gases combustion was decreased as the (F/A) was decreased. This suggests that a better estimation of the k_c is a value slightly higher than 0.86. For that reason, it is necessary to set a more reliable model than the k_c to emulate the behavior of organic dust combustion on 20L Sphere test.

4. CONCLUSIONS

The CFD model constructed provides a fully accurate prediction of the sphere pressure given that the deviations from the experimental points

(for the standard nozzle) do not overcome 8.6% for Wheat Starch and 5.5% for Carbon-black. Moreover, the initial agglomeration shape of Wheat starch does not have a considerable influence on the behavior of the sphere pressure with time. However, the geometrical differences between the nozzles and the turbulence levels reached in each case produce a variation of the pressure profile obtained.

The CFD model developed also leads to conclude that, during the dispersion step, the levels of turbulence undergo a significant decay at the first 20-30ms, followed by a less prominent decay up to the Ignition Delay Time that can be modelled by the inverse power-law relation proposed by Dahoe et al. [24]

On the other hand, the nozzle geometry modification marginally affects the de-agglomeration of Carbon-black particles on the sphere. However, the tendency is that the overriding stage of de-agglomeration is caused during the injection as the experimental and numerical results suggested, with a reduction of 68% and 45% of the mean diameter of Wheat starch and Carbon-black particles, respectively. This behavior is according to the high-pressure gradients when the particles moves through the canister exit to the nozzle, the baroclinic effect and the generation of rotary stresses. In addition, the PSD reduction with the cube configuration is closer to the experimental one than the obtained with the other shapes of Wheat starch. Therefore, this study suggested to use the Cube shape for future simulations that include agglomeration phenomena.

In addition, the real concentration is lower than the nominal concentration for all the different nozzle and agglomerates at the ignition time. For that reason, the MEC standard calculation has a significant disagreement. Nevertheless, the outlines of concentration ratio of carbon black with nozzle 6 develops a slightly better homogeneity, followed by nozzle, which can help to reduce the uncertainty in MEC determination.

Otherwise, the simulated combustion results show that the environment in which the pyrolysis gases are present at 60 ms is highly reactive, aided by the levels of turbulence that the system reaches. Moreover, the flame front is not perfectly spherical and, at certain times, has a preferred direction by the fact that there are still certain velocity gradients that direct the flame to a specific direction.

Additionally, the evaluation of $(dP/dt)_{max}$ of Wheat starch at different values of k_c have a significantly difference of one order of magnitude between the CFD and experimental data of combustion of the solid particles, validating the predominance and rate-limiting step of the pyrolysis during an organic dust explosion. Moreover, the use of a k_c to emulate the behavior of particles combustion is not practical, therefore it is necessary the study of the kinetics of the pyrolysis step of organic dust, as further work, to load to CFD software and generates a better fit to experimental data. Nevertheless, the CFD prediction has better agreement with the experimental data of pyrolysis gases combustion, because of the lack on the CFD simulations of the influence of solid particles on turbulence during dispersion stage and the absence of the interference of the solid particles on heat transfer upstream the flame front.

Finally, this study shows several uncertainties on assumptions and predictions of severity explosivity parameters on the 20L Sphere standard test, which affects the properly design of protection and safety devices. For that reason, it is suggested that a novel dust dispersion system should be considered to have more accurate and reliable results.

References

[1] A. Di Benedetto, P. Russo, R. Sanchirico, and V. Di Sarli, "CFD simulations of turbulent fluid flow and dust dispersion in the 20 liter explosion vessel," *AIChE J.*, vol. 59, no. 7, pp. 2485–2496, Jul. 2013.

[2] J. Cross and D. Farrer, *Dust Explosions*, First. New York: Plenum Publishing, 1982.

[3] R. K. Eckhoff, *Dust Explosions in the Process Industries*. 2003.

[4] T. Abbasi and S. A. Abbasi, "Dust explosions-Cases, causes, consequences, and control," *Journal of Hazardous Materials*, vol. 140, no. 1–2. pp. 7–44, 2007.

[5] P. R. Amyotte, "Some myths and realities about dust explosions," *Process Saf. Environ. Prot.*, vol. 92, no. 4, pp. 292–299, 2014.

[6] P. R. Amyotte and R. K. Eckhoff, "Dust explosion causation, prevention and mitigation: An overview," *J. Chem. Heal. Saf.*, vol. 17, no. 1, pp. 15–28, 2010.

[7] D. B. Mercer *et al.*, "The influence of injector design on the decay of pre-ignition turbulence in a spherical explosion chamber," *J. Loss Prev. Process Ind.*, vol. 14, no. 4, pp. 269–282, 2001.

[8] R. K. Eckhoff, "Understanding dust explosions. The role of powder science and technology," *J. Loss Prev. Process Ind.*, vol. 22, no. 1, pp. 105–116, 2009.

[9] A. Di Benedetto, P. Russo, P. Amyotte, and N. Marchand, "Modelling the effect of particle size on dust explosions," *Chem. Eng. Sci.*, vol. 65, no. 2, pp. 772–779, 2010.

[10] A. Di Benedetto *et al.*, "Flame Propagation of Dust and Gas-Air Mixtures in a Tube," *Chia Laguna, Cagliari, Sardinia*, vol. 1, pp. 11–13, 2011.

[11] G. Colonna, "Credible Risk," *NFPA J.*, 2015.

[12] O. Kalejaiye, P. R. Amyotte, M. J. Pegg, and K. L. Cashdollar, "Effectiveness of dust dispersion in the 20-L Siwek chamber," *J. Loss Prev. Process Ind.*, vol. 23, no. 1, pp. 46–59, 2010.

[13] ISO 6184-1, *Explosion protection systems. Part 1 : Determination of explosion indices of combustible dusts in air*, vol. 23, no. 1. 1985.

[14] ASTM, "ASTM E1226-12a Standard Test Method for Explosibility of Dust Clouds," *ASTM Int.*, pp. 1–13, 2012.

[15] ASTM, "ASTM E2019 - 03 Standard Test Method for Minimum Ignition Energy of a Dust Cloud in Air," *ASTM Int.*, pp. 1–13, 2003.

[16] A. G. Dastidar, "ASTM E2931: A new standard for the limiting oxygen concentration of combustible dusts," *Process Saf. Prog.*, vol. 35, no. 2, pp. 159–164, 2016.

[17] ASTM, "ASTM E1515-14: Standard Test Method for Minimum Explosible Concentration of Combustible Dusts," *ASTM Int.*, pp. 1–9, 2014.

[18] ASTM, "ASTM E1491 - 06(2012) Standard Test Method for Minimum Autoignition Temperature of Dust Clouds," *ASTM Int.*, pp. 1–12, 2012.

[19] R. Sanchirico, V. Di Sarli, P. Russo, and A. Di Benedetto, "Effect of the nozzle type on the integrity of dust particles in standard explosion tests," *Powder Technol.*, vol. 279, pp. 203–208, 2015.

[20] D. Vizcaya *et al.*, "CFD as an approach to understand flammable dust 20 L standard test: Effect of the ignition time on the fluid flow," *AIChE J.*, vol. 64, no. 1, pp. 42–54, Jan. 2018.

[21] J. Yuan, W. Huang, H. Ji, N. Kuai, and Y. Wu, "Experimental investigation of dust MEC measurement," *Powder Technol.*, vol. 217, pp. 245–251, 2012.

[22] Q. Zhang and B. Zhang, “Effect of ignition delay on explosion parameters of corn dust/air inconfined chamber,” *J. Loss Prev. Process Ind.*, vol. 33, pp. 23–28, 2015.

[23] A. E. Dahoe *et al.*, “Dust Explosions in Spherical Vessels : prediction of the pressure evolution and determination of the burning velocity and flame thickness,” *Proc. 7th Int. Colloq. Dust Explos.*, pp. 67–87, 1996.

[24] A. E. Dahoe, R. S. Cant, and B. Scarlett, “On the decay of turbulence in the 20-liter explosion sphere,” *Flow, Turbul. Combust.*, vol. 67, no. 3, pp. 159–184, 2002.

[25] A. E. Dahoe, R. S. Cant, M. . Pegg, and B. Scarlett, “On the transient flow in the 20-liter explosion sphere,” *J. Loss Prev. Process Ind.*, vol. 14, no. 6, pp. 475–487, 2001.

[26] B. Du *et al.*, “Visualization and analysis of dispersion process of combustible dust in a transparent Siwek 20-L chamber,” *J. Loss Prev. Process Ind.*, vol. 33, pp. 213–221, 2015.

[27] C. Murillo *et al.*, “Proposal of a new injection nozzle to improve the experimental reproducibility of dust explosion tests,” *Powder Technol.*, vol. 328, pp. 54–74, 2018.

[28] C. Murillo, “Experimental and numerical approaches to particles dispersion in a turbulent flow: application to dust explosions,” Université de Lorraine, 2016.

[29] O. Dufaud *et al.*, “Comparing pyrolysis gases and dusts explosivities: A clue to understanding hybrid mixtures explosions?,” *Industrial and Engineering Chemistry Research*, vol. 51, no. 22. pp. 7656–7662, 2012.

[30] N. Cuervo, “Influences of turbulence and combustion regimes on explosions of gas-dust hydrid mixtures,” University of Lorraine, 2015.

[31] P. G. J. van der Wel, J. P. W. van Veen, S. M. Lemkowitz, B. Scarlett, and C. J. M. van Wingerden, “An interpretation of dust explosion phenomena on the basis of time scales,” *Powder Technol.*, vol. 71, no. 2, pp. 207–215, 1992.

[32] S. Callé, L. Klaba, D. Thomas, L. Perrin, and O. Dufaud, “Influence of the size distribution and concentration on wood dust explosion: Experiments and reaction modelling,” in *Powder Technology*, 2005, vol. 157, no. 1–3, pp. 144–148.

[33] K. L. Cashdollar, “Coal dust explosibility,” *J. Loss Prev. Process Ind.*, vol. 9, no. 1 SPEC. ISS., pp. 65–76, 1996.

[34] R. Soundararajan, P. R. Amyotte, and M. J. Pegg, “Explosibility hazard of iron sulphide dusts as a function of particle size,” *J. Hazard. Mater.*, vol. 51, no. 1–3, pp. 225–239, 1996.

[35] R. K. Eckhoff, “Does the dust explosion risk increase when moving from µm-particle powders to powders of nm-particles?,” *J. Loss Prev. Process Ind.*, vol. 25, no. 3, pp. 448–459, 2012.

[36] T. Skjold, B. J. Arntzen, O. R. Hansen, I. E. Storvik, and R. K. Eckhoff, “Simulation of dust explosions in complex geometries with experimental input from standardized tests,” in *Journal of Loss Prevention in the Process Industries*, 2006, vol. 19, no. 2–3, pp. 210–217.

[37] Z. Salamonowicz, M. Kotowski, M. Półka, and W. Barnat, “Numerical simulation of dust explosion in the spherical 20l vessel,” *Bull. Polish Acad. Sci. Tech. Sci.*, vol. 63, no. 1, pp. 289–293, 2015.

[38] R. Redlinger, “Numerical simulation of hybrid dust/gas explosion experiments in the standard 20-L sphere,” *Fusion Eng. Des.*, vol. 100, pp. 419–424, 2015.

[39] A. K. Prasad, “Particle image

velocimetry," *Curr. Sci.*, vol. 79, no. 1, pp. 51–60, 2000.

[40] D. Torrado, N. Cuervo, S. Pacault, P. A. Glaude, and O. Dufaud, "Influence of carbon black nanoparticles on the front flame velocity of methane/air explosions," *J. Loss Prev. Process Ind.*, vol. 49, pp. 919–928, 2017.

[41] N. Cuervo, O. Dufaud, D. Torrado, N. Bardin-monnier, L. Perrin, and A. Laurent, "Experimental Study and Modelling of the Pyrolysis of Organic Dusts : Application to Dust Explosions," vol. 31, pp. 931–936, 2013.

[42] O. Bozier, "Contribution à l'étude des caractéristiques de combustion isochores d'une suspension de particules solides réactives. Génération de la suspension, influence de l'état initial du mélange," Universitè de Poitiers, 2004.

[43] H. Zhang *et al.*, "Effects of particle size on flame structures through corn starch dust explosions," *J. Loss Prev. Process Ind.*, vol. 50, pp. 7–14, 2017.

[44] T. Lu and C. K. Law, "A criterion based on computational singular perturbation for the identification of quasi steady state species: A reduced mechanism for methane oxidation with NO chemistry," *Combust. Flame*, vol. 154, no. 4, pp. 761–774, Sep. 2008.

[45] Siemens PLM, "STAR-CCM+ Simcenter Documentation," 2018. [Online]. Available: https://documentation.thesteveportal.plm.automation.siemens.com/starccmplus_latest_en/index.html?param=XxShn&authLoc=https://thesteveportal.plm.automation.siemens.com/AuthoriseRedirect.

[46] C. Murillo, N. Bardin-monnier, C. Blanchard, F. Munoz, N. Ratkovich, and D. Vizcaya, "CFD to Improve the Repeatability and Accuracy of Dust Explosion Tests in the 20-liters Sphere," *Chem. Eng. Sci.*, vol. 48, no. January, pp. 115–120, 2016.

[47] D. C. Wilcox, *Turbulence modeling for CFD*. 1993.

[48] S. R. Shah, S. V. Jain, R. N. Patel, and V. J. Lakhera, "CFD for centrifugal pumps: A review of the state-of-the-art," *Procedia Eng.*, vol. 51, no. NUiCONE 2012, pp. 715–720, 2013.

[49] C. Murillo, N. Bardin-Monnier, F. Muñoz, and O. Dufaud, "Application of CFD on the sensitivity analyses of some parameters of the modified Hartmann tube," *J. Loss Prev. Process Ind.*, vol. 36, pp. 296–307, 2015.

[50] H. Zhou, K. Cen, and J. Fan, "Detached eddy simulation of particle dispersion in a gas-solid two-phase fuel rich/lean burner flow," *Fuel*, vol. 84, no. 6, pp. 723–731, 2005.

[51] M. Wang, C. H. Lin, and Q. Chen, "Advanced turbulence models for predicting particle transport in enclosed environments," *Build. Environ.*, 2012.

[52] R. Ben Moussa, M. Guessasma, C. Proust, K. Saleh, and J. Fortin, "Thermal radiation contribution to metal dust explosions," in *Procedia Engineering*, 2015, vol. 102, pp. 714–721.

[53] H. Yu, W. Cheng, L. Wu, H. Wang, and Y. Xie, "Mechanisms of dust diffuse pollution under forced-exhaust ventilation in fully-mechanized excavation faces by CFD-DEM," *Powder Technol.*, vol. 317, pp. 31–47, 2017.

[54] A. Di Renzo and F. P. Di Maio, "Comparison of contact-force models for the simulation of collisions in DEM-based granular flow codes," *Chem. Eng. Sci.*, vol. 59, no. 3, pp. 525–541, 2004.

[55] D. Torrado, "Effect of carbon black nanoparticles on the explosion severity of gas mixtures," Université de Lorraine, 2017.

[56] M. Amin, "EXPERIMENTAL AND COMPUTATIONAL ASSESSMENT OF THE STANDARD TEST FOR

DUST CHARACTERIZATION BASED ON THE DEGREE OF AGGLOMERATION AND DE-AGGLOMERATION," Universidad de los Andes, 2017.

[57] A. Pinilla, "CFD study on the incidence of the change of nozzle on the dust dispersion in the 20 liters sphere.," Universidad de los Andes, 2017.

[58] P. Orlandi and J. Jiménez, "On the generation of turbulent wall friction," *Phys. Fluids*, vol. 6, no. 2, pp. 634–641, 1994.

[59] C. Weiler, M. Wolkenhauer, M. Trunk, and P. Langguth, "New model describing the total dispersion of dry powder agglomerates," *Powder Technol.*, vol. 203, no. 2, pp. 248–253, Nov. 2010.

[60] L. A. Turkevich, A. G. Dastidar, Z. Hachmeister, and M. Lim, "Potential explosion hazard of carbonaceous nanoparticles: Explosion parameters of selected materials," *J. Hazard. Mater.*, vol. 295, pp. 97–103, 2015.

[61] D. Torrado *et al.*, "Numerical study of the influence of particle reaction and radiative heat transfer on the flame velocity of gas/nanoparticles hybrid mixtures," *Process Saf. Environ. Prot.*, vol. 118, pp. 211–226, 2018.

[62] D. Torrado, P. Glaude, and O. Dufaud, "Effect of carbon black nanoparticles on methane/air explosions: Influence at low initial turbulence," *J. Phys. Conf. Ser.*, vol. 838, p. 012022, Jun. 2017.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

A Risk-based Dust Hazard Analysis (DHA)

Fuman Zhao*, Robert Weber
PSRG Inc.
800 W Sam Houston Pkwy S # 107, Houston, TX 77042
(713) 532-8800
*Presenter Email: fumanzhao@psrg.com

Keywords: combustible dust, dust hazard, risk-based, dust hazard analysis (DHA)

Abstract

Combustible dusts are finely divided particles that present an explosion hazard when suspended in air. Dust explosion may become more severe in a confined space, especially due to the occurrence of second dust explosion. Combustible dust explosions have caused numerous fatalities and catastrophic property damages in industries. They are now a recognized hazard that plant owners, managers, and workers cannot ignore. Many industry-specific NFPA dust standards (e.g., NFPA 61, 484, 655, 664) on combustible dust contain provisions for conducting DHAs. NFPA 654 applies to general combustible dusts for preventing combustible dust flash fires and explosion, which requires designing the fire and explosion safety provisions based on the dust PHA. The newest standard of NFPA 652 (Standard on the Fundamentals of Combustible Dust) became effective on September 7, 2015. It requires that dust hazards analysis (DHA) be completed on existing facilities and significant modifications before September 7, 2018. Assessment of what can go wrong, however, may not be an easy task for dust-handling plants. NFPA performance-based dust hazard assessment and OSHA regulatory compliance requirements lack detailed guidance on how to conduct DHA. Meanwhile, standard or code-based prescriptive DHA may create redundantly unnecessary overprotection for hazard-involved dust processes and equipment. In this research, a risk-based approach is developed by incorporating both likelihood analysis and consequence analysis to define safeguard requirements for any of potential process deviations, operating upsets, human errors, and equipment failures. By comparing safeguard requirements with the credit provided through safeguard availability analysis, a risk-based DHA will provide a sufficient understanding of dust hazards, as well as the safeguard level of demand for dust process safety work activity.

1. Background

A great many finely divided solid matters represent a serious industrial problem. A dust hazard, especially a dust explosion, is a great threat to industries handling combustible dusts. The U.S. Chemical Safety Board reported 281 major dust explosion incidents, which killed 119 workers and injured 718 more, from 1989 to 2005 [1]. Primarily the dust explosions are common in coal mining, flour milling, and grain storage [2]. Frank gives incident data reported by US CSB and FM Global, which illustrate that dust explosions have mainly occurred in the following industries [3]:

- Wood and paper products (e.g., dust from sawing, cutting, and grinding, etc.);
- Grain and foodstuffs (e.g., grain dust, flour);
- Metal and metal products (e.g., metal powders and dusts);
- Power generation (e.g., pulverized coal, peat and wood);
- Chemical process industry (e.g., acetate flake, pharmaceuticals, dyes, pesticides);
- Plastic/polymer production and processing;
- Mining (e.g., coal, sulfide ores, sulfur); and
- Textile manufacturing (e.g., linen flax, cotton, wool).

2. Dust Hazards

Any oxidizable material with sufficiently small particle sizes, under the right circumstances, is potentially capable of combustion. Combustible dust presents three types of combustible hazards: dust explosion, flash fire, and smoldering fires. A dust explosion is the most severe of these hazards.

A dust explosion requires five necessary conditions: fuel, oxidizer, suspension, ignition source, and containment, which is normally symbolized as a dust explosion pentagon. When dust disperses in air within a non-congested area or an open space, a rapidly burning flash fire can result at a certain range of dust concentration. Dust flash fires can cause fatal injuries. Dusts that settle on a hot surface (e.g., motors or steam piping) may develop smoldering and potentially auto-ignite due to exothermic oxidation. Dust smoldering fires can also occur in bulk solids in the absence of hot surfaces. If a dust layer is thick enough to prevent heat from escaping, the heat from oxidation can cause smoldering to continue. Smoldering fires themselves may not be immediately hazardous to people, but they can act as ignition sources for flash fires and explosions, as well as a source of toxic gases (e.g., CO) emission.

A Dust explosion domino can occur due to the secondary or tertiary dust explosions triggered by the initial one. That is usually the main contributor to the severe losses in the solid-processing industries. When the overpressure produced from the initial explosion reaches a dust layer, a potentially large amount of dust could be dispersed and ignited by the initial dust flames, resulting in far more destructive overpressure. Moreover, secondary or tertiary dust explosions are often observed far from the location where the primary one occurs, which induces difficulties in safety measure application.

Dust explosion DDT (deflagration-to-detonation) is a particularly hazardous event. It may cause an overpressure that is much greater than the strength of most industrial buildings. In a dust explosion accident, a detonation is unlikely to occur spontaneously. It usually requires a DDT

event. A DDT develops typically due to a dust flame propagation into a confined space combining with secondary/tertiary dust explosions.

3. Regulations and Standards for Dust Hazards Controlling

As a primary regulatory organization in charge of process safety, U.S. Occupational Safety and Health Administration (OSHA) began its combustible dust National Emphasis Program (NEP) in October 2007 to help lower the risk of workers being exposed to explosive dust hazards. In March 2008, OSHA issued the OSHA Fact Sheet of "Hazard Alert: Combustible Dust Explosions" to address the importance of dust hazard awareness. "In many combustible dust incidents, employers and employees were unaware that a hazard even existed. It is important to determine if a company has this hazard and, if it does, an action must be taken now to prevent tragic consequences [4]". From this Fact Sheet, OSHA also requires a thorough dust hazard analysis for all dust handled, all operations conducted (including by-products), all spaces (including hidden ones), and all potential ignition sources. In 2009, OSHA published Hazard Communication Guidance for Combustible Dust (OSHA 3371-08). This guidance is not a regulation, but an advisory document to help manufacturers and importers of chemicals recognize the potential for dust explosion and to identify appropriate protective measures as part of their hazard determination under the Hazard Communication Standard (HCS). As mandatory requirements, the following Federal OSHA standards address certain aspect of combustible dust hazards [5]:

- 29 CFR 1910.22 Housekeeping
- OSH Act: Section 5(a)(1) General Duty Clause
- 29 CFR 1910.94 Ventilation
- 29 CFR 1910.272 Grain Handling Facilities
- 29 CFR 1910.176 Housekeeping in Storage Areas
- 29 CFR 1910.269 Housekeeping at Coal-handling Operations
- 29 CFR 1910.1200 Hazard Communications
- 29 CFR 1910.178 Powered Industrial Trucks
- 29 CFR 1910.307 Hazardous (Classified) Locations
- 29 CFR 1910.132 Personal Protective Equipment (PPE)
- 29 CFR 1910.119 Process Safety Management
- 29 CFR 1910.252 Welding, Cutting, and Brazing Operations

In addition to OSHA standards, there are several industry consensus standards that address combustible dust issues. The primary National Fire Protection Association (NFPA) consensus standards and documents related to dust hazards include:

- NFPA 61, Standard for the Prevention of Fire and Dust Explosions in Agricultural and Food Processing Facility.
- NFPA 484, Standard for Combustible Metals.
- NFPA 655, Standard for the Prevention of Sulfur Fires and Explosions.
- NFPA 664, Standard for the Prevention of Fires and Explosions in Wood Processing and Wood-working Facility.
- NFPA 68, Standard on Explosion Prevention by Deflagration Venting.
- NFPA 69, Standard on Explosion Prevention Systems.

- NFPA 499, Recommended Practice for the Classification of Combustible Dusts and Hazardous (Classified) Locations for Electrical Installations in Chemical Process Areas.
- NFPA 77, Recommended Practice on Static Electricity.
- NFPA 654, Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids.
- NFPA 652, Standard on the Fundamentals of Combustible Dust.
- NFPA Fire Protection Handbook.

NFPA 652 was released in September 2015. It requires a dust hazard analysis (DHA) for those facilities and operations that manufacture, process, blend, convey, repackage, generate, or handle combustible dusts or particulate solids. A DHA for the existing facilities can be retroactive. The time limit to finish the DHA is three years from the date the standard became effective.

In addition to NFPA standards, OSHA has also referenced FM7-76, Prevention and Mitigation of Combustible Dust Explosions and Fires for dust hazard controlling. Some state and local fire codes may apply. There are two predominant model fire codes (International Code Council's International Fire Code, and NFPA's Uniform Fire Code) adopted by many jurisdictions.

4. A Risk-Based DHA

Based on CCPS's definition, a risk is a measure of human injuries, environmental damages, or economic losses in term of both the incident likelihood and the magnitude of the loss or injury. A risk-based DHA is a risk-analyzed approach for dust hazards identification and evaluation, which inherently includes the consequence prediction from a dust fire/explosion/toxic hazard and its likelihood estimation. A risk-based DHA can provide organizations with a method to implement risk tolerance criteria. It also provides a logical method of demonstrating that a performance-based protection option meets the intent of a regulatory or standards-based option. A risk-based approach may also be useful if standards don't have a prescriptive requirement for a particular piece of equipment [6].

In this paper, a systematic procedure is developed for a risk-based DHA study, which is illustrated in Figure 1 and discussed below in details.

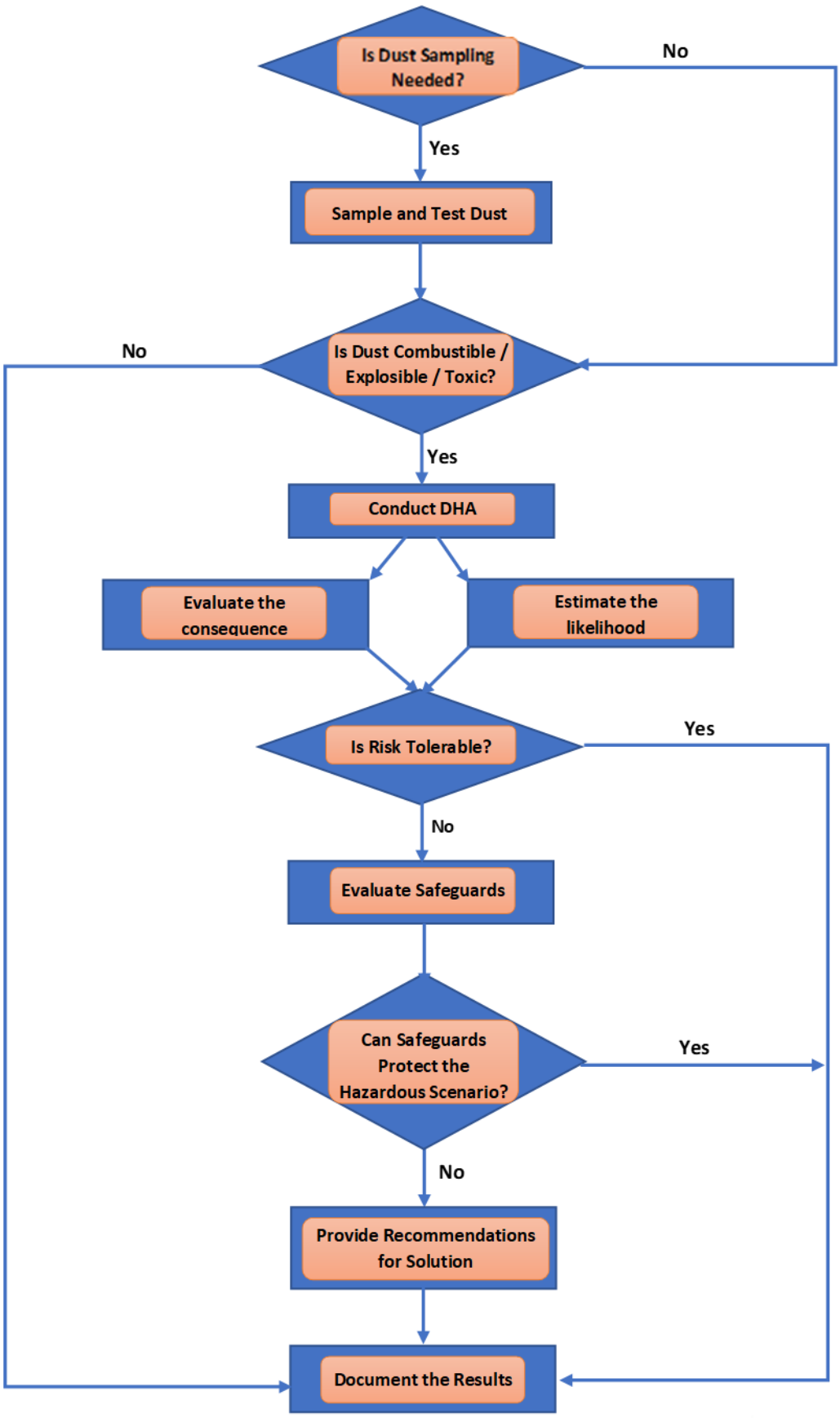


Figure 1 Flowchart for a Risk-based DHA

4.1 Dust Sampling

To identify dust hazards, a dust sampling plan should be developed and documented to provide data as needed to comply with the requirements from NFPA 652. Dust sampling may be optional under certain conditions, e.g., (1) Existing dust sampling/testing data are good representatives of the materials in dust process equipment or collected on surfaces at their near locations; or (2) Dust sampling/testing data are available from facility historical records or literature resources, which can be verified to be good representations of currently processing materials and operating conditions; or (3) Processing dust material is unlikely to be combustible or explosible. Material Safety Data Sheets (MSDS) are not reliable sources for a dust hazard identification. The U.S. Chemical Safety Board (CSB) reviewed the MSDS of 140 known substances that produce combustible dusts and found that 41% of the MSDS did not warn users about potential explosion hazards [1].

A successful dust sampling plan should include the following [7]:

- Identification of all the locations where dusts are present
- Identification and collection of representative samples
- Preservation of dust sample integrity
- Communication with the test laboratory regarding dust handling
- Documentation of samples taken

4.2 Dust Sample Testing

A number of dust physical properties (e.g., dust particulate size, moisture content, volume electrical resistance, etc.) and explosion parameters (e.g., K_{st}, P_{max}, MEC, MIE, MAIT, LOC, etc.) are commonly needed for a dust hazard analysis, particularly for a dust ignition probability analysis and a fire/explosion consequence prediction.

In general, dust sample testing shall be run on the materials as sampled. Many test procedures call for the sample to be dried to less than 5% moisture and screened, and the test run on material less than 200 mesh (75 microns) in size. This is done to represent a worst case for determining a material combustibility or explosivity property, but sometimes can be overly conservative.

To determine whether a dust has an explosion hazard or not, a “Go/No-Go” explosibility screening test is normally used by following ASTM E1226 standard. The pressure rise in the testing chamber is measured. If the ratio of the final pressure from the deflagration to the initial pressure is higher than 2, the dust is considered to be explosible. When the dispersed dust concentration in air falls within its flammability range, dust ignitibility is mainly dependent on the minimum ignition energy (MIE) if an ignition source exists, or the minimum autoignition temperature (MAIT) when no credible ignition sources are available. Dust MIE data can be collected by following the ASTM E2019 standard. ASTM E1491 provides the detailed guidance on MAIT testing. For dust layer fire due to a hot surface, a standard test by following ASTM E2021 can be applied. The parameters of dust minimum explosible concentration (MEC) and limiting oxygen concentration (LOC) are mostly referred for dust cloud inerting or dust flash fire/explosion prevention. The related standards ASTM E1515 and ASTM E2931 are designated for dust MEC and LOC testing, respectively.

4.3 Conduct a Risk-based DHA

Whenever a facility is determined to have combustible or explosible dust materials, the facility owner/employer shall be responsible to ensure a DHA is completed in accordance with the requirements of NFPA 652, as well as to comply with other applicable regulations and standards.

A DHA is designed to identify and evaluate dust-involved hazards to personnel, property, or the environment. Dust hazards may include flash fire, layer fire, explosion, or toxicity. A risk-based DHA analyzes a dust hazard's consequence, and the corresponding likelihood. A risk value will be assigned to each of the specific hazardous events, and then compared with organization's risk criteria to recommend prevention or mitigation measures if necessary. Similar to a typical HAZOP process hazard analysis, a risk-based DHA is a qualitative approach, which includes a systematic logic flow as follows:

4.3.1 Identify Initial Events

To be consistent with the requirements from NFPA 652, a dust hazard analysis should consider the combustible hazardous dusts present within the equipment, or dust accumulation on surfaces within buildings or building compartments. Dusts outside of buildings are not within the DHA scope unless frequent personnel exposures happen. If a large amount of toxic dusts or their by-products release to atmosphere, both onsite and off-site safety and/or environmental concerns are included in the risk-based DHA.

Based on insurance organization's data, FM-Global provides a list of common process equipment involved in dust fires and explosions [8]: air-material separators (e.g., cyclones, baghouse filters, cartridge filters); solid size reduction equipment (e.g., grinders, mills); dryers (e.g., spray dryers, flash dryers, fluid bed dryers, agitation dryers); dust storage vessels (e.g., silos, hoppers); conveyors (e.g., screw conveyers, belt conveyers, bucket conveyers, pneumatic conveyers); portable containers (e.g., RIBCs, FIBCs, fiber drums); blenders/mixers; and others. Dusts in equipment can always be treated as in a confined space. For most of dust-involved processes, air is present in the equipment therefore, dust explosion contingencies are primarily based on the potential ignition source's identification.

In the absence of good housekeeping practices, the accumulation of dust on different surfaces can occur slowly through nearly invisible fugitive dust leaks. In addition to floors under and around processing equipment, dust accumulation can occur on any horizontal or slightly inclined surface, including beams and supports, ledges, conduit and pipe racks, cable trays, ducts, above suspended ceilings, etc. Such surfaces can easily have enough dust to create a dust fire, or a worse dust explosion hazard, especially the secondary or tertiary dust explosions in congested areas. A risk-based DHA is required for a building with poor dust housekeeping. Same to the dust hazard contingencies analysis within equipment, potential ignition sources introduction or generation within the buildings will be analyzed systematically.

Process deviations within a pre-noded operation are the basis for dust hazards initial events identification. Compared with a typical HAZOP study, some generally applied parameters, e.g., temperature, pressure, flow, and level, may work but could not well represent an abnormal operation. For example, a high or low temperature is not normally a credible scenario as most dust processes are at ambient conditions; a high or low dust flowrate is not the dependence for dust explosion severity but a potential for the secondary or tertiary explosion. In a risk-based

DHA, any potential ignition sources introduction or generation is applied as a process deviation to identify a dust hazard initial event. Potential ignition sources may be an open flame, a hot surface, a mechanic/electrical spark, overheating from mechanical friction or abnormal heat input, an electrostatic discharge, or others. Here are some typical examples for a dust-involved process deviation:

- Overheating from mechanical friction, e.g., lubrication loss to a bearing, conveyer belt mis-alignment
- Overheating from an abnormal heat input, e.g., a control valve leading to more hot air inflow into a dryer
- Smoldering from a dust layer decomposition or reaction
- Loss of cooling
- Hot surfaces, e.g., furnaces, electrical motor, or exchangers
- Open flames
- Hot work, e.g., cutting, welding, and grinding
- Mechanic spark from, e.g., tramp metal, loss of hammer, or friction
- Ignition sources from an upstream feed
- Electrical spark/arc generated from electrical equipment
- Electrostatic discharge
- External events, e.g., Incident fires
- Industrial truck
- Others

4.3.2 Predict Dust Hazard Severity

An uncontrolled initial event may propagate into any of the ultimate consequences, e.g., onsite or off-site injuries or fatalities, property losses, and/or environment damages. As an example, Table 1 describes the dust hazard consequence categories.

Table 1 Risk-based DHA Consequence Categories

Category	Description	Onsite/Off-site People	Business/Asset	Environment
A	Catastrophic	Public: Serious injury or fatality Onsite: Several fatalities (≥ 2)	> 10 M dollars of loss	Large uncontained toxic release off-site
B	Very Serious	Public: Medical treatment Onsite: 1 fatality, or permanent disabilities	1 M – 10 M dollars of loss	Moderate toxic release off-site
C	Serious	Public: No impact Onsite: no fatality, irreversible disabilities	100 K – 1 M dollars of loss	Minor reportable toxic release off-site
D	Minor	Public: No impact Onsite: Minor reversible injuries	10 K – 100 K dollars of loss	On-site clean-up

In this risk-based DHA, prediction of dust hazard severity is a qualitative estimation in term of the combination effect from different factors, for example, dust combustibility or explosibility (e.g., K_{st}, P_{max}, $(dP/dt)_{max}$), dust toxicity (e.g., exposure limits on 8-hours TWA), dust physical properties (e.g., particulate size and moisture content), occupancy nearby, dust dispersion space and confinement, hybrid mixture, secondary dust explosion tendency, and so on. For a dust explosion, its severity will become worse if the dusts are:

- More finely divided
- Higher K_{st}, or more reactive
- More irregularly shaped
- With less moisture content, or drier
- Less agglomerated
- Slightly higher than the stoichiometric concentrations
- Larger amount of dust dispersion
- More turbulent conditions
- With a more confined degree
- Combustible gas/vapor contained (a hybrid system)

4.3.3 Estimate likelihood

Normally, the likelihood of a dust-involved failure scenario could not simply be taken as the frequency of initiating event. The probability of the series of other unplanned events needs to occur to lead to an undesirable consequence. For example, the presence of credible ignition sources, or the presence of suspended dust within the explosible range. The probability of occupancy is commonly used as a frequency modifier based on the data of time-at-risk. Eq. (1) below gives the formula to calculate the overall likelihood of a dust explosion failure scenario before safeguards are applied.

$$P_t = P_e \times P_i \times P_s \times P_r \qquad \text{Eq. (1)}$$

Where,

P_t is the overall likelihood of a dust-involved failure scenario before safeguards are applied in the unit of times per one year.

P_e is the frequency of an initial event in the unit of times per one year. A reliable data source should be sought after from the facility historical incidents or near-miss data records, or other facilities with the similar process operations. Industrial generic databases, e.g., CCPS books, UK HSE, or US OGP can be referred for an initial event frequency estimation if the facility's specific failure data is not available. Table 2 lists some generic initial events failure frequency data based on a CCPS book [9].

P_i is the probability of a dust ignition, which is dependent on the presence of credible ignition sources. It is unitless. The value of probability is between 0 and 1, where 0 means very unlikely, and 1 is very likely. Probability of a dust ignition is closely related to dust material characteristics (e.g., MIE, MAIT, particle size, moisture content, etc.) when combustible dusts suspend in air within flammability limit range. Dahn, Reyes, and Kusmierz gave some ignition ease criteria for dust fire and explosion engineering hazards analysis (in Table 3 below) based on

different stimuli and the levels of stimuli [10]. Some common ignition sources and ignition probabilities are discussed below:

- Open flames: The probability of a dust ignition can be 1 since an open flame is generally capable of igniting any combustible dust.
- Overheating from mechanic friction: Friction from hot bearings or jammed belts represents a very high portion of ignition sources [8]. A very high temperature may generate from mechanic friction due to a loss of lubrication or misalignment. The probability of dust ignition can be conservatively taken to be 1 for a bearing friction [11].
- Hot work (e.g., cutting, grinding, welding): Hot work can release very high energy intensity heat or spark, which may have 100% of potential chance to ignite combustible dusts [11].
- Overheating from abnormal heat input or loss of cooling: Combustible dust MAIT is a main factor to be referred to for this type of ignition probability estimation. Attention should be paid to dust moisture loss during the abnormal heat input or loss of cooling phase, since a drier dust may have a much lower MAIT than the sampled one, and the ignition probability can increase dramatically.
- Mechanical impact/friction sparks: Combustible dust ignition probability from mechanical sparks depends on both its MIE and MAIT. The International Social Security Agency (ISSA) provides some guidance on dust cloud ignitability prediction using spark equivalent electrical energy and ignition temperature. Figure 2 gives an example based on steel grinding spark and steel friction spark [12], where the intersection of the MIE and MAIT can be located to identify whether dust is ignitable from a mechanical grinding/friction spark.
- Electrical Sparks or arcs: Electrical equipment can produce sparks or arcs that may ignite a dust cloud. Combustible dusts ignition by electrical arcs has very high probability (can be 1 for a conservative purpose). Electrical sparks to ignite a dust cloud can be similar to mechanical sparks depending on dust MIE and MAIT.
- Electrostatic discharges: Static electricity is often generated by the flow of solids during handling, transfer and processing. The susceptibility of combustible dust to ignition by electrostatic discharge is a function of the MIE of the dust. Table 4 includes the data of ignition probability based on MIE range for a dust ignitability analysis [11].
- Smoldering: Smoldering is a flameless combustion. If a smoldering dust pile is disturbed, it can lead to a dust deflagration in the form of flash fire or explosion. The likelihood of ignition for smoldering nests depends on the material being handled. An organization needs to determine this from historical information or appropriate testing.

P_s is the probability of the presence of a suspended dust within the explosible range. It is unitless. Most explosible dusts have the explosible range of 50-100 g/m^3 on the lean side, and 2-3 kg/m^3 on the rich one [13]. Per NFPA 654, a dust layer larger than 1/32 inch accumulated on surface areas of at least 5% of a room's floor or above ceiling presents a significant explosion hazard [14]. The probability of dust suspension in air to form a combustible dust-air mixture is highly dependent on the total dust amount, air stability, and dust movement conditions. For conservative purpose, this probability is normally taken to be 1 unless there is a firm basis for other values.

P_o is the probability of time at risk, which can be determined based on the fraction of time the "at-risk" condition exists. In general, it can be calculated using equation as Eq. (2).

$$P_r = {Hours\ at\ risk}/{Total\ hours\ (1\ year)} \qquad \text{Eq. (2)}$$

By combining the initial event frequency with all other applicable probabilities from frequency modifiers and/or other unplanned events, the likelihood of a dust-involved failure scenario can be estimated and categorized as described in Table 5. Note that the estimated likelihood is before safeguards applied.

Table 2 Initial Event Frequencies

Item	**Description**	**Frequency**
BPCS Control Loop	The process parameter controlled by the BPCS control loop deviates without the ability to recover on its own, resulting in a consequence of concern.	0.1/yr
Safety Controls, Alarms, and Interlocks (SCAI)	The spurious operation of SCAI may lead to an upset or other consequence of concern.	0.1 - 1/yr
Human Error (Routine task performed >= 1/week)	A human error occurs on a task that is performed at a frequency of once per week or more often. The consequences are dependent on the task being performed by the person.	1/yr
Human Error (Routine task performed 1/week to 1/month)	A human error occurs on a task that is performed at a frequency between once per week to once per month. The consequences are dependent on the task being performed by the person.	0.1/yr
Human Error (Routine task performed < 1/month)	A human error occurs on a task that is performed at a frequency of less than once per month. The consequences are dependent on the task being performed by the person.	0.01/yr
Pressure Regulator Failure	This scenario covers a self-contained pressure regulator in pressure reducing or backpressure service, operating in continuous control mode, which fails to operate as designed (opened or closed)	0.1/yr
Screw Conveyor Failure	The failure of the screw conveyor stops the process flow, resulting in an upstream and/or downstream upset or other consequence of concern.	1 to 10/yr
Screw Conveyor Overheating of Materials	Overheating of the conveyed material, potentially resulting in ignition or decomposition of material within the conveyor.	0.1/yr
Fan or blower failure	This loss of operation could result in process upset, with a number of possible consequences as a result of process deviation.	0.1/yr
Single Circuit Loss of Power	Complete or partial loss of local power due to a component failure in single circuit. Does not include frequency of site-wide power loss.	0.1/yr

Hose failure, leak and rupture	Applies to leaks or complete failure due to age, external damage, wear, etc.	0.1/yr (leak) 0.01/yr (rupture)

Table 3 Ignition ease criteria for dust fire and explosion hazard analysis

Stimuli	**Ease of Ignition**	**Levels of Stimuli**
Thermal (Heat)	Low Temperature	< 100 ^{O}C
	Medium Temperature	100 ^{O}C-300 ^{O}C
	High Temperature	> 100 ^{O}C
Electrostatic Discharge	Easy	< 5 mJ
	Moderate	5-30 mJ
	Difficult	30-200 mJ
	Hard to Ignite	> 200 mJ
Impact	Low Energy	0.5 kg-m
	Moderate Energy	0.5-5 kg-m
	High Energy	> 5kg-m
Friction	Easy	100-2000 psi@7fps
	Moderate	2000-15000 psi@7fps
	Hard to Ignite	> 15000 psi@7fps
Chemical Decomposition	Low	< 100 cal/gm
	Moderate	100-500 cal/gm
	Higher	500-1500 cal/gm
	Highest	> 1500 cal/gm

Table 4 MIE *vs.* dust ignition probability

MIE	**Ignition Probability**
0 – 10 mJ	1
10 – 100 mJ	0.1
>100 mJ	0.01

Table 5 Likelihood and Frequency code for a Risk-Based DHA

Likelihood P_t (times/yr)	**Unmitigated Event Frequency Code**	**Description**
≥ 1	1	Very frequent: occurs at least once per year

0.1 - 1	2	Frequent: likely occurs at least once in 10 years
0.01 – 0.1	3	Infrequent: likely occurs at least once in 100 years
≤ 0.01	4	Improbable: likely occurs less than once in 100 years

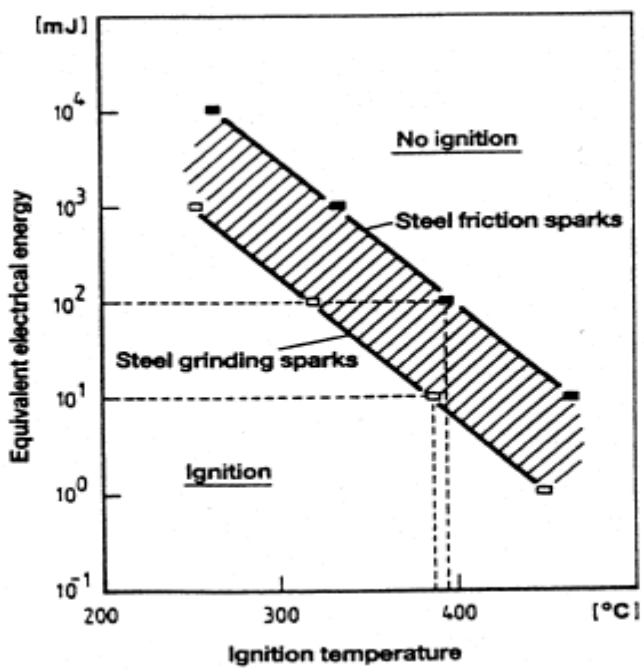


Figure 2 Conditions for ignition of dust by mechanical grinding and friction sparks.

4.3.4 Conduct Risk Ranking

By applying the organization approved risk matrix, each cause-consequence combination which constitutes a hazard scenario can be risk-ranked. As an example, Figure 2 shows the number of credible safeguards or independent protection layers (IPLs) required based on the initial event consequence and likelihood before safeguards applied, where risks are tolerable for failure scenarios of Severity “D”/Likelihood “3” and “4”, as well as Severity “C”/Likelihood “4”.

Likelihood

Consequence	**1**	**2**	**3**	**4**
A	4	4	3	2
B	4	3	2	1

C	3	2	1	NR
D	2	1	NR	NR

Figure 2 Risk Matrix for a Risk-based DHA

4.3.5 Determine Safeguard Credits

This step is designed to review and document credible safeguards or IPLs for prevention and/or mitigation of the consequences. Safeguards are engineered system(s) as defined in the P&IDs and other engineering information, and the administrative controls, such as operator response to alarms, that can prevent or mitigate the hazard including, but not necessarily limited to, such items as:

- Prevention safeguards
  - Prevent dust presence (e.g., no dust leakage)
  - Prevent dust dispersion (e.g., wet conditions, large particle size)
  - Control dust concentration outside of flammability range (e.g., inerting)
  - Remove ignition sources (e.g., no hot surface/flame, grounding and bonding, electrical area classification, control of hot work, lubrication, vibration/temperature monitoring)
- Mitigation safeguards
  - Explosion containment (e.g., vessel designed to contain explosion, install an explosion cover/shield)
  - Explosion suppression (e.g., inject explosion suppressants)
  - Explosion isolation (e.g., shut-off valve, rotary valve, physical barriers)
  - Explosion venting (e.g., overpressure venting and relief systems)
  - Fire and toxic response system (e.g., sprinklers, toxic powder/gas detectors)
- Administrative Safeguards
  - Housekeeping programs
  - Emergency response/PPE
  - Training programs

Each safeguard or IPL will be assigned a credit value. These values are obtained by referring to various databases and guidance books, such as CCPS and an example is shown in Table 6 [6, 15]. The assignment of the credit values should be verified with facility process engineers, operators and instrument professionals if extra information is needed.

4.3.6 Provide Recommendations

Based on the IPLs required and IPLs available, the gap will be calculated and the recommendations will be made if the IPLs required are less than credible safeguards or IPL credits. Additional IPLs recommended to be added should reduce the risk by: (1) preventing the consequences altogether via design alternatives; (2) lowering the likelihood of the failure scenarios; (3) and/or mitigating the consequences.

The risk-based DHA team should review the engineering design solutions or administrative controls to ensure that the proposed recommendations would sufficiently reduce the risk and not introduce new hazards or risks. After applying the recommended solutions, a revalidation of the failure scenarios should be conducted promptly to determine if the recommended solutions reduce the risk to an acceptable level.

During a risk-based DHA study, the DHA team may recommend some more detailed analysis, e.g., semi-quantitative LOPA, or quantitative QRA, for those failure scenarios with high severity or/and risk.

Table 6 Common Safeguards and Assigned Credits

Item	Description	credit
Safety Interlock	Safety interlocks prevent progression of a scenario to the consequence of concern following an initiating event.	1
SIS Loop	A SIS loop presents progression of a scenario following an initiating event.	SIL-1: 1 SIL-2: 2 SIL-3: 3
Explosion isolation valve	The explosion isolation valve protects against the propagation of flame between interconnected equipment.	1
Explosion panels on process equipment	Proper operation of explosion panels during an internal dust explosion can protect a vessel or duct from excessive overpressure.	2
Vent panels or enclosures	Vent panels prevent damage to an enclosure or room. However, activation of the panel does result in a pressure wave and loss of containment of dust. If the vent panel relieves into an occupied area, a vent panel may not be an effective IPL against impact to nearby workers.	2
Automatic fire suppression system	Within process equipment: the automated fire suppression system prevents propagation of a fire outside of process equipment.	1
Automatic fire suppression system	For local application: fire suppression systems for local application mitigate fires in small areas.	1
Automatic fire suppression system	For a Room: fire suppression systems mitigate fire in a room or small enclosure.	1
Human response to an abnormal condition	Human response to an abnormal condition can prevent a variety of possible consequences of concern.	1
Automatic explosion suppression system	The explosion suppression system protects against explosions that could cause equipment damage, including rupture. More quantitative analysis may support a lower PFD value for a specific system than the generic PFD provided.	1
Personal Protective Equipment (PPE)	PPE prevents consequences associated with exposure of people within the area of potential impact to a hazard of concern.	1
Dike	Will reduce the frequency of large consequences (widespread spill) of a tank overfill/rupture/spill etc.	2
Open Vent (no	Will prevent overpressure.	2

valve)		
Fireproofing	Will reduce rate of heat input and provide additional time for depressurizing/firefighting/etc.	2
Blast-wall/bunker	Will reduce the frequency of large consequences of and explosion by confining blast and protecting equipment/buildings/etc.	3
"Inherently Safe" Design	If properly implemented can significantly reduce the frequency of consequences associated with a scenario. Note: the LOPA rules for some companies allow inherently safe design features to eliminate certain scenarios (e.g., vessel design pressure exceeds all possible high-pressure challenges).	2
Flame/Detonation Arrestors	If properly designed, installed and maintained these should eliminate the potential for flashback through a piping system or into a vessel or tank.	2
Relief Valve	Prevents system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience.	2
Rupture Disk	Prevents system exceeding specified overpressure. Effectiveness can be very sensitive to service and experience.	2
Basic Process Control System	Can be credited as an IPL if not associated with the initiating event being considered.	1

4 Conclusion

For any facility with hazardous dusts that present an explosion, flash fire, layer fire, or toxic hazard, a dust hazard analysis is mandatorily required per NFPA 652. However, NFPA 652 lacks the detailed guidance on dust hazard assessment. Other industry-specified NFPA standards are mostly about the prescriptive DHA, which may not have a prescriptive requirement for a particular piece of equipment or may create unnecessary overprotection for some hazard-involved dust processes and equipment.

In this paper, a risk-based approach is developed by incorporating both likelihood and consequence to estimate the risk for any failure scenario. By applying the organization's risk tolerance criteria, a ranked risk value will be given to the analyzed scenario as the safeguard or IPL requirements. For any unacceptable consequence, safeguard availability review and IPL credit evaluation will be conducted. The gap between the IPL requirements and safeguard IPL credits will warn the risk-based DHA study team to provide risk-reduction recommendations. Compared to a prescriptive DHA, a risk-based DHA provides a sufficient understanding of dust hazards, as well as the appropriate safeguard level of demand for dust process safety work activity.

References:

[1] CSB, U.S., Chemical Safety and Hazard Investigation Board Investigation Report: Combustible dust hazard analysis, Report No. 2006-H-1, November 2006.

[2] Mannan, S.M., Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and control. ISBN: 0-7506-7857-7, Butterworth-Heinemann, MA: Elsevier, 2005.

[3] Frank, W.L., Dust Explosion and the Critical Importance of Housekeeping, Process Safety Progress, Vol 23 (3), 2004.

[4] OSHA, Hazard Alert: Combustible Dust Explosion, OSHA Fact Sheet, March 2008.

[5] OSHA, Combustible Dust: An Explosion Hazard, OSHA Standards.

[https://www.osha.gov/dsg/combustibledust/standards.html]

[6] CCPS, Guidelines for Combustible Dust Hazard Analysis, John Wiley & Sons, Inc., Hoboken, New Jersey, 2017.

[7] NFPA 652, Standard on the Fundamentals of Combustible Dust, National Fire Protection Association, 2016.

[8] FMG, Prevention and mitigation of combustible dusts, FM-Global Datasheet 7-76, Johnston, RI, 2013.

[9] CCPS, Guidelines in Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Center for Chemical Process Safety of American Institute of Chemical Engineers, New York, NY, 2015.

[10] Hahn, J.C., Reyes, B.N., and Kusmierz, A., A Methodology to Evaluate Industrial Vapor and Dust Explosion Hazards, Process Safety Progress, Vol. 19, Summer 2000.

[11] Howat, C.S., Tarverdi, D.F., and Hinkle, P.R., LOPA Application, Organization and Outcomes in the Food Processing Industry, Presentation to Global Congress for Process Safety, April 2006.

[12] ISSA, Working Group 6, Rules for dust explosion protection for machines and equipment–preventive and constructional measures. International Social Security Agency, Mannheim 1987.

[13] Eckhoff, R.K., Dust Explosion in the Process Industries, Elsevier Science, USA, 2003.

[14] NFPA 654, Standard for the prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids, National Fire Protection Association, 2013.

[15] CCPS, Layer of Protection Analysis: Simplified Process Risk Assessment, Center for Chemical Process Safety of American Institute of Chemical Engineers, New York, NY, 2001.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Advanced Fire Integrity Analysis and PFP Optimization Methods for Petrochemical Facilities

Dr. Necip Onder Akinci*, Krishna Parvathaneni, Dr. Abhimanyu Kumar[1], Hyun-Su Kim[1], Michael Stahl, Dr. Xiaowei Dai[1]
[1]*WS Atkins*
17220 Katy Freeway, Building 1 Suite 200, Houston, TX 77094, USA
[2]*Suncor Energy Services Inc.*
Calgary, AB, Canada
*Presenter E-mail: Onder.Akinci@atkinsglobal.com

Keywords: Fire integrity analysis, fire protection, facility siting, passive fire protection, API 2218, API RP-2FB, FABIG, intumescent, cementitious, flexible jacket, PFP, fire hazard analysis

Abstract

Design of process modules, piperacks and occupied structures for accidental fire loads is critical for a facility's operation, emergency planning, safe shutdown and evacuation strategy. In the oil and gas industry, hydrocarbon fire scenarios with high thermal loading should be accounted for. These accidental fire loads can be critical during the design phase. Recent improvements in fire analysis and design methodology for structures, piping systems and equipment are discussed in this study in regard to performance-based applications. Acceptance criteria for performance-based fire design have not been well documented in the literature. Prescriptive approach, utilization checks, limiting core temperatures, and deflection ratios or plastic strains for ductility level analysis are used as the basis of fireproofing requirements in the industry typically. However, actual response of safety critical elements supported by the subject structural members is typically not taken into account directly. Different acceptance criteria and response of supported piping systems are presented through case studies in this paper. Also, practical aspects of fire protection including three sided PFP application and coat-back optimization are discussed. For the structural fire integrity assessment, heat transfer and structural fire response analyses were performed utilizing USFOS and ABAQUS software packages.

Performance-based approach in fire response design of offshore and onshore structures has been successfully implemented using advanced numerical analysis tools and close collaboration between Safety, Structural, Construction and Operations teams. This approach involves an iterative analysis procedure considering interaction of load bearing (structural) and

other systems (piping, electrical etc.). The refined analysis and optimization process ensures that PFP is only applied to critical structural elements and fire performance of protected systems are verified through analysis. In addition to reducing the risk, this in turn precludes an overly conservative design recommending application of PFP in a broader area without analytical justification.

The main advantages of reducing application of PFP coating on non-critical members and equipment are cost savings and integrity management improvements during life cycle of a facility due to issues such as corrosion under insulation and long-term inspection and maintenance. Considering the fact that CAPEX and integrity management are major concerns for most structures at petrochemical facilities, optimization of PFP for plant structures has significant benefits for operators and owners of onshore and offshore assets. The integrated structural, foundation and equipment and piping systems fire analysis approach presented in this study is considered to be a significant addition to state of the art in fire protection design of oil & gas and petrochemical facilities. Improvements in analysis and design methods are expected to result in application of PFP at the critical locations only without compromising from safety requirements. This also ensures that safety critical elements are protected against credible hydrocarbon fire scenarios.

1. Introduction

Over the past few decades, steady increase in the consumption of energy has demanded for development of new facilities for oil and gas extraction and processing; both offshore and onshore. Due to the intrinsic nature of the Oil & Gas industry, fire is one of the main hazards threatening life and assets. When subjected to high thermal loading, the strength of structural components and safety critical equipment, piping and vessels degrade. The exact response and associated risk of potential escalation due to hydrocarbon fire depends on interaction between duration of fire event, heat flux, material properties, and the structural configuration. Therefore, risk assessment is essential for understanding the accident scenarios and for survival of structure and reducing vulnerability. This is also important for the development of appropriate mitigation solutions during every phase of a design project and repair planning during service life.

Several design standards around the world, such as American Petroleum Institute (API) [1] [2], British Standards (Eurocode) [3], and Det Norske Veritas (DNV) [4], recommend the use of active and passive fire protection systems for mitigation against accidental fires for offshore platforms and onshore plants. An active fire protection (AFP) system is a group of systems that require some amount of action or motion in order to work efficiently in the event of a fire, such as fire water deluge or sprinklers. On the contrary, a passive fire protection (PFP) is a structural and non-structural component that control the spread of fire and prevent or delay the collapse of structure/compartments such as firewalls and fire-retardant coatings. For safety critical structures, piping systems, vessels, and equipment PFP application is commonly utilized as a fundamental risk mitigation strategy.

During the pre-FEED and FEED stages of a design project, the PFP requirements for a structural component or safety critical equipment is based on simplistic/deterministic assumptions,

standards, and empirical calculations [3, 5]. With the evolution of project, more sophisticated methods such as that outlined in Fire and Blast Information Group (FABIG) Technical Note 11 [5] is often employed. The outlined methodology is a two-fold procedure: (1) Fire Risk Assessment (FRA), and (2) thermal-structural collapse analyses. FABIG [5] has also set out methodology to perform a detailed FRA to calculate Design Accidental Load (DAL). In this procedure, a risk-based approach is adopted to calculate DAL that takes into consideration of the probability of a fire event on the basis of the cumulative frequency of each fire scenario and the risk acceptance criteria. The obtained DAL is then utilized to assess the response of a structural system subjected to accidental fire loading. This analysis provides insights into the failure mechanism and structural collapse time for a given fire scenario that is used then to develop fire mitigation solutions as per process safety critical elements' survival duration requirements. Response information obtained from the aforementioned analysis is then utilized to determine the location and rating of PFP requirements for a facility.

Several research studies have been published on FRA methods [6, 7, 8, 9, 10]. These studies only estimate the risk associated with fire events. Very few researchers have considered FRA in conjunction with PFP requirements and optimization. For example, Shetty et al. [11] presented a theoretical method by utilizing probabilistic FRA to estimate the optimal design of PFP on offshore structures. De Sanctis et al. [12] proposed a reliability-based model to quantify the level of safety of prescriptive and performance-based steel building designs. Some researchers took experimental approach to assess the PFP requirements [13]. However, the use of large scale Finite Element Analysis (FEA) packages for determination and optimization of PFP is virtually lacking in literature. Hunt et al. [14] in 1997 utilized FEA to calculate the area and thickness requirements for PFP coating of the primary steel for the deck of the Mars Tension Leg Platform. In their work, the location of jet fire and pool fires were identified from a hazard analysis, which was utilized to calculate temperature flow of affected members of the primary members of the topsides as a function of time through heat transfer analysis. They found that that the temperature flow into the coated steel member is largely dependent on the thickness and composition of PFP coating. The "Zone" method of design in combination with 0.2% of strain assumption was employed to calculate the maximum allowable temperature for a critical structural member. The "Zone" method of design assigns a maximum allowable temperature that can develop in a steel member without reference to the stress level in the member prior to the fire [1]. To estimate the required PFP thickness and quality for the primary steel members due to localized jet fire under normal operating load conditions, ultimate strength analysis of the topsides was performed using USFOS FEA software package [15].

Similar techniques have been repeatedly reported for the optimization of PFP coating on steel structures [16, 17]. The common approach utilized in all these studies is to estimate fire loading scenarios using FRA followed by scenario based thermal structural analysis using USFOS. In the adopted procedure, progressive structural collapse analysis under thermal loading is performed by modeling an isolated structure with operating loads applied. The temperature dependent mechanical and thermal behavior of steel is captured by using the guidelines specified in FABIG [18] and Eurocode [3]. Through a series of thermal-structural collapse analysis, one or several coated members are removed, iteratively, from the protected members group to eliminate redundancy in PFP coating. Though this is useful during pre-FEED and FEED phase of a design project, such an approach often leads to conservative estimation of PFP coating requirements. The conservatism is attributed to the following reasons:

- The thermal-structural analysis does not account for the fire durations established through FRA studies;
- The assessment method takes the heat affected area into consideration in complete isolation without giving any credit for the possible escalation of hazard due to failure of any safety critical systems, such as piping, equipment, and collapse of neighboring structure;
- The loads due to processing equipment and systems are always active during the numerical simulation, irrespective of whether failure of a structural member has occurred or not. This does not take into consideration of possible loss of equipment/pipe support and subsequent redistribution of load.

To this end, authors propose a new more advanced methodology that attempts to eliminate the aforementioned deficiencies found in the commonly adopted approach. In the present work, we developed a PFP optimization method by adopting a multi-disciplinary approach to achieve a performance-based PFP scheme. In this, we perform non-linear thermal-structural analysis for whole topsides or a processing unit as one structural system. All process safety critical equipment and piping along with any neighboring structure are included in the FE Model. The temperature time history is obtained by a separate heat transfer analysis for both protected and unprotected members individually, which is later utilized in the stress analysis for the performance assessment and PFP optimization. In this study, we have taken advantage of the state of art ABAQUS FEA software package [19] which offers robust modeling capabilities as well as the capability to perform large scale simulations in short time. The proposed methodology is not only useful during detailed design phase but also can be utilized during the construction and execution phases of a project. Furthermore, the developed methodology can also assist in repair works during the operation of a facility.

2. Performance-based PFP Optimization Approach

Typical Passive Fire Protection Materials

For fire risk mitigation based on the result of Fire Integrity Assessment (FIA), Passive Fire Protection (PFP) materials are frequently applied to the structural members that are critical to prevent consequential hazards; i.e. contributing to the global stability and load-bearing in addition to integrity of safety critical elements.

Commonly used PFP types for structural members are Epoxy intumescent and lightweight cementitious types. Both are applied as a spray-coating to the substrates. Epoxy intumescent PFP materials contain thermally active chemicals for fireproofing. This type of PFP material is expands several times their volume when exposed to heat to form a protective char at the barrier that faces the fire [2]. Cementitious type PFP is another typical fireproofing material for the structures in relatively benign areas. However, cementitious PFP material may absorb relatively high moisture between the PFP layer and the substrate so that corrosion under fireproofing may bring problems for the steel structures [20]. Flexible Blanket type or endothermic warp type PFP are particularly suited for process equipment, piping systems, electrical cable trays or repair projects on operating plants. These are applied by surrounding the substrates with a couple of

composite panels or multiple layers. These materials can be directly added on to the existing insulations for fire protection purposes. For outdoor applications and protection against jet fire abrasion, stainless cladding or mesh is typically provided at the outer surface with proper fixation methods [2].

Performance-based Fire Integrity Assessment

Performance-based approach for FIA allows to understand structural fire response in rational basis and to estimate thermal capacity of the structures more accurately than prescriptive approach [2]. Following the performance-based approach for FIA, thermal response of the structural components subjected to fire loading should be defined, and PFP application to structural members shall be based on their relevance to global stability and criticality in terms of supported elements; i.e., process safety equipment such as vessels, piping and instruments. Since structural fire response is a complex problem [21], interaction of critical load carrying structural members and consideration of load redistribution during an accidental fire event should be taken into consideration. Therefore, a non-linear inter-disciplinary FIA is necessary for the engineering and optimization of PFP application.

For a reliable structural response, a multi-disciplinary approach has to be adopted while considering several important variables; such as impairment frequency, fire duration, leak probability, thermal material properties of the substrate and fireproofing material, and mechanical properties of the structural member, etc. From the structural reliability point of view, thermal material properties such as specific heat capacity, density, and thermal conductivity are essential to calculate temperature gradient for a structural member subjected to accidental fire loading. Eurocode [3] and FABIG [18] provide temperature dependent material properties for carbon steel and stainless steel. Flame emissivity, surface radiation emissivity, and convective heat transfer coefficient are, also, the important parameters that govern the response of a structural system depending on the fire type and the flame condition. The expected flame condition for hydrocarbon fire can be modeled according to the guidelines provided in Eurocode [3, 22] and API [1]. Thermal material properties of PFP vary by the product. These recommendations help in modeling a realistic response for a structural member, when applied, thanks to low thermal conductivity and high specific heat capacity of the PFP materials. It is worth noting that proper modeling of thermal behavior of the applied PFP is of utmost importance in order to estimate accurate thermal reaction of the structural components with PFP when subjected to accidental high temperature loading conditions.

Deterministic Fire Integrity Assessment

During the initial phase of project, the application of PFP is based on deterministic fire scenarios based on industry standards or consequence analysis. Process areas are grouped into fire zones and fireproofing is specified accordingly. In the fire integrity analysis, load cases and load factors are adopted from API RP-2FB. It is assumed that PFP is fit for purpose and can maintain core temperature of structural steel below 400°C for the specified duration. Commercial non-linear Finite Element Analysis (FEA) software packages such as USFOS [15] are used for analysis of process modules and piperacks included in the PFP scope. In these assessments, since

the PFP is assumed to be fit for purpose the core temperature of protected element is limited to 400°C; though this could be conservative for some members that may remain well below this limiting temperature. Additionally, non-linear behavior of frame members is captured by using a temperature dependent material model, and by accounting for non-linear geometry effects. For example, beam can yield when overloaded and columns can buckle (elastically or plastic) when overloaded. The ductility level analysis allows for load redistribution and prediction of structural failure times. In the analysis, failure is defined as excessive deformation of members supporting process safety critical elements (piping, valves etc.) or global failure such as collapse due to instability. Several iterations are performed by reducing the number of protected members until an optimized PFP scheme is obtained.

Risk-based Fire Integrity Assessment

Probabilistic Fire Risk Analysis Workflow

When the facility's design is matured, i.e., detail design phase, jet fire probabilistic data and fire impact exceedance frequencies can be calculated, and the probabilistic assessment of the facilities can be conducted for PFP requirement optimization. In the probabilistic assessment, fire load characteristics and the substrate thermal capacity are considered. Fire load characteristics such as release location, duration, and possible orientation are included in the risk-based fire scenario assessment. CCPS [23] provides one of the most widely accepted methodologies for the fire risk assessment. The methodology is also in line with other guidance such as Norsok Z-12 [24], FABIG TN 11 [5], API RP 14G [25] and 2FB [1], and UKOOA [26].

Figure 1 illustrates the overall Quantitative Risk Assessment (QRA) process for fire accident. Fire load characteristics and ignited event frequencies are extracted from the mature QRA model. Fire events are evaluated against structural impairment criteria that is determined through detailed structural analysis. Fire characteristics such as release location, duration, and possible orientation are considered in the FRA. Ignited event frequencies are also extracted for each scenario, which are further modified to determine cumulative impact event frequencies for individual points in 3D space. Figure 1 illustrates the detail procedure for FRA to identify design fire loads. Eventually, this process identifies the locations where the cumulative impact event duration exceeds the thermal capacity of a structure.

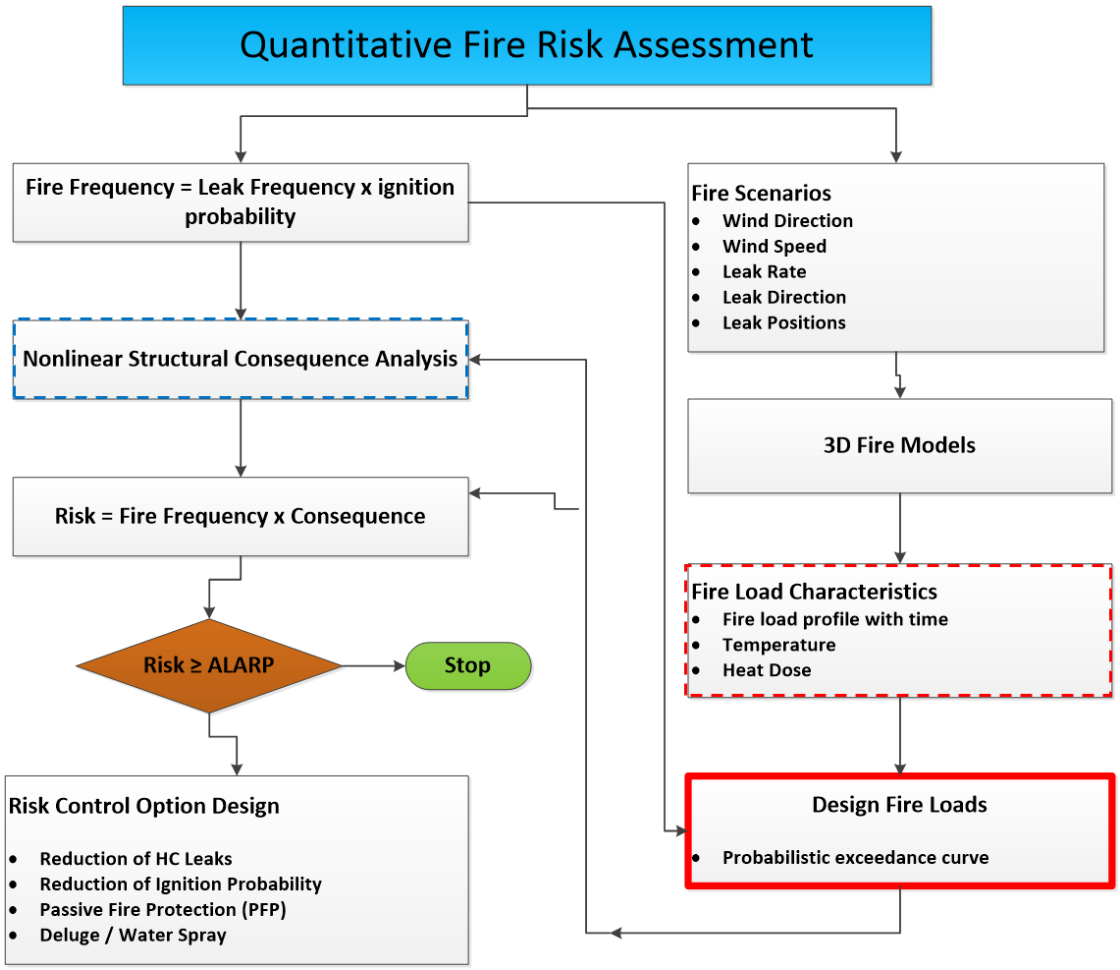


Figure 1. Overall QRA Workflow

Thermal Capacity of Structures

Thermal capacities of structures are established and refined through coupled structural-safety critical system fire response analysis. The structural failure time is determined through structural analysis, iteratively to estimate impairment durations for a fire scenario. This calculated failure time is subsequently utilized to evaluate the impairment frequency.

Structural exposure durations for thermal radiation levels vary depending on the fire zone. In general, the thermal radiation and the corresponding exposure durations are lower at higher elevations. However, the height of the fire zone can be extended for open steel beam structures based on project safety requirements. Conservatively, structural models may be evaluated in its entirety with target thermal radiation level and, typically, for a period longer than actual fire duration to ensure a complete understanding of any potential structural impairment, especially after the accidental fire events such as during cooling phase.

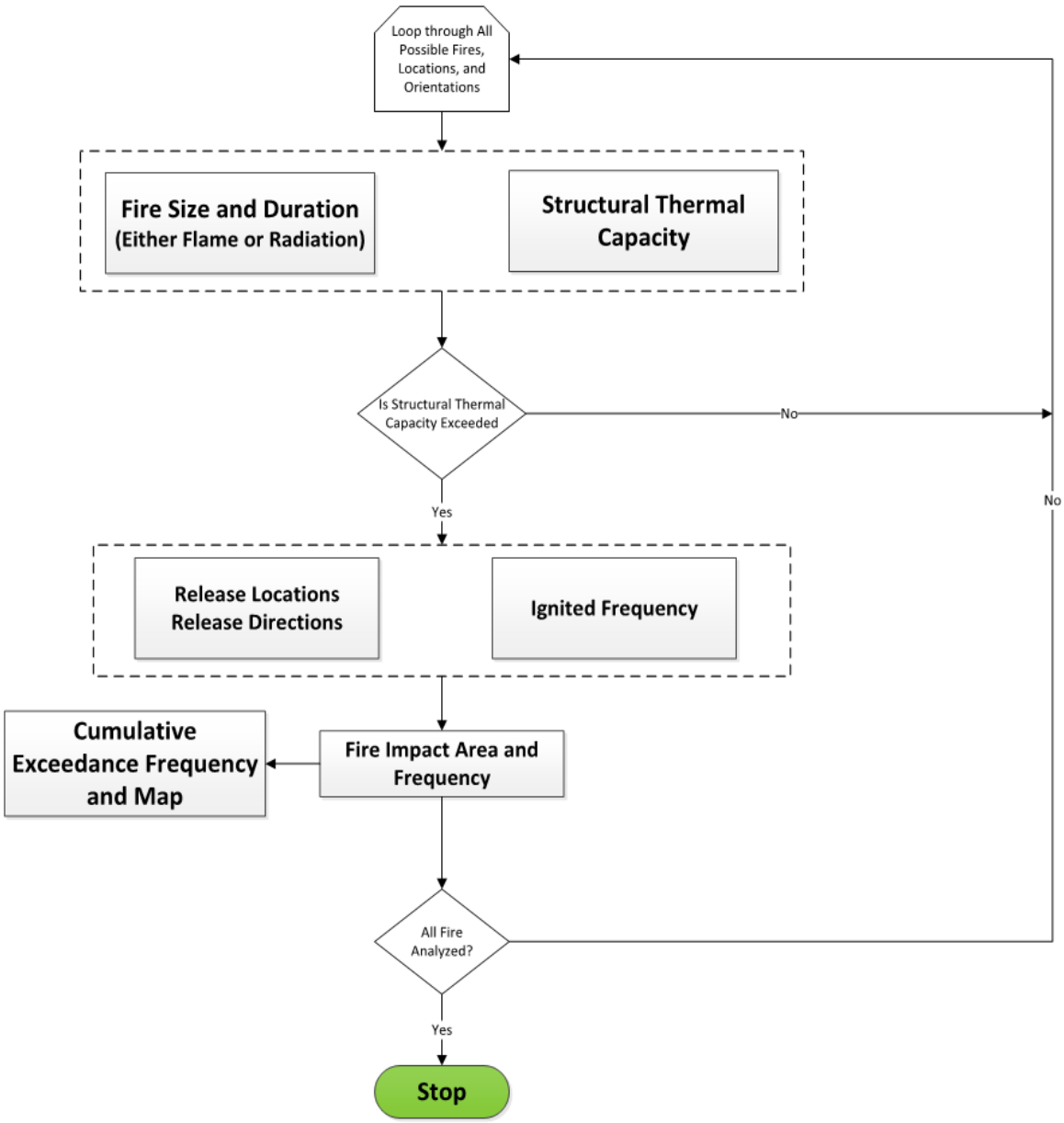


Figure 2. Design Fire Load Calculation Procedure

Fire Load Characteristics

All of the relevant inventories and fire scenarios from the QRA are evaluated for their potential to impact any given point in the target structures. Both pool and jet fire types are considered. Based on close review of the relevant inventories, the most likely discharge height and location for each inventory are identified. Releases from large process piping systems are assigned to multiple points so as to distribute the inventory release/ impact frequencies. Multiple release orientations are considered under all weather conditions to determine the most conservative

length and width of flame envelope and radiation contour dimensions. The most conservative dimensions of each are combined into a single scenario for further analysis. Each of these dimensions are not necessarily from the same release orientation or weather condition. Flame envelope and thermal radiation contours are handled slightly differently in order to calculate the 3D impact frequency.

Cumulative Event Frequency

Using a 3D approach common to that used for offshore platforms, individual event frequencies are calculated by determining the proportion of a spherical surface area that is enveloped by the fire or thermal radiation contour shape approximation. The radius of the hypothetical sphere is assigned as the distance from the release orifice to the impact location of interest. Dimensions of the thermal contours are not modified. Therefore, closer targets see higher directional probabilities as hypothetical spheres reduce in surface area. For accurate calculations of downward-impinging releases, conservative flame envelope and thermal contour dimensions are extracted from release orientations above the horizontal plane. The ignited event frequency associated with a given QRA inventory is modified by the directional impact probability for each event. Cumulative frequencies are calculated by summing the total frequency of individual flame or thermal contour events impacting a given point in 3D space, as illustrated in Figure 3.

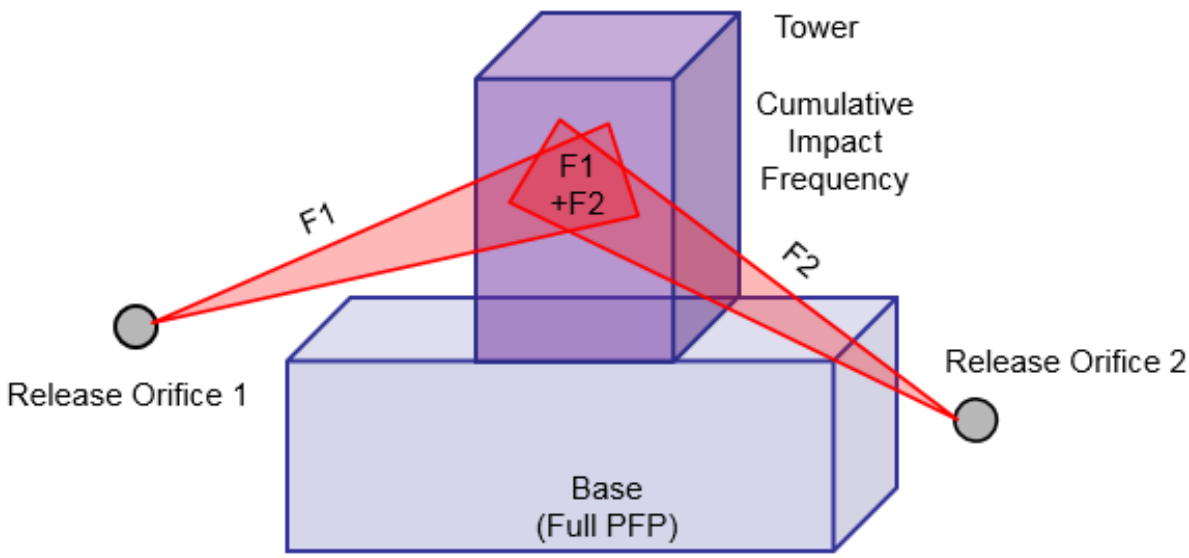


Figure 3. Individual and Cumulative Impact Frequency Concept

Thermal Capacity Exceedance

The frequency of exceeding the structural survivability criteria (i.e. capacity of the structure to maintain integrity for a given radiation intensity and duration) can now be calculated for all points in the fire zone. Durations of all QRA inventories are retrieved and paired with their corresponding impact event frequency. The cumulative frequency of all events where the structural capacity has exceeded is calculated and overlaid on the impingement exceedance map

for the whole facility. This information is then used according to flowchart in Figure 1 as input to the non-linear structural analysis. Annual exceedance frequency criteria intended for application towards aggregated risk criteria are used to evaluate the safety level under the accidental fire event. This analysis ultimately demonstrates risk to the structure and provides recommendations for design and optimization of PFP scheme.

Structural Fire Response Analysis

For understanding the structural response of individual members and the entire structural system, a series of fire response analyses are performed. In the structural fire response analysis, PFP requirements, and structural integrity of the steel structures and safety critical piping, valves, equipment and E&I systems under accidental fire conditions are considered. As a result of the risk-based fire durations and specific spatial fire threatened locations from the impingement exceedance maps, necessary PFP scheme for the structure and SCEs are determined.

3. Case Studies

Field Application: Fire Integrity of Steel Structures for Risk-based Fire Scenarios

Process safety studies for typical onshore oil and gas facilities were carried out to optimize initial PFP schemes by adopting the risk-based FIA as described in the previous section. The studies included QRA for the entire plant, fire integrity analyses, and PFP optimization for process modules, equipment and piperacks.

Risk-based fire duration calculations were performed for assessment and optimization of PFP during the QRA and probabilistic FRA. Release locations and directions were considered for calculation of risk-based jet fires impinging on certain process area. Calculations were performed for grade level and at several elevations for areas with large vertical equipment. In-house developed tools were used for calculations to determine the fire durations for cumulative frequencies reaching an exceedance frequency criterion of 10^{-5}/year. This approach resulted in calculation of more realistic jet fire durations based on leak frequencies, directionality of a jet and process conditions, release rate, and pressure (see Figure 4)

With the calculated risk-based fire durations per the exceedance frequency criterion, ductility level analyses were performed using ABAQUS software package [19]. The analyses included structural members and process safety critical equipment and piping systems. Large equipment (e.g. large bore piping, process vessels, ESD valves and actuators) were also included in the FE Model as shown in Figure 5. These detailed models enabled capturing the interaction between process safety critical systems and the supporting structure.

Structures were evaluated using jet flame impingement at 300 kW/m^2 for duration corresponding to fire impact exceedance frequencies less than or equal to 10^{-5}. Flame impingement of this manner may cause failure of unprotected steel structures within short order. Heat-up curves of members were developed using detailed transient heat transfer analyses for typical members. Since the objective of this study was to obtain an optimized scheme to ensure the integrity of

support structures, piping, and pressure vessels, the adequacy of PFP scheme was checked by comparing the calculated plastic strains with allowable limits per FABIG [5]. Similarly, the failure of structural members was evaluated based on UKOOA recommended performance criteria [26]. This study also examines thermal radiation exposure of entire structure due to 150 kW/m^2 near field jet fire radiation for its corresponding duration. These radiation values were chosen for evaluation to ensure structural integrity and to prevent escalation of fire hazard [1].

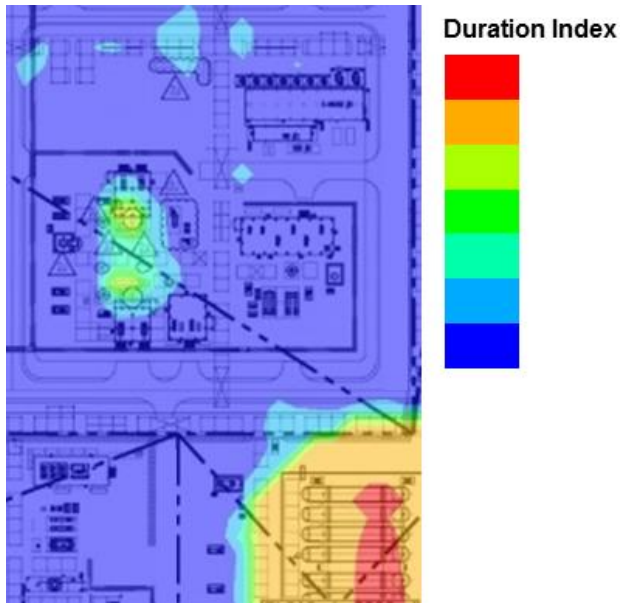


Figure 4. Impairment Duration Map for Jet Fire Impingement per 10^{-5} Annum for the Facility

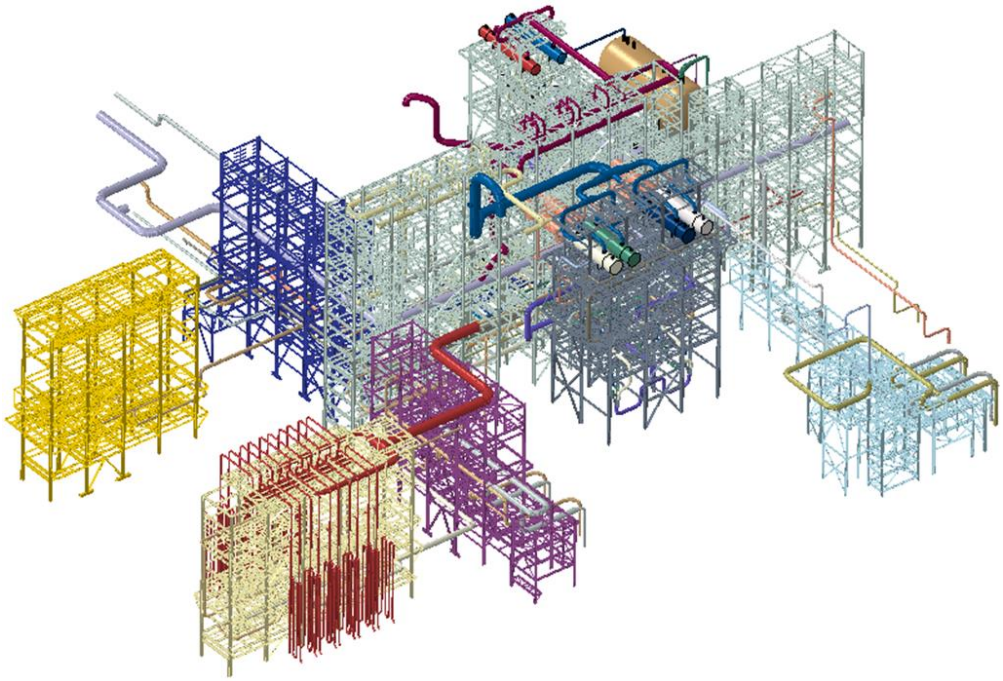


Figure 5. Finite Element Model with Large Equipment and Piping for PFP Optimization

The optimized PFP scheme depends on assessment approach; i.e., deterministic or performance-based approach. The reductions in PFP area are presented in Table 1 and Table 2. Using the performance-based approach, a further reduction of 20 to 30% in PFP coating areas of typical large process modules were achieved compared to the PFP schemes generated using prescriptive approach (Table 1). A maximum PFP reduction of 60% was attained for a typical piperack module (Table 2). This was accomplished by analyzing the entire processing unit in its entirety and by strategically protecting critical components such that the stability of supported piping is maintained.

Table 1 Comparison of Required PFP Areas for a Large Process Module

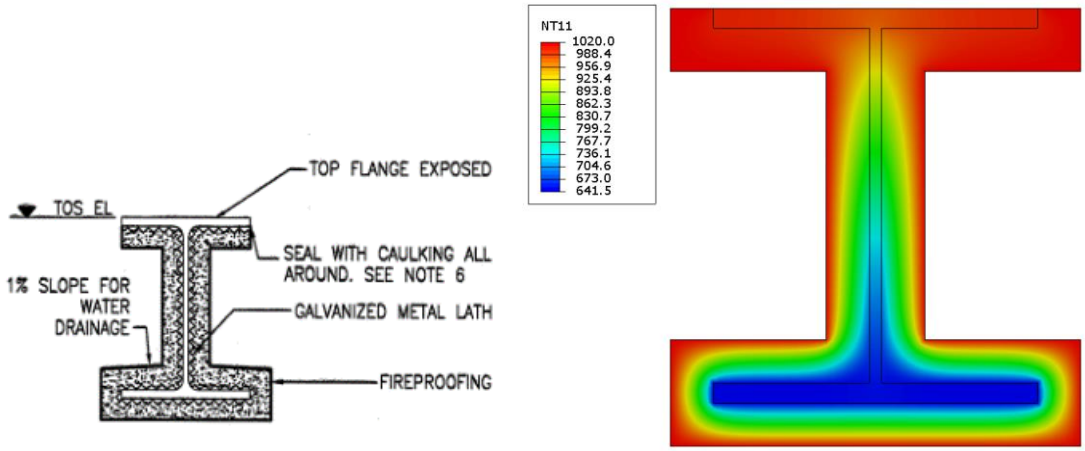
Description	**PFP Scheme Approach**	**Total Surface Area(m^2)**	**PFP Surface Area (m^2)**	**% PFP Reduction with respect to Prescriptive**
Typical Equipment Structure	Prescriptive	11000	7000	-
	Deterministic		5400	23%
	Risk Based		4700	33%

Table 2 Comparison of Required PFP Areas for a Typical Piperack

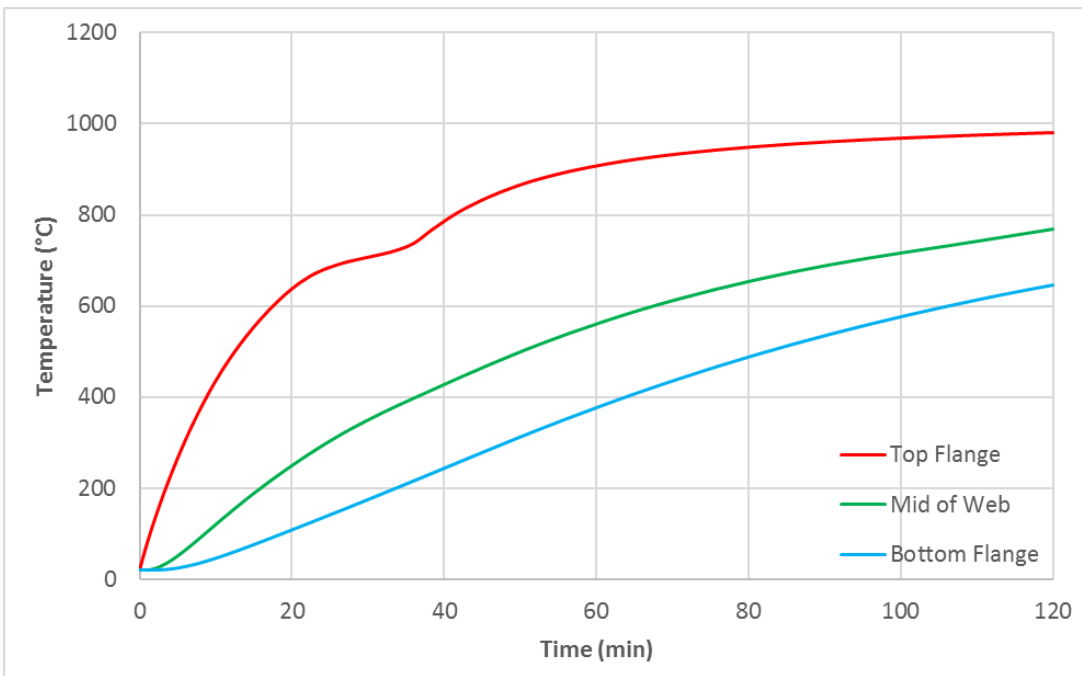
Description	**PFP Scheme Approach**	**Total Surface Area(m^2)**	**PFP Surface Area (m^2)**	**% PFP Reduction with respect to Prescriptive**
Typical Piperack	Risk Based	1900	810	57%

Fire Response Analysis for Exposed Top Flange Cases

Although API [27] allows the top flange exposed PFP application for horizontal beams, the effect of the partial PFP application should be fully understood with regards to jet fire risks. API 2218 does not account for jet fire cases and targets protection against pool fire where radiation from grade limits the heating of top flange due to not having line of sight. However, at facilities susceptible to jet fire, exposed top flanges can significantly lower the fire endurance limits. Case studies with partial PFP application for horizontal beams were carried out. Figure 6 shows an example of partial PFP application, i.e. top flange exposed beam section. With considerable temperature gradient over the top flange exposed beam subjected to a jet fire scenario, the partial PFP application was found to cause the section stiffness and capacity to decrease. Three cases of PFP application were investigated for load-bearing capacity comparison: beam with fully covered PFP, and top flange partially exposed and top flange completely exposed beams (Figure 7). The beam with top flange fully exposed resulted in reduction in both stiffness and capacity, i.e., 60% and 40% remaining, respectively. Although it may not be practical to apply PFP to top flanges on most places due to presence of piping and grating, reduced capacity of beams should be taken into account when jet fire risks are credible.

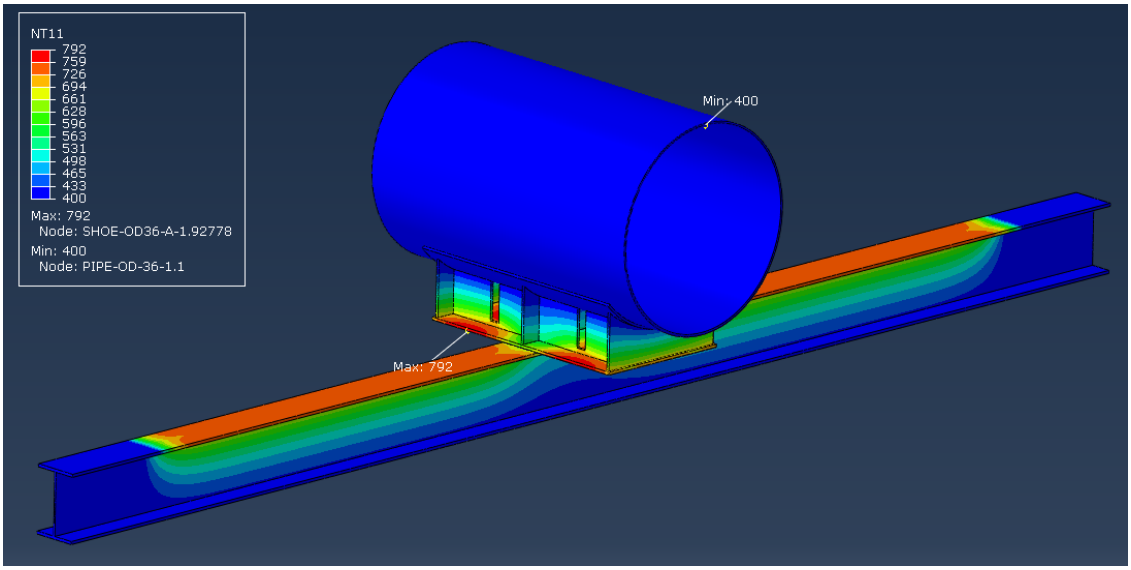


(a) Temperature Gradient for Typical Top Flange Exposed Beam Section

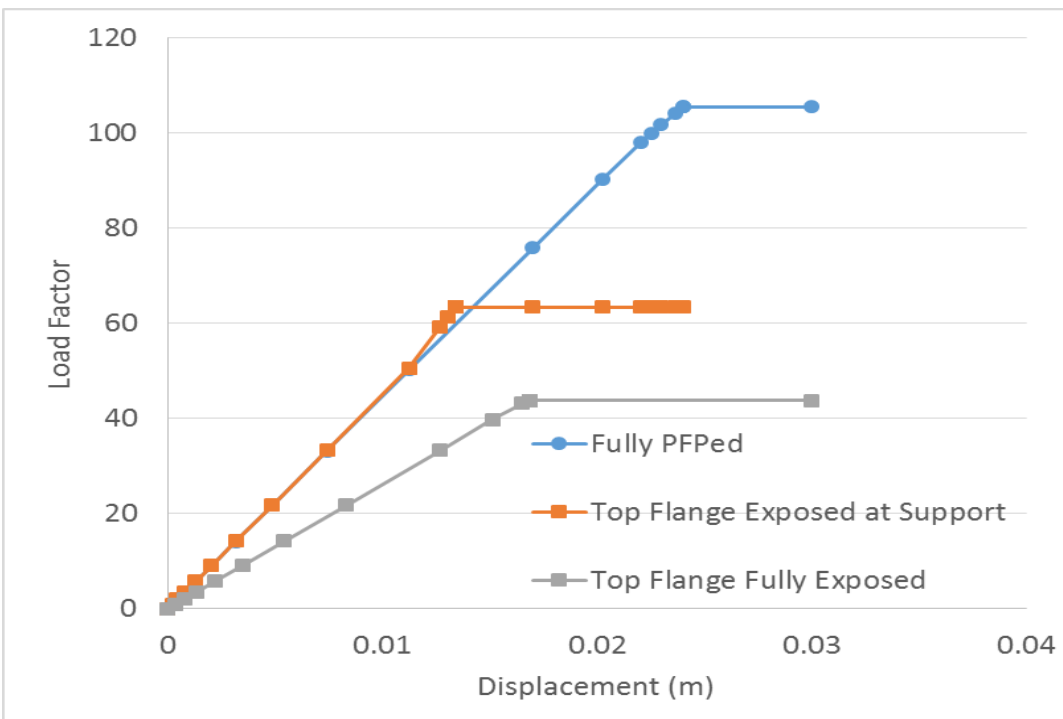


(b) Temperature Heat-up Curves Across Depth of Top Flange Exposed Beam

Figure 6. Typical Heat Transfer Analysis Results of Top Flange Exposed Beam Subjected to 150kW/m^2 Radiation: (a) Temperature Gradient, and (b) Different Temperature Heat-up Profiles



(a) 3D Heat Transfer Analysis Results for Top Flange Exposed Beam and PFP Applied Pipe



(b) Ultimate Strength Comparison between Fully and Partially Protected Beams

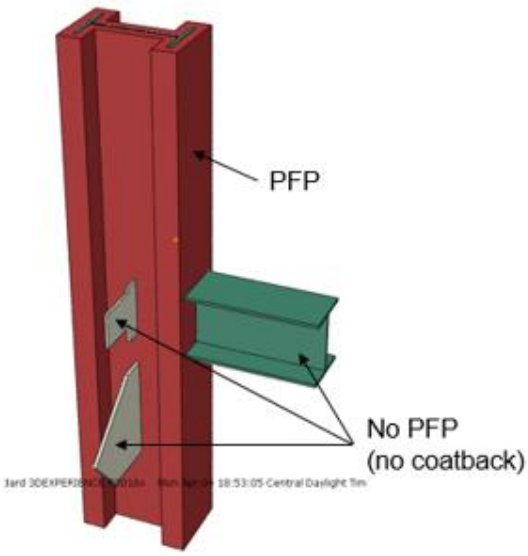
Figure 7. Capacity Degradation of Top Flange Exposed Beam Subjected to a Jet Fire Scenario

PFP Coatback Requirement Assessment

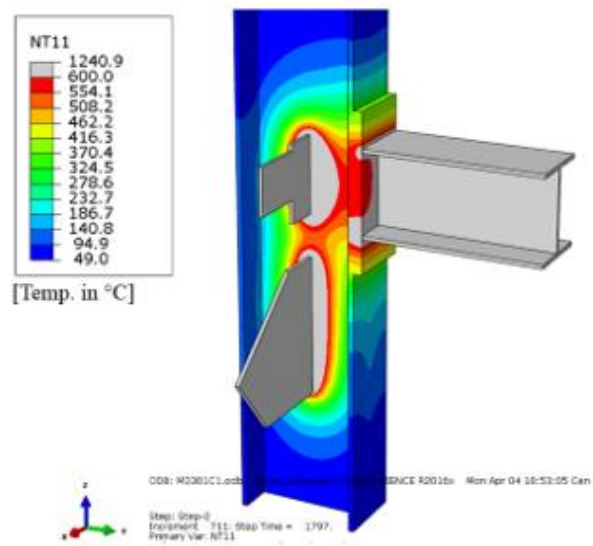
For the purpose of reducing the heat conduction into a protected steel element supplied from a physically attached unprotected steel element, a typical mitigation for steel connections is PFP coatback application. PFP is coated back from a protected steel element to limit the extent and severity of "hot spots" developing in the protected member at the region of the connection. The added PFP on the otherwise unprotected member, limits the distance between the connection and the surface directly exposed to fire. API [2] prescriptively specifies the PFP coatback length for exposed steel supports to be a minimum of 300 mm, and a range of 400 to 600 mm for the PFP coatback length is typically practiced for offshore structures [28].

The PFP coatback requirements for typical connections were also investigated using risk-based fire scenarios for onshore and offshore projects supported by the authors. The influence of PFP coatback was assessed for thermal response and the structural integrity of the selected connections. Based on the performance-based coatback analyses for typical steel connections of structures, necessity of PFP coatback at the steel connections between protected and unprotected members was evaluated.

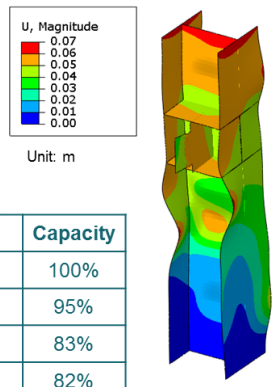
Detailed three-dimensional (3D) FEA models were developed for typical connections. A typical connection is shown in Figure 8-a. Transient heat transfer analyses followed by non-linear strength analysis for a given fire scenario was conducted using ABAQUS software package [19]. In the non-linear strength analysis, the load-bearing capacities of the critical connections were assessed using temperatures obtained from the heat transfer analyses. The analysis results (Figure 8-b and c) were reviewed and compared with fire event locations/durations to optimize the PFP coatback requirements. Based on the coatback analyses with risk-based approach the required PFP coatback lengths were reduced to 200 mm or completely removed for cases with a relatively thick PFP material applied to the protected element.



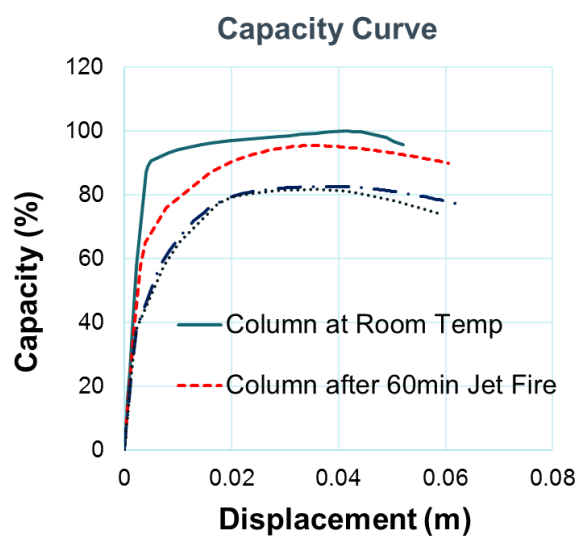
(a) FE Model for PFP'd Steel Connection



(b) Temperature Results for Strength Analysis



Condition	Capacity
Room Temperature	100%
After 60min Jet Fire	95%
After 90min Jet Fire	83%
After 2hr Pool Fire	82%
Actual Utilization	50%



(c) Ultimate Capacity Pushdown Analysis of Steel Column without Coatback Application on Framing Members

Figure 8. Performance-based FIA for Steel Connections and Coatback Analysis: (a) FEA Model (b) Temperature Distribution from Thermal Analysis, and (c) Ultimate Capacity Assessment

Fire Protection of Equipment and Piping

Safety critical equipment and piping systems within the fire zones were identified using hazard assessments to prevent escalation and facilitate the emergency operations. Although nominal amount of fireproofing materials is required for the equipment and piping systems, the protection

scheme is usually determined and applied by the fireproofing material suppliers. Verification of the adequacy of heat transfer characteristics, e.g., number of layers, installation configurations, and thicknesses, allows for PFP optimization for these systems without compromising from safety. In this study, performance-based FIA with deterministic fire scenario generation approach were considered for the verification of the PFP applications for the safety critical equipment and piping. For some cases heat conservation and fireproofing requirements were both met through engineered insulation solutions. Additionally, details along termination points and transitions were checked using analytical methods calibrated with respect actual fire test results.

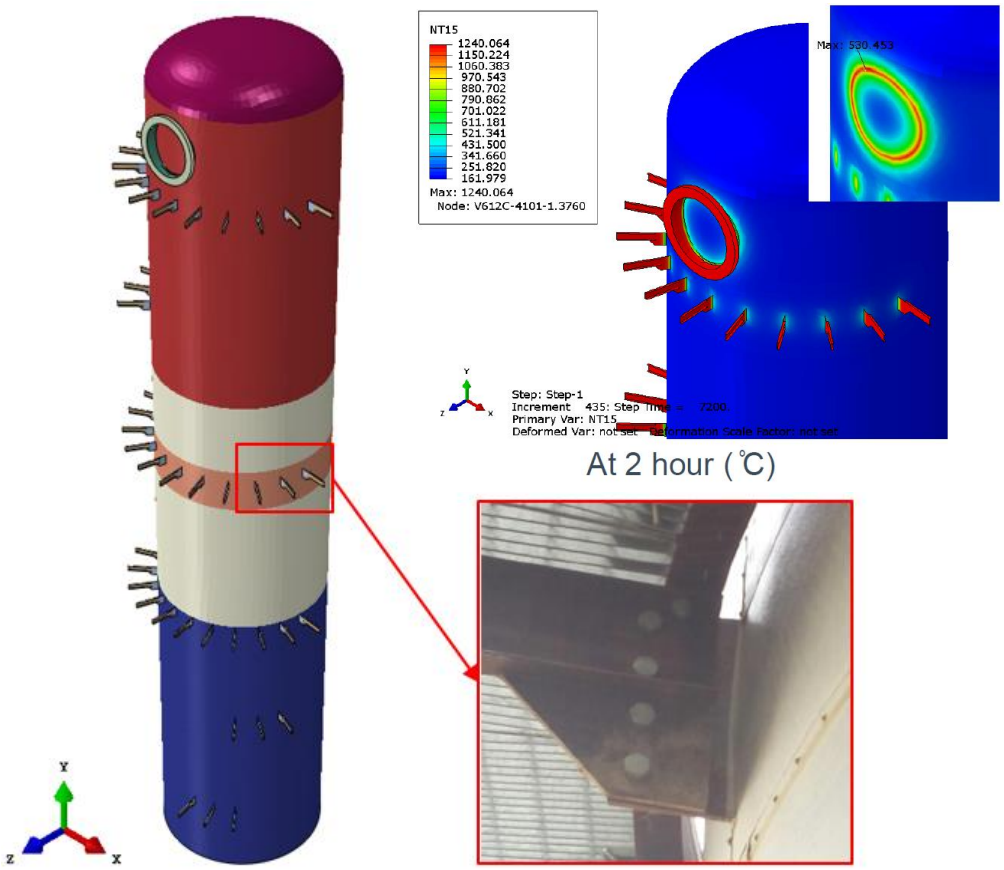
Fireproofing of the process equipment such as pressure vessels and vessel attachments were investigated using refined FE Models of the large process vessels. 3D transient hear transfer analyses were performed using ABAQUS software [19] for the local FE models that consist of pressure vessel shell, fireproofing material on the vessel shell, and the exposed attachments as illustrated in Figure 9. Temperatures at the outer surface of the protected shell were generally limited to 400˚C. Considering strength reduction of the steel material at elevated temperatures [3, 18], the coatback requirements for the exposed attachments were evaluated. In addition, Boiling Liquid Expanding Vapor Explosion (BLEVE) risk for the pressure vessel at elevated temperature was assessed using HYSYS dynamic process simulations and FEA based rupture analysis [29].

Fire Protection of Electrical Systems

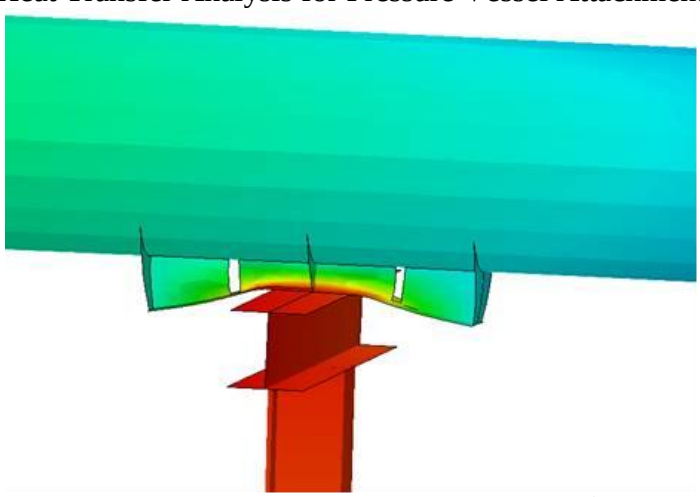
Electrical and Instrument (E&I) systems, which are required to remain functional up to a specified fire duration in order to control critical operations, should also be classified as safety critical systems. These safety critical E&I systems usually include electrical and instrument cables and trays, process shutdown/de-pressurization valves, control systems, etc. The E&I systems are, in general, protected with jet fire rated fireproofing materials that can be flexible jacket type with stainless steel/mesh cladding or endothermic material PFP [2].

For safety critical E&I systems, 3D FEA models were developed using ABAQUS [19] as shown in Figure 10. For the FIA, thermal properties of PFP materials were obtained from parametric calibrations with fire test data of the fireproofing materials vendors provided. In order to evaluate the thermal response and PFP requirements for various E&I systems, transient heat transfer analysis was performed. Deterministic fire scenarios were utilized in the analysis, and the maximum allowable fire durations for different number of PFP configurations were assessed. Residual strength assessment of cable trays and supports were performed at elevated temperatures by utilizing thermal response results from the heat transfer analyses.

Unprotected sacrificial cable tray supports can conduct heat to the protected cable tray through the contact area between exposed cable tray support and protected cable tray. This may lead to localized high temperature in cable trays and cables. To investigate the length of required coatback, 3D transient heat transfer analyses were also conducted. The inner surface temperature of cable tray, obtained from heat transfer analysis, was used as input for a 2D FE Analysis to evaluate the cable temperature under accidental fire events.

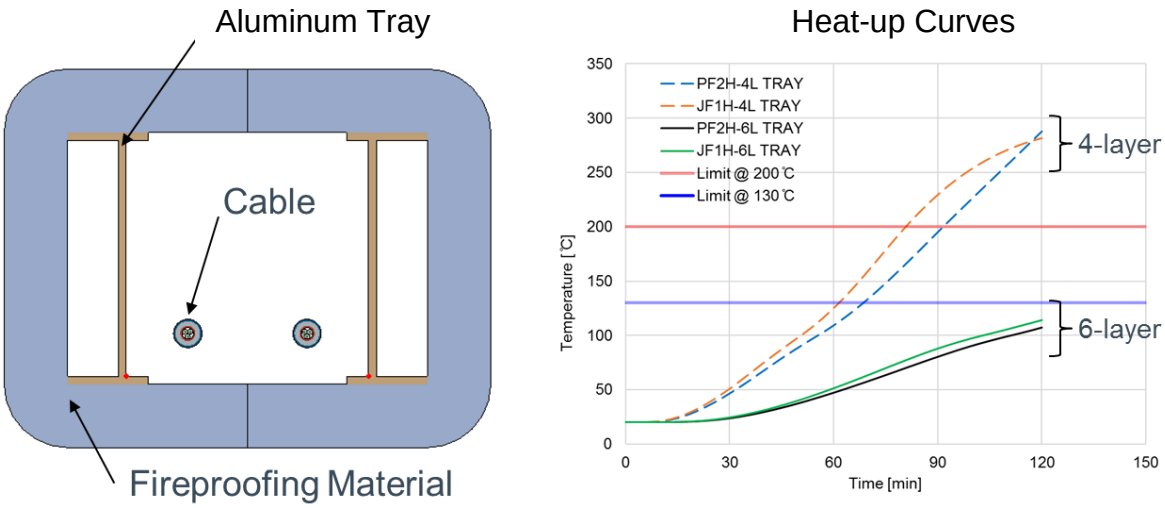


(a) Transient Heat Transfer Analysis for Pressure Vessel Attachment Coatback

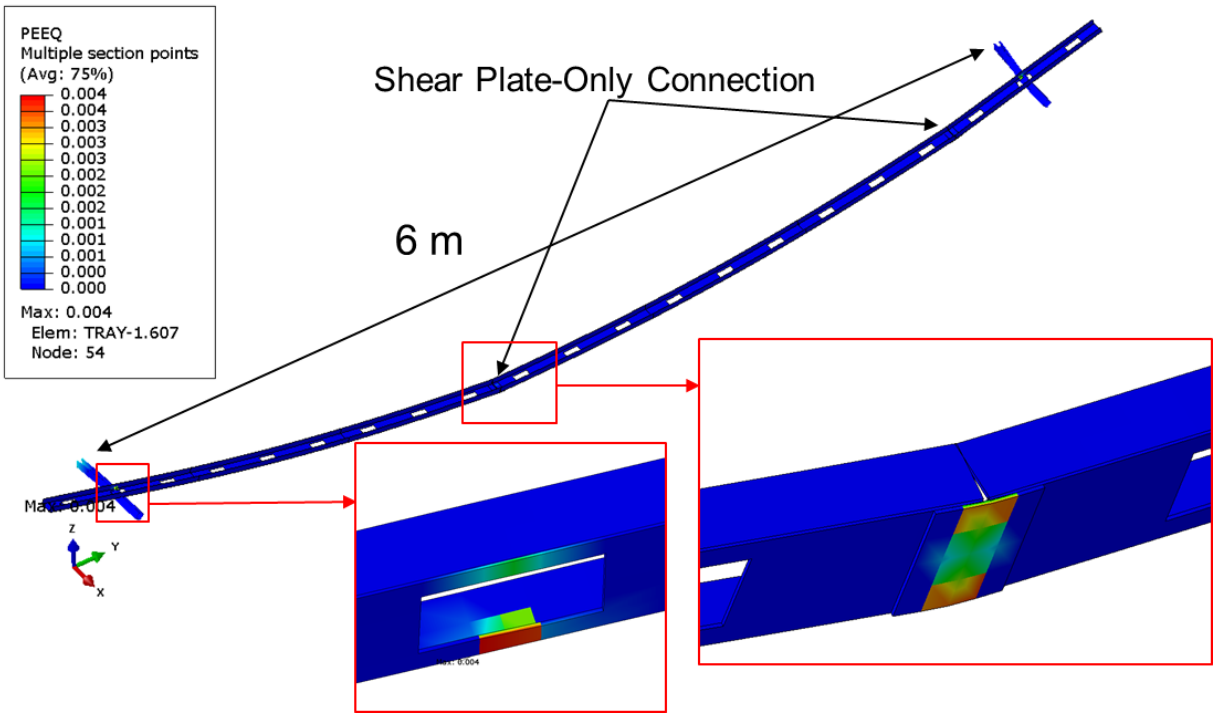


(b) Pipe-Shoe Permanent Deformation after 2 Hours 300 kW/m^2 Jet Fire Impingement through Exposed Portion of Pipe Shoe

Figure 9. Local FIA for PFP Optimization of Critical Equipment and Piping Systems: (a) Transient Heat Transfer Analysis for Pressure Vessel Attachment Coatback, and (b) Thermal-Strength Interaction Analysis for Piping and Pipe Supports with PFP



(a) Transient Heat Transfer Analyses for Cable Trays



(b) Ductility Level Fire Response Analysis for Protected Cable Trays

Figure 10. E&I Cable Tray FIA for PFP Optimization: (a) Transient Heat Transfer Analyses, and (b) Ductility Level Analysis

4. Conclusions

Various regulatory bodies require Oil & Gas production and processing facilities for an explicit identification, risk assessment, and mitigation solution to be prepared for fire hazards. QRA techniques are now increasingly used for the assessment of fire hazards at facility, and for the effective planning of remedial measures. The use of deterministic fire scenario is prevalent in industrial practice to develop required PFP scheme for protection against fire. Although deterministic approach yields a reduced fire protection requirement, there is still a room for further optimization of PFP application while properly identifying the safety critical aspects. In this paper, we have presented a PFP optimization methodology by adopting a holistic multi-disciplinary approach to achieve a performance-based PFP scheme balancing the hazard control and risk mitigation.

For a complete FIA, non-linear thermal-structural analyses for all typical modules / structures of the facility are performed. All safety critical equipment and piping along with any neighboring structure are included in the FE Models. The temperature time history is obtained by a separate heat transfer analysis for both protected and unprotected members individually, which is later utilized in the stress analysis for the performance assessment and PFP optimization. Through case study, we demonstrated that performance-based optimization approach resulted in 20 to 60% reduction in PFP requirements from that suggested by using prescriptive approach for typical modules. In addition, coatback requirements, top flange protection, fireproofing of E&I systems, pipe supports, vessels, valves, etc. can also be optimized by adopting a performance-based approach. Coatback and top flange fire protection requirements can be critical for structure susceptible to relatively long duration pool fires and jet fires.

Since it is not feasible to test all possible PFP configurations for all sections or process components at a plant, understanding and interpretation of fire tests plays a critical role in extrapolating test results through analytical methods. The parameters used as the inputs for FE Models shown in this study were calibrated and checked against test data. High fidelity simulation methods discussed in this paper resulted in better understanding of risk and more accurate calculation of fire response for a range of components protected with different types of PFP.

The main advantages of reducing application of PFP coating on non-critical members are cost savings and integrity management improvements during life cycle of a facility. Considering the fact that CAPEX and integrity management are major concerns for most structures at petrochemical facilities, optimization of PFP for plant structures has significant benefits for operators and owners of onshore and offshore assets without compromising the risk targets. The integrated structural, foundation and equipment and piping systems fire analysis approach presented in this study is considered to be a significant addition to state of the art in fire protection design of petrochemical facilities. Improvements in analysis and design methods are expected to result in better selection and engineered application of PFP at the critical locations only without compromising from safety requirements. This also ensures that safety critical elements are protected against credible hydrocarbon fire scenarios.

References

[1] American Petroleum Institute (API), "API 2FB - Recommended Practice for the Design of Offshore Facilities Against Fire and Blast Loading," 2012.

[2] American Petroleum Institute (API), "API RP 2218: Fireproofing Practices in Petroleum and Petrochemical Processing Plants," 2013.

[3] British Standards (BSi), "Eurocode 3: Design of Steel Structures EN 1993-1-2:2005," British Standards, 2005.

[4] Det Norske Veritas (DNV), *Offshore Standard DNV-OS-D301: Fire Protection,* 2008.

[5] FABIG (Fire and Blast Information Group), "FABIG Technical Note 11: Fire Loading and Structural Response," Steel Construction Institute (SCI), 2009.

[6] M. K. Mathews, D. M. Karydas and M. A. Delichatsios, "A Performance-based Approach For Fire Safety Engineering: A Comprehensive Engineering Risk Analysis Methodology, A Computer Model And A Case Study," *Fire Safety Science,* vol. 5, pp. 595-606, 1997.

[7] J. Krueger and D. Smith, "A practical approach to fire hazard analysis for offshore structures," *Journal of hazardous materials,* vol. 104, no. 1-3, pp. 107-122, 2003.

[8] S. B. Axelsen, O. Ø. Knudsen and R. Johnsen, "Protective Coatings Offshore: Introducing a Risk-Based Maintenance Management System—Part 1: Risk Analysis Methodology," *Corrosion,* vol. 65, no. 12, pp. 809-816, 2009.

[9] A. Ahmad, S. A. Hassan, A. Ripin, M. W. Ali and S. Haron, "A risk-based method for determining passive fire protection adequacy," *Fire safety journal,* vol. 58, pp. 160-169, 2013.

[10] N. Badri, H. K. Amirhosein Rad, B. Abdolhamidzadeh, R. Parvizsedghy and D. Rashtchian, "A risk-based decision making approach to determine fireproofing requirements against jet fires," *Journal of Loss Prevention in the Process Industries,* vol. 26, no. 4, pp. 771-781, 2013.

[11] N. K. Shetty, G. Soares, P. Thoft-Christensen and F. M. Jensen, "Fire safety assessment and optimal design of passive fire protection for offshore structures," *Reliability Engineering & System Safety,* vol. 61, no. 1, pp. 139-149, 1998.

[12] G. De Sanctis, M. Faber and M. A. R. I. O. Fontana, "Assessing the level of safety for performance based and prescriptive structural fire design of steel structures," *Fire Safety Science,* vol. 11, pp. 996-1009, 2014.

[13] N. Ö. Bezgin, "An experimental evaluation to determine the required thickness of passive fire protection layer for high strength concrete tunnel segments," *Construction and Building Materials*, vol. 95, pp. 279-286, 2015.

[14] "Hunt, R. J.; Shirvill, L. C.; Earles; G. A.; McDermott, J.," in *Offshore Technology Conference*, January 1997.

[15] SINTEF, *USFOS Non-Linear Program, Version 8.8*, Norway, 2015.

[16] E. Munoz-Garcia, "Risk-based passive fire-protection optimization," *Oil and Gas Facilities*, vol. 30, no. 01, pp. 67-75, 2014.

[17] Y. Jin and B. S. Jang, "Probabilistic fire risk analysis and structural safety assessment of FPSO topside module," *Ocean Engineering*, vol. 104, pp. 725-737, 2015.

[18] FABIG (Fire and Blast Information Group), "Technical Note 6: Design Guide for Steels at Elevated Temperatures and High Strain Rates," Steel Construction Institute (SCI), 2001.

[19] Dassault Systemes, *ABAQUS FEA Software, Version 2017*, 2016.

[20] G. Zuccaro, "A Case of Shoice of Passive Fire Protection (PFP) in an Oil & Gas EPC Project," in *Chemical Engineering Transactions*, 2012.

[21] Y. Wang, I. Burgess, F. Wald, "Performance-Based Fire Engineering of Structures," in *Boca Raton*, Florida: CRC Press, 2012.

[22] British Standards Institution, "Eurocode 1: Actions on structures - Part 1-2: General actions - Actions on structures exposed to fire," BS EN 1991-1-2, 2002.

[23] Center for Chemical Process Safety, *Guidelines fo rChemical Process Quantitative Risk Analysis*, 1999.

[24] Norsok Standard, *Z-013: Risk and emergency preparedness analysis, Rev. 2*, 2001.

[25] American Petroleum Institute (API), *API RP-14G: Recommended Practice for Fire Prevention and Control on Fixed Open-type Offshore Production Platforms*, 2007.

[26] UKOOA, *Oil & Gas UK Fire and Explosion Guidelinse Issue 1: Fire and Explosion GUidelines for QRA*, 2007.

[27] API RP 2FB, "Recommended Practice for the Design of Offshore Facilities Against Fire and Blast Loading," 2006.

[28] Jorgen Amdahl and Tore Holmas, "Performance Based Design of Offshore Structures Exposed to Fire," in *International Conference on Computational Methods in Marine*

Engineering , 2005.

[29] *HYSYS SS model "PSV-21161, 21229_fire.hsc" provided by the client.*

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Developing Safety Culture in an Undergraduate Chemical Process Safety Course

David W. Murhammer
Department of Chemical and Biochemical Engineering
The University of Iowa
Iowa City, Iowa 52242
E-mail: david-murhammer@uiowa.edu

Keywords: Safety experiments, flammability, reactivity, electrostatics, explosions

Abstract

In order to better prepare students for industry and to provide them with an appreciation of the importance of a dedicated safety culture, the Department of Chemical and Biochemical Engineering at the University of Iowa has been offering a required junior-level chemical process safety course since 1996. A major laboratory component was added to this course in 1998 to provide students with hands-on experiences to emphasize concepts learned in the lecture component of the course, particularly flammability, runaway reactions, electrostatics, explosions and relief sizing. Beyond these and other fundamentals, the course emphasizes accident prevention, inherently safety design strategies, HAZOP analysis, layer of protection analysis, and related topics. A significant portion of the lectures involve the discussion of previous accidents and how they could have been prevented through the application of techniques learned in class. Students completing this course have an appreciation of industrial hazards and how to utilize engineering principles and management techniques to minimize risk.

Introduction

Since 1996, the University of Iowa has offered a required three semester hour Chemical Process Safety course that has been taken by students during the Spring semester of their Junior year. The course will begin to be offered during the Fall semester of the students' Junior year beginning in the 2018-19 academic year. Incorporating this course into the curriculum required only a slight modification of our curriculum, which is inconsistent with the common excuse ("cannot fit it into our curriculum") given for not having a dedicated Chemical Process Safety course. A dedicated laboratory component was introduced in the 1998 offering of the course as described previously [1]. The course lecture and laboratory have been modified over the years. The current details of the course and laboratory are summarized in Tables 1 and 2. This course

utilizes the textbook written by Crowl and Louvar [2] and material from many websites, including Safety and Chemical Engineering Education (SAChE) [3-5], U.S. Chemical Safety Board [6], Chemical Reactivity Worksheet [7], and AIChE Design Competition [8]. The four laboratory experiments (flammability, reactivity, electrostatics, and explosions) conducted by students in the Chemical Process Safety course are described herein.

Table 1. Details of Chemical Process Safety Course at the University of Iowa

Major Topics Covered in Lecture

Government Regulation	Reactivity
Process Safety Management	Fires and Explosions
Toxicology	Fire and Explosion Prevention
Industrial Hygiene	Relief Design
Source Models	Hazard Identification
Dispersion Models	Risk Assessment/Reliability Engineering
Flammability	Case Studies
Electrostatics	Inherently Safety Design

Homework

There are weekly homework assignments.

Quizzes

There are weekly quizzes (~15-20 min). These seem to improve the learning process and to discourage student procrastination.

Exams

There is one midterm exam and a final exam.

Topical Papers

In recent years students have written two topical papers ("opinion pieces") of 500 to 1000 words: (i) Chemical Regulation – What Is The Best Approach For The U.S.? and (ii) Chemical Plant Security: Should Inherently Design Be Required?

Laboratory Reports

There are laboratory reports for each of the four experiments given in Table 2. The reports for the flammability and electrostatics experiments are individual reports, while the other two reports are written by groups of 2 students.

Project/Presentation

There is a project involving previous AIChE Design Problems (a variety of problems are distributed among student in the class). Specifically, the report consists of (i) a literature review of the process, (ii) a process flow diagram (PFD), (iii) a discussion of safety issues, including a complete HAZard and OPerability study (HAZOP) and location of relief valves, and (iv) a discussion of how inherently safer design strategies (i.e., minimize, substitute, moderate, and simplify) can be used to make the process safer. These projects are conducted in groups of 2 or 3 students.

Table 2. Chemical Process Safety Laboratory at the University of Iowa

Laboratory Experiment	Equipment Used	Comments
Flammability	• *Minimum Ignition Energy (MIE) Apparatus • *Flammability Chamber • Miniflash Automatic Flash Point Tester (Closed Cup)	This laboratory involves determining (i) the MIE of a flammable gas, (ii) the LFL, UFL, and LOC of a flammable gas, and (iii) the flash point of pure flammable liquids and mixtures. Thermodynamics of ideal and nonideal mixtures are used to calculate the flash points of the mixtures and compared to actual measurements.
Reactivity	• Advanced Reactive System Screening Tool	This laboratory involves collecting data for four different reactions and analyzing the resulting data. Furthermore, the data are used to size relief valves for specified scenarios.
Electrostatics	• Liquid Conductivity Apparatus • Powder Chargeabilty Apparatus • Powder Volume Resistivity Apparatus • Humidity Chamber • Van de Graaf Generator • Keithley Electrometers	This laboratory involves determining (i) liquid conductivity, (ii) powder chargeabilty resulting from transport through plastic, glass and metal tubes, and (iii) powder resisitivity. The laboratory also investigates (depending on the year) the chargeabilty of humans, charge accumulation due to mixing liquids, etc. The humidity chamber allows the humidity to be controlled in some of the experiments.
Explosions	• *Minimum Ignition Energy Apparatus • Modified Hartmann Tube • Hartmann Bomb	This laboratory involves characterizing gas phase and dust explosions.

*Custom made by Fauske & Associates

Flammability Experiments

The first laboratory conducted by students in the Chemical Process Safety laboratory at the University of Iowa involves investigating flammability issues (Table 2), specifically flash points (FPs), lower and upper flammability limits (LFLs & UFLs), limiting oxygen concentrations (LOCs), and minimum ignition energies (MIEs). The FPs of pure alcohols (methanol, ethanol, propanol, etc.), diluted alcohols (diluted with water) and mixtures of alcohols are measured with a Miniflash automatic FP tester (Figure 1). The FPs of the diluted alcohols and alcohol mixtures are calculated assuming ideal and real solutions as described previously [1], and then compared with measured values. The Flammability Chamber (Figure 2) utilizes mixtures of a flammable gas (usually methane or propane), oxygen and nitrogen to determine the LFL, UFL and LOC. The minimum ignition energy apparatus (Figure 3) was used to determine the MIE of a flammable gas.

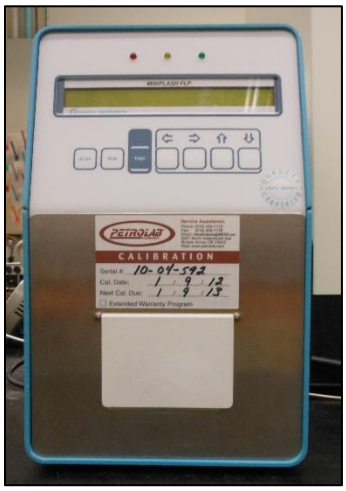


Figure 1. Miniflash automatic flash point (FP) tester (closed cup), purchased from Grabner Instruments, used to determine the FP of pure and diluted alcohols and alcohol mixtures.

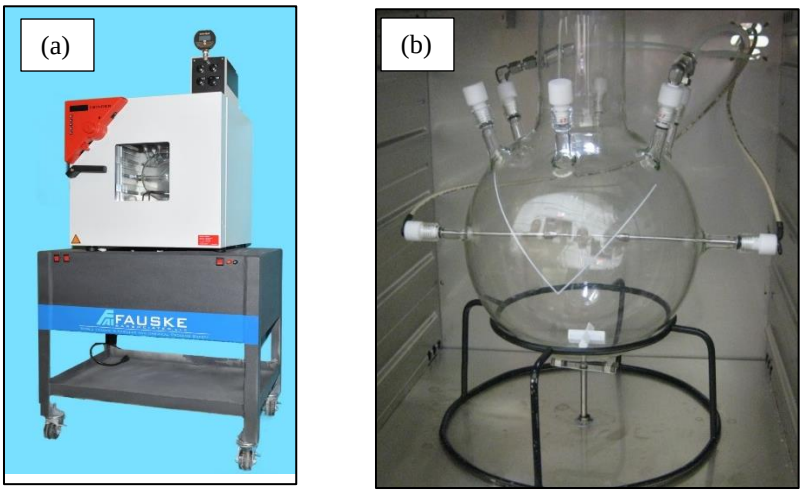


Figure 2. Flammability Chamber [(a) outside view and (b) glass test vessel], custom-made by Fauske & Associates, that is used to determine the lower and upper flammability limits and the limiting oxygen concentrations.

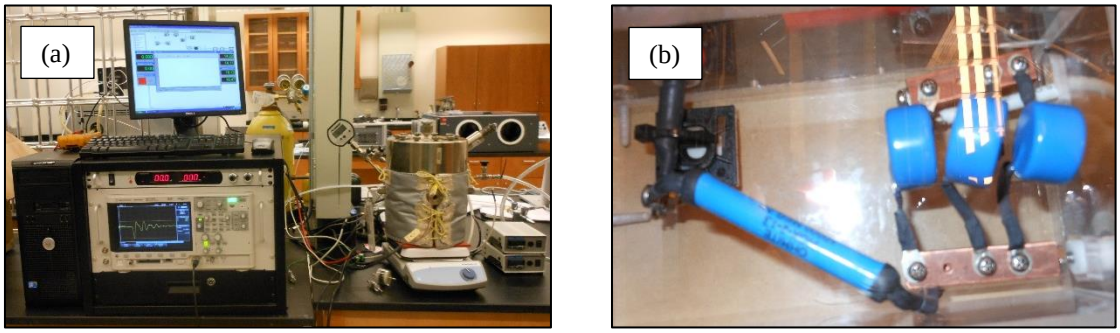


Figure 3. Minimum ignition energy (MIE) apparatus (a), custom-made by Fauske & Associates, that is used to determine the MIE of flammable gases. The amount of energy introduced to the flammable gas mixture is determined by the capacitance utilized (b).

Reactivity Experiments

The Advanced Reactive System Screening Tool (ARRST) [10] (Figure 4), purchased from Fauske & Associates, is used to evaluate the runaway reaction potential of four different reaction types. Each group of students collects data for one of these reactions, i.e., (i) methanol and acetic anhydride, (ii) ethanol and acetic anhydride, (iii) decomposition of 25% (v/v) di-tertiary-butyl peroxide in toluene (toluene serves as an inert solvent) or (iv) 0.5% (v/v) di-tertiary-butyl peroxide styrene (styrene polymerization), and then all students evaluate all 4 reactions as described previously [1]. Furthermore, a relief valve is sized for a specific scenario for each of these reactions as described previously [1].

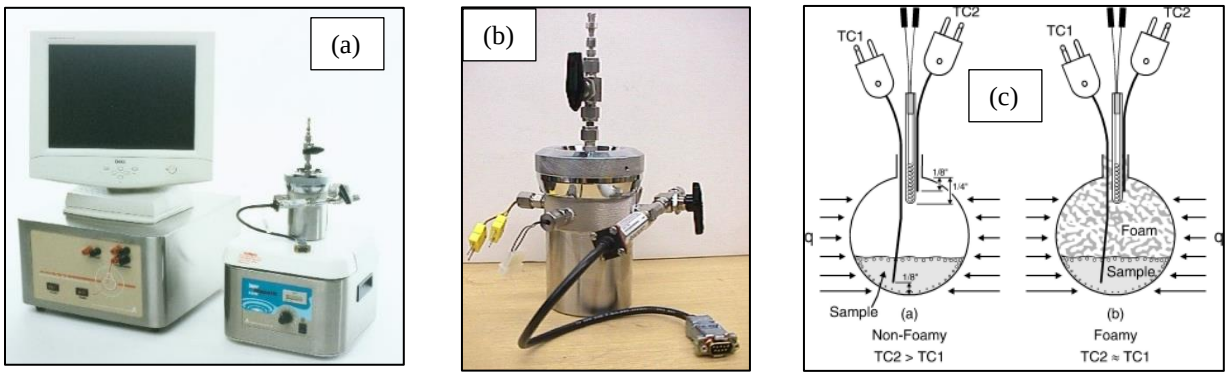


Figure 4. Advanced Reactive System Screening Tool (ARSST), purchased from Fauske & Associates, is used to determine the characteristics of reactive systems. The overall system (a) includes a stirrer, computer for data acquisition, and the vessel (b) in which the reaction takes place. The system can also distinguish between foamy and non-foamy reactions through the use of two thermocouples placed in the test cells (c).

Electrostatics Experiments

The electrostatics experiments include determining the liquid conductivity of hexane and other liquids using the apparatus shown in Figure 5. In addition, the powder volume resistivity (Figure 6) and powder chargeability (Figure 7) are determined for flour and corn starch. A humidity chamber (Figure 8) is utilized to control the humidity for the liquid conductivity and powder volume resistivity experiments Additional experiments, as described previously [1], include electrostatics involved with (i) human potential, (ii) unrolling plastic, (iii) pouring liquids and (iv) recirculating liquids. Furthermore, a demonstration of a propagating brush discharge is conducted as described previously [1].

Figure 5. Liquid conductivity apparatus purchased from Chilworth.

Figure 6. Powder volume resistivity apparatus purchased from Chilworth.

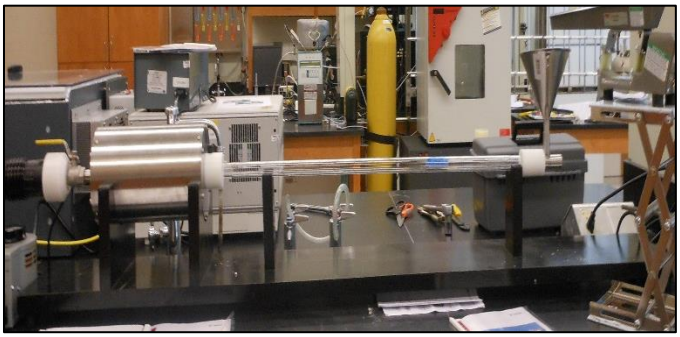


Figure 7. Powder chargeability apparatus purchased from Chilworth. This apparatus measures the change accumulated on powders resulting from transport through glass, metal and plastic tubes.

Figure 8. Humidity chamber purchased from Chilworth. This is used to control the humidity of electrostatic experiments that can be placed within the chamber.

Explosions Experiments

Gas phase and dust explosions are investigated in these experiments. The gas phase explosions (either methane or propane near stoichiometric concentration) are investigated in the MIE apparatus utilizing the highest energy level (Figure 3). This apparatus collects temperature-time and pressure-time data that is analyzed and used to size a deflagration vent as described previously [1]. Dust explosions are investigated qualitatively and quantitatively with a modified Hartmann Tube (Figure 9) and a Hartmann Bomb (Figure 10), respectively. The data collected from the modified Hartmann Tube are evaluated as discussed previously [1], while the Hartmann Bomb data include the pressure and rate of pressure increase. The deflagration index, St class and P_{max} are determined from the Hartmann Bomb data. These experiments utilize corn starch and wheat flour.

Figure 9. Modified Hartmann Tube Purchased from Adolf Kühner AG. This is used to obtain qualitative information about dust explosions.

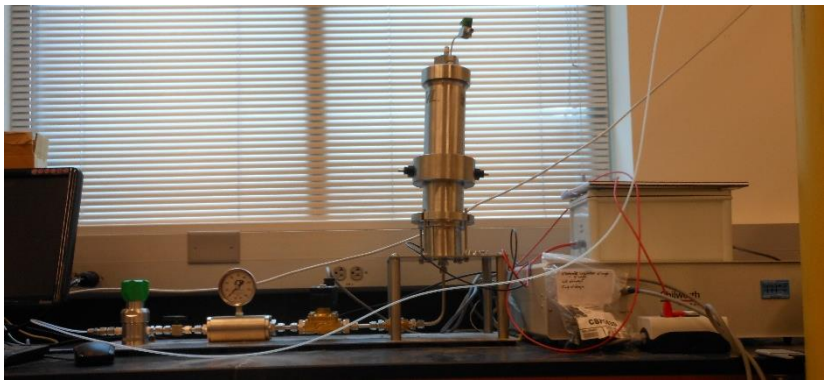


Figure 10. Hartman Bomb purchased from Chilworth. This instrument is used to investigate dust explosions and provide pressure-time data. These data are converted to rate of pressure (dP/dt) data with the equipment software.

Conclusions

The undergraduate Chemical Process Safety course at the University of Iowa is taken by chemical engineering juniors and consists of a lecture and a major laboratory component. The laboratory consists of flammability, reactivity, electrostatics and explosion experiments. The students also write extensive lab reports for each of these experiments. These hands on experiences make a major contribution to the students' understanding of chemical process safety.

References

1. Dorathy, B. D., Mooers, J. A., Warren, M. M., Mich, J. L., & Murhammer, D. W. (2001). Experiments to Demonstrate Chemical Process Safety Principles. *Chemical Engineering Education,* **35,** 36-44.
2. Crowl, D. A., & Louvar, J. F. (2011). *Chemical Process Safety: Fundamentals With Applications, 3rd ed.* Boston, MA: Prentice Hall.
3. SAChE Student Safety Certificate Program. (n.d.). Retrieved from http://sache.org/student_certificate_program.asp.
4. Products by Course. (n.d.). Retrieved from http://sache.org/products_by_course.asp.
5. Process Safety Messages for Manufacturing Personnel. (n.d.). Retrieved from http://sache.org/beacon/products.asp.
6. U.S. Chemical Safety Board. (n.d.). Retrieved from http://www.csb.gov/.
7. Chemical Reactivity Worksheet. (n.d.). Retrieved from http://response.restoration.noaa.gov/reactivityworksheet.
8. Student Design Competition. (n.d.). Retrieved from http://www.aiche.org/community/students/student-design-competition/past-problems.
9. Miniflash FLP/H/L Flash Point Tester. (n.d.). Retrieved from http://www.grabner-instruments.com/products/flashpoint/flphl.aspx.
10. Products. (n.d.). Retrieved from http://www.fauske.com/products.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Process Safety Academy (PSA) for first line supervisors

Hesham K. Al-Subait*, Seju Davis
Staff Process Safety Engineer – EHSS
Process Risk Management Dept.
SABIC
*Presenter Email: subaithk@sabic.com

Abstract

The intent of Process Safety Academy is to provide all operations day shift, shift Supervisors including new supervisors, a list of activities and behaviors considered proved practices that will help enhance their process safety leadership attributes and accelerate their assimilation into their jobs from the process safety perspective.

- These process safety specific behaviors that are not only aligned with but also complementary to the key EHSS leadership behaviors developed to help achieve EHSS excellence.

Key principles that are to be embedded in the supervisors approach to process safety.

- Process safety, the key element in SHEMS, OIMS, RCMS is the way, SABIC runs its Manufacturing Business.
- As operations leaders, it is critical that all supervisors show their process safety leadership. • It is not only about the words we use, it is about the quality time the supervisors spend on process safety and the way they act with regard to process safety as a core value.
- The organization will mirror what management thinks of process safety, so that these supervisors will place their energy on the areas they think are important to Kemya. The management's job is to make sure that what is important to SABIC, process safety in this case, matches what the supervisors perceive is important to SABIC management.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Flipping the assessment model: Teaching and assessing 'things that matter'

Christopher Lilburne*, Paul Lant, Maureen Hassall
UQ R!SK Research Group
School of Chemical Engineering
Faculty of Engineering, Architecture and Information Technology
University of Queensland, Australia
*Presenter Email: christopher.lilburne@uqconnect.edu.au

Key Words: Risk education, undergraduate education, knowledge transfer

Abstract

At The University of Queensland's (UQ) School of Chemical Engineering we are developing and delivering courses about operational risk concepts and practices for undergraduate engineers with a view to preparing them for work in the 'real world.' The courses on offer begin with the foundations of risk management (based on ISO31000) and professional engineering practice (based on guidance from professional bodies such as the IChemE, Engineers Australia and relevant legislation). We then challenge the students to move from *knowing* the concepts towards *acting* as and *being* professional engineers by conducting a number of immersive learning experiences across a variety of risk areas: personal safety, process safety, environmental, social, supply chains, projects and contractors.

Effective assessment of student's *acting* and *being* has proven a challenge using traditional methods such as exams and assignments. Until recently, assessment has been a combination of group assignments, online quizzes, a final exam and an individual end-of-semester interview. Our observation has been that aside from the individual interview, students have little opportunity to demonstrate their individual understanding of the course concepts beyond simple recall of definitions and case studies.

This paper is a review of the 2018 iteration of the final year undergraduate course that is on offer at the University. Significant changes were made to how content was delivered and how students were assessed.

Introduction

Across all industries effective risk management programs are necessary, and in many cases legislated, to meet business objectives. Over the last 100 years much has changed in how risk management is carried out (e.g. Mannan, Chowdhury et al. 2012, Hassall 2015) and it is now well established that mature risk management capabilities can reduce undesirable consequences such as work place fatalities, provide a platform to capitalise on the upside of uncertainty (Hillson 2010) and deliver and overall competitive advantages (Ernst & Young 2013). However, major safety and other types of incidents continue to occur (Marsh Energy Practice 2016) and be repeated (e.g. Pyy and Ross 2003, Fishwick 2012, Gill 2013, Waite 2013, Fishwick 2014).

Humans are crucial to risk management and at an individual level, mastery is heavily reliant on professionals adopting risk-based thinking that leverages experience, individual and industry knowledge, as well as the appropriate theoretical concepts and approaches. Early-career professionals, such as engineering graduates, often lack the experience and skill needed to effectively identify, assess and manage the wide range of risks that impact their industry.

The courses on offer at UQ seek to address this gap and provide students with a base level of knowledge of risk concepts to help them perform more effectively as graduate engineers. This paper focuses on the undergraduate, fourth year course which is undertaken by students in the School of Chemical Engineering: "Impact and Risk in the Process Industries." The course scope is broad, aiming to teach both fundamentals and detailed content that extends beyond health, safety and environment and includes social licence to operate, emerging technology, regulatory compliance, data management, climate change impacts, supply chain disruptions, and reputational risk (Hassall and Lant 2017). The breadth of risk management on which the course is based is shown in Figure 1. Approximately 200 students currently take the course.

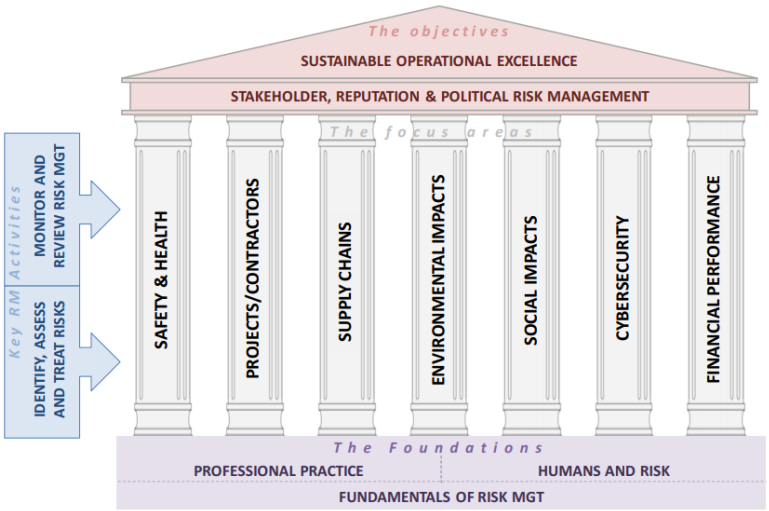


Figure 1 - The scope of risk management adapted from Hassall, Hannah et al. (2015)

The course

The course aims to help students understand, articulate and apply elements of risk management. The five course themes are shown below:

1. Understanding risks and their impacts – from technical, human, social, and environmental perspectives.
2. Professional engineering practice and risk – values, ethics, behaviour, accountabilities and obligations
3. Modern risk management approaches and tools
4. Humans and risk
5. Sustainability and risk

Importantly, the course seeks to push beyond the technical knowledge that the students already possess (shown in Figure 2) into a higher-level professional skill variously described as "phronesis & praxis", "acting and being" (Barnett and Coate 2005) or "hearts and hands" (Oliver and Dennison 2013). The higher-level, integrated thinking that is required from students is reflected in the 'pillar diagram,' which is referenced throughout the course (Figure 1) and the course learning activities (Table 1).

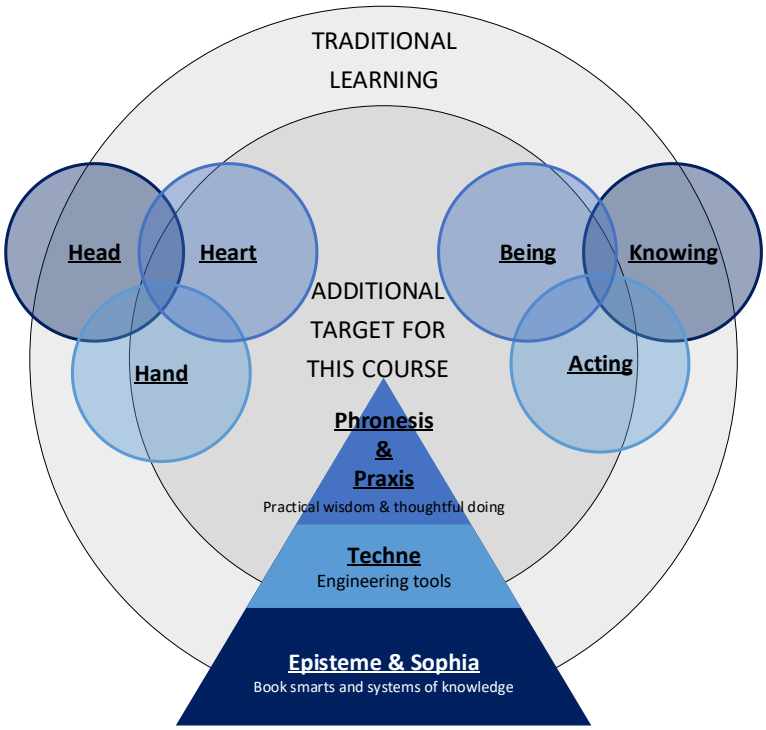


Figure 2 – Map of where course teaching and assessment methods are targeted

Table 1 - Course modules and learning activities adapted from Hassall and Lant (2017)

Modules	Key learning objectives
1. Fundamentals of risk management	What is risk and why is it so important? What types of risks are we considering? Risk, you and your decision making Understanding the risk management process (ISO31000) Understand risk identification and analysis theory and tools Understand and apply risk evaluation Selection and optimisation or risk controls and critical risk controls Management of controls – monitoring and review Communication and consultation
2. Professional practices	Understand what it means to be a professional engineer (ethics, competence and performance) Understand your own professional risk
3. Humans and risk	Understand the role that humans play in risk management in industry Understand that good engineering design is not just about preventing human error, it must also be about enabling successful human control Understand organisational safety cultures
4. Personal and process safety	Know the difference between personal and process safety Know the properties and classification of common workplace hazardous chemicals Know about some priority hazardous conditions that you are likely to encounter on manufacturing sites Discuss some of the major process incidents that have occurred and how they relate to personal and process safety
5. Risk review – event investigation	Use contemporary event investigation techniques which consider technical, human and organisational factors associated with incidents and unsuccessful events Consider how learnings can be integrated back into the business
6. Project risk	What is a project and what do we need to do to keep everyone safe? ALARP and HSE risk reduction in projects HAZID and HAZOP
7. Environmental risk	What does environmental risk look like? Legislation, regulation and the environmental impact assessment process Stakeholder analysis and management
8. Social risk	What does social risk look like? How are risks and opportunities identified and evaluated The social impact assessment process What is social licence to operate? Stakeholder analysis and management
9. Contractor and supply chain risk	What are supply chain risks and why do they matter? Understand contracting and the associated HSE risks Key activities in HSE contractor management

Focussed teaching methods

In the 2018 iteration of the course, contact time through formal lectures was significantly reduced although the modules and overall course content was retained (as per Table 1). Previously students attended a two-hour lecture (which included formal lectures, guest speakers and workshop-type activities) and a two-hour tutorial per week. In preparation for the 2018 course, transcribed lecture recordings were used to develop online, pre-recorded keynote lectures presented by the course coordinators, academic experts and guest lecturers. This process was resource intensive (100+ hours of work) however the outcome was a doubling of tutorial time i.e. time spent working in smaller groups collaborating and working with the teaching team. For example, in 2017, one tutorial session was used to cover all the incident investigation tools included in module 5 whereas in 2018 this was tripled to three sessions (which also allowed for time to work on assignments and ask questions). Figure 3 shows the differences between the 2017 and 2018 teaching activities.

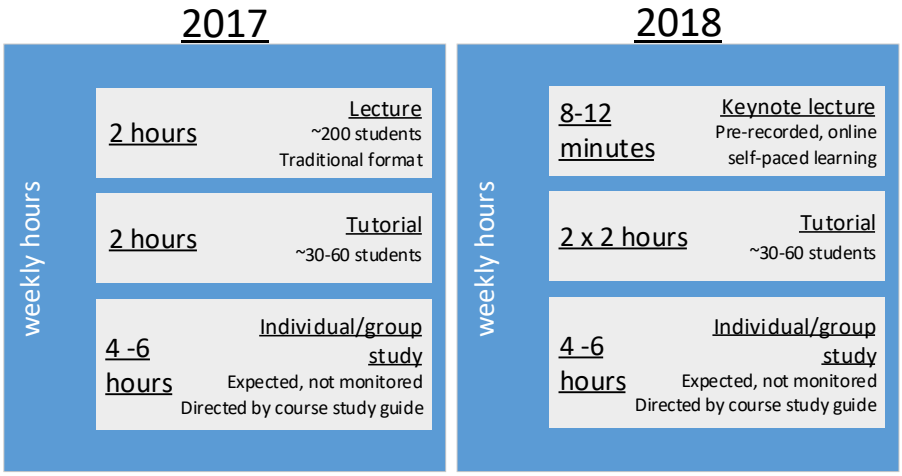


Figure 3 - Typically weekly learning activities (2017 compared to 2018)

Focussed assessment methods

As this course has evolved, the focus of the assessment has evolved from written assignments and an exam to the current model which comprises shorter technical submissions, two quizzes, and three oral exams. Figure 4 shows the differences in how the course is assessed - the oral exams now comprise 40% of the overall assessment. Since 2015, the course has used an end-of-semester oral exam to gauge student's understanding of the core course concepts. This one-on-one interview-based exam was originally introduced as a way to test critical thinking skills and how effectively students are able to apply concepts from the course. In 2018 the oral exam component of the course was nearly trebled and a group presentation was introduced. All the oral assessment, excluding the final interview is related to one of the three assignments and an average of 50% or more is needed in both of the individual oral assessments to pass the course. There are three key features built into the oral examination program designed to add transparency, robustness and integrity:

- All examiners (total of 12 in 2018) are qualified engineers with significant and current industry experience
- All interviews conducted by a single examiner are recorded

- A standard set of questions is used and interviews are marked using a standard marking rubric (which is given to students beforehand)
  The first and second oral exam are based on the written assignments which students produce in project teams of four students each. In the first written assignment (presented as a technical memorandum) students are required to conduct a risk assessment of a maintenance task and provide recommendations to site management. A short-technical report (with attachments) was chosen as the written deliverable to challenge students to prepare a synthesised summary of their findings and to mirror a more professional type of document. The technical memorandum also has the benefit that assessors can quickly read it in preparation for the interviews.
  In the first oral assessment, students are interviewed on their first assignment groups by two examiners. A half-hour group interview was chosen to ease the students into what might be an otherwise novel and intimidating process. The interview is framed around the students, having completed a risk assessment exercise, reporting their findings and being challenged by the client. The presentation and challenge process is useful in this instance as it allows the examiners to gauge how deeply the students have engaged with the task and to understand their thinking around ranking risks or designing recommendations. For this task, all members of groups were assigned the same grade although the written submission was subject to peer-review within groups.

  The second assignment requires students, in their groups to perform an incident investigation around an event related the scenario explored in assignment one – again the written component was presented as a technical memorandum. In the second, 15 minute, one-on-one interview students present their investigation findings and recommendations. They are challenged by the examiner on: how they came to their conclusions, the appropriateness of tools used and how investigation recommendations were prioritised. As with the first interview, this is a useful process to understand how well students understand the content and tools as well as how engaged they were with the task. Questions around strengths and limitations of different investigation techniques, priorities of recommendations, what are the 'must-dos' are useful to identify higher-level, critical thinking skills in students.
  The group presentations are framed around the third and final written assignment. The students, in their assignment groups prepare social impact management plans related to a proposed or actual project (e.g. carbon capture and storage or nuclear fuels transport). In the presentation they have 15 minutes to present their findings to an audience of stakeholders and respond to questions based on their presentation and written submission.

  Students take two quizzes through the semester to test their foundational knowledge of the course material however their overall knowledge of and engagement with the course is assessed in the final one-on-one interview. Students are asked to recall case studies covered during the course, describe one case study in detail and summarise the main learnings arising from it. They are also asked to synthesise other course topics with their chosen case study (such as describing the social risk aspects of the 2010 Macondo oil spill). To test their critical-thinking students are finally asked to describe how their overall learnings from the course might impact them when they work as graduates in industry or continue with further studies.

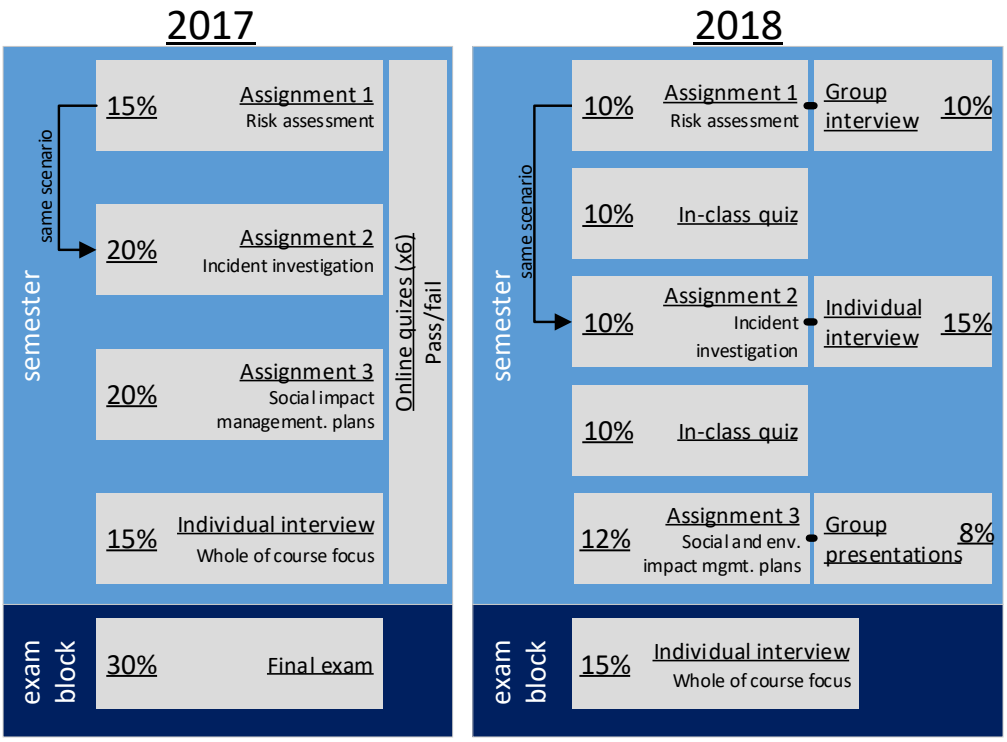


Figure 4 - Course assessment models (2017 compared to 2018)

Outcomes and discussion

In general, the new model of the course means a more costly product is delivered in terms of hours payed, number of people involved, complex logistics and the University facilities required. However, it is believed that more contact time in a tutorial setting and more effective assessment has led to a better overall outcome. From the authors' point of view the strengths, weaknesses, opportunities and threats around the changed teaching and assessment model are shown in Table 2.

A significant challenge has been gathering appropriate information to understand if the changes in the course have been effective from a student point of view. Informal feedback has been mixed but in general it seems students understand and accept the new assessment model without too much angst. At this stage, with the standard questions asked in the University's course evaluations, a detailed analysis has not yet been possible. More detail feedback and questioning will be put in place in the 2019 course to properly understand the impact of the changes.

Table 2 – Teaching and learning SWOT analysis of 2018 course delivery

Strengths	**Weaknesses**
Clearer focus on teaching and assessment activities in line with the targeted levels of knowledge (Figure 2) Increased 'time-on-task' i.e. small group tutorials led by experienced industry professionals Higher portion of teaching activities focused on helping students achieve a base level of expertise required of new professionals and masters level study (e.g. collaboration, workshopping, use of industry best practices) Higher portion of assessment activities aligned with the professional world (e.g. technical memoranda and interviews) allows identification of high and lower performers against course goals Greater focus on students' meaningful engagement with seminal case studies Online content provides a self-paced learning structure for students which easily be used for multiple iterations of the course	Learning objectives (particularly around professional practice and ethics) remain hard to clearly articulate and communicate to students i.e. hard to sign-post the course Resource intensive to develop, deliver and modify i.e. significant cost in terms of remuneration, coordination and room allocation Quality control in assessment may be an issue (real or perceived) due to high number of examiners with different backgrounds some of whom are not involved in delivering the course content Some students struggle in an interview scenario and outcomes may not reflect their knowledge e.g. English as a second language students Online lecture format makes incorporating guest speakers into the course a challenge Students can still be get a free ride in group work (though peer assessment helps identify 'passengers')
Opportunities	**Threats**
Expansion of risk, professional practice and ethics into other areas of curriculum and assessment is a significant opportunity Successful piloting of teaching and assessment format opens opportunities to expanded into different areas of the degree Opportunity to develop more online resources (e.g. videos of tools being used) – possibly shared across subjects, faculties and institutions Improved understanding of how students view the different methods of teaching and assessment via course more targeted surveys and feedback Sharing and feedback with other institutions offering similar subjects Continued integration of leading approaches (e.g. augmented reality) as well as further	Significant rework (and possibly cost) required if content becomes out-of-date or if course structure changed The non-conventional course content and structure means that the quality of the course is heavily reliant on existing staff and succession planning may be a challenge. Course content being taught and students being assessed by people without recognised competencies not experience in applying integrated risk-based optimisation approaches in process industry operations

exposure to real world environments and scenarios through field trips and practical learning	

Summary

This paper has provided an overview of the Risk and Impact in the Process Industries course taught to fourth year chemical engineering students at UQ. It has also described in some detail the assessment used to gauge the level to which students have learned about, and are adopting, risk-based thinking. Insights in the paper are based on some of the teaching team's (author's) observations and opinions. Further research is planned during the next iteration of the course to collect and assess students' perspectives on the course structure, teaching methods and how assessment is carried out.

References

Barnett, R. and K. Coate (2005). Engaging the Curriculum in Higher Education, Maidenhead : McGraw-Hill Education.

Ernst & Young (2013). Turning Risk into Results: How Leading Companies use Risk Management to Fuel Better Performance. https://www.ey.com/gl/en/services/advisory/turning-risk-into-results-managing-risk-for-better-performance, Ernst & Yound Global.

Fishwick, T. (2012). "Recurring accidents: Confined spaces." TCE The Chemical Engineer(854): 30-34.

Fishwick, T. (2014). "Recurring accidents: Slips, trips and falls." TCE The Chemical Engineer(873): 28-34.

Gill, G. (2013). "Recurring accidents: Inadequate isolations." TCE The Chemical Engineer(870): 52-56.

Hassall, M. E. (2015). Improving human control of hazards in industry. 19th Triennial Congress of the IEA, Melbourne.

Hassall, M. E., R. Hannah and P. A. Lant (2015). Lessons Learned from Teaching About Risks and Impacts in Industry. Hazards Australasia. Brisbane.

Hassall, M. E. and P. Lant (2017). Teaching Risk: a New Approach. The Chemical Engineer, The Institute of Chemical Engineers.

Hillson, D. (2010). Exploiting Future Uncertainty: Creating Value from Risk, Ashgate Gower.

Mannan, M. S., A. Y. Chowdhury and O. J. Reyes-Valdes (2012). "A portrait of process safety: From its start to present day." Hydrocarbon Processing **91**(6).

Marsh Energy Practice (2016). The 100 Largest Losses 1974-2015. Large Property Damage Losses in the Hydrocarbon Industry.

Oliver, P. and W. Dennison (2013). Dancing with Dugongs, IAN Press.

Pyy, P. and D. F. Ross (2003). Recurring events: a nuclear safety concern.

Waite, P. (2013). "Recurring accidents: Overfilling vessels." TCE The Chemical Engineer(861): 40-44.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Inherent Safer Design for Chemical Process of 1,4-dioldiacetate-2-butene Oxidized by Ozone

Min Hua, Lu Zhang, Xuhai Pan*, Xin-Miao Liang, Jiajia Jiang, Lei Ni
College of Safety Science and Engineering, Nanjing Tech University
Nanjing, Jiangsu, 210009, China
*Presenter E-mail: xuhaipan@njtech.edu.cn

Abstract

Oxidation reaction is the typical thermal runaway reaction. The reaction of 1,4-dioldiacetate-2-Butene oxidized by ozone was chosen to study the thermal hazards during the chemical process and the inherent safer designs (ISD) were proposed after analysis. The Qualitative Assessment for Inherently Safer Design (QAISD) was used to identify the risk during the chemical process. Meanwhile, the Reaction Calorimeter (RC1e) was used to analyze the thermal hazards of the chemical process. Two Inherent safer designs were proposed to increase the safe level of the process. ISD Ⅰ is the improved reaction condition of reaction temperature at -5℃ and ventilation rate of 200L•h-1, as well, ISD Ⅱ is using a tubular reactor. The results indicate that the classification of the reaction hazard was lower with improvements of two ISDs, and the severity was reduced by 43%. Moreover, the inherent safety level of the reaction was increased by ISD Ⅰ & Ⅱ of 63% and 43.4% respectively, which both have positive effects on inherent safety theories of "minimize", "substitute" and "moderate".

Keywords: runaway reaction, oxidation, thermal stability, inherent safer design.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Deficiencies Frequently Encountered in the Promotion of Process Safety Information

Horng-Jang Liaw
Department of Safety, Health, and Environmental Engineering
National Kaohsiung University of Science and Technology
1 University Road, Yanchao District, Kaohsiung, Taiwan
Email: hjliaw@nkfust.edu.tw

Abstract

Process Safety Information (PSI) is one of the fourteen elements of Process Safety Management (PSM). The findings of the PSI element in the PSM audit for more than 50 plants in Taiwan were reported in this manuscript, and such findings were not limited to the requirements of OSHA. The information pertaining to the hazards of the highly hazardous chemicals in process should not be limited to the Safety Data Sheet (SDS), although the information provided by the SDS satisfied the requirements of OSHA. The necessary information for the hazards of the highly hazardous process chemicals should considered the characteristics of the process. The unexpected process chemistry is more important than the expected one for the information pertaining to the technology of the process, from the safety viewpoint. The frequently encountered problem for the information pertaining to the equipment in the process is the inconsistence between the piping and instrument diagram and the real process.

Keywords: Process safety information; Process safety management; Safety data sheet

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

The Gulf Research Program's Initiative on Safer Offshore Energy Systems

Kelly Oskvig
Gulf Research Program
E-mail: KOskvig@nas.edu

Abstract

The Gulf Research Program (GRP) is a division of the National Academies of Sciences, Engineering, and Medicine established in 2013 as part of settlements in the criminal cases with the companies involved in the 2010 *Deepwater Horizon* disaster. Settlement funds totaling $500 million were designated toward a 30-year endowment to support grants, fellowships and other activities in three areas of responsibility: oil system safety, human health & well-being, and environmental resources.

In the initial years of the program, several initiatives were developed to focus the GRP's work and resources, one of which is the Safer Offshore Energy Systems Initiative. This initiative aims to foster minimization and management of risk to make offshore operations safer for both people and the environment in order to prevent oil spills, loss of life, and harmful exposures related to offshore operations.

Comprehensive risk awareness can help both industry and regulators to better anticipate, reduce, and avoid risks in the offshore energy environment. Through grants, workshops, studies, and other activities, the GRP aims to advance this understanding by supporting the following:

- Fundamental research needs in earth science, engineering and technology, and human and behavioral science that could promote safer offshore operations.
- Educational or training programs designed to promote a skilled and safety-oriented workforce, and
- Collaboration among researchers, industry, and regulatory agencies to advance understanding and communication about systemic risk in the offshore environment

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

How a Small E&P Company Manages SEMS (Safety and Environmental Management Systems) on Large Deepwater Drilling Operations

Charlie Culver
LLOG Exploration
E-mail: charliec@llog.com

Abstract

Presentation will cover how a relatively small company like LLOG (~200 employees) manages SEMS and HSE on large offshore drilling operations.

- Development of an effective SEMS (Safety and Environmental Management Plan).
- Benefits of the SEMS Plan
- Day to day implementation of the SEMS Plan – Offshore & Office
- Alignment of contractor policy and procedures with SEMS (bridging document)
- Using the right resources concurrently to implement contractor and operator SEMS
- Employee participation and management support of SEMS

Maximum 20 minutes of presentation from a power point presentation and 5 minutes for questions and answer.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

WellSafe Initiative– Chevron's Well Control Assurance Program

Mike French, *Chevron (Ret) WellSafe Project Manager*
Marcel Robichaux, *Chevron General Manager D&C Assurance*
Jeff Smith, *Chevron WellSafe System Manager*
Robert Hinojosa*, *P. E., WellSafe System Engineer*
*Presenter Email: RHinojosa@chevron.com

Abstract

Background

Well Control events are nothing new to the Oil and Gas Industry. Two of the more famous well control events took place more than 110 years apart; Lucas Gusher at Spindletop Jan 10, 1901 and Macondo April 20, 2010.

Whereas Spindletop was a welcomed event, Macondo was a catastrophe. Macondo was an event that cost 11 lives, the loss of a rig and billions of dollars in damages, and the untold cost associated with the Public's negative view of blowouts and the Oil & Gas Industry's inability to prevent them.

Shortly after the Macondo blowout, Chevron began looking inward to see what well control gaps existed in our operations. In late 2011 and early 2012 Chevron had two well control events of our own, Frade and Funiwa respectively. Through its review Chevron identified key opportunities to improve and standardize its well control practices.

The Creation of WellSafe

The creation of WellSafe began in the Fall of 2011 with an idea. That idea took shape In March of 2012, when the Chevron Drilling and Completions Leadership Team unanimously endorsed the WellSafe vision, "Design for Control, Guarantee Containment."

WellSafe is an assurance program that was created by Chevron's D&C community for Chevron's D&C community. WellSafe has one and only one focal point and that is Well Control. It is patterned after the United States Navy SUBSAFE program.

The Objective of WellSafe

The objective of WellSafe is to provide maximum reasonable assurance that well control is maintained at all times, on all operations under the direct control of the Chevron Drilling and Completions organization.

To provide this high level of assurance WellSafe encompasses all aspects and phases of well work. WellSafe is comprised of four Certification Types: 1) Business Unit Certification, 2) Rig Certification, 3) Well Design & Planning Certification, and 4) Well Execution Certification.

WellSafe Business Unit Certification

The foundation for Wellsafe is Engineering Standards. Within the Chevron system there are two types of Engineering Standards, D&C Process Standards and D&C Technical Standards. The Process Standards define the necessary steps and sequence for process used by Chevron. For example, the Planning Standard defines the timing and nature of information for the cross functional team to exchange in the planning sequence. It establishes, phase gates, hard lines for changes to objectives, after which MOC's are required. The objective of this standard is to ensure the D&C team is developing a plan that will meet the objectives of the Asset Team while optimizing the time and efforts of the D&C team. Another example of process standards is the Management of Change standard which details steps, required supporting documentation and approval level for changes in the plan at various points in the planning and execution of a well. Technical Standards, on the other hand, define the various design requirements specific to the equipment included in the standard. An example is the casing and tubing design standard which dictates, among other things, required design factors and confirmation testing requirements.

To achieve WellSafe Business Unit Certification a business unit or profit center must establish standard operating procedures that align with the Chevron D&C Engineering Standards. Exceptions are allowed only after being clearly defined, risk assessed and approved through the D&C Management of Change Process. The business unit must also establish systems for tracking of well control certification and specialized training, a system to induct personnel coming into the business unit and a system to on-board personnel as they are assigned to specific rigs. Also required are well control procedures for special operations, a defined review and approval process for well program, and all inflow tests (negative test). Defined processes for pre-tour checks, site supervisor handover, well control roles and responsibilities for 3rd party personnel where applicable. A program of well control drills is required. And a program for tracking defined metrics, quarterly rig assessments, annual rig audits, business unit self-audit and self-assessment processes must be in place.

WellSafe Rig Certification

The first pillar of WellSafe Certification is Rig Certification. To achieve Wellsafe Certified a rig must have in place systems or processes related to well control that include; a well control bridging document and a system for tracking contractors well control certification. Also required are rig specific procedures for hole monitoring and shut-in for the various activities the rig will or may regularly encounter, procedures to avoid or mitigate well control events, and procedures to comply with Chevron's specifications for, maintenance, calibration and documentation of,

well control equipment must be in place. Compliance with Chevron's requirement for well control drills must also be met, well control information must be posted on the rig floor, and driller's daily well control pre-tour checks must be completed.

Well Design & Planning Certification

The Second Pillar of WellSafe Certification is Well Design Certification. Requirements to achieve design certification include; definition of Value Based Well Objectives and listing of specific Design Uncertainties Impacting Well Control and the Potential Impact of All Uncertainties, an offset well review, Well Design Alternatives, Risk Assessments and Peer Review at specific points in the planning process, G&G Operations Review. Additionally, information for maintaining well control during construction and service life is required. The Well Specific requirements and success definitions are logged in Execution Assurance Requirements (EAR) Checklist. The contents of the EAR Checklist are reviewed and approved by a WellSafe Examiner who is external to the business unit.

Well Execution Certification

The final pillar of WellSafe Certification is satisfactory completion of the components in the well specific EAR Checklist. Each well's EAR Checklist serves as a roadmap through the WellSafe Well Execution Certification process. The WellSafe Well Execution Certification requirements define the verification criteria for each activity in the EAR Checklist. The WellSafe Examiner ensures compliance with the EAR Checklist by comparing the WellSafe Well Execution Certification requirements against the Morning Report, which serves as the OQE. The WellSafe Examiner signs off each activity in the EAR Checklist after final verification that the requirement has been fully satisfied during the execution phase. The BU shall initiate a management of change for any deviation from the EAR Checklist in accordance with the MOC process

WellSafe Authority

The WellSafe Authority is the organization within Chevron that is charged with maintaining the WellSafe Process and assisting each BU in compliance. The group consists of two parts: Firstly, the System Team which maintains the process and conducts regularly scheduled Assessments of each Business Unit to assist with compliance with the BU and Rig Certification Requirements. The second part of the WellSafe Authority is the Examination Team. This team is comprised of two region managers each with independent examiners assigned to individual Business unit. This portion of the WellSafe Authority is focused on assisting with compliance with the Well Planning and Execution requirements. The WellSafe Authority reports to Chevron's VP of D&C, through the General Manager of D&C Assurance.

Conclusion

WellSafe is a process designed and implemented by Chevron with one and only one focal point and that is Well Control. The WellSafe Program is built upon four Certification Types, Business Unit Certification, Rig Certification, Well Design & Planning Certification, and Well Execution Certification. Each certification is comprised of clearly defined requirements and objective definitions of compliance. When all components of the process are satisfied the well is deemed WellSafe Certified.

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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Ocean Energy Safety Institute, the First Five Years

M. Sam Mannan, Hans Pasman, James C. Pettigrew*,
Ocean Energy Safety Institute, 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: jim.pettigrew@mail.che.tamu.edu

Abstract

On 20 April 2010, the offshore drilling and production environment was tragically changed for both the American Oil and Gas industry and the U.S. Regulator. With the explosion and sinking of the Deepwater Horizon, the deaths of 11 rig workers, and the resultant 12-week oil spill; changes would be coming to the Industry. The Ocean Energy Safety Advisory Committee was soon commissioned and met for approximately two years. During this time the Committee, which had membership from Government, Industry, Academia and Non-Governmental Organizations, met and developed many recommendations for the Secretary of the Interior. One of these recommendations was for the creation of an 'Ocean Energy Safety Institute' or OESI. Specifically, "The DOI (Department of the Interior) should establish an OESI, reporting to the Director of the Bureau of Safety and Environmental Enforcement (BSEE) … the Institute would support BSEE missions regarding offshore safety and environmental management through various means." In 2013, a partnership of three Tier 1 research institutions was selected to conduct the mission of the OESI. These schools include Texas A&M University, the University of Houston, and the University of Texas – Austin. The OESI was charged to engage all stakeholders in Offshore Energy production, including Government, Industry, Academia and Non-Governmental Organizations. This engagement should be through opportunities for dialogue, collaborative research, and training opportunities. Throughout its first five years, OESI has led multiple Forums for Dialogue, which have developed topics for research as well as further discussion. Collaborative research efforts have begun between the partner universities, as well as other top research organizations, to help further enable safer offshore operations. Training and education opportunities began with classes for the Regulator, and have evolved into multiple Continuing Education selections. OESI is well on its journey to help further enable safer and environmentally responsible offshore energy operations; and with its new Consortium will be positively empowering all stakeholders offshore.