Summer 2015

Investigating new accident causation, risk assessment, and mitigation strategy selection tools in the petroleum industry

Mohammad A. AlKazimi

Department: Geosciences and Geological and Petroleum Engineering

Recommended Citation

AlKazimi, Mohammad A., "Investigating new accident causation, risk assessment, and mitigation strategy selection tools in the petroleum industry" (2015). *Doctoral Dissertations*. 2402.
https://scholarsmine.mst.edu/doctoral_dissertations/2402

INVESTIGATING NEW ACCIDENT CAUSATION, RISK ASSESSMENT, AND MITIGATION STRATEGY SELECTION TOOLS IN THE PETROLEUM INDUSTRY

by

MOHAMMAD ABDULHAMEED. ALKAZIMI

A DISSERTATION

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

In

PETROLEUM ENGINEERING

2015

Approved
Ralph Flori, Advisor
Susan Murray, Co-Advisor
Runar Nygaard
Francisca Oboh-Ikuenobe
Muthanna Al-Dahhan

PUBLICATION DISSERTATION OPTION

This dissertation has been prepared in the format of the publication option. Five articles are presented.

1. Pages 10-42 present this paper:
Hanan Altabbakh, Mohammad A. AlKazimi, Susan Murray, Katie Grantham, STAMP – Holistic system safety approach or just another risk model?, Journal of Loss Prevention in the Process Industries, Volume 32, November 2014, Pages 109-119, ISSN 0950-4230.

2. Pages 43-71 present this paper:
Mohammad A. AlKazimi, Katie Grantham, Investigating new risk reduction and mitigation in the oil and gas industry, *Journal of Loss Prevention in the Process Industries*, Volume 34, March 2015, Pages 196-208, ISSN 0950-4230.

3. Pages 72-80 present this paper:

"Exploring Risk Reduction and Strategy Selection Methodologies in the Petroleum Industry" which will be published in the proceeding of both the 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the 1st International Conference of Human Factors and System Interactions.

4. Pages 81-96 present this paper:

"Safety Awareness in Undergraduate Engineering Students." with authors Altabbakh, Hanan; AlKazimi, Mohammad A.; Murray, Susan and Grantham, Katie. Paper under 2nd review by *Professional Safety Journal*.

5. Pages 97-109 present this paper:

AlKazimi, M., & Altabbakh, H. (2014). Bridging the Health, Safety, and Environment Risk Management Proficiency Gap for Future Petroleum Engineers. *The ALJ in Student Research, 2*(Spring 2014).

ABSTRACT

The inherent complexity of the processes and the volatile nature of petroleum products compel the petroleum industry to continually seek and develop tools and techniques to identify, evaluate, and mitigate potential risks that can negatively impact their process operations. Additionally, government agencies and nonprofit professional societies guide the petroleum industry with regulatory guidelines, standards, and recommended best practices. The industry and these agencies and societies work to improve operational management, to ensure safe working conditions, and to minimize risk of all kinds, so that if failures occur, damage is contained within tolerable limits (Health and Safety Executives, 2013).

The currently used of both qualitative and quantitative risk assessment tools “fall short in identifying and ranking potential risks” in the petroleum industry and they “fail to demonstrate that risks have been reduced as low as reasonably practicable (ALARP)” (Fitzgerald, 2004, p. 3). Moreover, the tools are “limited to large, complex, and expensive studies” (Fitzgerald, 2004, p. 3). Because accidents due to both human errors and electromechanical failures still occur and result in various consequences, critics have raised concerns about the petroleum industry’s safety and risk mitigation credentials and question its ability to prevent major accidents.

The purpose of this research is to introduce new methods that provide more detailed and structure information to decision makers. They are more robust and easier-to-use so that novice engineers can successfully apply them without experts’ need. This dissertation employs the publication option, where the research results are reported by presenting the text of five journal-conference publications.

ACKNOWLEDGMENTS

First and foremost, I would like to thank Allah, the one and only, who has granted countless blessing, knowledge, and opportunity to successfully accomplish my PhD in petroleum engineering.

The devoted work of this dissertation could have not been done without the encouragement and guidance of a marvelous team of advisors. I thank Dr. Ralph E. Flori, my advisor, for his continuous support and trust to achieve my goal. In addition, I would like to express my deep thankfulness to Dr. Susan Murray, the committee co-advisor, who gave an inordinate amount of time structuring this project with her guidance, knowledge, and patience. Her support to oversee the completion of this project is exceedingly treasured.

Special thanks to Dr. Katie Grantham who served as a significant recourse and was of marvelous support during the progress of this work. In addition, I would like to thank Drs. Francisca Oboh-Ikeunobe, Runar Nygaard and Muthanna Al-Dahhan, for their direction, dedication and invaluable contribution as committee members on this project.

I am especially thankful to my beloved wife, Dr. Hanan Altabbakh, for her continuous encouragement, standing by me at all times, and her love and support to persuade my goal. Thanks to my children (Malak, Abdullah, and Jana) for understanding, patience, and nonstop love and care, as they were my ultimate reason to earn my degree. As a family, we are thankful, and blessed, to have a new precious member to our small family; A baby boy, who will bring more joy and happiness to our home.

I cannot forget to thank my wonderful mother who always kept me in her prayers and surrounded me with her never-ending love and encouragement. Thanks to my brothers and sister (Ali, Zaid and Noor) who always believed in me and motivated me to peruse my dream in achieving my goal. To all my friends, especially my dearest best friend Mr. Mohammad AlSarraf, and all my colleagues; thank you so much.

I would like to conclude by extending my sincere gratitude to both Kuwait Petroleum Corporation and Kuwait Oil Company, respectively, for giving me the opportunity to pursue my higher degree.

TABLE OF CONTENTS

Page

SECTION

PAPER

SECTION

LIST OF ILLUSTRATIONS

Paper 1 Page

Paper 2

Paper 3

Paper 4

LIST OF TABLES

Introduction Page

Paper 2

Paper 3

Paper 4

Conclusion

1. INTRODUCTION

The petroleum industry's commitment to safety has been criticized due to some catastrophic highly publicized accidents. For example, in December 2, 1984, more than 40 tons of methyl-isocyanate gas leaked from the Bhopal pesticide plant in India. This accident immediately killed more than 3,800 people, and an additional fifteen thousand died over the next few years as a result of inhaling the toxic fumes. Union Carbide India Limited (UNCIL) paid more than $470 million compensations (Broughton, The Bhopal disaster and its aftermath: a review, 2005). In July 6, 1988, the worst offshore accidents in the petroleum industry occurred off the coast of Aberdeen, Scotland in the North Sea. The Piper Alpha platform exploded, killing 167 out of the 228 crew members on board. The explosion destroyed the platform and the subsequent fires took three weeks to be brought under control. The damage greatly impacted the oil production in that sector, thus the company suffered more than $3.4 billion in financial losses (Cullen, 1993). In June 25, 2000, while maintenance crews were attempting to control a gas leak from a Liquefied Natural Gas (LNG) pipeline at Kuwait National Petroleum Company (KNPC) refinery, an explosion occurred and destroyed the entire facility. The explosion killed five workers who were near the leakage and injured more than 50 workers who were performing their routine maintenance activities on site. KNPC suffered financial losses exceeding $840 million from production losses, export operations, and cost to rebuild the facility.

Domestically, a series of explosions destroyed BP's Texas City Refinery during the start-up process of their Hydrocarbon-Isomerization unit in March 25, 2003. The accident resulted in 15 casualties and more than 170 workers were injured. This accident impacted BP financially with more than $2 billion in penalties and other compensations (Saleh, Haga, Favarò, & Bakolas, 2014). In April 20, 2010, Trans-Ocean's Deepwater Horizon rig experienced a disastrous blowout while preparing to move-off of the well in BP's Macondo Prospect of the Mississippi Canyon block 252 in the Gulf of Mexico. Of the 126 crewmembers onboard the rig, 11 were killed in the initial explosion and many of the rest of the surviving crewmembers were air lifted to get medical treatment. The rig sank after burning for two days. This blowout resulted in the worst environmental catastrophe in U.S. history by gushing more than 4.9 million barrels of crude oil into the Gulf of Mexico. In addition, BP suffered financial losses exceeding $25 billion (Kerr, Kintisch, & Stokstad, 2010). In August 25, 2012, a gas leak in Venezuela's Paraguana Refinery Complex created a massive explosion, destroying the refinery, and killing 41 workers (Petroleumworld.com, 2014).

Major petroleum industry accidents such as these result in many significant impacts. Environmentally, oil spills and their refined products contain toxins that contaminate both land and marine ecosystems (The Commonwealth Scientific and Industrial Research Organisation, 2013). For example, hydrocarbon products do not dissolve in water. As a result, the thick layer of sludge can block plankton and photosynthetic aquatic plants (sea-life food) from reproduction, prevent birds from flying due to oil caught on their feathers, and kill fish and other marine life due to asphyxiation (The Commonwealth Scientific and Industrial Research Organisation, 2013). Moreover, the environmental damage includes underwater soils and reefs that are natural habitat to marine life (Ronza, Lázaro-Touza, Caro, & Joaquim, 2009). A major tool used to battle oil spills is the use of chemical dispersant agents, but these have their own toxicity and deleterious effects, regardless of their benefits in dispersing crude oil (Etkin, 1999). As a final example, more than eight hundred Kuwaiti oil wells were set on fire by retreating Iraqi forces during the 1999 Desert Storm war, producing a terrible and senseless environmental disaster (Seacor, 1994).

Human health and wellness have been impacted by major accidents in the petroleum industry. The Bhopal gas leak disaster in 1984 killed more than 3800 in the first few days of the accident as a result of inhaling Methyl-Isocyanate (MIC) gas (Sharma, 2002). Moreover, an estimate of 15,000 to 20,000 premature deaths reportedly occurred in the subsequent two decades following the accident, as the Indian government reported that more than half a million people were exposed to the gas (Broughton, 2005). Seactor (1994) reported an increase lung cancer and skin diseases in Kuwait due to exposure to toxins from burned hydrocarbons from Kuwaiti oil wells. The 1988 Piper Alpha explosion claimed one hundred sixty seven lives, but many more of lost crew members' families and relatives were psychologically impacted due to the loss of their loved ones (Kirchsteiger, 1999).

Financially, nearby communities and various stakeholders suffered from the impact of the petroleum accidents. Financial impacts include operational losses instead of profit, loss in compensation, and legal penalties. Accidents suspend operations causing a loss of production and downtime losses, reducing a company's marginal profit (Cohen, 1993). The tourism industry in the Gulf Coast generates an average of $34 billion in revenues; the Deepwater Horizon oil spill resulted in contaminating the Gulf shores and resulted in a significant loss of $11 billion due to tourists avoiding those areas. To recoup their losses, Gulf shore business owners such as real estate, recreation, and fisheries, filed civil lawsuits from which BP could face $20 billion in legal penalties (Perry, 2011). These accidents and many more, are some of the few examples that negatively impacted the petroleum industry (Anderson & LaBelle, 1994; Davies, 2010). Table 1 list 15 example cases out of a 319 major industrial accidents since 1917. Of the 319 total, an astonishing 307 were in the petroleum industry (Mihailidou et. al, 2012). .

Table 1. List of Industrial Accidents

Accident #	Country	Location	Function of Failed Part	Failure Mode	Mitigation Strategy
1	USA	Gulf of Mexico	import mixture/transfer mixture/export mixture (pipeline/tube)	creep buckling/stress rupture	shape part
2	China	Harbin	nont petroleum		
3	India	Jaipur	import mixture/transfer mixture/export mixture (pipeline/tube)	ductile rupture/stress rupture/surface fatigue	regulate flow/stabilize flow
4	Australi a	Varanus Island	import mixture/transfer mixture/export mixture	corrosion fatigue	convert material
5	China	Guangxi Zhuang	no detailed case studies were available		
6	S. Korea	Icheon	import mixture/store mixture/export mixture (reservoir)	cracking/stress rupture	extract containment/stop process/inhibit temperature/
7	Iran	Arak	import mixture/store mixture/export mixture (Reservoir)	cracking/stress rupture	extract containment/stop process/inhibit temperature/

Table 1. List of Industrial Accidents (cont.)

8	UK	SunBury	import mixture/transfer mixture/export mixture (pipeline/tube)	cracking/stress rupture	inhibit moisture
9	Nigeria	Lagos City	import mixture/transfer mixture/export mixture (pipeline/tube)	stress rupture/impact fracture	decrease load
10	USA	Texas	import mixture/store mixture/export mixture (Reservoir)	brittle rupture/stress rupture	inhibit temperature
11	UK	Hertfordshire	import electrical energy/change electrical energy/guide electrical energy/regulate electrical energy/guide electrical energy/transfer electrical energy/ guide electrical energy (circuit board)	bonding defect	decrement noise/inhibit noise
12	China	Jilin	import mixture/store mixture/export mixture (Reservoir)	brittle rupture/stress rupture	regulate flow/stabilize flow/extract containment/inhibit containment
13	Algeria	Skikda	import mixture/store mixture/export mixture (Reservoir)	low cycle fatigue/surface fatigue wear	condition material/condition part/regulate flow
14	USA	Dalton	import mixture/transfer mixture/export mixture (pipeline/tube)	Electro-migration/cracking/stress rupture/	inhibit temperature/inhibit containment/separate containment
15	Belgium	Ghislenghien	import mixture/transfer mixture/export mixture (pipeline/tube)	impact fracture/brittle fracture/impact wear	decrease load/secure part

The inherent complexity of the processes and volatile nature of petroleum products compel the petroleum industry to continually seek and develop tools and techniques to identify, evaluate, and mitigate potential risks that can negatively impact their process operations. Additionally, government agencies and nonprofit professional societies guide the petroleum industry with regulatory guidelines, standards, and recommended best practices. The industry and these agencies and societies work to improve operational management, to ensure safe working conditions and to minimize risk of all kinds, so that if failure occur, damage is contained within tolerable limits (Health and Safety Executives, 2013). Important in this are risk assessment tools, which are used to assist in the systematic identification and assessment of risk.

The currently used qualitative and quantitative risk assessment tools "fall short in identifying and ranking potential risks" in the petroleum industry and they "fail to demonstrate that risks have been reduced as low as reasonably practicable (ALARP)" (Fitzgerald, 2004, p. 3). Moreover, the current qualitative and quantitative risk assessment tools are "limited to large, complex, and expensive studies" (Fitzgerald, 2004, p. 3). Because accidents due to both human error and electro-mechanical failures still occur and result in various consequences, critics have raised concerns about the petroleum industry's safety and risk mitigation credentials and question its to prevent future major accidents.

The purpose of this research is to introduce several new accident causation, risk ranking and assessment, and mitigation strategy selection methods which provide more detailed and structure information to decision makers. These new methods, though sophisticated, are more robust and easier-to-use so that novice engineers can successfully apply them. They do not require experts. This dissertation employs the publication option, where the research results are report by presenting the text of five journal/conference publication.

The first paper titled "STAMP - Holistic System Safety Approach or Just Another Risk Model?" is published in the *Journal of Loss Prevention in the Process Industries*. Researchers in the safety field are facing more challenges everyday with the expanding modern socio-technical systems. Safety analysis such as hazard analysis, accident causation analysis, and risk assessment are being revisited to overcome the shortcoming of the conventional safety analysis. Different risk assessment models have been analyzed to explore both their advantages and disadvantages (Altabbakh, Murray, Damle, & Grantham, 2012). However, with increasingly complex human system interaction in today's modern systems, new safety challenges are being faced that need to be assessed and addressed. Indeed, new or improved risk assessment tools that can address these complexities are needed. Unlike conventional accident causation models, System Theoretic Accident Modeling and Processes (STAMP) is not based on chain of events. It is based on system theory where each level or the organization plays a major role in contributing to an accident or attaining successful system safety controls. Thus, STAMP prevails conventional accident models by accounting for organizational factors, human error, and adaptation to change over time. In STAMP, system safety is not achieved by preventing component failure measures; in fact, it is achieved by enforcing safety constraints continuously (Leveson, 2004). Therefore, accidents do not occur because of failure of components, they occur because of ineffective safety constraint where main focus is not on how to prevent failure, but on how to design better safety controls.

The second paper titled “Investigating New Risk Reduction and Mitigation in the Oil and Gas Industry” is also published in the *Journal of Loss Prevention in the Process Industries*. The paper addresses the need for an early and precise risk assessment is essential to forecast and mitigate potential accidents from taking place, especially at the conceptual design stages (M.F. Milazzo, 2013; Lough et. al, 2009). The team developed Risk in Early Design (RED) theory to generate a list of possible product risks. The software allows users with limited experience to predict both when and where a product may fail by simply knowing the function of their product. The product risks are based on historical data of product input function and rank them by their occurrence likelihood and consequence (Lough et. al, 2008). Functioning as both as failure mode identification and risk ranking tool, Risk in Early Design (RED) is custom software that allows users to leverage failures from other products to help predict what may go wrong with the user's product. RED promotes failure prevention by identifying failure risks as early as the conceptual design phase, where impacts of failure prevention are furthermost. It does this by using subject specific knowledge-bases populated by historical failure events in a variety of categories such as product failures, software failures, and business failures. The user simply selects the functions of the item that is undergoing a risk assessment and the type of assessment desired. The information quickly communicated by the RED software is the function (i.e. potential failure location), failure mode, risk likelihood, and risk consequence via mathematical mapping processes (Grantham Lough, Stone, & Tumer, 2005). It also categorizes the output into high, medium, and low risk areas. To verify RED’s capability in identifying failure modes, approximately thirty major accidents due to electro-mechanical failures were randomly selected to undergo the evaluation. Hence, the software was not originally designed to identify potential failure modes in the oil and gas industry.

The first step in performing an accurate RED analysis is selecting the functions performed by components in the system. These functions can be selected from a list of "electromechanical functions" cataloged in the RED software tool. The analysis identifies potential causes of failures that could interrupt operations. The generated RED analysis signifies failure modes for the selected component. In order to verify the results of RED analysis, accident reports issued by either government agencies were cross-referenced. Hence, the reports identify both the component location and the cause of the failure. Four case studies with different causes of failure modes are list to demonstrate the capability of the software to identify failure modes contributed to the accidents.

The third paper titled "Exploring Risk Reduction and Strategy Selection Methodologies in the Petroleum Industry" is an accepted conference paper in the *6th International Conference on Applied Human Factors and Ergonomics*. The paper addresses proposed solutions are providing prompt and inexpensive tool to risk identification, ranking and mitigation of potential electromechanical failure modes in the petroleum industry by applying both Risk in Early Design (RED) and Generated Risk Effect Event Neutralization (GREEN), respectively. The specific applications of their approaches will focus on the following petroleum production systems such as, but not limited to, pipelines, gas turbines, pumps, heat exchangers, and distributed control systems (DCS). These focused areas were chosen since they have a high failure rate (EPA, 2013; Barends et. al, 2012) and both RED and GREEN have shown to reduce and mitigate risks of electromechanical failure modes in these types of electromechanical components in previous work (Lough et. al, 2009). RED identifies, and ranks, potential failure modes with their locations in electromechanical products (Lough et. al, 2009). GREEN recommends risk mitigation strategies methods to reduce the failure mode likelihood and/or consequence (Krus & Grantham, 2013). The major difference between the products in the petroleum industry and those in which RED and GREEN have been previously tested is the operations environment. The new addition to this tool is amalgamating the human factor aspect in the industry due to its importance with the merging complex technologies. The close interaction between human and machines in a very volatile process environment makes it necessary to consider human system integration and human factors part of the overall system design. Hence, this consecration will look into risk from different perspectives resulting in design safety and operating efficiency.

“Safety Awareness in Undergraduate Students” is the title of the fourth paper submitted to the *Professional Safety Journal*. It discusses accidents among engineering and science students in college workshops and labs have resulted in either severe injuries or tragic fatalities. Students with technical majors are required to take scientific laboratory courses and they apply their knowledge by engaging in various competitive technical design teams. Such involvement requires them to spend time in labs and/or workshops, both of which can be hazardous environments. Consequently, college students’ safety mindset can be essential in both in and outside the classroom setting. In a few years, and after earning their degrees, these students will put their knowledge into practice to be engineers and scientists in the workforce. Their safety awareness and attitude towards risk is often being formed in college and will follow them into their professional career. In an effort to prevent accidents and improve safety cognition in young engineers and scientist, this study examines the training exposure and knowledge within technical competition teams from the students’ perspectives. A survey targeting different OSHA safety areas was conducted to measure safety training, knowledge, and attitude of these undergraduate students. The paper, also, explores potential causes of unsafe decision making by the students surveyed.

Finally, the fifth paper titled “Bridging the Health, Safety, and Environment Risk Management Proficiency Gap for Future Petroleum Engineers” focuses on investing in human capital, by establishing health, safety, and environmental risk management course to young engineers as another method of risk mitigation due to ongoing demand for more HSE engineers to be part of the petroleum industry. The expansion of the oil industry resulted in a scarcity of these engineers to overlook both the performance of process operations and potential risk management strategies. The paper also defines the establishment of a new focus area in health, safety, and environment risk management in the petroleum engineering program at Missouri University of Science and Technology. The goal of the program is to meet the job market demand for engineers in that focus area in petroleum engineering. In addition, the availability of the program will enhance student’s communications skills, safety awareness, ethical responsibilities, and most importantly, creating an improved safety culture by exposing different health, safety and environment risk management awareness and knowledge specifically to cater for the oil and gas industry

PAPER

I. STAMP – HOLISTIC SYSTEM SAFETY APPROACH OR JUST ANOTHER RISK MODEL?

Hanan Altabbakh, Missouri S&T
Mohammad Alkazimi, Missouri S&T
Susan Murray, Missouri S&T
Katie Grantham, Missouri S&T

Abstract

Risk management has a number of accident causation models that have been used for a number of years. Dr. Nancy Leveson (2002) has developed a new model of accidents using a systems approach. The new model is called Systems Theoretic Accident Modeling and Processes (STAMP). It incorporates three basic components: constraints, hierarchical levels of control, and process loops. In this model, accidents are examined in terms of why the controls that were in place did not prevent or detect the hazard(s) and why these controls were not adequate to enforcing the system safety constraints. A STAMP accident analysis is presented and its usefulness in evaluating system safety is compared to more traditional risk models. STAMP will be applied to a case study in the oil industry to demonstrate the practicality and validity of the model.

Keywords

Risk assessment, Accident causation, Hazard analysis, Human error, Complex System

1. Introduction

Researchers in the safety field are facing more challenges everyday with the expanding modern socio-technical systems. Safety analysis such as hazard analysis, accident causation analysis, and risk assessment are being revisited to overcome the shortcoming of the conventional safety analysis. With increasingly complex human system interaction in today's modern systems, new safety challenges are been faced that needed to be assessed and addressed. Indeed, new or improved risk assessment tools that can address these complexities are needed.

2. Hazard Analysis

Hazard analyses are tools used to detect and classify hazards within a system, subsystem, components, and their interactions. The main purpose of the analysis is to identify hazardous conditions or risks and eliminate them or mitigate them (Federal Aviation Administration, 2008). Hazard analyses identify hazards, their consequences, and their causes to determine system risk and means of mitigating or eliminating those hazards (Ericson, 2005). Ericson categorized hazard analyses into types and techniques.

Types would typically determine analysis timing, depth of details and system coverage; while techniques would specify the methodology used in the analysis. There are seven types of hazard analysis with regards to system safety (Ericson, 2005):

- Conceptual design hazard analysis type (CD-HAT) (concept)
- Preliminary design hazard analysis type (PD-HAT) (preliminary)
- Detailed design hazard analysis type (DD-HAT) (preliminary)
- System design hazard analysis type (SD-HAT) (test)
- Operations design hazard analysis type (OD-HAT) (test)
- Health design hazard analysis type (HD-HAT) (operation)
- Requirements design hazard analysis type (RD-HAT) (final design)

Each category describes a stage of system life, details required from analyses, information available to begin with, and analysis outcome. There are more than 100 hazard analysis techniques available (Stephens & Talso, 1999; Federal Aviation Administration, 2008).

Hazards analysis not only identifies what could fail in a system, but also identifies the potential consequences, the reason why it could happen, what are the causal factors, and the likelihood of it happening. Unfortunately, conventional hazard analyses are more focused on direct cause and effect relationship following the famous dominos chain of events (Hollnagel, 2004). There are several techniques for hazard analysis to be considered when assessing hazards in a system. Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Hazard and Operability Analysis (HAZOP) are examples of the traditional ones. However, the available tools are not designed to accommodate all the different complex systems available. It is the job of the analyst to choose the model that best fit the system under investigation. Depending on the type of risks to be assessed, whether risks at components level, human error, human machine interaction or organizational level (Altabbakh et al, 2012). An overview of each of the methods is discussed below.

2.1 Failure Mode and Effects Analysis

Failure Mode and Effect Analysis (FMEA) is a bottom up inductive (forward approach) risk assessment tool that can be used to identify failure modes that would negatively impact the overall system. FMEA is classified as a DD-HAT type of hazard analysis. It evaluates the effect of these potential failure modes to determine if changes are necessary at any stage of the system to overcome such adverse events (Ericson, 2005). It is very advantageous to apply FMEA at early stages of the system to increase safety since changes, if suggested by FMEA, can be with minimal cost (Dhillon, 1999).

On the other hand, FMEA emphasizes on single failure in isolation and it is not geared toward multiple failures in combination although some hazards arise from other multiple hazards or events and not necessarily mechanical or electrical failure modes (Ericson, 2005). Another drawback is that FMEA does not account for failures that occur due to human error in complex systems (Foster, et al., 1999). In addition, FMEA is considered time consuming due to the detailed structure of the analysis.

2.2 Fault Tree Analysis

Fault Tree Analysis (FTA) is a top down deductive (backward approach) risk assessment tool that determines failures and contributing factors of adverse events in a system. FTA is classified as a DS-HAT and DD-HAT hazards analysis type. Fault trees employ graphical diagrams and logic gates to represent the relationship between failures and other events in the system and its primary objective is to identify the causal factors of a hazard in the system. Fault trees are based on root cause analysis and they depict the cause effect relationships between the root cause events visually (Ericson, 2005). In spite of the fact that fault trees requires that analysts study systems under investigation thoroughly to eliminate overlooking potential risks factors (Dhillon, 1999), it still lacks the ability to capture human error due to the complexity of human behavior that will complicate the analysis (Kirwan & Ainsworth, 1992). In addition, due to its lengthy details nature, fault trees consume time and accumulate size, which makes it hard to form into reliability reports.

2.3 Event Tree Analysis

Event Tree Analysis (ETA) is a bottom up inductive risk analysis technique that identifies and evaluates potential accident and its possible related chain of events (Ericson, 2005; Khan & Abbasi, 1998). ETA is classified as a SD-HAT type of hazard analysis. The analysis starts with an initiating event and goes further in evaluating every possible outcome that can results accordingly. Safety constraints are evaluated in each path (accident scenario) whether they are enforced adequately or needs to be addressed in order for the selected path to execute smoothly without a failure or an accident. Event trees are easy to learn and apply and they combine human, machine, environment, and human interaction (Ericson, 2005). Unfortunately, event trees only allow one initiating event at one time. Multiple initiating events will have different trees, which will be time consuming and trees will be lengthy.

2.4 Hazard and Operability Analysis

HAZard and OPerability analysis (HAZOP) is a technique that is used to identify hazards in a system to prevent adverse events. (Kletz, 1999). It is classified as a PD-HAT and the DD-HAT hazard analysis type. It starts with a brainstorming session where concerned people in an organization will use their imagination to determine all possible scenarios where hazards or failure might occur, in a systematic way (Kletz, 1999). HAZOP is useful to apply to systems that involve human performance and behavior or any system that involve hazards that are hard to quantify or detect. On the other hand, HAZOP does not take into account the cognitive ability of human as of why they would commit an unsafe act, which is a weakness point of HAZOP. Thus, HAZOP analysis is not standardized worldwide, hence, the analysis is performed differently with variation in results for the same system (Pérez-Marín & Rodríguez-Toral, 2013). Moreover, HAZOP study does not take into account the interaction between different component in a system or a process (Product Quality Research Institute, 2013), and it also can be lengthy, time consuming and expensive (Redmill, 2002).

3. System Theoretic Accident Model and Processes - Introduction

System-Theoretic Accident Model and Processes (STAMP) is a new comprehensive accident causation model created by Dr. Nancy Leveson to analyze accidents in systems (Leveson, A New Accident Model for Engineering Safer Systems, 2004). Leveson suggested that with the evolving changes in technology since WWII and the emerging massive complexity of systems components a new approach is needed to overcome such pitfalls of traditional accident models. Rapid speed of technology revolution and digitalized systems, introduced new types of accidents and hazards. Accordingly the human system integration relationship is becoming more complex.

System analysis is useful when analyzing complex accident involving software, organization hierarchical and management, human limitations including decision-making and cognitive complexity. Traditional accident causation models lack the ability to investigate such complex systems. Not only can STAMP be used to analyze existent accidents, but also it can be utilized to design for a safer system during the system development stage to prevent accidents (Leveson, 2003). STAMP views systems as dynamic processes with continuous changes with respect to product/process design, management, technologies, workforce and such. At the design stage, STAMP emphasizes enforcing not only safety constraints to the existent design, but also for future change and adaptation such as change of technologies, nature of accidents, type and nature of hazards, complexity of human system interaction, and safety regulations (Leveson, 2004).

Most conventional accident causation models view an accident as a result of a series of events adapted from the Domino Theory (Hollnagel, 2004), where one event leads to the next. Using this approach, efforts are made by investigators to identify the first adverse event in the chain and prevent it from happening without considering environmental, organizational, or human contributions. FMEA, FTA, ETA, and Cause-Consequence Analysis are based on this approach (Leveson, 1995). They do not work well for complex system involving human behavior because they are based on linear chain of events and assume accident is a result of a component failure not accounting for accident happening where all components are compromised without failure (Hollnagel, 2004). A common drawback of these conventional chain based accident models is that once the root cause was identified, the blame tends to be assigned (often to the operator) and the analysis stops (Leveson, 2004).

The three main principles of STAMP are safety constraints, hierarchical control structure, and process models (Leveson, 2012). First, safety constraints are enforced through safety controls, which if adequately implemented will prevent adverse events from happening. An example of safety constraints in the Space Shuttle Challenger would be that the temperature should be greater than or equal to 53 degrees in order for the shuttle to launch (Kerzner, 2009). Second, hierarchical control structure represent an essential step in applying STAMP where each level of the system contributes to the safety or to accidents in a system. Each level of the hierarchy enforce safety constraints to the level below it, and each level below have to give feedback on how these constraint are successfully implemented or ineffectively failed. Consequently, higher levels of hierarchy are responsible of the performance of the lower levels through enforcing safety constraints. Missing constraints, inadequate safety control command, commands not executed properly at lower level, or inadequate feed back communications about constraints are the main reasons of inadequate controls. Third, four conditions must exist for a process to be controlled under STAMP model (Leveson, 2012). Goal (enforcing safety constraints in each level of the hierarchy structure by controllers), Action Condition (implement actions downward the hierarchy structure), Observatory condition (Upward the hierarch), and model condition (the controller's model of the process being controlled), which in our case is the process model. Essentially, without the latter one, a process would not adequately be controlled.

Unlike traditional accident causation models where the root cause consist of an event or chain of events, STAMP focus on investigating the cause of an accident by identifying the safety control that were inadequately enforced, or sometimes not enforced at all (Leveson, 2012). Accidents therefore are considered as a result of interactions among system components and the lack of control of safety related constraints, no blame is pointed to a single component nor blame pointed towards and individual human (Leveson, Daouk, Dulac, & Marais, 2003). For example, in the Space Shuttle Challenger Disaster, the main cause for the accident was the faulty of the solid rocket booster (SRB) o-ring seal. However, applying system approach risk assessment models revealed more contributing factors such as decision makers, line managements, politics, safety environment, and ineffective communication (Altabbakh, Murray, Damle, & Grantham, 2012). Furthermore, STAMP would continue the analysis with questions such as, why did the o-ring fail to adequately control the released propellant gas? In STAMP, accidents are not viewed as failures; instead they represent violation of safety constraints.

They can occur when existing safety controls are missing or ineffective. Thus the safety of a system is considered a control problem, a control of the safety constraint. Dr. Leveson explains, "Accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system (Leveson, 2004)."

3.1 STAMP Analysis

Unlike conventional accident causation models, STAMP is not based on chain of events. It is based on system theory where each level or the organization plays a major role in contributing to an accident or attaining successful system safety controls. Thus

STAMP prevails conventional accident models by accounting for organizational factors, human error, and adaptation to change over time. In STAMP, system safety is not achieved by preventing component failure measures; in fact, it is achieved by enforcing safety constraints continuously (Leveson, 2004). Therefore, accidents do not occur because of failure of components, they occur because of ineffective safety constraint where main focus is not on how to prevent failure, but on how to design better safety controls.

STAMP has been utilized to analyze multiple post accidents (Leveson, 2002) (Leveson & Laracy, 2007). Studies showed that utilizing STAMP to analyze accidents have revealed more hazards and potential failures in systems than other traditional hazard analysis or accident causation models (Song, 2012). Figure 1 depicts the taxonomy of contributory factors in accidents by investigative each component of a control loop and identifying how each component’s, if improperly operated, can add to the inadequacy of safety control.

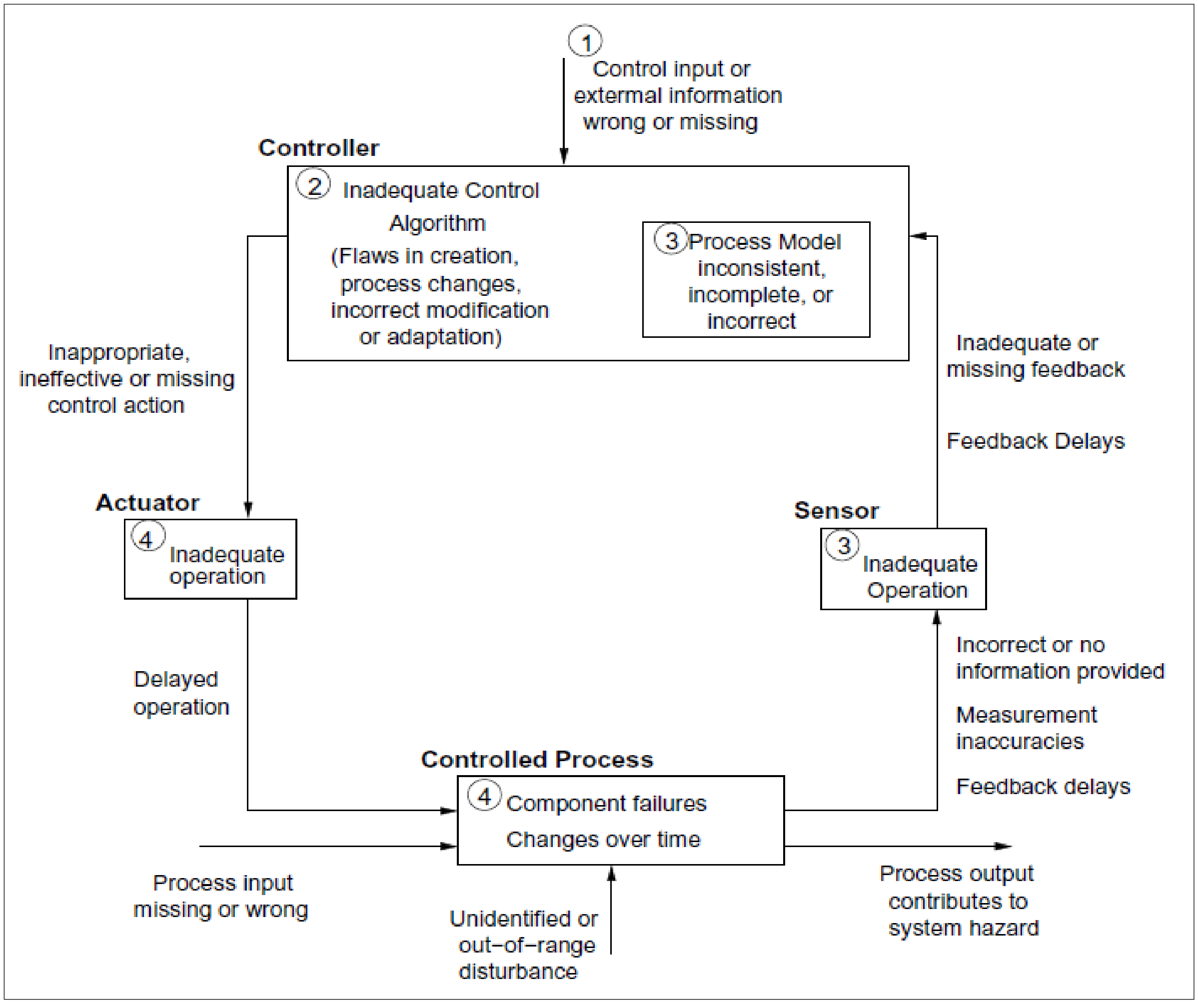


Figure 1: Classification of Control Flaws Leading to Hazards (Leveson, 2012)

Causal factors have been divided into three main categories. The controller operation, the behavior of actuators and controlled processes, and communication and coordination among controllers and decision makers. Figure 2 shows the general classification of the flaws in the components of the system development and system operations control loops during design, development, manufacturing, and operations (Leveson, 2004). This classification can be applied to all levels of the organization under investigation during accident analysis or as an accident prevention to prevent future or potential adverse events.

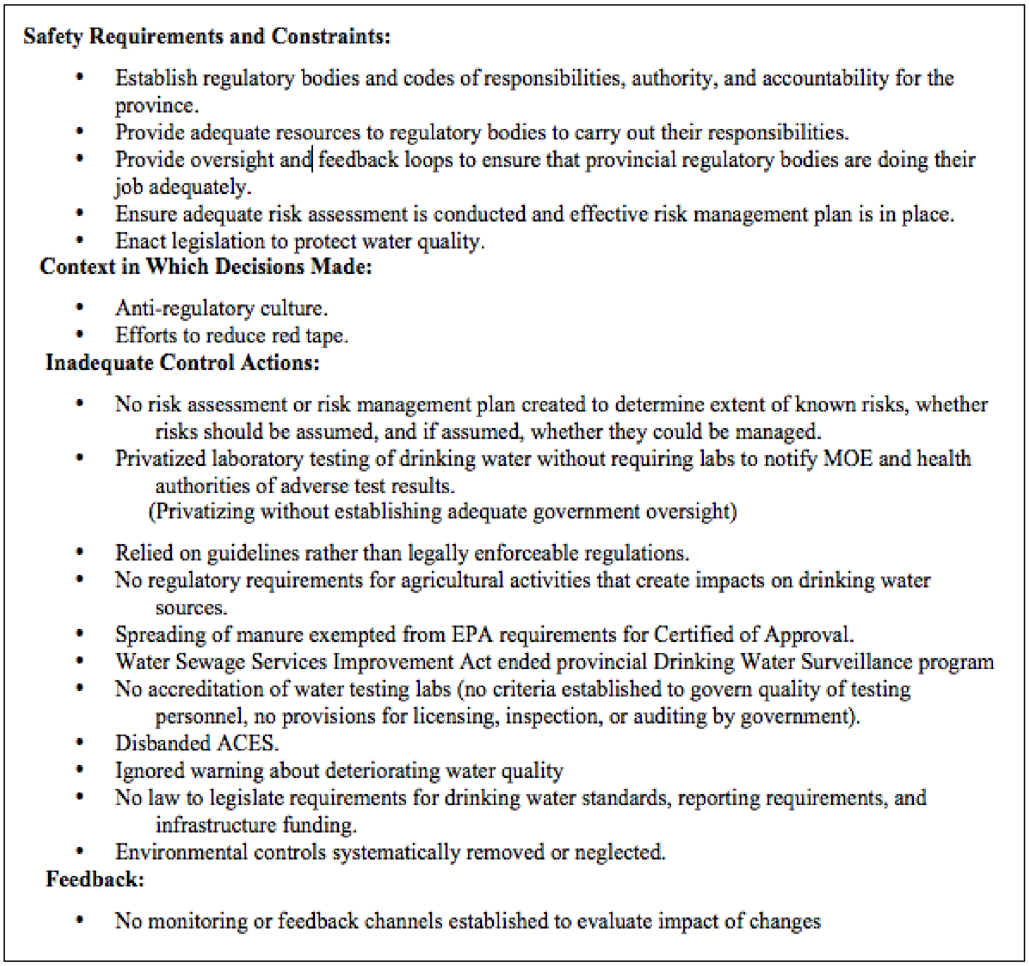
1. Inadequate enforcements of constraints (control actions)
1.1. Unidentified hazards
1.2. Inappropriate, ineffective or missing control actions for identified hazards
1.2.1. Design of control algorithm (process) does not enforce constraints
—Flaws in creation process
—Process changes without appropriate change in control algorithm (asynchronous evolution) —Incorrect modification or adaptation.
1.2.2. Process models inconsistent, incomplete or incorrect (lack of linkup)
—Flaws in creation process
—Flaws in updating process (asynchronous evolution)
—Time lags and measurement inaccuracies not accounted for
1.2.3. Inadequate coordination among controllers and decision makers
2. Inadequate execution of control action
2.1. Communication flaw
2.2. Inadequate actuator operation
2.3. Time lag
3. Inadequate or missing feedback
3.1. Not provided in system design
3.2. Communication flow
3.3. Time lag
3.4. Inadequate sensor operation (incorrect or no information provided

Figure 2: Classification of Control Flaws Leading to Hazards (Leveson, 2004)

For each level of the hierarchy, the three main categories should be investigated and determine their contribution to the accident (Leveson, 2004):

- Control actions: inadequate handling of control actions by controllers
- Execution of control action: inadequate execution of action
- Feedback: missing or inadequate feedback and communication

Another category can be added if humans are involved in the organization being investigated, which is the context in which the decision has been made and influenced the behavior mechanism (Leveson, 2004). Figure 3 is an example the structure of STAMP analysis for one level of the hierarchy (Leveson, Daouk, Dulac, & Marais, 2003).



Safety Requirements and Constraints:

- Establish regulatory bodies and codes of responsibilities, authority, and accountability for the province.
- Provide adequate resources to regulatory bodies to carry out their responsibilities.
- Provide oversight and feedback loops to ensure that provincial regulatory bodies are doing their job adequately.
- Ensure adequate risk assessment is conducted and effective risk management plan is in place.
- Enact legislation to protect water quality.

Context in Which Decisions Made:

- Anti-regulatory culture.
- Efforts to reduce red tape.

Inadequate Control Actions:

- No risk assessment or risk management plan created to determine extent of known risks, whether risks should be assumed, and if assumed, whether they could be managed.
- Privatized laboratory testing of drinking water without requiring labs to notify MOE and health authorities of adverse test results.
  (Privatizing without establishing adequate government oversight)
- Relied on guidelines rather than legally enforceable regulations.
- No regulatory requirements for agricultural activities that create impacts on drinking water sources.
- Spreading of manure exempted from EPA requirements for Certified of Approval.
- Water Sewage Services Improvement Act ended provincial Drinking Water Surveillance program
- No accreditation of water testing labs (no criteria established to govern quality of testing personnel, no provisions for licensing, inspection, or auditing by government).
- Disbanded ACES.
- Ignored warning about deteriorating water quality
- No law to legislate requirements for drinking water standards, reporting requirements, and infrastructure funding.
- Environmental controls systematically removed or neglected.

Feedback:

- No monitoring or feedback channels established to evaluate impact of changes

Figure 3: Accident Causal Factor of Provincial Governments - the Walkerton Water Contamination Accident (Leveson, Daouk, Dulac, & Marais, 2003)

4. Applying STAMP to an accident in the Oil and Gas Industry

XYZ is a major oil company that handles crude oil production operations. Two separate crude oil processing facilities, (A) and (B), collect the crude oil from a constellation of near-by wells. The oil is processed to meet market physical characteristics and chemical composition prior to sending it to storage tanks within the facility premises. Industrial export pumps are used to send crude oil via a joint a 30” diameter pipeline to central storage tank farm stationed near-by export harbors and then shipped to potential customers. Figure 4 illustrated the layout of the two facilities.

During normal operation, and at approximately 9:30 PM, a major accident occurred that created massive damage due to explosion at crude oil processing facility B.

The accident resulted in fatalities and caused millions of dollars in site damages as well as production suspension. The cause of the accident was due to an oil leak from a ruptured export pipeline. A spark ignited the pool of leaking crude oil, illustrated in figure 5, and resulted in series of massive explosion that destructed the entire facility. In addition, the accident resulted in the death of two facility operators and severe injuries to 20 contractor employees who were at the scene.

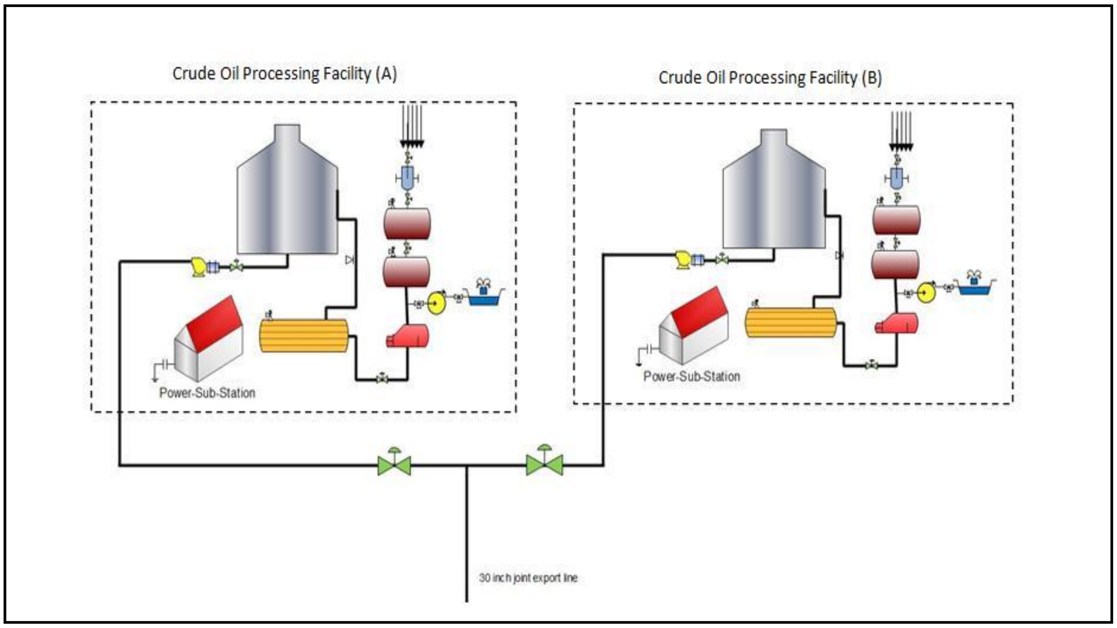


Figure 4: Layout of crude oil processing facilities (A) and (B)

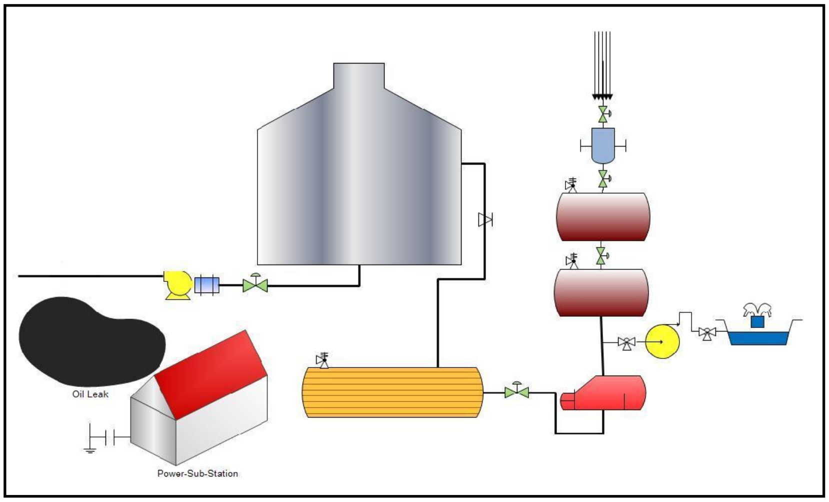


Figure 5: Oil leak and in Facility (B)

4.1 The Accident

At 3:40 PM, An electrical malfunction occurred in facility (A) resulted in a temporary suspension of export operations. This led to a pressure drop in the joint crude oil export pipeline. Operators in facility (A) informed area supervisor as well as operators in facility (B) to take proper actions in maintaining the pressure until the malfunction is rectified. Operators in facility (B) partially closed the control flow valve to maintain, and build up, the operating pressure in the joint export pipeline. In parallel, the maintenance crew in facility (A) managed to restore the electrical and resume production operations; hence, increase the pressure in the joint export crude oil pipeline.

Simultaneously, the operators in facility (B) started opening the control flow valve back to the original position prior to the shutdown of facility (A). This task is to assist in reducing both the backpressure and the built-up pressure resulting from resuming production operations in facility (A). Unfortunately, the flow control valve did not fully open to its original position. As a result, a backflow generated a build-up pressure in the 30-inch joint crude oil export pipeline.

At 9:30 PM, an over pressure in the pipeline resulted in a pipeline rupture and caused a leak of approximately 18,000 barrel of crude oil for over a period of 2 hours. Once acknowledged, the operators in Facility (B) immediately pushed Emergency

Shutdown Button. This is a part of Emergency ShutDown System (ESD) is designed to minimize the consequences of escape of hydrocarbons. This process consists of shutdown of equipment, isolate crude oil by containing it storage tanks, and stop hydrocarbon flow to assure maintain the safety and integrity of the facility.

Unfortunately, the main flow control valve, which is motor operated, failed to fully shutdown and secure the pipeline from flowing any crude oil back in to the facility.

Hence, the leak continued to flow from the ruptured pipeline. The operators in facility (B) managed to close the main flow control valve manually and were successful in stopping the leak. Yet, the large amount of leaked crude oil was accumulating nearby an electrical generating station. Since crude oil contains volatile organic fumes and vapor, and in an effort to prevent any electrical discharge, electrical maintenance contractors in facility (B) disconnected the electrical power supplied to the power-sub-station. Simultaneously, the mechanical maintenance crew utilized vacuum trucks to collect the spilled crude oil. This resulted in a static electric discharge and caused series of explosions. The explosions resulted in a total demolition of the facility as well as fires that lasted more than 16 hours to extinguish. In terms of casualties, the explosion resulted in the death of four facility operators and severe injuries to 20 contractor employees who were at the scene

4.2 Proximity of events:

- At 3:40 PM, An electrical malfunction occurred in facility (A)
- Operators in facility (B) tried close the flow control valve
- Electrical power restored in facility (A)
- Production resumed in Facility (A)
- Operator in Facility (B) opened flow control valve
- Flow control valve did not open to its original position
- Backflow generated a build-up pressure in the 30-inch joint crude oil export
- pipeline
- 30-inch pipeline rupture
- 18,000 barrel of crude oil leak

- Operator in Facility (B) pushed emergency shutdown button
- Suspend all ongoing operations within the facility and close all valves
- Flow control valve failed to fully shutdown
- The leak continued to flow from the ruptured pipeline
- Assistant Operators in facility (B) manually, close the main flow control valve
- Leak stopped
- Leaked crude oil was accumulating nearby an electrical generating station
- Operators in facility (B) disconnected the electrical power supplied to the power
- station
- Maintenance crew utilized vacuum trucks to collect the spilled crude oil
- Static electric discharge and caused series of explosions
- The explosions resulted in a total demolition of the facility
- Explosion resulted in the death of two facility operators and severe injuries to 20
- contractor employees who were at the scene

4.3 Hierarchical Control Structure

Each hierarchical level of the control structure of company XYZ, as depicted in figure 6, will be discussed in terms of inadequacy of enforcing safety constraint, inadequacy in executing actions, context, and mental flow. Each box represents a summary of the discussion above it**.**

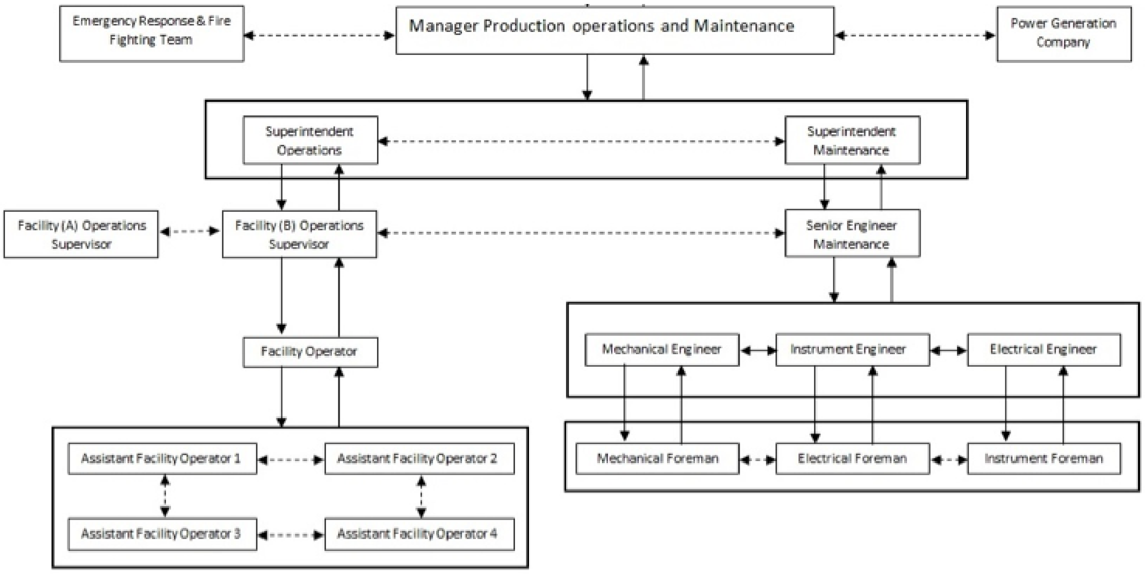


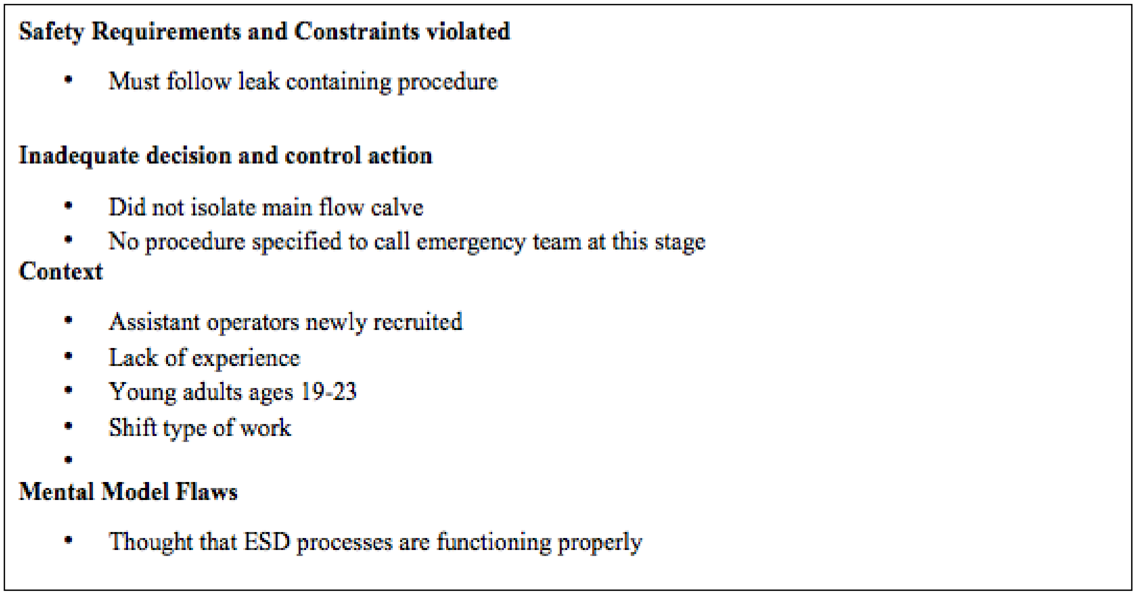
Figure 6: Hierarchical Level Control Structure of Company XYZ

Pipeline Mechanical Integrity

- Oil and gas industry refer to the recommended practices and standards issued by the American Petroleum Institute for their activities (Thomas, Thorp, & Denham, 1992). The recommended maximum piping inspection interval for crude oil pipeline is five years as per the Piping inspection code (API 570). "Smart Pigs", a propelling cylinder-shaped electronic devices inserted into the pipeline, are utilized to evaluate the metal loss due to corrosion, cracks, and any other anomaly in the pipeline (Kishawy & Gabbar, 2010). Since the inspection of pipelines requires the suspension of production, hence, loss of generated profit, operations, Company XYZ recommended all 30-inch pipelines to undergo routine inspections every seven years.

Assistant Facility Operators

- Assistant facility operators conducted a site visit every 4 hours to collect readings from various equipment and pressure gauges as part of their routine task. When reaching the main export transfer pump, an assistant facility operator observed ruptured pipeline with a pool crude oil leaking. Immediately, he contacted the facility operator via intrinsically safe radio, a standard means of communication inside the facility to prevent a spark, to initiate an Emergency ShutDown procedure by pushing the ESD located in the control room. This is an emergency standard procedure designed to minimize the consequences of escape of hydrocarbons in case of an oil leak. Consequently, the rest of the assistant facility operators started to manually isolate and secure the remaining manually operated valves to avoid flow of crude oil through pipelines since not all valves within the facility are motors operated neglecting the main flow control valve.



Safety Requirements and Constraints violated

- Must follow leak containing procedure

Inadequate decision and control action

- Did not isolate main flow calve
- No procedure specified to call emergency team at this stage

Context

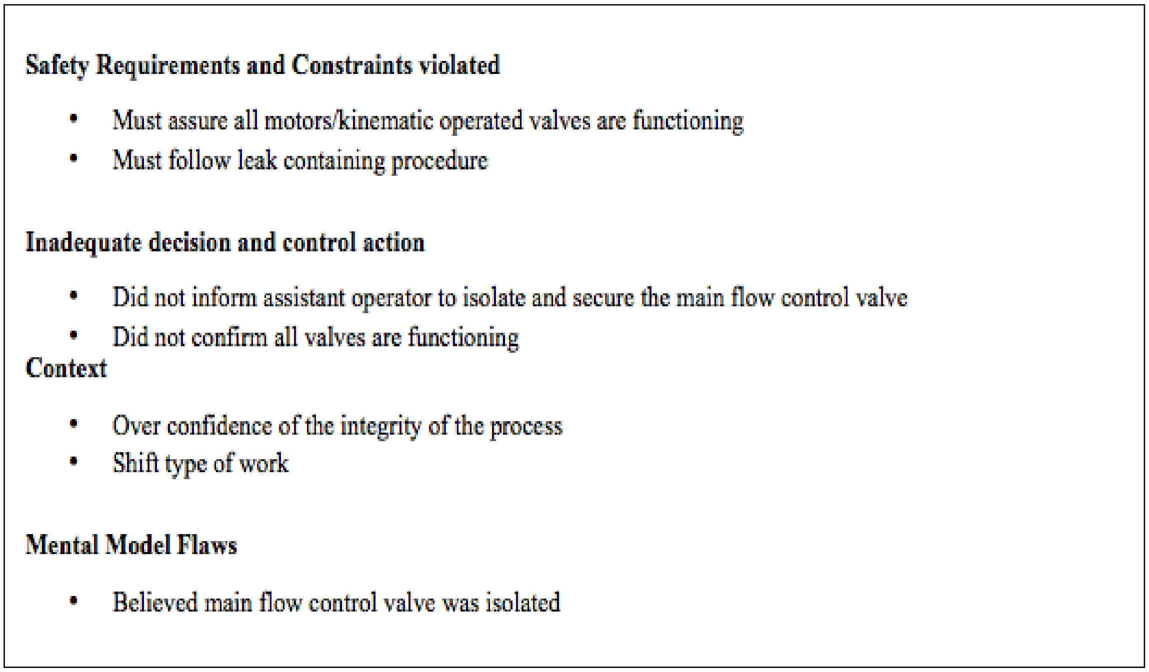
- Assistant operators newly recruited
- Lack of experience
- Young adults ages 19-23
- Shift type of work
-

Mental Model Flaws

- Thought that ESD processes are functioning properly

Facility (B) Operator

- The facility (B) operator initiated the emergency shutdown (ESD) procedure and pushed the (ESD) button located in the control room as per the radio communication with the assistant facility operator. This procedure closes both motor and pneumatically operated flow control valves to prevent the flow of hydrocarbons. Accordingly, facility operator contacted the on-call/off-site facility (B) supervisor by phone and informed him with the leak as part of the emergency response procedure.



Safety Requirements and Constraints violated

- Must assure all motors/kinematic operated valves are functioning
- Must follow leak containing procedure

Inadequate decision and control action

- Did not inform assistant operator to isolate and secure the main flow control valve
- Did not confirm all valves are functioning

Context

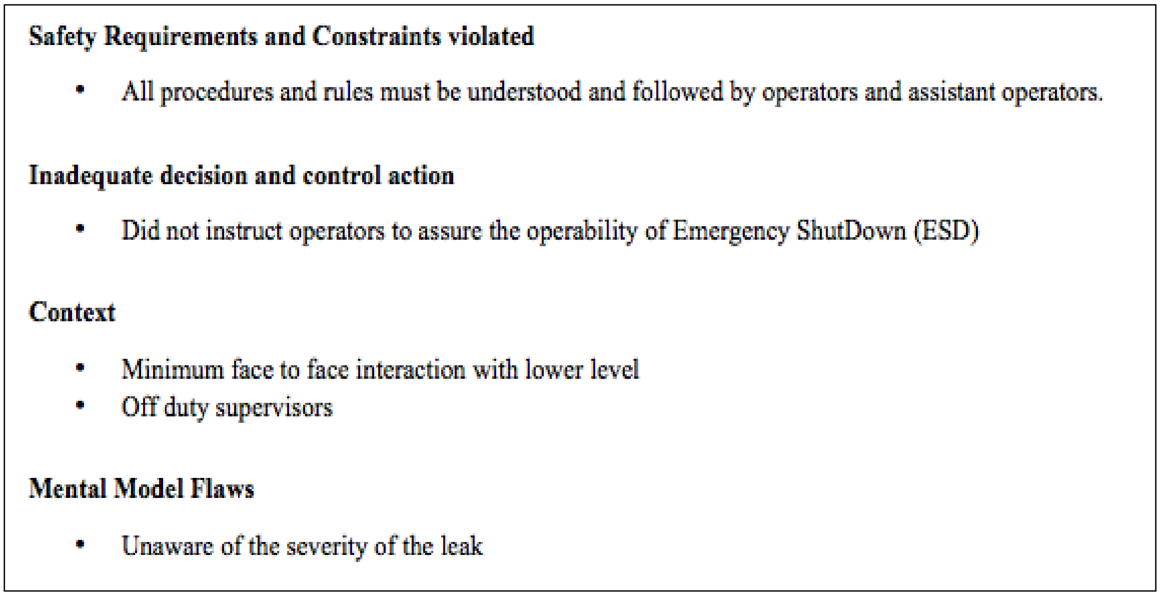
- Over confidence of the integrity of the process
- Shift type of work

Mental Model Flaws

- Believed main flow control valve was isolated

Facility (B) Supervisor

- Facility (B) supervisor contacted the Senior Maintenance engineer by phone and updated him with the ongoing leak in the facility (B)
- Facility (B) supervisor contacted the operations superintendent as he was informed by phone with the oil leak in the facility and action taken by operation staff



Safety Requirements and Constraints violated

- All procedures and rules must be understood and followed by operators and assistant operators.

Inadequate decision and control action

- Did not instruct operators to assure the operability of Emergency ShutDown (ESD)

Context

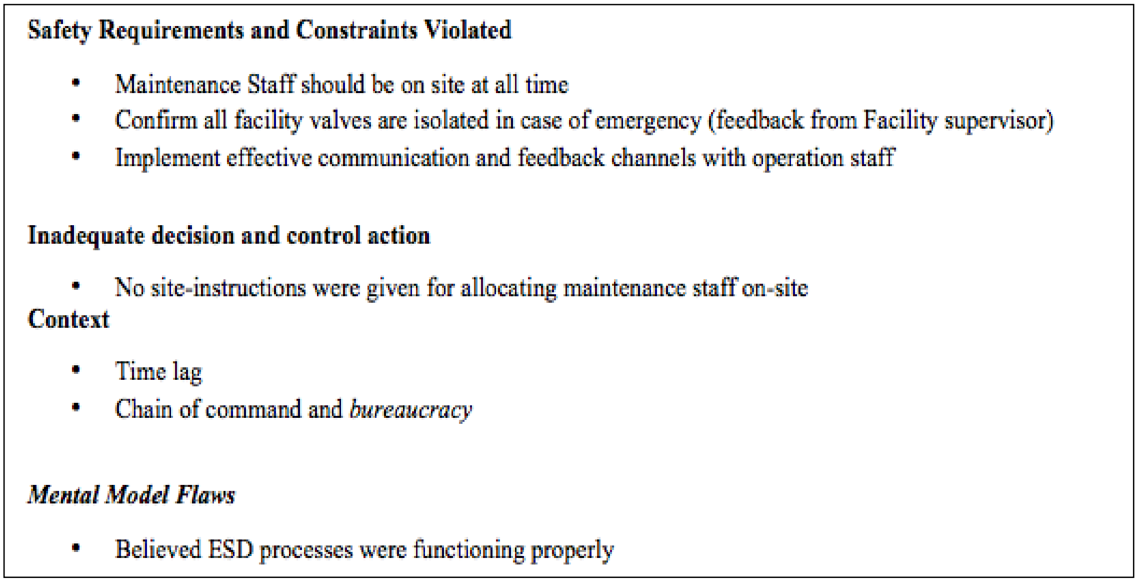
- Minimum face to face interaction with lower level
- Off duty supervisors

Mental Model Flaws

- Unaware of the severity of the leak

Senior Maintenance Engineer

- Senior maintenance engineer, who is on-call/off-site, contacted the off-site/on-call mechanical, electrical, and instrument engineers by phone to contact the off-site/on-call foremen, who perform the onsite activities with the assistance of maintenance contractor, to head to the facility and rectify the leak by using pipeline clamps. These clamps are temporary leak prevention tools secured around a pipeline.
- Senior maintenance engineer contacted by the phone the maintenance superintendent and informed with the leak and action taken by maintenance staff



Safety Requirements and Constraints Violated

- Maintenance Staff should be on site at all time
- Confirm all facility valves are isolated in case of emergency (feedback from Facility supervisor)
- Implement effective communication and feedback channels with operation staff

Inadequate decision and control action

- No site-instructions were given for allocating maintenance staff on-site

Context

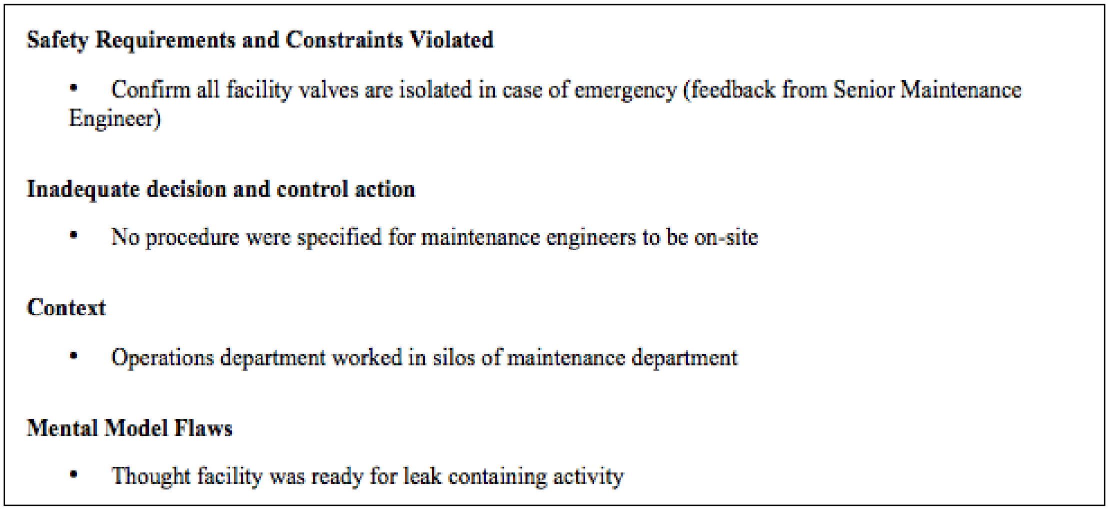
- Time lag
- Chain of command and *bureaucracy*

Mental Model Flaws

- Believed ESD processes were functioning properly

Maintenance Engineers:

- The maintenance engineers contacted their off-site/on-call foremen by phone and instructed them to deploy the contractor’s mechanical, electrical, and instrument maintenance crew to rectify the leak.



Safety Requirements and Constraints Violated

- Confirm all facility valves are isolated in case of emergency (feedback from Senior Maintenance Engineer)

Inadequate decision and control action

- No procedure were specified for maintenance engineers to be on-site

Context

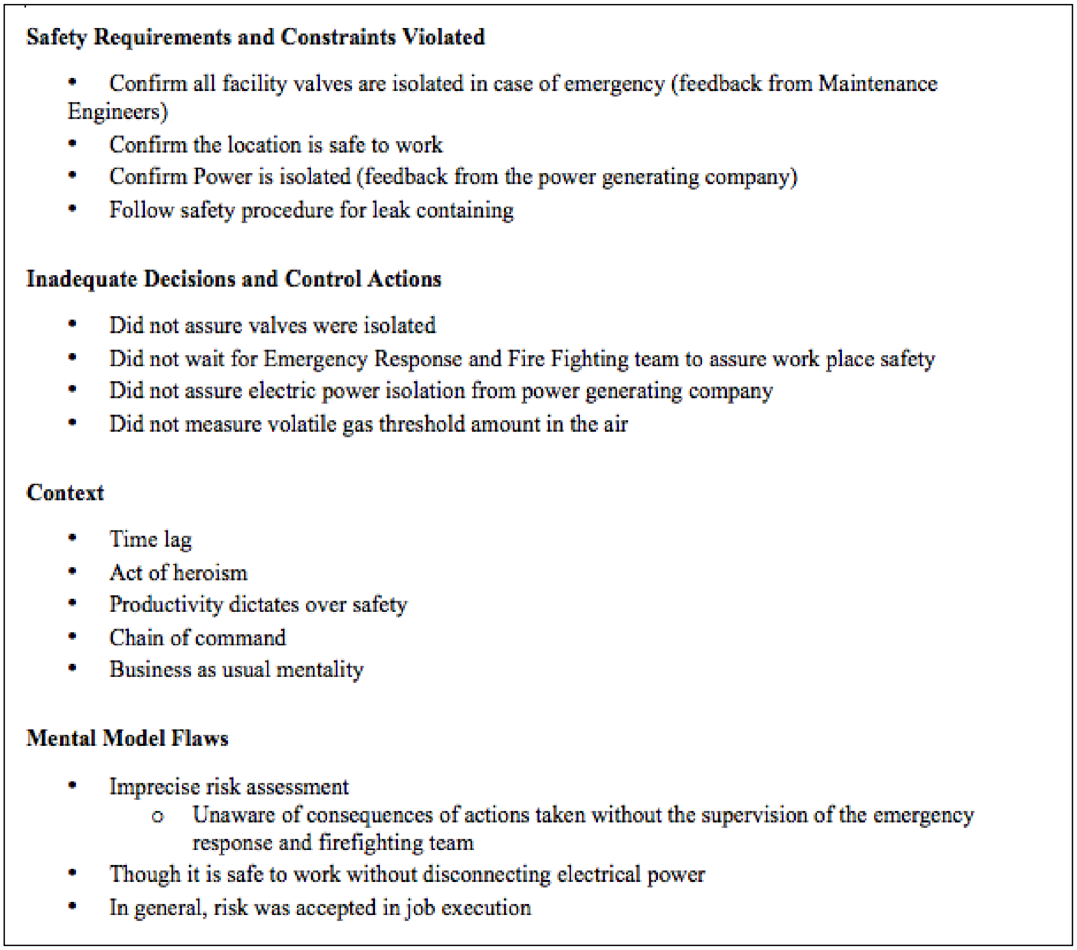
- Operations department worked in silos of maintenance department

Mental Model Flaws

- Thought facility was ready for leak containing activity

Foremen

- The maintenance foremen (mechanical, electrical, and instrument) contacted the off-site/on-call maintenance contractor crew to head to facility (B) which took them approximately an hour and a half to reach the facility.
- Mechanical maintenance crew was successful to stop the leak by clamping the ruptured pipeline and using a vacuum tank to gather the leaked crude oil.
- Electrical/instrument maintenance crew tried isolating the electrical power from the nearby power-sub-station in a parallel activity with mechanical maintenance.



Safety Requirements and Constraints Violated

- Confirm all facility valves are isolated in case of emergency (feedback from Maintenance Engineers)
- Confirm the location is safe to work
- Confirm Power is isolated (feedback from the power generating company)
- Follow safety procedure for leak containing

Inadequate Decisions and Control Actions

- Did not assure valves were isolated
- Did not wait for Emergency Response and Fire Fighting team to assure work place safety
- Did not assure electric power isolation from power generating company
- Did not measure volatile gas threshold amount in the air

Context

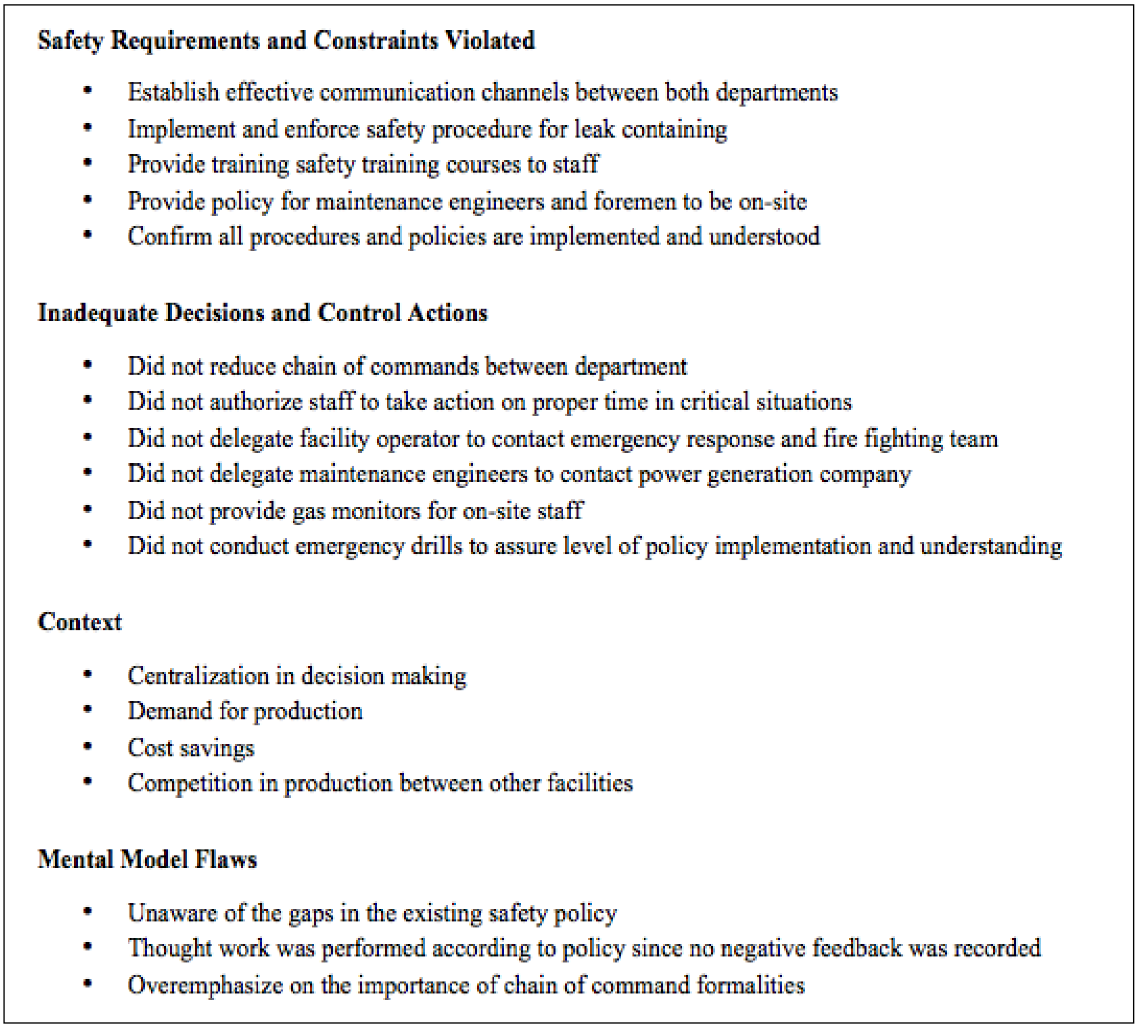
- Time lag
- Act of heroism
- Productivity dictates over safety
- Chain of command
- Business as usual mentality

Mental Model Flaws

- Imprecise risk assessment
    - Unaware of consequences of actions taken without the supervision of the emergency response and firefighting team
- Though it is safe to work without disconnecting electrical power
- In general, risk was accepted in job execution

Operations and Maintenance Manager

- The manager of production operations and maintenance contacted by phone both the emergency response and firefighting team to deploy to facility (B) and assure that all leak stopping activities are performed safely. The power generation company is also contacted by the operations and maintenance manager to be ready to disconnect the power once requested since power to the facility is supplied by the power-generation-company. In compliance with the emergency response procedures, both the team and power generation company were updated with the crude oil leak at facility (B).
- The executive managing director was contacted by phone and updated with the leak as well as the action taken by both maintenance and operations staff.



Safety Requirements and Constraints Violated

- Establish effective communication channels between both departments
- Implement and enforce safety procedure for leak containing
- Provide training safety training courses to staff
- Provide policy for maintenance engineers and foremen to be on-site
- Confirm all procedures and policies are implemented and understood

Inadequate Decisions and Control Actions

- Did not reduce chain of commands between department
- Did not authorize staff to take action on proper time in critical situations
- Did not delegate facility operator to contact emergency response and fire fighting team
- Did not delegate maintenance engineers to contact power generation company
- Did not provide gas monitors for on-site staff
- Did not conduct emergency drills to assure level of policy implementation and understanding

Context

- Centralization in decision making
- Demand for production
- Cost savings
- Competition in production between other facilities

Mental Model Flaws

- Unaware of the gaps in the existing safety policy
- Thought work was performed according to policy since no negative feedback was recorded
- Overemphasize on the importance of chain of command formalities

5. Recommendation

The oil industry utilizes HAZOP risk analysis in its design stages to recognize the hazard and operability problems in order to minimize the likelihood and consequences of an incident in the facilities (Flin, Mearns, Fleming, & Gordon, 1996). However, Root-Cause analysis is considered a fundamental tool to identify causes of accidents within the oil industry (Vinnem, Hestad, Kvaløy, & Skogdalen, 2010) as investigators utilized it in the case of facility (B) explosion. This method identified the causes of explosion as improper human performance that initiated a spark and ignited the pool of leak. In addition, the method went into further details in recognizing the cause of the leak was due to a ruptured 30 inch export pipeline. Yet, Root-Cause analysis failed to identify any procedural and hierarchical gaps negatively influenced decision-making and work performance.

STAMP analysis revealed several delinquencies in different aspects in Company XYZ which if identified in proper time; it would have prevented this catastrophe from occurring. Different levels of the organizational hierarchy contributed to the accident, where the main cause of the accident was the spark. Ineffective safety policy, inadequate communication between and within departments, poor supervision, and improper allocation of resources are some of the factors that contributed in this tragic accident. Policies and regulations must be implemented in Company XYZ to ensure safety to human, equipment, and environment.

If the following scenario has been followed, four lives could have been saved and financial losses in terms lost production, facility reconstruction, workers compensation, environmental impact, and legal claims/fines could have been avoided. In case of an oil leak, the assistant facility operators must ensure that all valves are isolated and securely shut to prevent the flow of any hydrocarbons through the pipelines. Thus, gas monitors should available with the assistant facility operators to assure that the threshold level of evaporating hydrocarbon fumes are within recommended safety limit. Consequently, contact the facility operator to proceed with the emergency shutdown processes to isolate all motor and pneumatically operated valves. The facility operator, after evaluating the situation and assuring that all valves are isolated and the facility is safe to perform any maintenance activity, will contact the facility operations supervisor with details of the emergency situation and the emergency procedures that were followed while emphasizing that the facility is safe for maintenance staff to proceed with their activity.

Concurrently, the facility operator will contact the emergency response and firefighting team with details of the situation for them to deploy their equipment and staff to supervise the work to be performed by the maintenance staff. The facility operator will contact maintenance engineers (mechanical, electrical, and instrument) who are on- site as shift-working-type-base and provide details of the emergency situation as they, along with the maintenance foremen and maintenance contractors, await for the emergency response and firefighting team to ensure the safety of the workplace and give them clearance to proceed with the rectification activities. Meanwhile, the power generation company will be notified by the electrical maintenance engineer to be ready for emergency power shutdown when instructed. This procedure will cut the power supply for the facility’s power-sub-station. Both the facility operator and maintenance engineer will update both facility operations supervisor and senior maintenance engineer, respectively. Hence, both the facility operations supervisor and the senior maintenance engineer will inform both the production operations superintendent and the maintenance superintendent who will be in touch with the operations and maintenance manager with status update as they assure that all safety procedures are emphasized and followed to prevent undesired accidents.

All effort from different levels of the hierarchy must collaborate to design a safer system in the company. Policies and procedures should be revised, new regulations must be established, implemented to assure that the previous scenario be active and understood. Finally, procedures and policy should be designed to accommodate the complexity of the human mind, machine components, software, environment, and the interaction among them.

6. Conclusion

STAMP goes beyond the conventional accident causation methods by pinpointing the reasons at human performance and component failure and takes it to another level of investigation. STAMP goes beyond acknowledging these factors and adds organizational hierarchy, working practices, and the roles and responsibility of each staff member in the organization. STAMP was simple to apply in the oil industry case study above without the need for special analytical skills or expertise, which can be a value added to the analysis, to identify the safety violations resulted in the catastrophe. However, for STAMP to be successful, it is essential for the user to have access to some essential information. The organization's hierarchy can assist in identifying their contribution to the safety constraint violation in terms of their influence to their subordinates. Policies, standards, and regulations that shape work practices and how activities are performed is key information in detecting improper task execution. The roles and responsibilities of each staff members identify the flow of communication channels used and how decisions made and conveyed to the lower hierarchy. Having this information will build a body of knowledge enabling the user to recognize limitations in each safety constraint level and where they have been violated in each hierarchical level.

STAMP identifies the violations against the existence safety constraints at each level of the control structure and investigates why these controls have not been adequately enforced or if they were adequately designed originally.. The method outperforms other accident causation models by considering all levels of complex systems including environment, human error, physical component failure, the context in which the accident happen, and the interrelationship between components, machine, human and other components of the system. The model is easy to apply in accident investigation and it provides a clear guidance for investigators to conduct the analysis.

STAMP has proven that it can be applied to different environment such as aerospace systems (Leveson, 2004), U.S. Army friendly fire shootings (Leveson, Allen, & Storey, 2002), water contamination accident (Leveson, Daouk, Dulac, & Marais, 2003), aviation (Nelson, 2008) (Hickey, 2012), financial crises (Spencer, 2012), and medical industry (Balgos, 2012). STAMP is a useful holistic model to apply in complex system. Hickey states, compared to other accident causation models, STAMP will reveal more causal factors contributing to accidents (Hickey, 2012).

Traditional accident analyses are more focused on sequence of events leading to a root cause. Once that root is identified all effort will be applied to eliminate it, which does not necessarily eliminate other causes from arising. STAMP in contrast is more focused on enforcing safety constraints behavior in systems rather than preventing failures. Accidents are viewed as a result of inadequate safety control. Moreover, STAMP assist in recognizing scenarios, inadequate controls, the dysfunctional interaction, and the incorrect process models, which will be used in process design for a safer system.

References

1. Altabbakh, H., Murray, S. L., Damle, S. B., & Grantham, K. (2012). Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster. *Engineering Management Journal.* 25:2 (June 2013), pp.13-24.

2. Balgos, V. H. (2012, February). A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices. Massachusetts Institute of Technology.

3. Dhillon, B. S. (1999). *Design Reliability: Fundamentals and applications.* Boca Raton: CRS Press.

4. Dhillon, B. S. (1999). *Design Reliability: Fundamentals and applications.* Boca RAton: CRC Press.

5. Ericson, C. A. (2005). *Hazard Analysis Techniques for System Safety.* Fredericksburg, Virginia: John Wiley & Sons.

6. Federal Aviation Administration. (2008, 5 21). *System Safety Handbook.* Retrieved January 6, 2013, from http://www.faa.gov: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/

7. Flin, R., Mearns, K., Fleming, M., & Gordon, R. (1996). *Risk perception in the offshore oil and as industry.* Aberdeen: Health and Safety Executives.

8. Foster, M., Beasley, J., Davis, B., Kryska, P., Liu, E., McIntyre, A., et al. (1999).

   Hazards Analysis Guide: A Reference Manual for Analyzing Safety Hazards on Semiconductor Manufacturing Equipment. International SEMATECH. www.sematech.org/docubase/document/3846aeng.pdf.

9. Hickey, J. (2012, May). A System Theoretic Safety Analysis of U.S. Coast Guard Aviation Mishap involving CG-6505. Massachusetts Institute of Technology.

10. Hollnagel, E. (2004). *Barriers and Accident Prevention.* Aldershot, Hampshire, England: Ashgate.

11. Khan, F. I., & Abbasi, S. (1998). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries* , 261-277.

12. Kerzner, H. (2009). *Project Management: Case Studies.* New Jersey: Wiley & Sons.

13. Kirwan, B., & Ainsworth, L. K. (1992). *A Guide to Task Analysis.* Washington DC: Taylor & Francis Inc.

14. Kishawy, H. A., & Gabbar, H. A. (2010). Review of pipeline integrity management practices. *International Journal of Pressure Vessels and Piping* , 373-380.

15. Kletz, T. A. (1999). *Hazop & Hazan: Identifying and Assessing Process Industry Hazards.* UK: Institution of Chemical Engineers.

16. Leveson, N. (2004, April). A New Accident Model for Engineering Safer Systems. *Safety Science* , 237-270.

17. Leveson, N. (2003, August). A New Approach to Hazard Analysis for Complex Systems. *In Proceedings of the International Conference of the System Safety Society*.

18. Leveson, N. (2012). *Engineering a Safer World, System Thinking Applied to Safety.* Massachusetts Institute of Technology.

19. Leveson, N. (1995). *Safeware; System Safety and Computers, A Guide to Preventing Accidents and Losses Caused By Technology.* Addison Wesley.

20. Leveson, N. (2002). *System Safety Engineering: Back to the Future.* MIT Press.

21. Leveson, N., & Laracy, J. (2007). Apply STAMP to Critical Infrastructure Protection. *IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability,*, (pp. 215-220). Woburn.

22. Leveson, N., Allen, P., & Storey, M.-A. (2002). The Analysis of a Friendly Fire Accident using a Systems Model of Accidents. *20th International Conference on System Safety.*

23. Leveson, N., Daouk, M., Dulac, N., & Marais, K. (2003, September). Applying STAMP in Accident Analysis. *Workshop on the Investigation and Reporting of Accidents*.

24. Nelson, P. S. (2008, June). A STAMP Analysis of the LEX Comair 5191 Accident. *Thesis*. Sweden: Lund University.

25. Pérez-Marín, M., & Rodríguez-Toral, M. (2013). HAZOP – Local approach in the Mexican oil & gas. *Journal of Loss Prevention in the Process Industries* , 936- 940

26. Product Quality Research Institute. (2013, May 11). *PQRI.* Retrieved 2013, from http://www.pqri.org/publications/index.asp: http://www.pqri.org/pdfs/MTC/HAZOP_Training_Guide.pdf

27. Redmill, F. (2002). Risk Analysis - a Subjective Process. *Engineering Management Journal , 12* (2), 91-96.

28. Song, Y. (2012, April 1). Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. *Open Access Dissertations and Theses , 6801*. McMaster University.

29. Spencer, M. B. (2012, June). Engineering Financial Safety : A System-Theoretic Case Study from the Financial Crisis. Massachusetts Institute of Technology.

30. Stephens, R. A., & Talso, W. (1999). *System Safety Analysis Handbook: Asource Book for Safety Practitioners* (Vol. 2). System Safety Society.

31. Thomas, G., Thorp, G., & Denham, J. (1992). The Upstream Oil and Gas Industry's Initiative in the Development of International Standards Based on API Standards. *Offshore Technology Conference.* Houston, Texas: Offshore Technology Conference.

32. Vinnem, J. E., Hestad, J. A., Kvaløy, J. T., & Skogdalen, J. E. (2010). Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. *Reliability Engineering & System Safety* , 1142- 1153.

33. Altabbakh, H., Murray, S. L., Damle, S. B., & Grantham, K. (2012). Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster. *Engineering Management Journal.* 25:2 (June 2013), pp.13-24.

34. Balgos, V. H. (2012, February). A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices. Massachusetts Institute of Technology.

35. Dhillon, B. S. (1999). *Design Reliability: Fundamentals and applications.* Boca Raton: CRS Press.

36. Dhillon, B. S. (1999). *Design Reliability: Fundamentals and applications.* Boca RAton: CRC Press.

37. Ericson, C. A. (2005). *Hazard Analysis Techniques for System Safety.* Fredericksburg, Virginia: John Wiley & Sons.

38. Federal Aviation Administration. (2008, 5 21). *System Safety Handbook.* Retrieved January 6, 2013, from http://www.faa.gov: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/

39. Flin, R., Mearns, K., Fleming, M., & Gordon, R. (1996). *Risk perception in the offshore oil and as industry.* Aberdeen: Health and Safety Executives.

40. Foster, M., Beasley, J., Davis, B., Kryska, P., Liu, E., McIntyre, A., et al. (1999). *Hazards Analysis Guide: A Reference Manual for Analyzing Safety Hazards on Semiconductor Manufacturing Equipment.* International SEMATECH. www.sematech.org/docubase/document/3846aeng.pdf.

41. Hickey, J. (2012, May). A System Theoretic Safety Analysis of U.S. Coast Guard Aviation Mishap involving CG-6505. Massachusetts Institute of Technology.

42. Hollnagel, E. (2004). *Barriers and Accident Prevention.* Aldershot, Hampshire, England: Ashgate.

43. Khan, F. I., & Abbasi, S. (1998). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries* , 261-277.

44. Kerzner, H. (2009). *Project Management: Case Studies.* New Jersey: Wiley & Sons.

45. Kirwan, B., & Ainsworth, L. K. (1992). *A Guide to Task Analysis.* Washington DC: Taylor & Francis Inc.

46. Kishawy, H. A., & Gabbar, H. A. (2010). Review of pipeline integrity management practices. *International Journal of Pressure Vessels and Piping* , 373-380.

47. Kletz, T. A. (1999). *Hazop & Hazan: Identifying and Assessing Process Industry Hazards.* UK: Institution of Chemical Engineers.
48. Leveson, N. (2004, April). A New Accident Model for Engineering Safer Systems. *Safety Science* , 237-270.
49. Leveson, N. (2003, August). A New Approach to Hazard Analysis for Complex Systems. *In Proceedings of the International Conference of the System Safety Society*.
50. Leveson, N. (2012). *Engineering a Safer World, System Thinking Applied to Safety.* Massachusetts Institute of Technology.
51. Leveson, N. (1995). *Safeware; System Safety and Computers, A Guide to Preventing Accidents and Losses Caused By Technology.* Addison Wesley.
52. Leveson, N. (2002). *System Safety Engineering: Back to the Future.* MIT Press.
53. Leveson, N., & Laracy, J. (2007). Apply STAMP to Critical Infrastructure Protection. *IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability,*, (pp. 215-220). Woburn.
54. Leveson, N., Allen, P., & Storey, M.-A. (2002). The Analysis of a Friendly Fire Accident using a Systems Model of Accidents. *20th International Conference on System Safety.*
55. Leveson, N., Daouk, M., Dulac, N., & Marais, K. (2003, September). Applying STAMP in Accident Analysis. *Workshop on the Investigation and Reporting of Accidents*.
56. Nelson, P. S. (2008, June). A STAMP Analysis of the LEX Comair 5191 Accident. *Thesis*. Sweden: Lund University.

57. Pérez-Marín, M., & Rodríguez-Toral, M. (2013). HAZOP – Local approach in the Mexican oil & gas. *Journal of Loss Prevention in the Process Industries* , 936- 940

58. Product Quality Research Institute. (2013, May 11). *PQRI.* Retrieved 2013, from http://www.pqri.org/publications/index.asp: http://www.pqri.org/pdfs/MTC/HAZOP_Training_Guide.pdf

59. Redmill, F. (2002). Risk Analysis - a Subjective Process. *Engineering Management Journal , 12* (2), 91-96.

60. Song, Y. (2012, April 1). Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. *Open Access Dissertations and Theses , 6801*. McMaster University.

61. Spencer, M. B. (2012, June). Engineering Financial Safety : A System-Theoretic Case Study from the Financial Crisis. Massachusetts Institute of Technology.

62. Stephens, R. A., & Talso, W. (1999). *System Safety Analysis Handbook: A source Book for Safety Practitioners* (Vol. 2). System Safety Society.

63. Thomas, G., Thorp, G., & Denham, J. (1992). The Upstream Oil and Gas Industry's Initiative in the Development of International Standards Based on API Standards. *Offshore Technology Conference.* Houston, Texas: Offshore Technology Conference.

64. Vinnem, J. E., Hestad, J. A., Kvaløy, J. T., & Skogdalen, J. E. (2010). Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. *Reliability Engineering & System Safety* , 1142- 1153.

II. INVESTIGATING NEW RISK REDUCTION AND MITIGATION IN THE OIL AND GAS INDUSTRY

Mohammad A. AlKazimi [a], Katie Grantham [b]

[a] Petroleum Engineering Dept, Missouri University of Science and Technology
[b] Department and Engineering Management and System Engineering, Missouri University of Science and Technology

Abstract

The complexity of the processes and the nature of volatile petroleum products urged the oil and gas industry to utilize various risk assessment techniques to identify potential failure modes that can interrupt operation processes. Consequently, government agencies and nonprofit professional societies guide the industry with regulatory guidelines, standards, and best recommended practices to oversee the operations management, assure safe working environment, and contain failures within tolerable limits. Yet, accidents due to electro-mechanical failures still occur and result in various consequences. Accordingly, critics have raised concerns about the petroleum industry's safety and risk mitigation credentials and question its ability to prevent future major accidents. Therefore, new risk assessment tools need to be introduced to provide decision makers and novice engineers with a diverse perception of potential risks. The aim of this paper is verify the application of Risk in Early Design (RED), a product risk assessment tool, in identifying potential failures in the oil and gas industry. Approximately thirty major accident underwent the RED analysis to verify the software's application to identify and rank potential failure modes

Keywords

Risk assessment; Oil and gas; Failure mode; RED

1. Introduction

The complexity of the processes and the nature of volatile petroleum products urged the oil and gas industry to utilize various risk assessment techniques to identify potential failure modes that can interrupt operation processes. Consequently, government agencies and nonprofit professional societies guide the industry with regulatory guidelines, standards, and best recommended practices to oversee the operations management, assure safe working environment, and contain failures within tolerable limits. Yet, accidents due to electro-mechanical failures still occur and result in various consequences. Accordingly, critics have raised concerns about the petroleum industry’s safety and risk mitigation credentials and question its ability to prevent future major accidents. Therefore, new risk assessment tools need to be introduced to provide decision makers and novice engineers with a diverse perception of potential risks. The aim of this paper is verify the application of Risk in Early Design (RED), a product risk assessment tool, in identifying potential failures in the oil and gas industry.

2. Impact of major accidents in the petroleum industry

The oil and gas industry has been criticized for accidents that resulted in catastrophes on different scales. The following lists some of these accidents; Deepwater Horizon drilling rig explosion and major oil spill in the Gulf of Mexico, Piper-alpha rig explosion in the North Sea, Kuwait’s Mina al-Ahmadi refinery explosion, and Venezuela’s Amuay refinery explosion (Anderson & LaBelle, 1994; Davies, 2010). The result of these accidents negatively impacted the oil and gas industry as well as the surrounding communities on different aspects.

Environmentally, the pollutants spread due to oil or its refined products contaminate both land and marine ecosystem (The Commonwealth Scientific and Industrial Research Organisation, 2013). The environmental damage includes underwater soils and reefs that are natural habitat to marine life (Ronza, Lázaro-Touza, Caro, & Joaquim, 2009). Containing oil spill accidents requires the usage of chemical dispersant agent. Although they remedy pollution, using the chemicals causes toxicity regardless of their capability diluting the concentrated crude oil (Etkin, 1999).

Health has been impacted by major accidents in the oil and gas industry. The Bhopal gas leak disaster in 1984 killed more than 3800 in first few days of the accident as a result of inhaling methyl-isocyanate (MIC) gas (Sharma, 2002). Moreover, an estimate of "15,000 to 20,000 premature deaths reportedly occurring in the subsequent two decades" following the accident as "the Indian government reported that more than half a million people were exposed to the gas" (Broughton, 2005). The eight hundred burning oil wells in Kuwait due to sabotage during desert storm war resulted in an increase in lung cancer, reparatory, and skin diseases (Seacor, 1994). The piper alpha tragedy claimed one hundred sixty seven lives due to a gas leak that resulted in an explosion; families and relatives of the lost crew member were psychologically impacted due to the loss of their loved ones (Kirchsteiger, 1999).

There are different financial losses due to an accident; operational profit and compensation and legal penalties are types financial impacts. Accidents can suspend the flow of operations causing a loss of production and downtime losses. Hence, postponing production operation results in decline in the company's marginal profit (Cohen, 1993). The tourism industry in the Gulf coast generates an average of $34 billion in revenues; the Deepwater Horizon oil spill resulted in contaminating the Gulf shores and resulted in a significant loss of $11 billion due to tourists avoiding those areas. In addition, Gulf shore business owners such as real estate, recreation, and fisheries, filed civil lawsuits, which BP could face $20 billion in legal penalties, to compensate for their losses (Perry, 2011).

Government agencies and nonprofit professional societies guide the industry with regulatory guidelines, standards, and best recommended practices to oversee the operations management, assure safe working environment, and contain failures within tolerable limits. Thus, The oil and gas industry utilizes different risk assessment tools to mitigation potential failures within tolerable limits.

3. Common Risk Assessment tools in the petroleum industry

The petroleum industry utilizes different risk mitigation methods to contain operational failures. These strategies aim to mitigate potential electromechanical failures that can interrupt operations within its facilities. For example, Failure Mode and Effect

Analysis (FMEA) examines the effect of potential failure modes to classify necessary phase alterations of the system to overcome failures (Stamatis, 2003; Altabbakh et al., 2013).

Fault Tree Analysis (FTA) surveys failures and contributing factors of breakdown in a system by applying diagrams and logic gates to indicate the relationship between failures and other events in the system (Hauptmanns, 2004; Altabbakh et al., 2013). This method identifies the probability for base event to occur; the corresponding event tree shows possible sequence of the triggered event (Zolotukhin & Gudmestad, 2002).

Event Tree Analysis (ETA) classifies and evaluates possible accident along with chain of events (Altabbakh et al., 2013). The method starts with an instigating event and continues to evaluate corresponding possible outcomes (Khan & Abbasi, 1998). ETA is a bottom up method where it starts with a triggered failure and progresses with the following consequences; it is considered as both qualitative and quantitative risk assessment technique (Mannan, 2004).

Bow-Tie Analysis demonstrates the causes of accidental events, potential consequence, and strategic actions to mitigate hazards. Saud et al. (2013) consider it as a easy to understand and apply method due to its graphical representation. Yet, the method mandates expertise in the operating system and its safety components, difficult to relate it to quantitative risk assessment tools, and sophisticated to model inter-related risk controls (Lewis & Smith, 2010).

What–If Analysis "is a structured brainstorming method of determining what things can go wrong and judging the likelihood and severity of those situations occurring" (University of Arizona Risk Management Services). The valuation is a brainstorming session and based on expertise, nevertheless, unidentified hazards are difficult to recognize in the process. Therefore, the hazard remains unrecognized (Nolan, 2011; Khan & Abbasi, 1998).

Hazard and Operability analysis (HAZOP) identifies hazards in a system to prevent malfunctions by brainstorming session where specialists utilize different hazardous scenarios that might affect the process system (Kletz, 2001). HAZOP risk analysis is expressively applied in the design stages to recognize potential hazards prior to construction. This method is advantageous to reduce both the likelihood and consequences of any failure (Flin, Mearns, Fleming, & Gordon, 1996)

Layer of Protection Analysis (LOPA) is another widely used risk assessment tool in the process industry (Young & Crowe, 2006). The method evaluates the competence of protection layers used to mitigate risk (Summers, 2003). LOPA is a process hazard analysis (PHA) tool where it utilizes the hazardous events, event severity, initiating causes, and initiating event likelihood database established during the hazard and operability analysis (HAZOP).

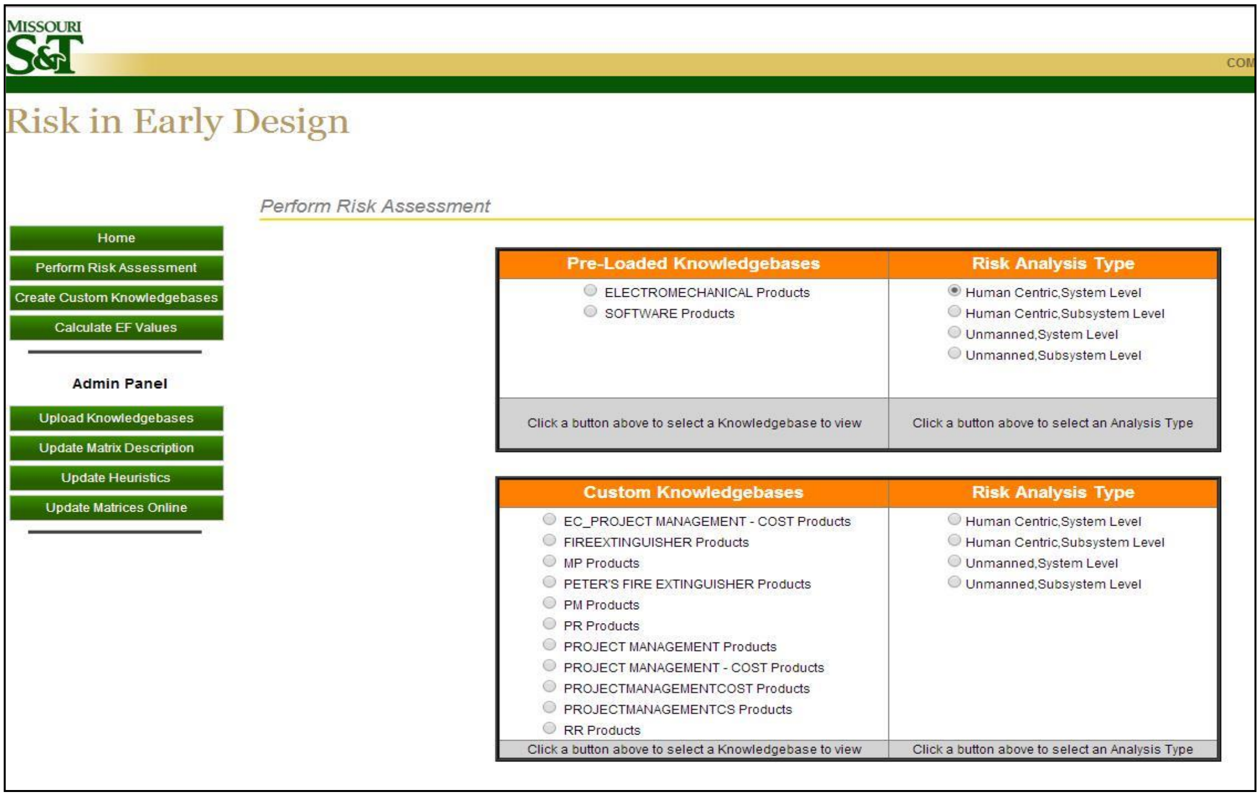
Consequently, and based on the analysis of the mitigation methodologies, the petroleum industry utilizes different strategies to contain failure modes within tolerable limits. Hence, these strategies assure the operations' process safety without jeopardizing the integrity of the facility's equipment. Asset integrity management (AIM) which is an inclusive maintenance and inspection program designed to ensure facility's reliability, is one of common strategies applied in the industry (Rezae & Abbas, 2013; Milazzo et. al, 2010). Risk based inspection (RBI) follows the footsteps of API RP 580/581 and it is corner stone of AIM programs. RBI is the practice of establishing an inspection action plan based on knowledge of the risk of failure of the equipment (API RP, 2009). It combines an assessment of the probability, or the likelihood of failure due to degradation or deterioration with an assessment of the potential resulting consequences due to the corresponding failure. Hence, Risk Based Inspection recognizes, evaluates and charts potential risks that can impact equipment's' mechanical integrity (API RP, 2009; Milazzo, Maschio, & Uguccioni., 2010). The gathered information assist in identifying the both the type and the rate of the potential failure that might harm the corresponding operating equipment. The program is essential to monitor the equipment's degradation due to operating and environmental conditions as it forecasts and recommends corrective measures (Marley, Jahre-Nilsen, & BjØrnØ, 2001).

These thorough methods, to name several, evaluate potential risks and try to sustain them within tolerable limits (Flin, et. al, 1996; Vinnem et al., 2010; Yasseri & Mahani, 2013). Yet, with stringent techniques and risk mitigation tools utilized in the petroleum industry, major accidents occur with catastrophic consequences affecting the environment, society and oil and gas industry's stakeholders. These accidents, and many others, are wake up calls to the petroleum industry to explore new tools to avoid similar accidents from occurring (Mihailidou, Antoniadis, & Assael, 2012).

4. Risk in Early Design (RED)

Having an early and precise risk assessment is essential to forecast and mitigate potential accidents from taking place, especially at the conceptual design stages (M.F. Milazzo, 2013; Lough et. al, 2009). The team developed Risk in Early Design (RED) theory to generate a list of possible product risks. The software allows users with limited experience to predict both when and where a product may fail by simply knowing the function of their product. The product risks are based on historical data of product input function and rank them by their occurrence likelihood and consequence (Lough et. al, 2008). Functioning as both as failure mode identification and risk ranking tool, Risk in Early Design (RED) is custom software that allows users to leverage failures from other products to help predict what may go wrong with the user's product. RED promotes failure prevention by identifying failure risks as early as the conceptual design phase, where impacts of failure prevention are furthermost. It does this by using subject specific knowledge-bases populated by historical failure events in a variety of categories such as product failures, software failures, and business failures. The user simply selects the functions of the item that is undergoing a risk assessment and the type of assessment desired. The information quickly communicated by the RED software is the function (i.e. potential failure location), failure mode, risk likelihood, and risk consequence via mathematical mapping processes (Grantham Lough, Stone, & Tumer, 2005). It also categorizes the output into high, medium, and low risk areas.

To demonstrate the process, and via Missouri S&T intranet , the user selects the corresponding matrix/Knowledgebase whether it is on *System Level;* compare this product against all the other products in the database or *Subsystem Level;* looks at the product itself to determine “potentially risky parts” for which reliability need be investigated. Figure 1 illustrated the selection options.

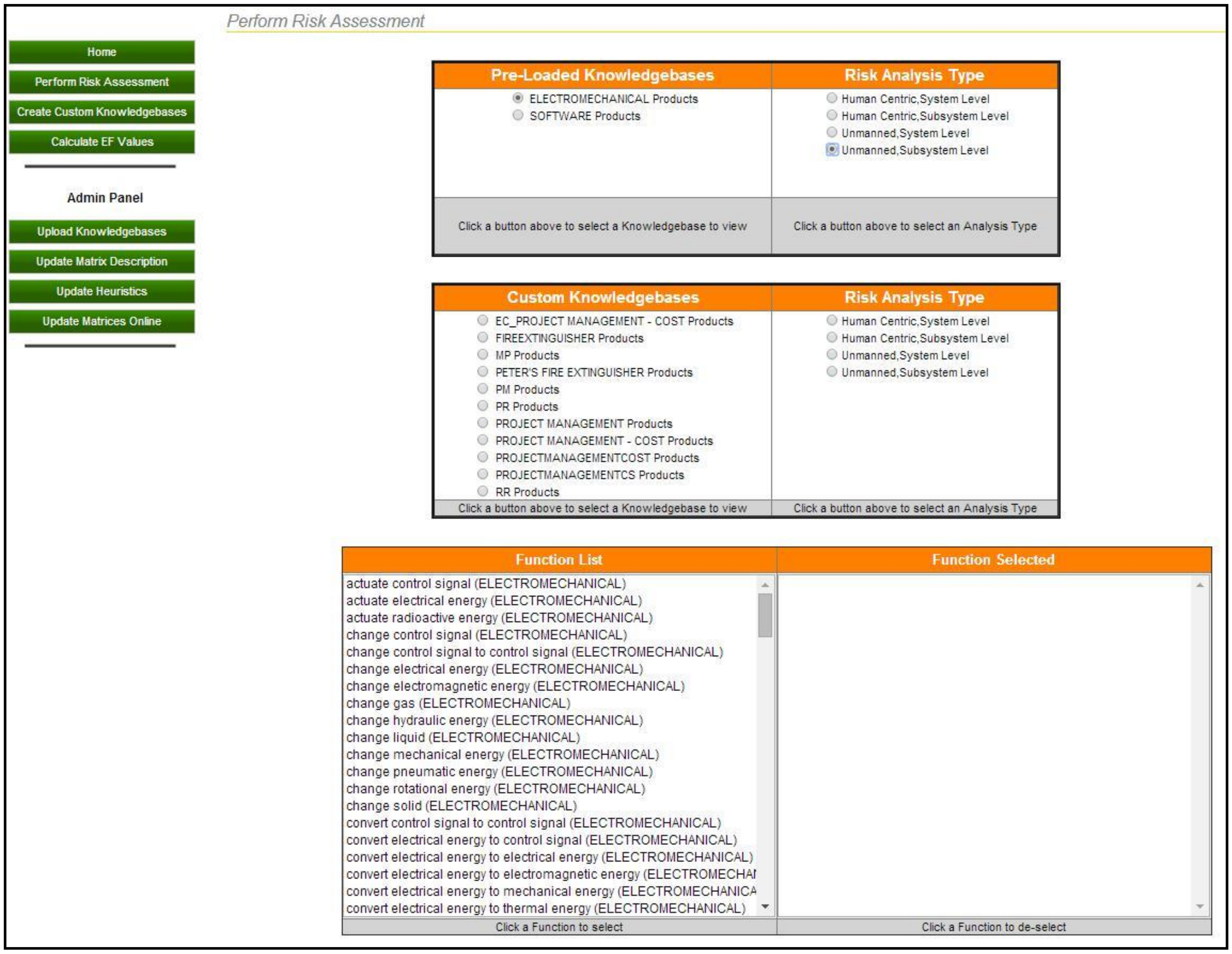


Pre-Loaded Knowledgebases	Risk Analysis Type
○ ELECTROMECHANICAL Products	● Human Centric,System Level
○ SOFTWARE Products	○ Human Centric,Subsystem Level
	○ Unmanned,System Level
	○ Unmanned,Subsystem Level
Click a button above to select a Knowledgebase to view	Click a button above to select an Analysis Type

Custom Knowledgebases	Risk Analysis Type
○ EC_PROJECT MANAGEMENT - COST Products	○ Human Centric,System Level
○ FIREEXTINGUISHER Products	○ Human Centric,Subsystem Level
○ MP Products	○ Unmanned,System Level
○ PETER'S FIRE EXTINGUISHER Products	○ Unmanned,Subsystem Level
○ PM Products	
○ PR Products	
○ PROJECT MANAGEMENT Products	
○ PROJECT MANAGEMENT - COST Products	
○ PROJECTMANAGEMENTCOST Products	
○ PROJECTMANAGEMENTCS Products	
○ RR Products	
Click a button above to select a Knowledgebase to view	Click a button above to select an Analysis Type

Figure 1. Selecting the appropriate risk analysis type

Accordingly, the user selects multiple functions that pertain to the corresponding product. Figure 2 depicts the selection process**.**



Pre-Loaded Knowledgebases

● ELECTROMECHANICAL Products
○ SOFTWARE Products

Click a button above to select a Knowledgebase to view

Risk Analysis Type

○ Human Centric,System Level
○ Human Centric,Subsystem Level
○ Unmanned,System Level
● Unmanned,Subsystem Level

Click a button above to select an Analysis Type

Custom Knowledgebases

○ EC_PROJECT MANAGEMENT - COST Products
○ FIREEXTINGUISHER Products
○ MP Products
○ PETER'S FIRE EXTINGUISHER Products
○ PM Products
○ PR Products
○ PROJECT MANAGEMENT Products
○ PROJECT MANAGEMENT - COST Products
○ PROJECTMANAGEMENTCOST Products
○ PROJECTMANAGEMENTCS Products
○ RR Products

Click a button above to select a Knowledgebase to view

Risk Analysis Type

○ Human Centric,System Level
○ Human Centric,Subsystem Level
○ Unmanned,System Level
○ Unmanned,Subsystem Level

Click a button above to select an Analysis Type

Function List

actuate control signal (ELECTROMECHANICAL)
actuate electrical energy (ELECTROMECHANICAL)
actuate radioactive energy (ELECTROMECHANICAL)
change control signal (ELECTROMECHANICAL)
change control signal to control signal (ELECTROMECHANICAL)
change electrical energy (ELECTROMECHANICAL)
change electromagnetic energy (ELECTROMECHANICAL)
change gas (ELECTROMECHANICAL)
change hydraulic energy (ELECTROMECHANICAL)
change liquid (ELECTROMECHANICAL)
change mechanical energy (ELECTROMECHANICAL)
change pneumatic energy (ELECTROMECHANICAL)
change rotational energy (ELECTROMECHANICAL)
change solid (ELECTROMECHANICAL)
convert control signal to control signal (ELECTROMECHANICAL)
convert electrical energy to control signal (ELECTROMECHANICAL)
convert electrical energy to electrical energy (ELECTROMECHANICAL)
convert electrical energy to electromagnetic energy (ELECTROMECHAI
convert electrical energy to mechanical energy (ELECTROMECHANICA
convert electrical energy to thermal energy (ELECTROMECHANICAL)

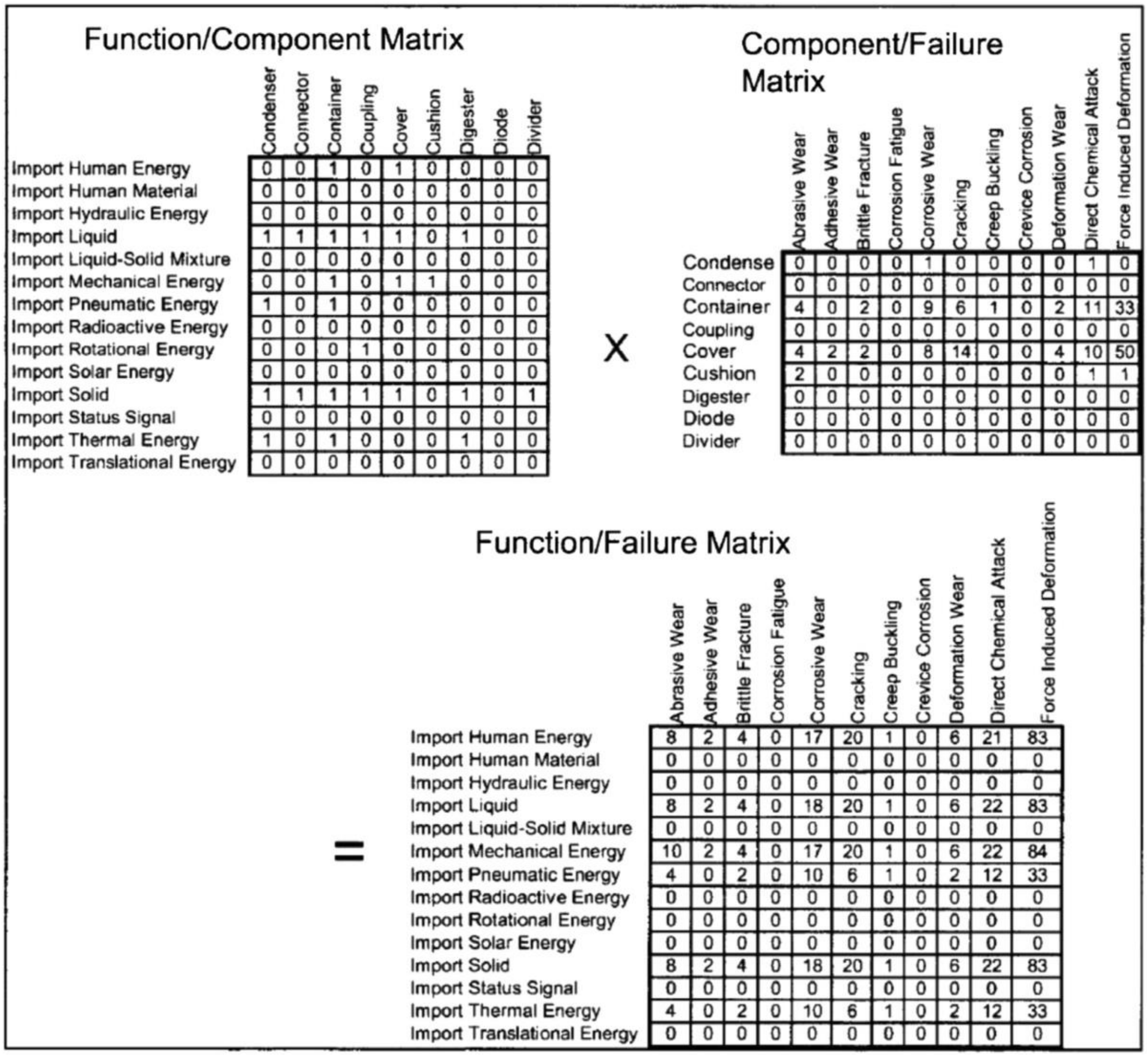
Click a Function to select

Function Selected

Click a Function to de-select

Figure 2. Function selection process

Once selected, the software will generate preliminary results in risk matrix chart with list of selected functions. This graphical color-coded depiction of the risk elements divides them into three categories – low (green), medium (yellow), and high (red), respectively. This is essential graphical illustration to aid in the understanding of what risk elements demand the most attention from engineers and designers (Lough et. al, 2008). Accordingly, RED analysis provides the total number of risks where each risk type has a link for a tale of the details of the selected risk matrix. The matrix indicates the link between function and risk in early design by presenting a mathematical mapping from product function to risk assessments. Accordingly, the knowledge base for RED is "stored and manipulated in three types of matrices" containing function-component matrix and component-failure matrix, respectively (Mitchell et al., 2005, p. 723) where their product results in function-failure matrix as illustrated in Figure 3. RED utilizes populated database from historical failure, as well as potential product failure modes that have been researched and documented by experts in the risk assessment field (Mitchell et al., 2005).



Function/Component Matrix

	Condenser	Connector	Container	Coupling	Cover	Cushion	Digester	Diode	Divider
Import Human Energy	0	0	1	0	1	0	0	0	0
Import Human Material	0	0	0	0	0	0	0	0	0
Import Hydraulic Energy	0	0	0	0	0	0	0	0	0
Import Liquid	1	1	1	1	1	0	1	0	0
Import Liquid-Solid Mixture	0	0	0	0	0	0	0	0	0
Import Mechanical Energy	0	0	1	0	1	1	0	0	0
Import Pneumatic Energy	1	0	1	0	0	0	0	0	0
Import Radioactive Energy	0	0	0	0	0	0	0	0	0
Import Rotational Energy	0	0	0	1	0	0	0	0	0
Import Solar Energy	0	0	0	0	0	0	0	0	0
Import Solid	1	1	1	1	1	0	1	0	1
Import Status Signal	0	0	0	0	0	0	0	0	0
Import Thermal Energy	1	0	1	0	0	0	1	0	0
Import Translational Energy	0	0	0	0	0	0	0	0	0

X

Component/Failure Matrix

	Abrasive Wear	Adhesive Wear	Brittle Fracture	Corrosion Fatigue	Corrosive Wear	Cracking	Creep Buckling	Crevice Corrosion	Deformation Wear	Direct Chemical Attack	Force Induced Deformation
Condense	0	0	0	0	1	0	0	0	0	1	0
Connector	0	0	0	0	0	0	0	0	0	0	0
Container	4	0	2	0	9	6	1	0	2	11	33
Coupling	0	0	0	0	0	0	0	0	0	0	0
Cover	4	2	2	0	8	14	0	0	4	10	50
Cushion	2	0	0	0	0	0	0	0	0	1	1
Digester	0	0	0	0	0	0	0	0	0	0	0
Diode	0	0	0	0	0	0	0	0	0	0	0
Divider	0	0	0	0	0	0	0	0	0	0	0

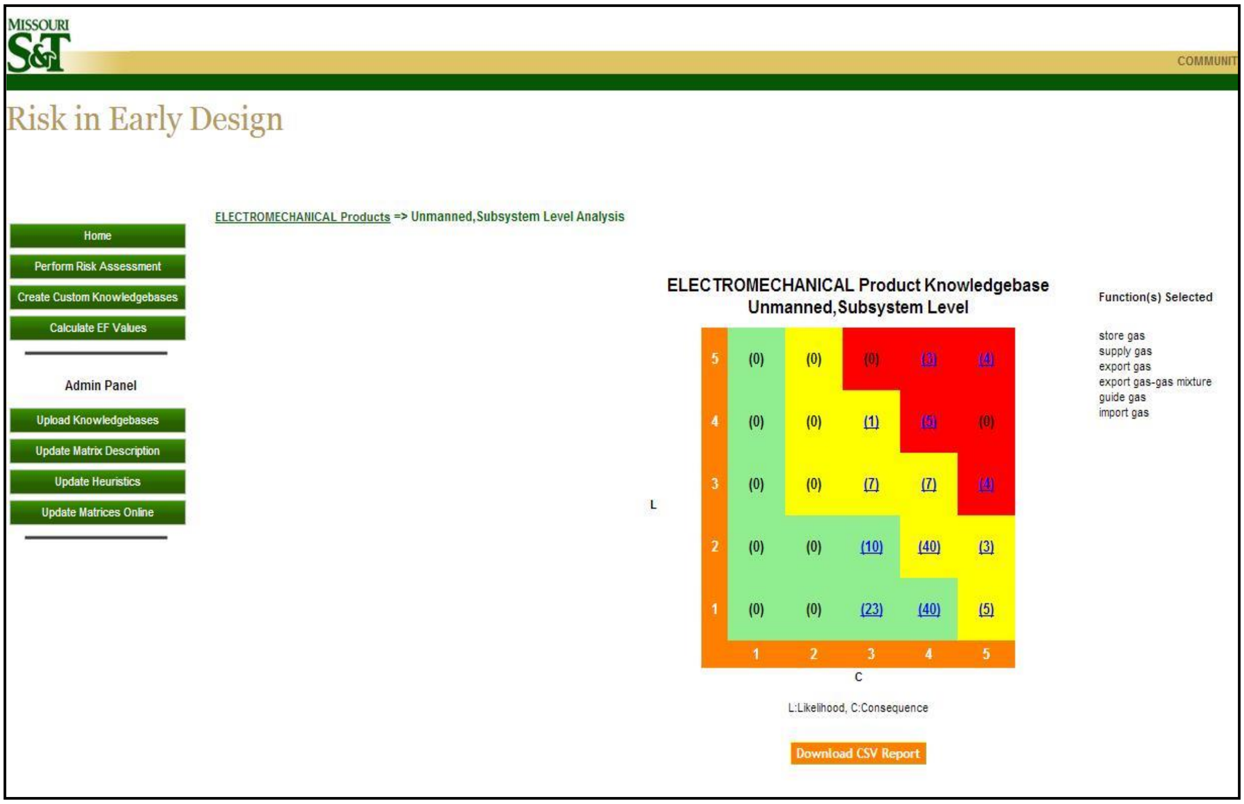
Function/Failure Matrix

=

	Abrasive Wear	Adhesive Wear	Brittle Fracture	Corrosion Fatigue	Corrosive Wear	Cracking	Creep Buckling	Crevice Corrosion	Deformation Wear	Direct Chemical Attack	Force Induced Deformation
Import Human Energy	8	2	4	0	17	20	1	0	6	21	83
Import Human Material	0	0	0	0	0	0	0	0	0	0	0
Import Hydraulic Energy	0	0	0	0	0	0	0	0	0	0	0
Import Liquid	8	2	4	0	18	20	1	0	6	22	83
Import Liquid-Solid Mixture	0	0	0	0	0	0	0	0	0	0	0
Import Mechanical Energy	10	2	4	0	17	20	1	0	6	22	84
Import Pneumatic Energy	4	0	2	0	10	6	1	0	2	12	33
Import Radioactive Energy	0	0	0	0	0	0	0	0	0	0	0
Import Rotational Energy	0	0	0	0	0	0	0	0	0	0	0
Import Solar Energy	0	0	0	0	0	0	0	0	0	0	0
Import Solid	8	2	4	0	18	20	1	0	6	22	83
Import Status Signal	0	0	0	0	0	0	0	0	0	0	0
Import Thermal Energy	4	0	2	0	10	6	1	0	2	12	33
Import Translational Energy	0	0	0	0	0	0	0	0	0	0	0

Figure 3. Process of calculating the function-Failure matrix (Mitchell et al., 2005)

RED applies simple mathematics to communicate archived historical product specific risks in both hierarchical integer and color-coded format. The matrix is linked to data base of potential failure modes that can interrupt operation (Lough, Stone, & Tumer, 2008; Grantham Lough, Stone, & Tumer, 2005). Figure 4 illustrates the generated corresponding risk matrix chart.



ELECTROMECHANICAL Products => Unmanned,Subsystem Level Analysis

ELECTROMECHANICAL Product Knowledgebase
Unmanned,Subsystem Level

L					
5	(0)	(0)	(0)	(3)	(4)
4	(0)	(0)	(1)	(5)	(0)
3	(0)	(0)	(7)	(7)	(4)
2	(0)	(0)	(10)	(40)	(3)
1	(0)	(0)	(23)	(40)	(5)
	1	2	3	4	5
			C		

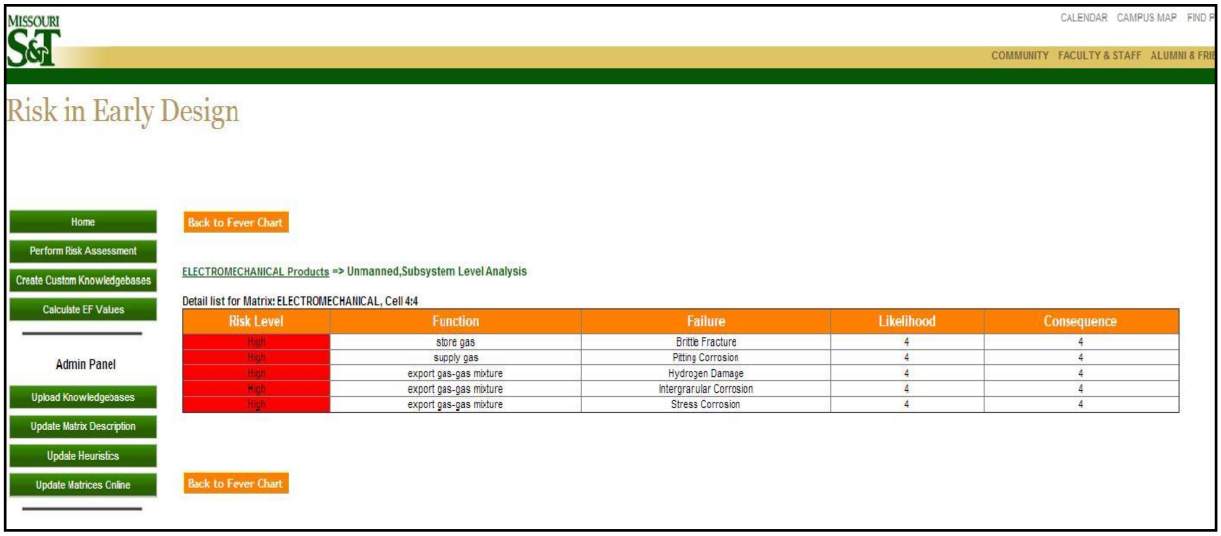
L:Likelihood, C:Consequence

Function(s) Selected

store gas
supply gas
export gas
export gas-gas mixture
guide gas
import gas

Figure 4. Generated risk matrix

The user can explore further specific information about the product's risks and consequences. This will generate comprehensive report, via an excel sheet, that will include the potential failure, likelihood and consequence. The availability of this information enables the user to separate data into columns and rows and allows to sort by their various levels of risk for simplicity and ease of use. The table will provide the user with risk level, component functions, potential failure modes, likelihood and consequence. Figure 5 illustrates the corresponding details list for the matrix for likelihood 4 and consequence 4, respectively, where five failure modes were identified by the software based on the selected component functions. These failure modes indicate a high risk level with likelihood and consequence of four and four, respectively.



ELECTROMECHANICAL Products => Unmanned,Subsystem Level Analysis

Detail list for Matrix: ELECTROMECHANICAL, Cell 4:4

Risk Level	Function	Failure	Likelihood	Consequence
High	store gas	Brittle Fracture	4	4
High	supply gas	Pitting Corrosion	4	4
High	export gas-gas mixture	Hydrogen Damage	4	4
High	export gas-gas mixture	Intergrarular Corrosion	4	4
High	export gas-gas mixture	Stress Corrosion	4	4

Figure 5. Detail of potential failures

When compared to other risk assessment tools, RED does not require specialists to detect possible failures as it employs a historical knowledgebase to produce the potential risks (Grantham Lough, Stone, & Tumer, 2005; Lough, Stone, & Tumer, 2009). This feature is advantageous for engineers lacking basic product failure knowledge.

5. RED and the oil industry

As RED analyzes the risk and consequences of a component in a system, the catalogued historical failure database tabulated into the software are intended for generic product functions (Lough et al, 2009). To verify RED's capability in identifying failure modes, approximately thirty major accidents due to electro-mechanical failures were randomly selected to undergo the evaluation. Hence, the software was not originally designed to identify potential failure modes in the oil and gas industry. The first step in performing an accurate RED analysis is selecting the functions performed by components in the system. These functions can be selected from a list of "electromechanical functions" cataloged in the RED software tool. The analysis identifies potential causes of failures that could interrupt operations.

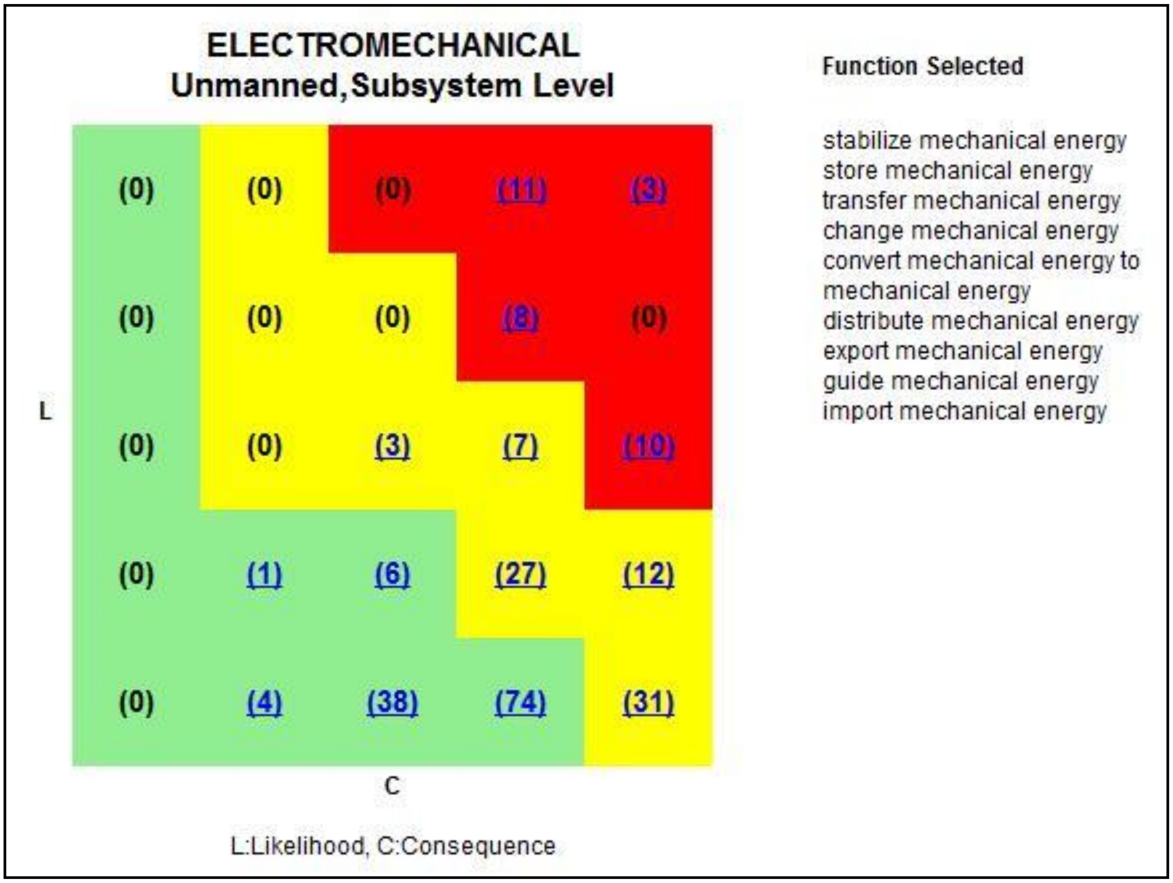
The generated RED analysis signifies failure modes for the selected component. In order to verify the results of RED analysis, accident reports issued by either government agencies were cross-referenced. Hence, the reports identify both the component location and the cause of the failure. Four case studies with different causes of failure modes are list to demonstrate the capability of the software to identify failure modes contributed to the accidents.

5.1 Alexander Kielland Accident

In 1980, the Norwegian oil drilling rig Alexander Kielland collapsed in Ekofisk oil field in the Norwegian sector of the North Sea resulting in 123 fatalities on board of the rig (Huse, 2011). The investigative report concluded that the rig collapsed due to a fatigue crack in one of its six bracings due to poor welding (Saini, 2011); figure 6 illustrates a section of the rig Norwegian Petroleum Museum in Stavanger.

Figure 6. Section of the supporting braces (Saini, 2011)

To verify, RED was utilized to analyze the functionality of the supporting braces and evaluate potential failure modes. The functions of supporting brace were entered in RED software. Figure 7 illustrates the likelihood and consequences of potential failures.



ELECTROMECHANICAL
Unmanned,Subsystem Level

(0)	(0)	(0)	(11)	(3)
(0)	(0)	(0)	(8)	(0)
(0)	(0)	(3)	(7)	(10)
(0)	(1)	(6)	(27)	(12)
(0)	(4)	(38)	(74)	(31)

L:Likelihood, C:Consequence

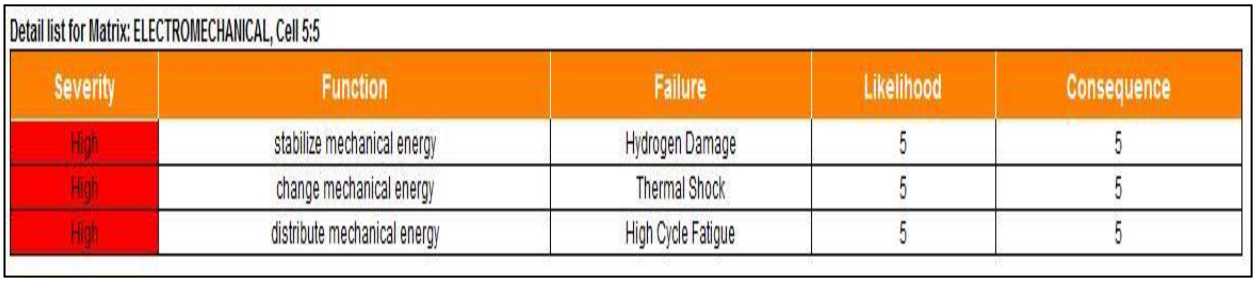
Function Selected

stabilize mechanical energy
store mechanical energy
transfer mechanical energy
change mechanical energy
convert mechanical energy to mechanical energy
distribute mechanical energy
export mechanical energy
guide mechanical energy
import mechanical energy

Figure 7. Alexander Kielland’s likelihood and consequences of potential failures

The RED analysis identified several potential failures with different ranks for likelihood and consequence. With likelihood 5 and consequence 5 in the risk matrix, the user recognizes three potential failures for the supporting brace; Hydrogen damage, thermal shock, and high cycle fatigue, as illustrated by table 1.

Table 1. Alexander Kielland's risk matrix details of potenital failures (Severity 5/ Consequence 5)

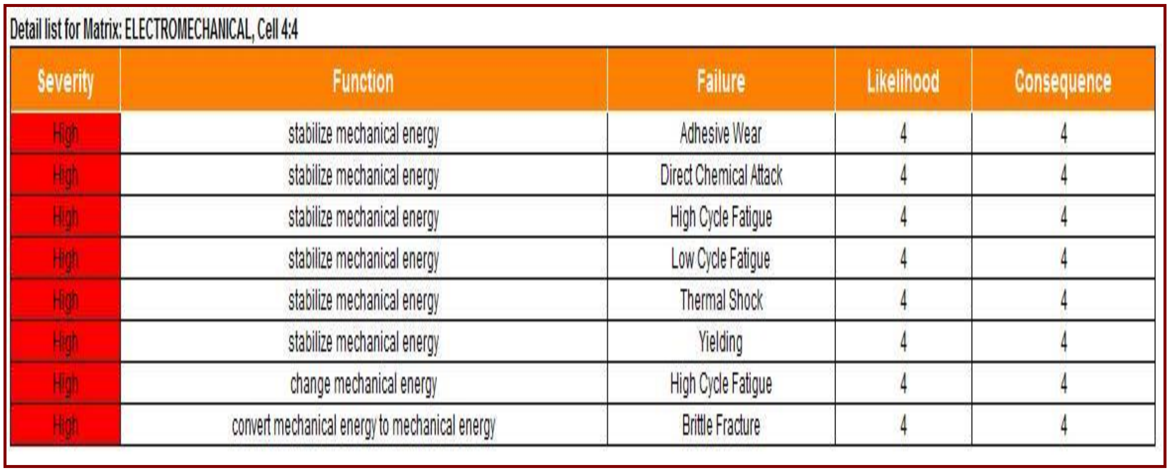


Detail list for Matrix: ELECTROMECHANICAL, Cell 5:5

Severity	Function	Failure	Likelihood	Consequence
High	stabilize mechanical energy	Hydrogen Damage	5	5
High	change mechanical energy	Thermal Shock	5	5
High	distribute mechanical energy	High Cycle Fatigue	5	5

Similarly, high cycle fatigue appeared as a potential failure mode in addition to other failure modes that can obstruct the systems function. Table 2 list the potential failures with likelihood and severity of four and four, respectively.

Table 2. Alexander Kielland's risk matrix details of potential failures (Severity 4/ Consequence 4)



Detail list for Matrix: ELECTROMECHANICAL, Cell 4:4

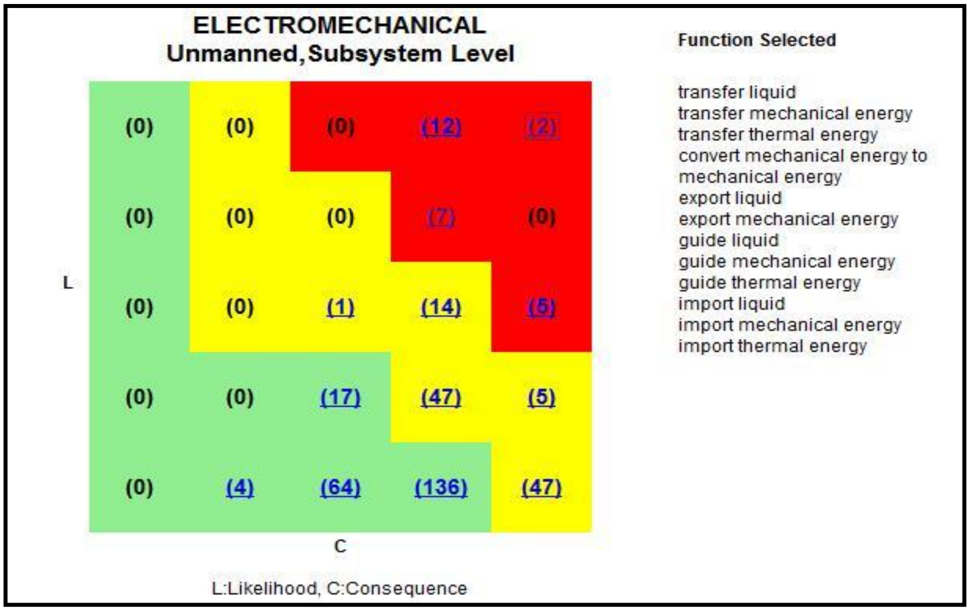
Severity	Function	Failure	Likelihood	Consequence
High	stabilize mechanical energy	Adhesive Wear	4	4
High	stabilize mechanical energy	Direct Chemical Attack	4	4
High	stabilize mechanical energy	High Cycle Fatigue	4	4
High	stabilize mechanical energy	Low Cycle Fatigue	4	4
High	stabilize mechanical energy	Thermal Shock	4	4
High	stabilize mechanical energy	Yielding	4	4
High	change mechanical energy	High Cycle Fatigue	4	4
High	convert mechanical energy to mechanical energy	Brittle Fracture	4	4

The conducted investigations concluded that one of the lower tubular bracings failed due to fatigue, hence, the attached support was torn off resulting in a capsizing the platform (Almar-Naess, Haagensen, Lian, Moan, & Simonsen, 1982). In addition, the investigations concluded that the design fatigue life of the bracing was inadequate (Moan, 2007; Clinton et al, 1981). Hence, the RED analysis resulted in the same failure mode indicated by the investigation report in addition to other potential failure modes that can impact the integrity of the brace.

5.2 Enbridge pipeline oil spill

In 2010, a thirty-inch pipeline transporting crude oil ruptured near Marshall, Michigan. According to EPA, the leak resulted in more than one million gallons of crude that entered Lake Michigan tributary, Kalamazoo River. The National Transpiration Safety Board investigation report concluded that overload fracture, due to an increase from 50 psi to 200 psi by the Canadian Enbridge Energy, caused the pipeline to rupture (Committee on Transportation and Infrastucture, 2010). According to Dr. Heiderbach, high cycle fatigue is the most common cause of pipeline failure in the oil and gas industry (Heidersbach, 2010)

RED was utilized to analyze the functionality of the pipeline and to evaluate potential failure modes. The functions of pipeline were entered in RED software. Figure 8 illustrates the likelihood and consequences of potential failures.



ELECTROMECHANICAL
Unmanned, Subsystem Level

	(0)	(0)	(0)	(12)	(2)
	(0)	(0)	(0)	(7)	(0)
L	(0)	(0)	(1)	(14)	(5)
	(0)	(0)	(17)	(47)	(5)
	(0)	(4)	(64)	(136)	(47)
			C		

L:Likelihood, C:Consequence

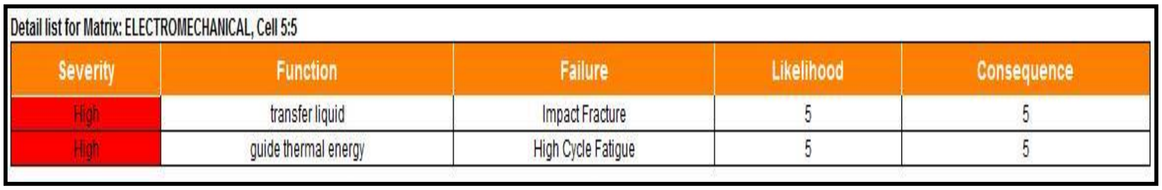
Function Selected

transfer liquid
transfer mechanical energy
transfer thermal energy
convert mechanical energy to mechanical energy
export liquid
export mechanical energy
guide liquid
guide mechanical energy
guide thermal energy
import liquid
import mechanical energy
import thermal energy

Figure 8. Enbridge accident likelihood and consequences of potential failures

The RED analysis identified several potential failures with different ranks for likelihood and consequence. With likelihood 5 and consequence 5 in the risk matrix, the user recognizes two potential failures for the pipeline; impact fracture and high cycle fatigue, as illustrated by table 3.

Table 3. Enbridge risk matrix details of potenital failures (Severity 5/ Consequence 5)

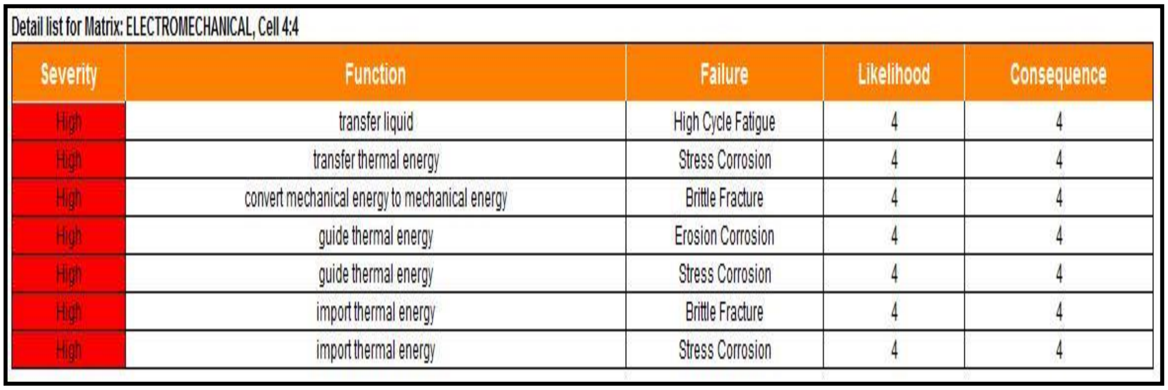


Detail list for Matrix: ELECTROMECHANICAL, Cell 5:5

Severity	Function	Failure	Likelihood	Consequence
High	transfer liquid	Impact Fracture	5	5
High	guide thermal energy	High Cycle Fatigue	5	5

Similarly, high cycle fatigue appeared as a potential failure mode in addition to other failure modes that can obstruct the systems' function. Table 4 list the potential failures with likelihood and severity of four and four, respectively.

Table 4. Enbridge risk matrix details of potenital failures (Severity 4/ Consequence 4)



Detail list for Matrix: ELECTROMECHANICAL, Cell 4:4

Severity	Function	Failure	Likelihood	Consequence
High	transfer liquid	High Cycle Fatigue	4	4
High	transfer thermal energy	Stress Corrosion	4	4
High	convert mechanical energy to mechanical energy	Brittle Fracture	4	4
High	guide thermal energy	Erosion Corrosion	4	4
High	guide thermal energy	Stress Corrosion	4	4
High	import thermal energy	Brittle Fracture	4	4
High	import thermal energy	Stress Corrosion	4	4

The results of RED analysis corresponds to the result of the accident report issued by the National Transpiration Safety Board investigation report (Committee on Transportation and Infrastucture, 2010). Additional potential failure modes were part of the analysis which the used must consider to assure the integrity of the pipeline.

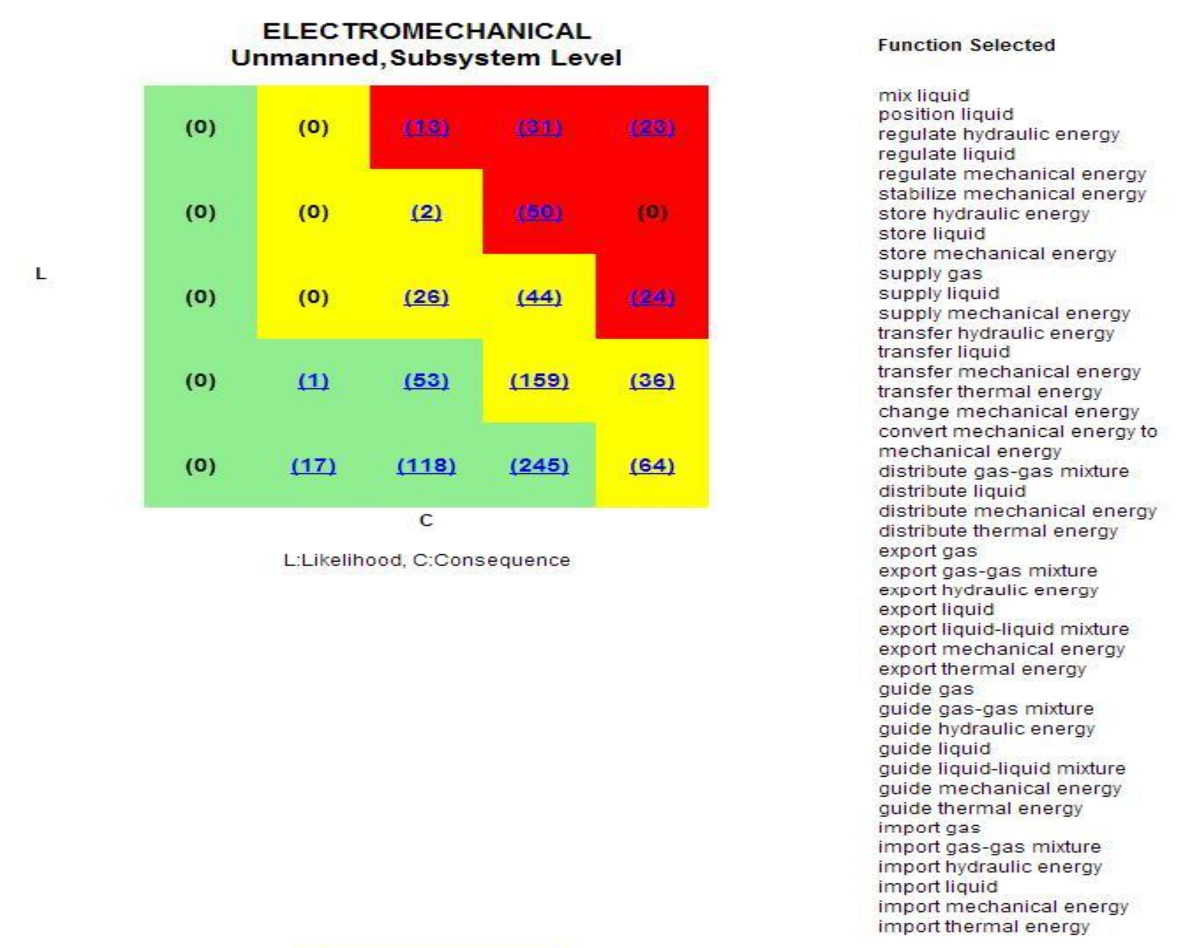
5.3 Kuwait's Mina Al-Ahmadi Accident

Kuwait's Mia A-Ahmadi is the largest of three crude oil refinery with a refining capacity over 460,000 barrel per day (KNPC, 2014). The refinery produces Benzene, jet fuel, and diesel for both domestic and export markets. In June 25, 2000, while maintenance crew were attempting to control a gas leak from a Liquefied Natural Gas (LNG) pipeline at the refinery, an explosion occurred and destroyed the entire facility. The explosion killed five workers near-by, more than fifty workers on site were injured and financial losses of more than $840 million both from production loss and revamping the facility as illustrated in Figure 9 (KNPC, 2014).

Figure 9. One of the Benzene units destroyed during the explosion (KNPC, 2014)

The cause of the gas leak was due to several reasons. Stress corrosion cracking caused the pipeline to burst (Thomson, 2013). The flutuation in flow of the liqufied natural gas due to compressors' cyclic pumping resulted in high-cycle fatigue's superimposed the corrosion in the pipeline (Blanco & Dobmann, 2013). In addtion, The existance of Carbon dioxide, Hydrogen Sulfide, and other corrosive substances, negatively impacted the overall mechanical integrity of the pipeleine (Thompson, 2013). Hece, stress corrosion was another contributing factor to the cause of the accident (Thomson, 2013; KNPC, 2014).

The functionality of the pipeline has been analyzed by RED software. The result of the analysis determines the potential failure modes accordingly. The functions of pipeline were entered in RED software where Figure 10 illustrates the likelihood and consequences of potential failures.



ELECTROMECHANICAL
Unmanned, Subsystem Level

	(0)	(0)	(13)	(31)	(23)
	(0)	(0)	(2)	(50)	(0)
L	(0)	(0)	(26)	(44)	(24)
	(0)	(1)	(53)	(159)	(36)
	(0)	(17)	(118)	(245)	(64)
			C		

L:Likelihood, C:Consequence

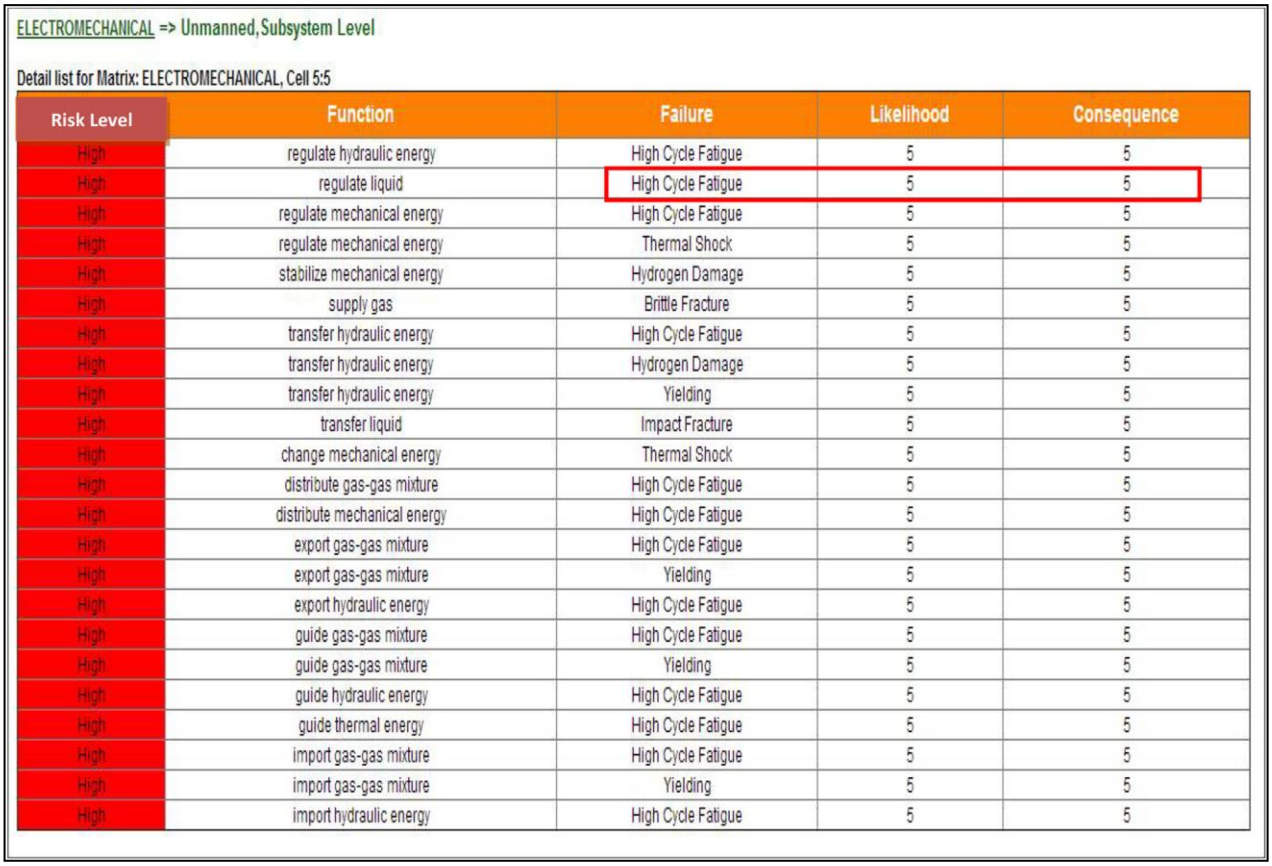
Function Selected

mix liquid
position liquid
regulate hydraulic energy
regulate liquid
regulate mechanical energy
stabilize mechanical energy
store hydraulic energy
store liquid
store mechanical energy
supply gas
supply liquid
supply mechanical energy
transfer hydraulic energy
transfer liquid
transfer mechanical energy
transfer thermal energy
change mechanical energy
convert mechanical energy to mechanical energy
distribute gas-gas mixture
distribute liquid
distribute mechanical energy
distribute thermal energy
export gas
export gas-gas mixture
export hydraulic energy
export liquid
export liquid-liquid mixture
export mechanical energy
export thermal energy
guide gas
guide gas-gas mixture
guide hydraulic energy
guide liquid
guide liquid-liquid mixture
guide mechanical energy
guide thermal energy
import gas
import gas-gas mixture
import hydraulic energy
import liquid
import mechanical energy
import thermal energy

Figure 10. Kuwait’s Mina Al-Ahmadi accident likelihood and consequences of potential failures

The RED analysis identified several ranks of potential failures of different likelihood consequences, as illustrated in Figure 10. The software recognized twenty three potential failure modes for likelihood five and consequence 5 in the risk matrix, as illustrated in table 5. The list includes high cyclic fatigue as one of the highest failure mode risk in the system in addition to other potential failure modes.

Table 5. Kuwait's Mina Al-Ahmadi risk matrix details of potenital failures (Likelihood 5/ Consequence 5)



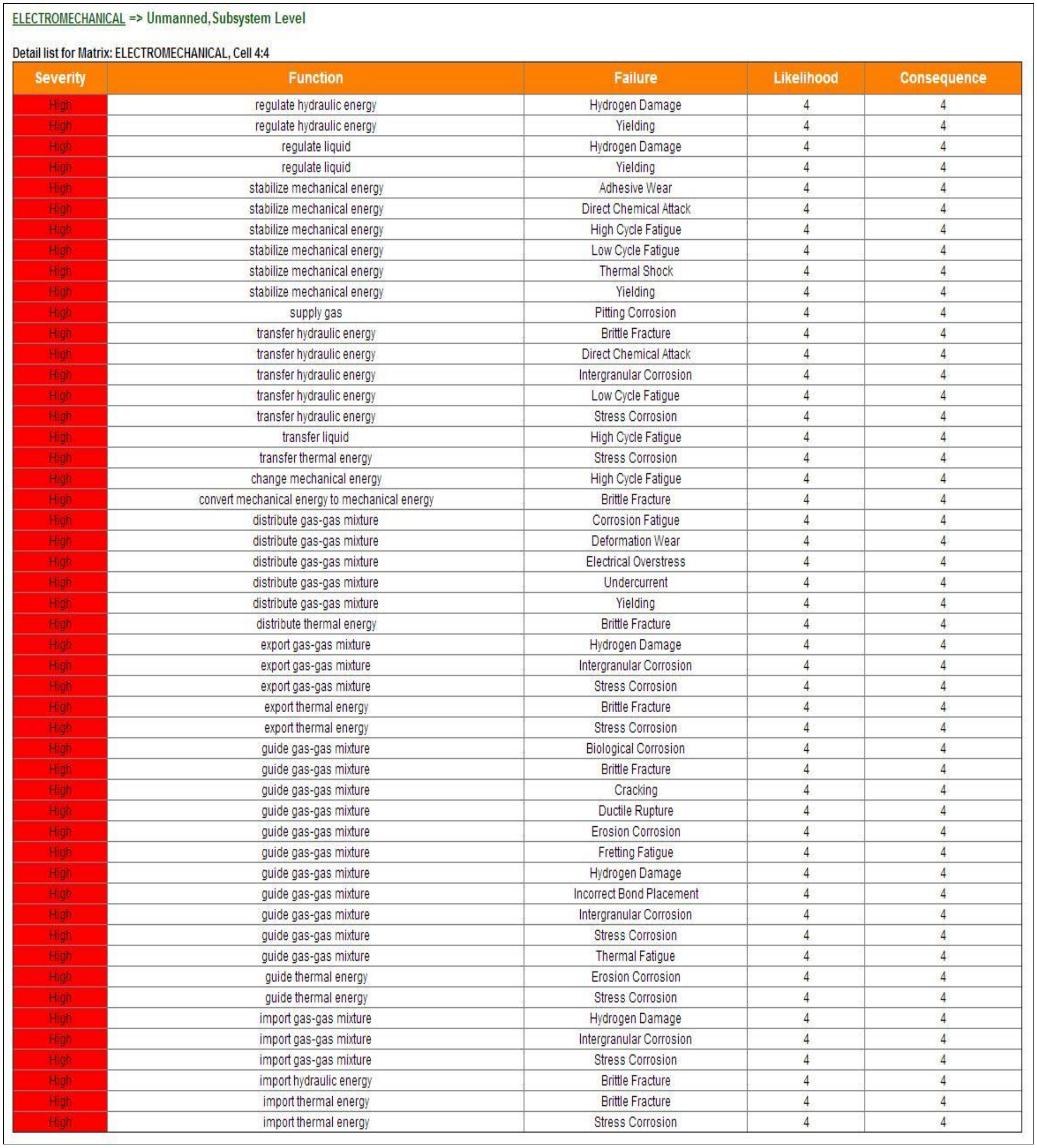
ELECTROMECHANICAL => Unmanned, Subsystem Level

Detail list for Matrix: ELECTROMECHANICAL, Cell 5:5

Risk Level	Function	Failure	Likelihood	Consequence
High	regulate hydraulic energy	High Cycle Fatigue	5	5
High	regulate liquid	High Cycle Fatigue	5	5
High	regulate mechanical energy	High Cycle Fatigue	5	5
High	regulate mechanical energy	Thermal Shock	5	5
High	stabilize mechanical energy	Hydrogen Damage	5	5
High	supply gas	Brittle Fracture	5	5
High	transfer hydraulic energy	High Cycle Fatigue	5	5
High	transfer hydraulic energy	Hydrogen Damage	5	5
High	transfer hydraulic energy	Yielding	5	5
High	transfer liquid	Impact Fracture	5	5
High	change mechanical energy	Thermal Shock	5	5
High	distribute gas-gas mixture	High Cycle Fatigue	5	5
High	distribute mechanical energy	High Cycle Fatigue	5	5
High	export gas-gas mixture	High Cycle Fatigue	5	5
High	export gas-gas mixture	Yielding	5	5
High	export hydraulic energy	High Cycle Fatigue	5	5
High	guide gas-gas mixture	High Cycle Fatigue	5	5
High	guide gas-gas mixture	Yielding	5	5
High	guide hydraulic energy	High Cycle Fatigue	5	5
High	guide thermal energy	High Cycle Fatigue	5	5
High	import gas-gas mixture	High Cycle Fatigue	5	5
High	import gas-gas mixture	Yielding	5	5
High	import hydraulic energy	High Cycle Fatigue	5	5

Moreover, both stress corrosion and corrosion fatigue, which were the main cause of the gas leak, appeared as a potential failure mode with both likelihood and consequence of four and four, respectively. Hence, RED successfully identified the main causes of the failure, in addition to a long list of potential failure modes that can obstruct the systems function and impact the integrity of the component (pipeline). Table 6 list the potential failures with likelihood and consequence of four and four, respectively.

Table 6. Kuwait's Mina Al-Ahmadi risk matrix details of potential failures (Likelihood 4/ Consequence 4)



ELECTROMECHANICAL => Unmanned, Subsystem Level

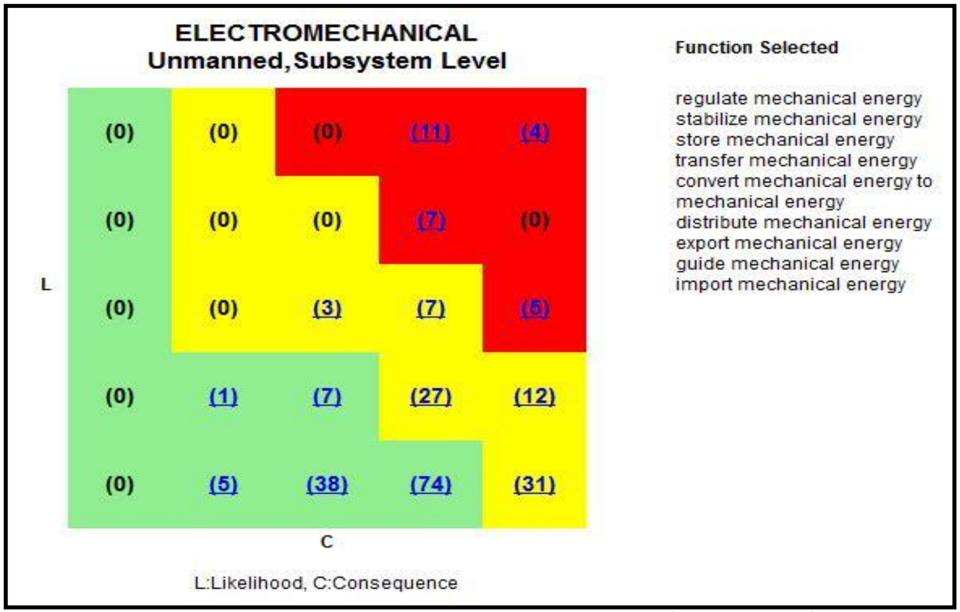
Detail list for Matrix: ELECTROMECHANICAL, Cell 4:4

Severity	Function	Failure	Likelihood	Consequence
High	regulate hydraulic energy	Hydrogen Damage	4	4
High	regulate hydraulic energy	Yielding	4	4
High	regulate liquid	Hydrogen Damage	4	4
High	regulate liquid	Yielding	4	4
High	stabilize mechanical energy	Adhesive Wear	4	4
High	stabilize mechanical energy	Direct Chemical Attack	4	4
High	stabilize mechanical energy	High Cycle Fatigue	4	4
High	stabilize mechanical energy	Low Cycle Fatigue	4	4
High	stabilize mechanical energy	Thermal Shock	4	4
High	stabilize mechanical energy	Yielding	4	4
High	supply gas	Pitting Corrosion	4	4
High	transfer hydraulic energy	Brittle Fracture	4	4
High	transfer hydraulic energy	Direct Chemical Attack	4	4
High	transfer hydraulic energy	Intergranular Corrosion	4	4
High	transfer hydraulic energy	Low Cycle Fatigue	4	4
High	transfer hydraulic energy	Stress Corrosion	4	4
High	transfer liquid	High Cycle Fatigue	4	4
High	transfer thermal energy	Stress Corrosion	4	4
High	change mechanical energy	High Cycle Fatigue	4	4
High	convert mechanical energy to mechanical energy	Brittle Fracture	4	4
High	distribute gas-gas mixture	Corrosion Fatigue	4	4
High	distribute gas-gas mixture	Deformation Wear	4	4
High	distribute gas-gas mixture	Electrical Overstress	4	4
High	distribute gas-gas mixture	Undercurrent	4	4
High	distribute gas-gas mixture	Yielding	4	4
High	distribute thermal energy	Brittle Fracture	4	4
High	export gas-gas mixture	Hydrogen Damage	4	4
High	export gas-gas mixture	Intergranular Corrosion	4	4
High	export gas-gas mixture	Stress Corrosion	4	4
High	export thermal energy	Brittle Fracture	4	4
High	export thermal energy	Stress Corrosion	4	4
High	guide gas-gas mixture	Biological Corrosion	4	4
High	guide gas-gas mixture	Brittle Fracture	4	4
High	guide gas-gas mixture	Cracking	4	4
High	guide gas-gas mixture	Ductile Rupture	4	4
High	guide gas-gas mixture	Erosion Corrosion	4	4
High	guide gas-gas mixture	Fretting Fatigue	4	4
High	guide gas-gas mixture	Hydrogen Damage	4	4
High	guide gas-gas mixture	Incorrect Bond Placement	4	4
High	guide gas-gas mixture	Intergranular Corrosion	4	4
High	guide gas-gas mixture	Stress Corrosion	4	4
High	guide gas-gas mixture	Thermal Fatigue	4	4
High	guide thermal energy	Erosion Corrosion	4	4
High	guide thermal energy	Stress Corrosion	4	4
High	import gas-gas mixture	Hydrogen Damage	4	4
High	import gas-gas mixture	Intergranular Corrosion	4	4
High	import gas-gas mixture	Stress Corrosion	4	4
High	import hydraulic energy	Brittle Fracture	4	4
High	import thermal energy	Brittle Fracture	4	4
High	import thermal energy	Stress Corrosion	4	4

5.4 Ula oil field accident

On September 2012, a significant amount of crude oil leaked on one of Ula's oil field production faculties. The oil field is located at the southern end of the Norwegian continent shelf. According to the Norwegian Petroleum Safety Authority (PSA), the cause of the accident was due to fracturing of the bolds holding together a valve attached to a separation vessel (Lauridsen, 2012). Furthermore, the accident report concluded that "Seepage in the valve exposed the bolts to produced water with a high content of chlorides and a temperature of about 120°C," the seepage commenced "chloride stress corrosion cracking which weakened the bolts until they finally fractured" (Lauridsen, 2012, p. 30). Several incidents petroleum fields and installations in the North Sea have been related to bolt failures; fatigue, Hydrogen embrittlement, ductile torsional overload, and corrosion are among the most common failures encountered (Bøgner, Rørvik, & Marken, 2005).

RED was utilized to analyze the functionality of the bolt and to evaluate potential failure modes. Figure 11 illustrates the likelihood and consequences of potential failures.



ELECTROMECHANICAL
Unmanned,Subsystem Level

L

(0)	(0)	(0)	(11)	(4)
(0)	(0)	(0)	(7)	(0)
(0)	(0)	(3)	(7)	(5)
(0)	(1)	(7)	(27)	(12)
(0)	(5)	(38)	(74)	(31)

C

L:Likelihood, C:Consequence

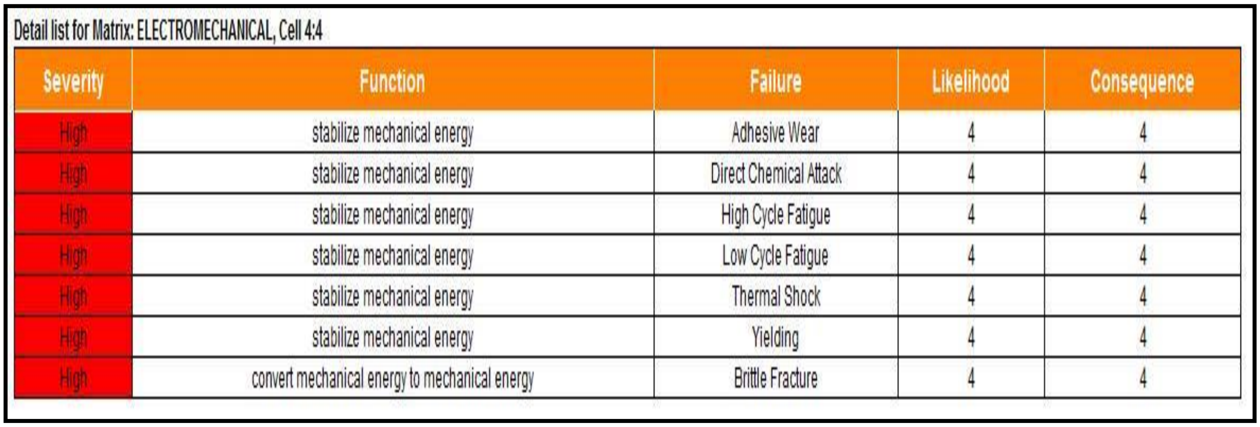
Function Selected

regulate mechanical energy
stabilize mechanical energy
store mechanical energy
transfer mechanical energy
convert mechanical energy to mechanical energy
distribute mechanical energy
export mechanical energy
guide mechanical energy
import mechanical energy

Figure 11. Ula's likelihood and consequences of potential failures

The software identified several potential failure modes with different likelihood and consequence ranking. When selecting the likelihood 4 and consequences four, the detailed analysis of the software recognized both high and low cycle fatigue, as depicted in table 7. Thus, direct chemical attack from corrosive environment was also identified in RED as potential failure mode for the bolt; confirms the Ula oil field bolt failure accident.

Table 7. Ula Oil field risk matrix details of potential failures (Severity 4/ Consequence 4)



Detail list for Matrix: ELECTROMECHANICAL, Cell 4:4

Severity	Function	Failure	Likelihood	Consequence
High	stabilize mechanical energy	Adhesive Wear	4	4
High	stabilize mechanical energy	Direct Chemical Attack	4	4
High	stabilize mechanical energy	High Cycle Fatigue	4	4
High	stabilize mechanical energy	Low Cycle Fatigue	4	4
High	stabilize mechanical energy	Thermal Shock	4	4
High	stabilize mechanical energy	Yielding	4	4
High	convert mechanical energy to mechanical energy	Brittle Fracture	4	4

6. Conclusion

Accidents of different scales urged the oil and gas industry to innovate new risk assessment tools to prevent future failure from occurring. Risk in Early Design (RED), a product risk assessment tool, was applied to identify different failure modes that might interrupt operation in the oil and gas industry. The software successfully identified the failure modes in different major accidents, in addition to other potential failure modes that can impact the integrity of the selected component. The results of the RED analysis were verified by the corresponding accident reports.

The software is a supporting tool and compliments other Process Hazard Analysis (PHA) tools currently used in the industry. However, RED is advantageous in generating a list of prelude risk assessment based on cataloged historical product failure record. The proposed new method aspires in assisting both novice engineers and designers lacking the necessary experience. The software provides preliminary risk assessments and potential failure mode identification leverage for electromechanical products based on archived knowledge of past failures. The archived knowledge used to generate the RED risk results is mathematically associated to product function. This relationship to product function provides designers the ability to project failures related to their product's function as early as the conceptual design stages and identify consequent mitigation strategies.

As an ongoing project, the software compliments another software, Generated Risk Event Effect Neutralization (GREEN), which proposes mitigation strategies. These strategies can aid the end user to minimize the likelihood and/or consequence of the potential failure modes that can negatively impact process operations. Hence, both software will be verified by experts in the field of risk assessment and accident causation. Accordingly, both RED and GREEN will be validated by petroleum industry's end users. The end-user can be, but not limited to, facility design engineer, risk assessment specialist, reliability engineers, and managers in charge of assets' integrity.

Works Cited

Almar-Naess, A., Haagensen, P. J., Lian, B., Moan, T., & Simonsen, T. (1982). Investigation of the Alexander L. Kielland Failure - Metallurgical and Fracture Analysis. *14th Annual Ofshore Technology Conference* (pp. 79-87). Houston, Texas: Offshore Technology Conference.

Al-Shamari, A., Al-Sulaiman, S., Al-Mithin, A., Jarragh, A., & Prakash, S. (2013). Corrosion Monitoring for Kuwait's Pipeline Network System. *18th Middle East Oil & Gas Show and Conference* (pp. 164190-MS). Manama, Bahrain: Society of Petroleum Engineers.

Altabbakh, H., & Grantham, K. (2012). Towards Quantifying the Safety Cognition in the Undergraduate Engineering Student. *2013 Student Safety Innovation Challenge - ME Today.* Houston, Texas: ASME.

Altabbakh, H., Murray, S., Grantham, K., & Siddharth Damle. (2013). Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster. *Engineering Management Journal*, 13-24.

Anderson, C. M., & LaBelle, R. P. (1994). Comparative occurrence rates for offshore oil spills. *Spill Science & Technology Bulletin*, 131-141.

API RP. (2009). 580 Recommended Practice for Risk-Based Inspection. Washington, DC, USA: American Petroleum Institute.

Baeckmann, W. v., Schwenk, W., & Prinz, W. (1997). *Handbook of Cathodic Corrosion Protection.* Houston, TX: Gulf Professional Publishing.

Blanco, I. C., & Dobmann, G. (2013). Surface Open Corrosive Wall Thinning Effects. *NDT in Canada 2013 Conference & NDT for the Energy Industry.* Calgary, Alberta, Canada: Canadian Institue for NDE.

Bøgner, B., Rørvik, G., & Marken, L. (2005). Bolt failures - Case histories from the Norway. *Microscopy and Microanalysis*, 1604-1605.

Bosch, C., Herrmann, T., & Jansen, J. P. (2006). Fit-for-Purpose HIC Assessment of Large-Diameter Pipes for Sour Service Application. *CORROSION 2006* (p. 06124). San Diego, California: NACE International.

Broughton, E. (2005). *The Bhopal disaster and its aftermath: a review*. Retrieved July 21, 2013, from Environmental Health: A Global Access Science Source,: http://www.ehjournal.net/content/4/1/6

Clinton, J. S., Clarkson, J. A., Cook, S. J., & Walker, S. (1981). Project to Upright the Alexander Kielland. *13th Annual Offshore Technology Conference* (pp. 175-195). Houston, Texas: Offshore Technology Conference.

Cohen, M. J. (1993). Economic impact of an environmental accident: A time-series analysis of the Exxon Valdez oil spill in southcentral Alaska. *Sociological Spectrum*, 35-63.

Committee on Transportation and Infrastucture. (2010). *Enbridge Oil Spill in marshall, Michigan.* Washignton, DC: U.S Government Pringting Office.

Davies, S. (2010). Deep Oil Dilemma. *Engineering & Technology*, 44-49.

Etkin, D. S. (1999). Estimating the cleanup costs for oil spills. *International Oil Spill Conference* (pp. 35-39). Seattle, USA: International Oil Spill Conference.

Flin, R., Mearns, K., Fleming, M., & Gordon, R. (1996). *Risk perception and safety in the offshore oil and gas industry.* Sheffield: HSE Books.

Foucher, B., Boullie, J., Meslet, B., & Das, D. (2002). A review of reliability prediction methods for electronic devices. *Microelectronics Reliability*, 1155-1162.

Grantham Lough, K., Stone, R. B., & Tumer, I. Y. (2005). Function based risk assessment: mapping function to likelihood. *Proceedings of 2005 ASME International Design Engineering Technical Conferences & Computers and Information in Engineering Conference.* Long Beach, California: American Society of Mechanical Engineers.

Hauptmanns, U. (2004). Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges. *Journal of Loss Prevention in the Process Industries*, 339-345.

Health and Safety Executives. (n.d.). *Health and Safety Executives*. Retrieved November 18, 2012, from http://www.hse.gov.uk

Heidersbach, R. (2010). *Metallurgy and Corrosion Control in Oil and Gas Production.* Singapore: John Wiley & Sons.

Huse, J. R. (2011). Safety Case - A Perspective. *Offshore Technology Conference* (pp. 1-4). Houston, Texas: Offshore Technology Conference .

Khan, F. I., & Abbasi, S. (1998). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries*, 261-277.

Kirchsteiger, C. (1999). Trends in accidents, disasters and risk sources in Europe. *Journal of loss prevention in the process industries*, 7-17.

Kletz, T. A. (2001). *Hazop and Hazan.* Rugby, UK: The Institution of Chemical Engineers.

KNPC. (2014, 04 1). *Kuwait National Petroleum Company KNPC*. Retrieved from http://www.knpc.com.kw/en/AboutKNPC/Pages/default.aspx

Krus, D., & Grantham, K. (2013). Failure Prevention Through the Cataloging of Successful Risk Mitigation Strategies. *Journal of Failure Analysis and Prevention*, 712-721.

Krus, D., Grantham, K., & Murray, S. (2012). Generated risk event effect neutralization: identifying and evaluating risk mitigation strategies during conceptual design. *The 22nd Annual INCOSE International Symposium (IS 2012).* Roma, Italy: International Council on Systems Engineering.

Lauridsen, Ø. (2012). *Hydrocarbon leak on the Ula P facility, 12 September 2012.* Stavenger, Norway: Petrolem Safety Authority.

Lewis, S., & Smith, K. (2010). Lessons Learned from Real World Application of the Bow-tie Method. *6th Global Congress on Process Safety.* San Antonio, Texas: American Institute of Chemical Engineers.

Lilley, S. (2011, December). *System Failure Case Studies.* Retrieved July 25, 2013, from http://pbma.nasa.gov

Lough, K. G., Stone, R. B., & Tumer, I. (2008). Implementation Procedures for the Risk in Early Design (RED) Method. *Journal of Industrial and Systems Engineering*, 126-143.

Lough, K. G., Stone, R., & Tumer, I. Y. (2009). The risk in early design method. *Journal of Engineering Design*, 155-173.

Lough, K. G., Stone, R., & Tumer, I. Y. (2009). The risk in early design method. *Journal of Engineering Design*, 155-173.

M.F. Milazzo, G. M. (2013). The frequency of release from piping: A case-study to compare approaches quantifying organizational and managerial factors. *Chemical Engineering TransactionsVolume, 32*, 127-132.

Mannan, S. (2004). *Lees' Loss Prevention In The Process Industries: Hazard Identification, Assessment And Control.* Oxford: Butterworth-Heinemann.

Marley, M., Jahre-Nilsen, C., & BjØrnØ, O. (2001). RBI Planning For Pipelines. *The Eleventh International Offshore and Polar Engineering Conference* (pp. I-01-140). Stavanger, Norway: The International Society of Offshore and Polar Engineers.

Mihailidou, E. K., Antoniadis, K. D., & Assael, M. J. (2012). The 319 Major Industrial Accidents Since 1917. *nternational Review of Chemical Engineering, 4*(6).

Milazzo, M. F., Maschio, G., & Uguccioni., G. (2010). The influence of risk prevention measures on the frequency of failure of piping. *International Journal of Performability Engineering*, 19.

Moan, T. (2007). Fatigue Reliability of Marine Structures, from the Alexander Kielland Accident to Life Cycle Assessment. *International Journal of Offshore and Polar Engineering*, 1-21.

Natural Gas Supply Association. (2013, June 19). *NaturalGas.org*. Retrieved June 19, 2013, from www.naturalgas.org

Nolan, D. P. (2011). *Safety and security review for the process industries : application of HAZOP, PHA and What-If and SVA reviews.* Oxford : Elsevier/GPP.

Perry, R. (2011). Deepwater Horizon Oil Spill and the Limits of Civil Liability. *The Washington Law Review Association*.

Rezae, C., & Abbas, A. A. (2013). Asset Integrity Management System Implementation. *18th Middle East Oil & Gas Show and Conference* (pp. 164303-MS). Manama, Bahrain: Society of Petroleum Engineers.

Rodrigues, C. C., & Simmons, R. J. (2012). Development of an Engineering-based Master's Degree Program in HSE for the Petroleum Industry. *SPE Middle East Health, Safety, Security, and Environment Conference and Exhibition* (pp. 1-10). Abu Dhabi, UAE: Society of Petroleum Engineers.

Ronza, A., Lázaro-Touza, L., Caro, S., & J. C. (2009). Economic valuation of damages originated by major accidents in port areas. *Journal of Loss Prevention in the Process Industries*, 639-648.

Saini, A. (2011, June). Learning from failures. *MRS BULLETIN*, pp. 416-417.

Saud, Y. E., Israni, K. C., & Goddard, J. (2013). Bow-tie diagrams in downstream hazard identification and risk assessment. *Process Safety Progress*.

Seacor, J. E. (1994). Environmental terrorism: lessons from the oil fires of Kuwait. *Am. UJ Int'l L. & Pol'y*, 481.

Sharma, D. C. (2002). Bhopal's health disaster continues to unfold. *The Lancet*, 359.

Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution.* Milwaukee, WI : Asq Press.

Summers, A. E. (2003). Introduction to layers of protection analysis. *Journal of Hazardous Materials* , 163-168.

The Commonwealth Scientific and Industrial Research Organisation. (2013, June 6). *The Commonwealth Scientific and Industrial Research Organisation*. Retrieved Juky 19, 2013, from http://www.csiro.au/

Thomson, J. (2013). *Refineries and Associated Plant: Three Accident Case Studies .* New York, New York: Safety In Engineering Ltd.

U.S. Coast Guard. (1982). *Mobile Offshore Drilling Unit (MODU) Ocean Ranger .* Belvoir, Virginia: Deffence Technical Information Center.

University of Arizona Risk Management Services. (n.d.). *The University of Arizona.* Retrieved July 22, 2013, from Health and Safety: http://risk.arizona.edu/healthandsafety/

Vinnem, J. E., Hestad, J. A., Kvaløy, J. T., & Skogdalen, J. E. (2010). Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. *Reliability Engineering & System Safety*, 1142-1153.

Wilhelm, S. M., & Kane, R. D. (1986). Selection of Materials for Sour Service in Petroleum Production. *Journal of Petroleum Technology*, 1051-1061.

Yasseri, S., & Mahani, R. (2013). *Quantitative Risk Assessment for Oil and Gas Facilities.* Manchester, UK: Smart Petroleum Ltd. Retrieved July 19, 2013

Young, G. G., & Crowe, G. S. (2006). Modifying LOPA for Improved Performance. *ASSE Professional Development Conference and Exposition.* Seattle, Washington: American Society of Safety Engineers.

Zolotukhin, A. B., & Gudmestad, O. T. (2002). Application of Fuzzy Sets Theory In Qualitative And Quantitative Risk Assessment. *International Journal of Offshore and Polar Engineering*, 288-296.

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015)
and the Affiliated Conferences, AHFE 2015

III. EVALUATING GENERATED RISK EVENT EFFECT NEUTRALIZATION AS A NEW MITIGATION STRATEGY TOOL IN THE UPSTREAM INDUSTRY

Mohammad A. AlKazimi[a], Hanan Altabbakh[b], Susan Murray[c], Katie Grantham[d]

[a,] *Missouri University of Science and Technology* 129 McNutt Hall, 1400 N. Bishop, Rolla, MO 65409-0140
[b,c,d]*Missouri University of Science and Technology* 223 Engineering Management, 600 W. 14th St., Rolla, MO 65409-0370

Abstract

The upstream industry uses diverse risk mitigation approaches to mitigate eventual failures within its facilities. Yet, these approaches could not avert major accidents, on different scales, from happening as they negatively affect the industry. The purpose of this paper is to assess Generated Risk Event Effect Neutralization (GREEN) as a new tool to select suitable risk mitigation approach to prevent prospective failures in upstream industry. More than 200 hundred major accidents in the industry underwent GREEN evaluation and compared with existing risk mitigation approaches used in to mitigate eventual failures. Kuwait's' Mina Al-Ahmadi explosion was chosen as a case study to apply GREEN. The results of GREEN analysis were verified to both upstream industry's standards and best practices, thus an opinion from the design team at Kuwait's Mina Al-Ahmadi to validate the result.

Peer-review under responsibility of AHFE Conference.

***Keywords**: Risk Mitigation, Upstream Industry, GREEN*

1. Introduction

The increasing global demand for petroleum is the driving mechanism for the petroleum companies to continuously upgrade their facilities and implement the latest technological advancements in equipment, computerized software, and synchronized human-system interaction (Health and Safety Executives, 2013). Government agencies and professional societies guide the upstream industry with the best practices and regulatory guideline, to assure safe working environment and to administer the operations' management (Health and Safety Executives, 2013). Consequently, the industry utilizes a wide range of risk assessment tools to mitigate potential operational risks. Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bow Tie Analysis, What–If Analysis, Hazard and Operability analysis (HAZOP), and Layer of Protection Analysis (LOPA) are the most widespread tools used in the oil and gas industry. These meticulous tools evaluate potential risks and try to sustain them within tolerable limits (Flin, et al., 1996; Vinnem et. al, 2010; Yasseri & Mahani, 2013).

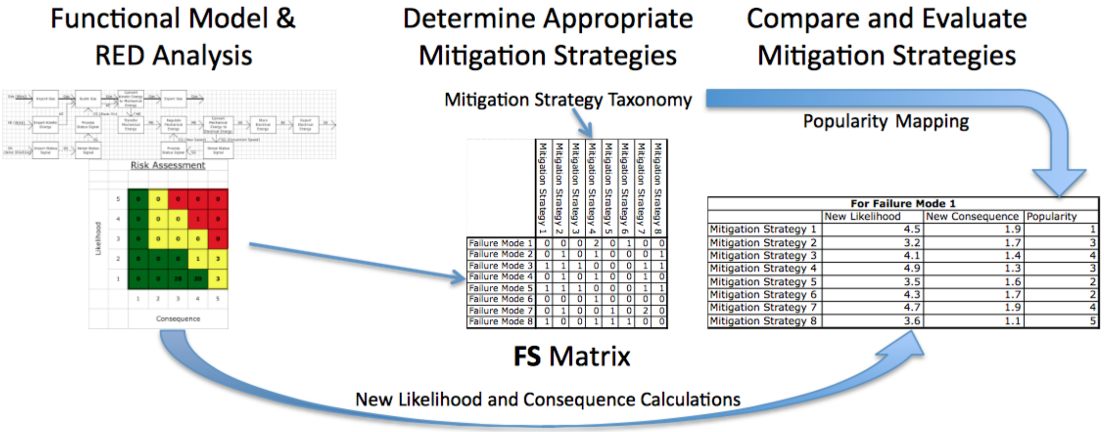
The purpose of this paper is to evaluate Generated Risk Event Effect Neutralization (GREEN) as a new tool to aid, both engineers and managers, in choosing suitable risk mitigation approach. GREEN will assist in exploring different mitigation approaches and their competences in averting prospective failures in the upstream industry. In order to validate the results of GREEN, more than two hundred major accidents were selected and underwent GREEN evaluation. The origin of the failures was electro-mechanical, material failure, and design flaws. The causes of the accidents were validated by accident report. Thus, GREEN evaluation was associated with existing risk mitigation approaches used to contain prospective failures and their consequences. In addition, upstream industry's professionals were consulted to validate both GREEN and industry's risk mitigation approaches and best precise as foundation of rationalization.

These thorough systems, to name some, assess prospective risks and try to sustain them within allowable limits (Flin, et. al, 1996; Vinnem et al., 2010; Yasseri & Mahani, 2013). Yet, with rigorous techniques and risk mitigation tools utilized in the upstream industry, major accidents occur with catastrophic consequences affecting the environment, society and petroleum industry's stakeholders. Accordingly, the need assess the conceivable risk mitigation approach is necessary to aid, both engineers and decision makers, to choose the optimal risk mitigation strategy. Hence, Generated Risk Event Effect Neutralization (GREEN) is an innovative will assist in exploring different mitigation approaches and their capabilities in preventing potential failures in the upstream industry.

1.1 The Generated Risk Event Effect Neutralization method (GREEN)

The Generated Risk Event Effect Neutralization method (GREEN) is a risk mitigation approach-selecting tool (Krus & Grantham, 2013). The method, following Risk in Early Design (RED), developed by Dr. Grantham and her team identifies and selects the dominating and optimal risk mitigation strategy (Lough, Stone, & Tumer, The risk in early design method, 2009). Hence, GREEN matrices define possible mitigation strategies where these matrices include "information on potential failure modes and their parameters, parameters that have been changed by mitigation strategies, and the likelihood and consequence changes for a given mitigation strategy**"** (Krus, Grantham, & Murray, 2012)**.** Figure 1. illustrates the overall GREEN process of selecting the optimal and dominating risk mitigation strategy to potential failures (FS). The result of the functional model and RED analysis are the base for both determining the possible mitigation strategies and evaluating the optimal strategy to fit the system, respectively.

In order to explore the validity of GREEN, the tool will be applied to a case study in the upstream industry. The results of the analysis will be validated with industry recommended practices and confirmed by industry's professionals.



Risk Assessment

Likelihood					
5	0	0	0	0	0
4	0	0	0	1	0
3	0	0	0	0	0
2	0	0	0	1	3
1	0	0	28	20	3
	1	2	3	4	5

Consequence

	Mitigation Strategy 1	Mitigation Strategy 2	Mitigation Strategy 3	Mitigation Strategy 4	Mitigation Strategy 5	Mitigation Strategy 6	Mitigation Strategy 7	Mitigation Strategy 8
Failure Mode 1	0	0	0	2	0	1	0	0
Failure Mode 2	0	1	0	1	0	0	0	1
Failure Mode 3	1	1	1	0	0	0	1	1
Failure Mode 4	0	1	0	1	0	0	1	0
Failure Mode 5	1	1	1	0	0	0	1	1
Failure Mode 6	0	0	0	1	0	0	0	0
Failure Mode 7	0	1	0	0	1	0	2	0
Failure Mode 8	1	0	0	1	1	1	0	0

For Failure Mode 1			
	New Likelihood	New Consequence	Popularity
Mitigation Strategy 1	4.5	1.9	1
Mitigation Strategy 2	3.2	1.7	3
Mitigation Strategy 3	4.1	1.4	4
Mitigation Strategy 4	4.9	1.3	3
Mitigation Strategy 5	3.5	1.6	2
Mitigation Strategy 6	4.3	1.7	2
Mitigation Strategy 7	4.7	1.9	4
Mitigation Strategy 8	3.6	1.1	5

Figure 1. The GREEN Process (Krus, Grantham, & Murray, 2012)

2. Applying GREEN in the Upstream Industry

For GREEN to effective in selecting the optimal risk mitigation strategies, cataloged historical failure database imbedded in the Risk in Early Design (RED) software are cataloged for the upstream industry. More than two hundred accident caused by electro-mechanical failures in the industry underwent GREEN evaluation to identify both failure modes and corresponding optimum risk reduction and mitigation strategies. The process is a series of steps that links the mitigation strategies with failure modes, compares the potential strategies, and chooses the optimal strategies. An accident due to electro-mechanical failure from the upstream industry was selected to validate the consistency of GREEN analysis. The method utilizes the analysis of Risk in Early Design (RED) software and indicates the optimal mitigation strategy accordingly. The first step in performing an accurate RED analysis is selecting the functions performed by components of the system. These functions can be selected from a list of "electromechanical functions" cataloged in the RED software tool. Consequently, GREEN will identify the recommended optimal mitigation strategies to be applied for the selected process.

2.1 Kuwait's Mina Al-Ahmadi Accident

Kuwait's Mia A-Ahmadi is the largest of three crude oil refinery with a refining capacity over 460,000 barrel per day (KNPC, 2014). The refinery produces Benzene, jet fuel, and diesel for both domestic and export markets. In June 25, 2000, while maintenance crew were attempting to control a gas leak from a Liquefied Natural Gas (LNG) pipeline at the refinery, an explosion occurred and destroyed the entire facility as illustrated by figure 2. The explosion killed five workers near-by, more than fifty workers on site were injured and financial losses of more than $840 million; both from production loss and revamping the facility (KNPC, 2014). The cause of the gas leak was due to several reasons; stress corrosion cracking caused the pipeline to burst (Lough, Stone, & Tumer, 2009; Thomson, 2013). The flutuation in flow of the liqufied natural gas due to compressors' cyclic pumping resulted in high-cycle fatigue's superimposed the corrosion in the pipeline (Blanco & Dobmann, 2013). In addtion, stress corrosion, the result of the sour nature of the natural gas due to the existence of Carbon dioxide, Hydrogen Sulfide, and other corrosive substances, negatively impacted the overall mechanical integrity of the pipeleine (Thomson, 2013).

Figure 2. A Benzene unit destroyed during the explosion (KNPC, 2014)

In order to Apply GREEN for the optimal risk mitigation approach, the functionality of the pipeline has been analyzed by RED software. As a result, and utilizing GREEN Matrices (Krus, Grantham, & Murray, 2012), the potential mitigation stratigies were determined for this case study. The results of GREEN anayslsis identified 20 mitigation strategies for high cycle fatigue, 23 for corrosion fatigue, and 22 for stress carrion, respectively. Tables 1 illustrates the collection of mitigation strategies presented by the **FS** matrix with the number of occurrences, in addition the likelihood and consequence changes provided from the **SC** matrix (Krus, Grantham, & Murray, 2012).

Table 1. GREEN results for high cycle fatigue new popularity, likelihood and consequence

Strategy	Popularity	New Likelihood	New Consequence
Change natural frequency	0	5	<5
Condition Material	1	5	<5
Condition Part	1	5	<5
Convert Material	3	4.8	4.8
Convert Part	1	5	4.9
Couple Part	0	5	<5
Decrease Motion	0	5	<5
Decrease Power Assist	0	5	<5
Import Lubricant	0	5	<5
Import Material	0	5	<5
Import Part	0	5	<5
Import Stress	0	5	<5
Increase Control	1	<5	<5
Increase Flow	0	5	<5
Remove Part	0	<5	<5
Secure Part	1	<5	<5
Separate Contaminant	0	5	<5
Shape Part	5	5	<5
Stabilize Process	0	5	<5
Stop Process	0	5	<5

3. Conclusion

As the upstream industry applies different risk assessment tools to mitigate potential failures, accidents on different scales continue to occur as they negatively impact the industry. Generated Risk Event Effect Neutralization (GREEN) analysis was utilized to examine potential risk mitigation strategies upstream industry. The analysis successfully identified potential failure modes for different major accidents with different causes of failures and the possible strategies to control them. The analysis was successful in capturing the failure modes that caused catastrophes in twenty-six major accidents, in addition to potential risk mitigation strategies to prevent similar future accidents. GREEN is advantageous in producing a list of prelude risk assessment based on cataloged historical product failure record, and their corresponding control strategies. The tool can assist novice engineers and decision makers in the upstream industry in recognizing potential failure modes in the process system and how to accurately mitigate their likelihood and consequence; especially in the design conceptual design stages.

As a future work, the tool will address the human factor aspect n the industry due to its importance with the merging complex technologies. The close interaction between human and machines in a very volatile process environment makes it necessary to consider human-system integration and human factors part of the overall system design. Hence, this consecration will look into risk from different perspectives resulting in design safety and operating efficiency.

References

Flin, R., Mearns, K., Fleming, M., & Gordon, R. (1996). *Risk perception and safety in the offshore oil and gas industry*. Sheffield: HSE Books.

Health and Safety Executives. (2013). *Health and Safety Executives*. Retrieved November 18, 2012, from http://www.hse.gov.uk

KNPC. (2014, 04 1). *Kuwait National Petroleum Company KNPC*. Retrieved from http://www.knpc.com.kw/en/AboutKNPC/Pages/default.aspx

Krus, D., & Grantham, K. (2013). Failure Prevention Through the Cataloging of Successful Risk Mitigation Strategies. *Journal of Failure Analysis and Prevention*, 712-721.

Krus, D., Grantham, K., & Murray, S. (2012). Generated risk event effect neutralization: identifying and evaluating risk mitigation strategies during conceptual design. *The 22nd Annual INCOSE International Symposium (IS 2012).* Roma, Italy: International Council on Systems Engineering.

Lough, K. G., Stone, R., & Tumer, I. Y. (2009). The risk in early design method. *Journal of Engineering Design*, 155-173.

Thomson, J. (2013). *Refineries and Associated Plant: Three Accident Case Studies* . New York, New York: Safety In Engineering Ltd

IV. SAFETY AWARENESS IN UNDERGRADUATE ENGINEERING STUDENTS

Altabbakh, Hanan; AlKazimi, Mohammad A.; Murray, Susan; Grantham, Katie

ABSTRACT

Accidents among engineering and science students in college workshops and labs have resulted in either severe injuries or tragic fatalities. Students with technical majors are required to take scientific laboratory courses and they apply their knowledge by engaging in various competitive technical design teams. Such involvement requires them to spend time in labs and/or workshops, both of which can be hazardous environments. Consequently, college students' safety mindset can be essential in both in and outside the classroom setting. In a few years, and after earning their degrees, these students will put their knowledge into practice to be engineers and scientists in the workforce. Their safety awareness and attitude towards risk is often being formed in college and will follow them into their professional career. In an effort to prevent accidents and improve safety cognition in young engineers and scientist, this study examines the training exposure and knowledge within technical competition teams from the students' perspectives. A survey targeting different OSHA safety areas was conducted to measure safety training, knowledge, and attitude of these undergraduate students. The paper, also, explores potential causes of unsafe decision making by the students surveyed.

Key Words: Safety Attitudes and Culture, Undergraduate College, Laboratory Accidents

1. INTRODUCTION

Young engineering and science students participate in various technical design teams and class project teams during their academic years. Teams at Missouri University of Science and Technology such as Formula SAE racecars, ASCE Concrete Canoe, robotics competitions, and aircraft designs are few examples of different college design teams students can participate in competitions across the nation (Student Design and Experiential Learning Center, 2014) . As part of their preparation for the competitions, students spend time in campus workshops where they encounter different types of hazardous and flammable materials, machines, and other hazards. Similarly, students majoring in either engineering or science majors conduct lab experiments as part of their required academic curriculum. Often without adequate safety training, these college students are exposed to numerous hazards.

In the past decade, there have been increased concerns regarding the frequency of academic laboratory accidents occurring across the country. These accidents resulted in either severe injuries or even deaths. For example, a graduate student was severely injured; lost three fingers, burned both his hands and face, and injured one of his eyes at a chemistry lab at Texas Tech University. The explosion destroyed the entire laboratory facility as shown in Figure 1 (U.S. Chemical Safety and Hazard Investigation Board, 2010). Another accident involved a twenty-three years old year old female student died of second and third degree burns over 43% of her body while doing a research experiment in a UCLA lab (Christensen, 2009). An unfortunate student died of asphyxiation due to neck compression when her hair caught in one of the lathe machines in Yale University’s workshop (Henderson, Rosenfeld, & Serna, 2012). Four students from the University of Missouri-Columbia were severely injured during a hydrogen explosion in June of 2010 (U.S. Chemical Safety and Hazard Investigation Board, 2010). Two students from the University of Maryland were severely injured due to a chemical explosion due to improper waste management that resulted in first and second-degree chemical burns, respectively ((The Safety Zone by C&EN, 2014). The accidents reports for the accidents cited improper safety procedures; lack of training, improper documentation of training sessions, inadequate rectification to unsafe act within lab premises such as not wearing personal protective equipment (PPE) (Kemsley, 2009). These accidents, along with others, raise questions whether college students lack both the minimum safety awareness and if they safe work habits that could prevent undesired tragedies.

Figure 1. Texas Tech University laboratory explosion U.S. Chemical Safety and Hazard Investigation Board, 2010

2. LITERATURE REVIEW

The U.S. workforce employed 19.5 million young workers between the age of 16 and 24 years old in July 2012. That number was approximately 12% increase compared to 21.4 million in April 2011 (Bureau of Labor Statistics, 2012). During the period of 1998-2007, the U.S. recorded 3.6 deaths per 100,000 young workers (Bureau of Labor Statistics, 2012). Furthermore, 7.9 million non-fatal injuries in the same age group were treated in emergency departments (Centers for Disease Control and Prevention, 2010). To better understand potential causes of these accidents, a survey was conducted to measure safety training, knowledge, and attitude of college students in engineering and science fields at Missouri University of Science and Technology.

Researchers have indicated that young workers are at more risk than their older colleges when it comes to work place injuries (Salminen, 2004; McCabe, 2008; Breslin et al., 2008). Other study showed that emerging adults tend to be higher sensation seeking (Zuckerman, 1979). Psychologists define higher sensation seeking as pursuing intense experiences and the willingness to take different levels of risks to reach that experience (Zuckerman, 1994). Numerous researchers have discussed the variables that account for such behavior in emerging adults; these include both cognitive and psychosocial factors (Steinberg & Cauffman, 1996).

Theories have tackled the risk taking behavior in emerging adults and adolescents and they fall into three essential categories. First, biological based on hormonal effects, asynchronous pubertal timing, or genetic predispositions; second, psychological or cognitive deficiencies in self-esteem, cognitive immaturity, or affective disequilibrium; the third category is environmental causes that focus on social influence related to family and peer interactions, or community and societal norms (DiClemente, Hansen, & Ponton, 1995).

Psychologist conducted studies to explore potential causes of unsafe decision making within adolescent and college students (Laursen, 2009). The result of the studies showed that the frontal lobes in the human brain contain all the neurological brain “executive functions” in the process of decision making; preparation, evaluating, and historical referencing in terms of both long and short term memories (Johnson, Blum, & Giedd, 2009) In a study conducted by neuroscientist to evaluate adolescents brain development, especially the frontal lobe, the brain “maturation” requires “opportunities to interact in group situations which facilitate concern for others, problem solving, and responsible behavior” (Laursen, 2009, p. 8). As a result, the frontal lobe establishes the ability to indicate and weigh potential consequences of any act to be executed, and this function is relatively slowly developing compared to adults (Laursen, 2009). As a result, and due to exposure to different social environment, adolescents will achieve intellectual control over their behavior (Laursen, 2009).

According to the National Research Council (2011), the undergraduate chemistry laboratory courses are the first step toward familiarizing students with the basics of safety culture. These instructor are assigned to supervise a group of inexperienced students to conduct experiments in the laborites without comprehending minimal "risk management techniques that are designed to eliminate various potential dangers in the laboratory" (National Research Council, 2011, p. 3).

In order to ensure the health and safety of its laboratory users, and to avoid lawsuit claims for liability and negligence, universities should adhere to federal regulatory requirement that is related to laboratory standards. They include, and not limited to, OSHA Hazard Communication Standard (29 CFR 1910.1200), OSHA Lab Standard (29 CFR 1910.1450), and the EPA's Resource Conservation and Recovery Act (RCRA), which regulates both hazardous waste and air pollutants to protect the working environment, (Amherst College, 2014; Hays, 2005). The campus environmental health and safety department are the campus resource for regulatory compliance, hazardous waste management, laboratory and radiation safety, and admistring the safety programs. American Chemical Society (2012) conducted comparative studies to examine existing laboratory safety procedures from different universities. The result of studies indicated that university labs adhere to state laws as well both OSHA and EPA minimum requirements to safely perform laboratory experiments. Hence, these requirements avoid liability due to negligent behaviors as they provide suggestive recourses for promoting safety practices (Hill, 2012)

Prior to supervising laboratory experiments, both hired laboratory technicians and/or graduate students undergo safety-training sessions. The purpose of these sessions is to familiarize them with the previously stated regulatory compliance and assuring adherence to safety guidelines. The type of training offered to laboratory instructors consists of either classroom lectures or online training videos. The topics include interpreting Material Safety Data Sheet (MSDS), hazardous waste management and chemical waste tags, chemical compatibility and storage, spill response procedures, the use of fire safety equipment and personal protective equipments, ensure both electrical and machine safety (OSHA, 2014). Thus, to assure safety and compliance, a periodic refresher-training courses are offered periodically to the both lab technicians and/or returning graduate students supervising lab activities (National Research Council, 2011).

Once completed, the lab technician and/or the graduate student are eligible to supervise undergraduate students conducting curriculum laboratory experiments Consequently, the instructors are then assigned to supervise a group of inexperienced undergraduate students to conduct experiments in the laborites. However, and prior to the commencement of any lab activities, prospective science or engineering students must complete a safety orientation seminar. This can be done either by attending sessions conducted by the lab instructors or video session. Once successfully completed, a signed form of completion or passing a questionnaire grants the eligibility of the student to perform supervised lab tasks. Unfortunately, the students lacks the comprehension of minimal “risk management techniques that are designed to eliminate various potential dangers in the laboratory” since the training session do not cover all topics related to lab safety (National Research Council, 2011, p. 3)

3. METHODOLOGY

In order to measure safety training, knowledge and attitude of college students at Missouri University of Science and Technology, a survey was constructed based on the Goal Question Metric (GQM) approach (Basili, Caldiera, & Rombach, 1994). The Survey was with reference to OSHA Guidelines 54 Fed Register #3904-3916 (Basili, Caldiera, & Rombach, 1994). The GQM method required a top down methodology in constructing the survey (Basili, Caldiera, & Rombach, 1994). First, goals need to be specified and focused. Table 1 illustrates the goals of the survey utilizing the GQM method.

Table 1. The Goal Question Metric Survey Model

Goals	Questions	Metrics
Evaluate the amount of safety training of Missouri S&T design team members	Have you been trained to use the personal protective equipment (PPE)?	- "No, never" - "Yes, no formal training" - "Yes, formal training" - "Can't remember"
	Have you been trained on how to prepare/understand lockout/tagout?	
	Have you been trained on using material safety data sheet (MSDS)?	
	Have you been trained on machine guarding?	
	Have you been trained on evacuation from your workplace or lab(s) in case of an emergency?	
Evaluate the student design team members' safety knowledge	In which of the following situations are you required to wear safety glasses? (Please check all that apply)	- Percentage of correct response
	Lockout/tagout is required when. (Please check all that apply)	
	Locks should always stay on the equipment during the shift change? True or false	
	When working in a workshop/lab, when do you use MSDS (please check all the apply)	
	Which statement(s) are true about machine guarding?	
	Please check all that applies regarding emergency evacuation.	
Evaluate the student design team members' safety attitude	In situations where safety glasses are required, how often do you wear them?	- Likert scale & Open ended discussion
	Do you refer to the MSDS whenever a chemical or a hazardous material is spilled?	
	How often do you check if machine guards re installed on the machine you are about to use?	

Table 1. The Goal Question Metric Survey Model (cont.)

-	In case of an emergency, how often would you follow the instructions written for the emergency action plan?	-
	If you feel that PPE is not necessary when working in workshops and labs. Please discuss why below.	
Evaluate the student design team members' safety consciousness	How safety conscious are you?	- Likert scale & Open ended discussion

Next, based on these goals, a set of questions is used to measure the information needed to accomplish these goals. Finally, metrics are used to quantify the data answered in the questions (Basili, Caldiera, & Rombach, 1994). A questionnaire with 23 items together with five demographic questions was used to collect the data. The goal of the survey was to determine the amount of training the students have on OSHA procedures, evaluate their knowledge, and application, of general safety procedures, their safety attitude, and consciousness. Five questions were asked about the amount of training they had on personal protective equipment (PPE), lockout/tagout, material safety data sheets, machine guarding, and emergency evacuation as recommended by OSHA guidelines 54 Fed Register #3904-3916. Six questions were asked to test their knowledge on OSHA procedures. Five questions were asked to evaluate their attitude toward safety in labs or workshops. Finally two questions to discuss their safety consciousness as a self-assessment.

4. RESULTS AND ANALYSIS

A total of 93 web-based questionnaires were distributed, via Missouri S&T email, by the workshop supervisor to students participating in the competitive design teams. The questionnaires were returned with the following results; 68% of the respondents were male, 31% were female, and 1% preferred not to answer. The majority of the respondents' were undergraduate students (32% seniors, 25% juniors, 17% sophomores, and 18% freshmen), the others were alumni (3%) and graduate students (3%) with 95% of the total students majoring in engineering. 95% of the students were either involved in one or more design competition team in the present or past and only 5% were never involved in any design team. The students were asked if they undergone any safety training during their academic years. The survey response showed that 97% of the students were exposed to some safety training. OSHA 10 hour training, first aid CPR and AED, and high school shop training are example of their exposure to former safety training.

4.1 Goal one: Evaluate the amount of safety training of design team student members

Students were asked if they had any formal safety training during their academic years. They were given the response options of chemistry laboratory safety training, workshop safety training, safety engineering or similar classes offered on campus, and any other related form of safety education they might consider a safety course. When analyzing the students' feedback to the amount of safety training they have received; it was found that less than 30% of the respondents had any type of formal training. Most of the respondents were exposed to shop safety training, which is limited to certain types of equipment within the facility. Thus, the training does not expose the students to OSHA's recommended five domain of safety. Hence, the majority of these young engineers have been working in the labs or workshops without the proper training. Neglecting in the minimum safety requirements places these young engineers makes them vulnerable.

4.2 Goal two: Evaluate the student design team members' safety knowledge

The students were asked about workshop and laboratory safety procedures. The question were aiming at identifying students' knowledge of material safety and data sheets (MSDS), facility evacuation procedures, wearing protective equipment, and machine guarding requirements. When evaluating students' response, only 47% of the students were able to identify the safety requirements for laboratory or workshop task execution. The responses to the survey question were common sense or previous knowledge based on exposure to similar training session. Hence, the students do not acquire the necessary work safety procedures and knowledge as well, where it essential to properly response in case of hazardous material spill, machine guard while idle, or evacuation exit route and assembly point. .

4.3 Goal three: Evaluate the student design team members' safety attitude

The questionnaire had a self-reporting section for students to describe their attitude toward safety. 70% of the participants did not answer that question; the reaming 30% indicated that they would often follow safety procedures while they are in workshops or labs working on their projects. Their notion of not being hurt and assuring that work is performed safely dictated their response. However, 73% of the respondents to the safety attitude question would follow the procedures occasionally. The remaining 27% would adhere to the procedures only when they are mandated. This is an indication that the students executing laboratory experiments underestimate the potential consequences when violating procedures. Thus, they tend to take short cuts to perform the required laboratory experiments by taking advantage of not being supervised or mornitered. This shows that students lack the proper safety attitude and self-consciousness toward executing laboratory assignments in positive safe behavior.

4.4 Goal four: Evaluate the student design team members' safety consciousness

The respondents were requested to evaluate their overall safety consciousness. Spector (1994) argues that self-reporting questionnaire may portrait what the respondent would think is the correct to emphasize on social-desirability and can be bias in response.

Yet, studies indicated that self-reporting questionnaire indicates respondent's truthfulness by reporting their non-adherence without being disciplined (Goodman, Meltzer, & Bailey, 1998). The results of the questionnaire regarding the overall safety consciousness showed that 58% of the respondents find themselves as safety conscious. Twenty five percent of the participants indicated they are very conscious. However, participant who consider themselves very conscious were only 3% and the remaining participant indicated that they are neutral when it comes to evaluating themselves in terms of overall self-consciousness.

5. UTILIZING BEST PRACTICES

Training cards are certificates indicating that the user has successfully passed and approved and accredited safety program modules to perform the required task for both petroleum and process industries (API.org, 2041). The program aims at recognizing individuals who are competent to execute the required tasks as per safety standards and procedures (API.org, 2041). Due to its hazardous environment, the industries are committed to zero accidents and do not tolerate negligence (Vinnem, Hestad, Kvaløy, & Skogdalen, 2010). The cards enables the user to perform tasks once the facility supervisor issues "permit-to-work" document. The document assures that hazards are acknowledged and controlled; hence, the premises are safe to proceed with activities (Health and Safety Services, 2014).

Industrial laboratories utilize different practices to minimize potential risks and assure that hazards are contained within tolerable limits. Permit to work system is documentation system to administer activities on facilities to prevent accidents (Permit to work systems, 2014). The University of Reading (2011) applies permit to work system prior to using labs and workshops for activities in these facilities. The form will identify all hazards in the premises and certifies, to the lab or workshop user, that all safety precautions have been considered to perform the tasks with any recommendation of PPE or any related safety measures (Health and Safety Services, 2014). This document enables lab and workshop supervisors to manage access to their families and identify potential hazards that the users might encounter during performing their routine activities (Health and Safety Services, 2014).

6. CONCLUSION

The analyses of the results show that science students in college workshops and laboratories receive informal safety training prior to participating in either laboratory experiments or participating in design teams' machine shops. The outcome of this is often ineffective, where accidents in university laboratories or machine shops still occur. This is an indication that these types of training sessions do not always assure positive safety attitude or safety performance. As a result, the frequent neglect of minimum safety requirements in machine shops or laboratories can result in avoidable accidents and losses.

In addition, the survey showed that the young engineers' knowledge of five domains of the OSHA guidelines: PPE, lockout/tagout, MSDS, machine guarding, and emergency action plan was insufficient. Lack of knowledge in these minimum essential domains can cause undesired consequences when accidents occur and the students fail to adhere to the proper safety guidelines. Consequently, the lack of overall safety attitude is reflected in their attitude toward risk associated with their shop projects and class assignments. Hence, the students underestimate the potential consequences when positive safety attitude is not part of their work ethic behavior to execute assigned tasks safely.

Furthermore, utilizing administrative system, such as training cards and permit-to-work, can add successive layers of defense and safeguard (Altabbakh et. al, 2013). Hence, adding different layer of protection to perform tasks can mitigate potential consequences due to prior knowledge of existing hazards. Thus, both lab and/or workshop supervisors and students are held liable for the executing tasks, which can raise safety cautiousness and better understanding of potential failure consequences.

As a result, training should be conducted through highly skilled, experienced, and competent safety professionals rather than randomly selected organization with informal training that is based on general knowledge (Fanning, 2012; Robotham, 2001; Cekada, 2011). In order to reap the fruits of safety culture, it is essential to implement such culture for novice engineers in their college education. Serious chemical or laboratory incidents are often thought to be the result of a weak or deficient safety culture; a principal root cause of the incident (Committee on Chemical Safety, 2012). Implementing an effective safety culture is essential to protect employees as well as enhancing the students' safety awareness. Students need to be able to identify hazards, assess the risk associated with them, and respond to an emergency situation if the occur.

Industry would benefit from a new breed of engineer and scientist with safety culture and awareness ingrained in them. Today's young engineers are future decision makers and managers. Creating a safety-awareness environment and exposing them to real accident case studies will impact their thinking process toward decision-making and risk management. Training them in college can shape their safety attitude positively and influence organizational culture as they are promoted up the ranks. Their commitment towards safety has the potential to make a great impact on safety over time.

Works Cited

Altabbakh, H., Murray, S., Grantham, K., & Siddharth Damle. (2013). Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster. *Engineering Management Journal*, 13-24.

Amherst College. (2014, March 18). *Amherst College Laboratory Health and Safety Training.* Retrieved from www.amherst.edu

API.org. (2041, August 30). *Service Station Contractor Safety*. Retrieved from American Petroleum Institute : http://www.api.org/events-and-training/api-worksafe/service-station-contractor-safety

Basili, V. R., Caldiera, G., & Rombach, D. (1994). The Goal Question Metric Approach.

Encyclopedia of Software Engineering , 2, 528-532.

Breslin, F. C., Tompa, E., Zhao, R., Pole, J. D., Amick III, B. C., Smith, P. M., et al. (2008). The Relationship between Job Tenure and Work Disability Absence among Adults: A Prospective Study. *Accident Analysis and Prevention, , 40* (1), 368-375.

Bureau of Labor Statistics. (2012, August 21). *Employment and Unemployment Among Youth Summary*. Retrieved September 3, 2012, from Bureau of Labor Statistics: http://www.bls.gov/news.release/youth.nr0.htm

Cekada, T. L. (2011). Need Training? Conducting an Effective Needs Assessment. *Professional Safety , 56* (12), 28-34.

Centers for Disease Control and Prevention (CDC). (2010). Occupational injuries and deaths among younger workers. *Morbidity and Mortality Weeekly Report , 59* (15), 449-455.

Christensen, K. (2009, March 1). *Los Angeles Times*. Retrieved September 3, 2012, from http://www.latimes.com/:http://articles.latimes.com/2009/mar/01/local/me-uclaburn1

Committee on Chemical Safety. (2012). *Creating Safety Cultures in Academic Institutions: A Report of the Safety Culture Task Force of the ACS Committee on Chemical Safety.* New York: American Chemical Society.

DiClemente, R. J., Hansen, W. B., & Ponton, L. E. (1996). *Handbook of Adolescent Health Risk Behavior.* New York: Plenum Press.

Fanning, F. E. (2011). Engaging Learners: Techniques to Make Training Stick. *Professional Safety , 56* (8), 42-48.

Goodman, R., Meltzer, H., & Bailey, V. (1998). The Strengths and Difficulties Questionnaire: a pilot study on the validity of the self-report version. *uropean child & adolescent psychiatry*, 125-130.

Health and Safety Services. (2014, August 28). *Safety Note 58 Permit to Work for Laboratories and Workshops.* Retrieved from University of Reading: https://www.reading.ac.uk/web/FILES/health-and-safety/SN58_Permit_to_work.pdf

Henderson, D., Rosenfeld, E., & Serna, D. (2012, April 13). *Yale Daily News*. Retrieved September 3, 2012, from www.yaledailynews.com: http://www.yaledailynews.com/news/2011/apr/13/student-dies-accident-sterling-chemistry-laborator/

Johnson, S. B., Blum, R. W., & Giedd, a. J. (2009). Adolescent maturity and the brain: the promise and pitfalls of neuroscience research in adolescent health policy. *Journal of Adolescent Health*, 216-221.

Kemsley, J. N. (2009, August 3). Learning From UCLA. *C&EN*, *87*(31), pp. 29-31, 33-34.

Laursen, E. K. (2009). Positive youth cultures and the developing brain. *Reclaiming Children and Youth, 18*(2), 8-11.

McCabe, B., Loughlin, C., Munteanu, R., Tucker, S., & Lam, A. (2008). Individual Safety and Health Outcomes in the Construction Industry . *Canadian Journal of Civil Engineering , 35* (12), 1455-1467.

National Research Council. (2011). *Prudent practices in the laboratory : handling and management of chemical hazards.* Washington, D.C.: National Academies Press.

Neal, A., Griffin, M. A., & Hart, P. M. (2000). The Impact of Organizational Climate on Safety Climate and Individual Behavior. *Safety Science , 34* (1–3), 99-109.

Robotham, G. (2001). Safety Training that Works. *Professional Safety , 46* (5), 33-37.

Salminen, S. (2004). Have Young Workers More Injuries than Older Ones? An International Literature Review. *Journal of Safety Research , 35* (5), 513-521.

Spector, P. E. (1994). Using self-report questionnaires in OB research: A comment on the use of a controversial method. *Journal of Organizational Behavior*, 385-392.

Steinberg, L., & Cauffman, E. (1996). Maturity of Judgment in Adolescence: Psychosocial Factors in Adolescent Decision Making. *Law and Human Behavior , 20*.

Student Design and Experiential Learning Center. (2014, March 30). *Student Design and Experiential Learning Center*. Retrieved from Missouri University of Science and Technology: http://design.mst.edu/

The Safety Zone by C&EN. (2014, August 27). Retrieved from C&EN (Chemical and Engineering News): http://cenblog.org/the-safety-zone/2011/09/explosion-at-the-university-of-maryland/

Thompson, R. C., Hilton, T. F., & Witt, L. A. (1998). Where the Safety Rubber Meets the Shop Floor: A Confirmatory Model of Management Influence on Workplace Safety. *Journal of Safety Research* , *29* (1), 15-24.

U.S. Chemical Safety and Hazard Investigation Board. (2010). *Texas Tech University Laboratory Explosion.* Washington, DC: CSB.

Whiles, A. (1999, September). Workplace Training The Learning Curve. 10. Australia: Occupational Health and Training Magazine.

Zuckerman, M. (1979). *Sensation Seeking: Beyond the Optimal Level of Arousal.* Hillsdale, NJ: Lawrence Erlbaum Associates.

Zuckerman, M. (1994). *Behavioral expressions and biosocial bases of sensation seeking. New York:*. New York, New York: Cambridge University Press.

V. BRIDGING THE HEALTH, SAFETY, AND ENVIRONMENT RISK MANAGEMENT PROFICIENCY GAP FOR FUTURE PETROLEUM ENGINEERS

Mohammad AlKazimi
Missouri University of Science and Technology
Ph.D. Student
Petroleum Engineering
Hanan Altabbakh
Missouri University of Science and Technology
Ph.D.
Engineering Management

Abstract

Health, Safety, and Environment Risk Management performance has become essential in the upstream industry due to the evolving complexity of the processes. In the recent years, accidents in the oil and gas industries resulted in catastrophic consequences as they captured the news and had an overwhelming impact to health, environment, financial, and social aspects of both the companies and their customers. Health, Safety and Environment Risk Management specialist and professionals play a major role in mitigating both risk and consequences of hazards as they assure the companies comply with different standards and perform best-recommended practices. Most of these professionals are engineers with different disciplines who have undergone intensive training courses by their employer as part of professional development programs. Subsequently, they continue their career path as HSE specialists once they successfully complete the program. Unfortunately, there is a gap where academia lacks the adequate educational knowledge base in Health, Safety and Environment Risk Management to establish the necessarily knowledge for potential candidates in that field. This paper

defines the establishment of “Health, Safety and Environment Risk Management in the Oil Industry” course in the Petroleum Engineering Department at Missouri University of Science and Technology. Not only it is designed to cover the technical aspects of HSE in the oil and gas industry, but it also enhances soft skills many students tend to overlook such as communications skills, safety awareness, ethical responsibilities, and most importantly, creating safety culture by exposing HSE awareness and knowledge to cater for the oil and gas industry. This course will be the corner stone for establishing a new petroleum engineering focus area where the department tries to expand it into a certificate program by collaborating with other departments on campus which offer different courses on a variety of topics related to HSE.

Introduction

The ongoing industrial evolution made processes more complex as organizations strive to integrate Environmental, Health and Safety Risk Management as part of their corporate responsibility to their staff (Health and Safety Executives, 2012). As a result, organizations find challenges, to continuously, manage HSE issues due to cost and duration as they become more liable for any failure that can endanger either their employees or the public welfare (Cheremisinoff & Cnaffia, 1995). The stakeholders in the oil and gas industry ranging from employees, governments, and communities, are closely monitoring the Health, Safety and Environment Risk Management performance as demand continues for "world-class performance and operational-excellence" (Beull, 2006). British Petroleum's Deepwater Horizon in the Gulf of Mexico was an example of both management and engineering failure. Hence, it was their responsibility to mitigate any hazardous failure and protect the human health and environment by adequately utilizing their knowledge and proficiency (Kavianian et al., 1993).

The demand for more HSE engineers to be part of the oil and gas industry is increasing. The expansion of the oil industry resulted in a scarcity of these engineers to overlook both the performance of process operations and potential risk management strategies. This paper defines the establishment of a new focus area in Health, Safety, and Environment Risk Management in the Petroleum Engineering Department at Missouri University of Science and Technology. The goal of the program is to meet the job market demand for engineers in that focus area in petroleum engineering. In addition, the availability of the program will enhance student's communications skills, safety awareness, ethical responsibilities, and most importantly, creating an improved safety culture by exposing different Health, Safety and Environment Risk Management awareness and knowledge specifically to cater for the oil and gas industry.

The Department of Petroleum Engineering at Missouri S&T approached different professional societies and concerned oil companies to construct a course that fits the industry's need for highly skilled and qualified petroleum engineers. The goals are assuring that the suggested curriculum topics meet the job market needs, meeting the required roles and responsibilities of the job description of potential candidates, and to fulfill both societal and legislative demands (Johnson, 2001).

The existence of a professional safety advocacy will introduce students to the importance of safety in the industry as it illustrates to them how it became an indispensable state of mind in numerous industries. Consequently, the new program will bridge the gap between both industry and academia by preparing a new breed of petroleum engineers who are aware of ethics, associated risks managements, decision consequences, and Health, Safety and Environment Risk Management related issues that can impact on operations.

Background

Accidents in the process industries can result in catastrophic consequences (Rodrigues & Simmons, 2012). In the previous years, they captured the news and resulted in an overwhelming impact to on the health, environmental, financial, and social aspects of both the companies and their customers. The ConocoPhillips' Bohai Bay in China's east coast, Pemex's spill in the Mexican Bay of Campeche, and China National Petroleum Corporation in Xingang Harbour are just a few examples of major accidents in the petroleum industry (Anderson & LaBelle, 1994). The most current accident was by BP's Deepwater Horizon, an offshore drilling rig in the Gulf of Mexico, which was performing drilling operations (Davies, 2010). The disaster was caused by a loss of control over the pressure in the well. This loss of control was followed by the failure of the well's blowout preventer; Blowout preventers (BOPs) are standard safety equipment on any offshore facility. BOPs are "engineering control system" (Fthenakis, 1993, p. 7) consisting of both a series of valves and hardened steel sheering surfaces to cut through the pipeline. The accident is considered the largest offshore oil spill in US history (Snow, 2010).

Once an organization syndicates different factors such as HSE proficiency, management systems and processes, developmental psychology, and technology, and then it is heading toward establishing an organizational culture (Beull, 2006). Thus, creating a strong HSE culture requires not only commitment, but also a continuous development, monitoring and improvement in all aspects as part of "HSE cultural maturity level." (Beull, 2006). Hence, the benefit of having this culture will result in a progressive impact on productivity where reducing workers injuries results in less downtime. It also diminishes incapacity expenses and the hidden overheads from lower employee self-esteem (Sandoe, 2012). The oil and gas industry is booming, yet, facing both a dearth of technical specialists and an aging workforce (Gould, *et al*., 2006). The need for more petroleum engineers with, HSE focus area is needed to compensate for the shortage in skilled technical workforce. Thus, as these engineers progress in their career, they embed awareness and safety culture with their acquired knowledge.

The role of HSE professionals

By recognizing hazards, HSE professional evaluate, develop recommendations for controlling, and advise members of the management team on means to mitigate the risk of hazards while adhering to regulations. HSE professionals can focus on different areas within their discipline, industrial hygienists, occupational safety, fire protection engineering, environmental safety, human factor engineers, construction safety, institutional safety management are few examples of the potential fields HSE professionals can focus on for future career (American Society of Safety Engineers, 2007). As a result, these specialties can enhance the work place safety by focusing on making it more user-friendly to workers' compensation, turnover, absenteeism, and other major cost optimization (MacLeod, 1994). Such professions requires an extensive knowledge in different Health, safety and environment codes along with risk assessment tools to identify and control hazards (Harms-Ringdahl, 2004).

Potential job market for HSE professionals

There are different sectors HSE engineers can engage in; public sectors and federal/state agencies benefit from their expertise especially in emergency response and crisis management teams. Research and technology institutions are another field to look into for a career. Chemical processing and oil gas companies have an escalating demand for HSE engineers due to the large magnitude of damage these industries can cause in case of an accident. The aviation and commercial aircraft industries demand for HSE engineers; airplane manufacturing process, luggage handling and other related aviation activities some of the tasks that needs to be addressed by HSE professionals. The level of complexity and operations in the nuclear power industry strongly benefit for the knowledge and expertise HSE professionals as they strive to prevent accidents and cater for a safe working environment.

The HSE profession was originated from the industrial engineering discipline. However, the HSE has grown tremendously from the 1980s to include several specialties that can enhance the working environment in a safe manner to optimize work performance (Health and Safety Executives, 2012).

HSE professionals' background

As the HSE profession developed over the decades to cover different industries, it become a multidisciplinary field requiring broad knowledge in areas such as the physical, chemical, biological and behavioral sciences, mathematics and engineering (Dembe, 1996). However, HSE professionals come from a wide variety of undergraduate and graduate degree programs, including biology, chemistry, management, psychology, occupational safety and health, and engineering. According to the American society of safety engineers, 34,000 members are safety professionals and approximately 1,250 of them are licensed professional engineers.

Approaching the Industry: The HSE education within the South Central region

Among the four University of Missouri System Campuses; Columbia, Kansas City, Saint Louis, and Rolla, none of them grant a degree in Health Safety and Environment to their students (ASSE, 2007). When looking at other colleges in Missouri, only Metropolitan Community Colleges in Kansas City, MO, offers an Associate in Applied Science (AAS), and not a Bachelor of Science, Environmental Health and Safety. Therefore, Missouri University of Science and Technology will establish a new path for its future students to enroll in a highly desired and sought discipline in various industries such as manufacturing, aviation, maritime, pharmaceutical and biotechnology. In addition, the discipline will create a diverse population within the university campus by attracting more female students seeking a degree in Industrial Hygiene, Occupational health, or Health Physics (Jennings, 2002)

Establishing HSE Curriculum

Students in the Petroleum Engineering program at Missouri University of Science and Technology undergo intensive courses in oil and gas drilling, production, reserves estimation, and the prediction of future production. Additionally, they study the technology of well logging, well testing, well stimulation, petroleum reservoir engineering, secondary and tertiary recovery and geology. In order to keep up with ongoing changes in the industry, a continuous evaluation of the curriculum takes place to stay competitive and up-to-date (Missouri University of Sciene and Technology, 2012). Conferences or symposia represent an excellent opportunity for faculty to hear from experts about the latest innovation in technology. Thus, the open forums in these gatherings are an excellent tool to evaluate the current curriculum to sustain the best practices from some of the leading oil companies.

The Petroleum Engineering department at Missouri University of Science and Technology noticed the importance of HSE in the oil and gas industry. Thus, the shortage in HSE specialist and professionals in the industry was seen as a perceived demand to take this program into consideration (Bihani, 2013). In a vision to bridge the gap between both academia and the oil and gas industry, the department approached different experts in the Health, Safety and Environment Risk Management in major oil companies and professional societies to assist in constructing an introductory course in that field. The goal of the course is to expose students to different essential topics related to Health, Safety and Environment Risk Management in the oil industry. Thus, provide the industry with new breed of engineers having safety culture imbedded within. As a result, the department established a new introductory course to be taught in 2014 academic year.

“Risk Management in the Oil Industry” is an introductory course that exposes petroleum engineering students to different technical aspects of HSE in the oil and gas industry. The overarching goals of the course are enhancing overlooked soft skills that most engineers lack according to a recent study conducted by Altabbakh and Grantham (2012). Communications skills, safety awareness, unconventional problem solving, and ethical responsibilities are some of the skills that the course will focus on. In addition, constructing a safety culture will be featured by exposing the students to HSE awareness topics and broadening their knowledge base to cater for the oil and gas industry (Altabbakh & Grantham, 2012). In order to reach these goals, a new curriculum containing the essential oil and gas HSE topics was developed, in collaboration with Health, Safety, and Environment Risk Management experts in the industry, to be presented to students. The course will cover different important aspects such working environment and safety. This topic will consist of containing, storing and transporting biohazardous materials. Thus, students will be aware of different occupational safety in terms of allowable exposure and threshold limits of noise, fumes, and other materials existing in the oil field facilities.

Moreover, personal safety is another concerned topic especially in hazardous and highly flammable areas. With the help of a certified Occupational Safety and Health Administrator (OSHA) expert, students will have hands on class on different personal protective equipment and how to use them accordingly in case of emergency. The human factors in executing tasks on site, working in heights, and confined space entry are some essential topics the students will learn in personal safety aspect of the course (Occupational Safety and Health Administrator, 2014).

Students will be exposed to a range of topics concerned with Process Safety. Assuring operations and process safety, evaluating potential risks, and implement the proper management of change are some of the topics concerned with assuring safe process operations. Thus, the students will acquire the different risk assessment tools and proper mitigation strategies to minimize resulting consequences. Best practices in work, adapted by professional societies' standards, are a recourse of assuring process safety which students will encounter.

In addition, the course will cover different managerial skills and corporate responsibilities. Engineering ethics and case studies in engagement with potential constituent and company's stakeholders will enhance students' soft skills. Thus, they will be able to provide justifiable resolutions to any type of conflict within an organization as they learned different negotiation skills and techniques in organizational leadership.

Thus, the course will satisfy HSE vocational qualifications (VQ's) by offering more practical learning experience to the student as they gain the necessary knowledge and skills in that area (Health and Safety Executive, 2009). Moreover, the students will have an advantage in applying their gained skills and knowledge where the industry needs it in quality assurance, risk assessment and mitigation, and management of change where standards and best practices are in continuous evaluation to keep up with human-system interaction technological advancement (Wiegmann & Shappell, 2012).

The topics offered in the this course will be the corner stone for establishing new HSE focus area in the petroleum engineering department . Thus, the department strives into expanding its potential with this initiative to offer a graduate certificate program in HSE. This broader goal can be achieved by collaborating with other departments on campus who offer different courses on variety of topics related to HSE.

There are several courses at Missouri University of Science and Technology that focus on Health, safety, and Environment Risk Management. Different Departments offer these courses, both on campus and via distance learning. The Department of Psychological Science offers a "Psych-315 Environmental Psychology" class where students learn about environmental attitudes, perception, cognition, environmental influences, crowding, and applying different environmental designs to working environments (Missouri University of Science and Technology, 2012).

Also the Civil, Architectural, and Environmental Engineering offer several classes related to Health, Safety, and Environment Risk Management. One of these classes is "CE-360 Environmental Law and Regulations" where the class exposes students to comprehensive coverage of federal and international environmental laws and regulations concerning smog and wastewater. Hence, the students will learn how the industry performs its operations within compliance protocols both domestically and internationally (Missouri University of Science and Technology, 2012). In addition, the department offers "Remediation of Contaminated Groundwater and Soil" class where the students study case studies in applied remediation technologies. Moreover, the issue of solid waste management and the methods used for their collection, reclamation, and ultimate disposal is the focus of "CE-363 Solid Waste Management." Both "CE 366: Indoor Air Pollution" and "CE 368: Air Pollution Control" introduce students to different applications to controlling emission from fossil fuels and various engineering analyses to minimize exposure to different types of pollutants (Missouri University of Science and Technology, 2012).

Additionally the Engineering Management and System Engineering Department offer courses that focus on reliability, risk analysis, and risk assessment. "EMGT-350 Risk Assessment and Reduction" explores techniques for systematically identifying hazards and estimating risk improve the safety performance and security of manufacturing facilities. "EMGT-381 Management and Methods in Reliability" provides students with basic concepts in reliability as they apply to the efficient operation of industrial systems. Accordingly, "EMGT-386 Safety Engineering Management" focuses on principles of safety engineering applied to the industry in different aspects. Job safety analysis, reduction of accident rates, protective equipment, safety rules and regulations, environmental hazards, health hazards, and ergonomic hazards are some of the topics addressed in this course.

When combining these courses with the current petroleum engineering courses, they become a foundation to form a new Health, Safety and Environment Risk Management engineering focus area the Petroleum engineering department. Students can take the assigned number of courses as part of science and technology elective courses which can be granted toward a minor in Health, Safety and Environment Risk Management while earning either undergraduate or graduate degree in petroleum engineering.

Conclusion

As the Petroleum industries become systematically more complex, the need for Health, Safety, and Environment specialists has become critical as part of the task force. The proposed launch of Health, Safety, and Environment focus area in the Petroleum Engineering Department at Missouri University of Science and Technology will boost the credentials of both the department and the university as pioneers in that in that field within the South Central region. In addition, students will be exposed to different HSE , as they will enhance their communications skills, safety awareness, ethical responsibilities, and most importantly, creating safety culture by exposing HSE awareness and knowledge to cater for the oil and gas industry.

The Petroleum Engineering Department at Missouri University of Science and Technology has approached major oil and gas companies, as well as experts in the HSE field, to sponsor the program while sharing their knowledge and expertise with the students to gain the utmost from this course. Collaborating with both the industry and safety experts will promote safety culture within young engineers and enhance awareness in decision making, especially when it comes to understanding potential consequences ad associated risks.

Acknowledgement

The author would like to express his deepest appreciation to all those who provided the possibility to establish, support, and guide us in this initiative. A special thanks go to Dr. Runar Nygaard, Dr. Katie Grantham, and Dr. Susan Murray at Missouri S&T. Additionally, Mr. Ala Abou-hamdan from Midlinx Consulting Inc., and Mrs. Laura Johnson, Recourse and Planning manager from ExxonMobil, for all the support and guidance.

References

Altabbakh, H., & Grantham, K. (2012). Towards Quantifying the Safety Cognition in the Undergraduate Engineering Student. *2013 Student Safety Innovation Challenge - ME Today.* Houston, Texas: ASME.

American Society of Safety Engineers. (2007). *Career Guide to the Safety Profession, Third Edition.* Des Plaines, IL: American Society of Safety Engineers Foundation.

Anderson, C. M., & LaBelle, R. P. (1994). Comparative occurrence rates for offshore oil spills. *Spill Science & Technology Bulletin* , 131-141.

Beull, R. S. (2006). Creating a culture to deliver sustainable HSE performance. *SPE international Coference on Health, Safety, and Environment in Oil and Gas Exploration Production* (pp. 1-8). Abu Dhabi, UAE: Society of Petroleum Engineers.

Bihani, R. (n.d.). Retrieved December 08, 2013, from Fleming Gulf: http://hse.fleminggulf.com/hse-energy-forum/skill-shortage--hse-forum-in-energy-2013--fleming-gulf.

Cheremisinoff, N. P., & Cnaffia, M. L. (1995). *Ehvironmental and health & safety management : a guide to comploance.* Park Ridge, New Jersey: Noyes Publications.

Davies, S. (2010). Deep Oil Dilemma. *Engineering & Technology* , 44-49.

Dembe, A. E. (1996). The Future of Safety and Health in Engineering Education. *Journal of Engineering Education* , 163-167.

Gould, L., Naha, M., Chlds, R., Nyati, P., Rew, I., Foster, R., *et al*. (2006). *Workforce Crisis in Upstream Oil & Gas Sector.* Houston, Texas: ASF Bauer College of Business, University of Houston.

Harms-Ringdahl, L. (2004). Relationships between accident investigations, risk analysis, and safety management. *Journal of Hazardous Materials* , 13-19.

Health and Safety Executive. (2009). *GUIDELINES FOR PIPELINE OPERATORS ON .* London: Health and Safety Executives Publications.

Health and Safety Executives. (2012). *Health and Safety Executives*. Retrieved November 18, 2012, from http://www.hse.gov.uk.

Jennings, M. B. (2002). *Enviremental health & safety engineering fundamentals.* San Jose, CA: San Jose State University.

Johnson, J. A. (2001). Principles of Effective Change: Curriculum Revision that Works . *The Journal of Research for Educational Leaders* , 5-18.

Kavianian, H. R., Meshkati, N., Wentz, C. A., & Rao, J. K. (1993). Should engineering schools address occupational and environmental safety and health issues? *Professional Safety;* , 48-49.

MacLeod, D. (1994). *The Ergonomics Edge: Improving Safety, Quality, and Productivity.* New York, New York: John Wiley & Sons, Inc.

Missouri University of Science and Technology. (2012). *Civil Engineering.* Retrieved January 08, 2014, from http://catalog.mst.edu/.

Missouri University of Science and Technology. (2012). *Psychology.* Retrieved January 08, 2014, from http://catalog.mst.edu/.

Missouri University of Sciene and Technology. (2012). *Petroleum Engineering* . Retrieved January 3, 2013, from : http://petroleum.mst.edu/.

MS&T. (n.d.). *Petroleum Engineering - program overview*. Retrieved January 3, 2013, from Missouri University of Science and Technology: http://petroleum.mst.edu/.

Occupational Safety and Health Administrator. (2014, January 08). *United States Department of Labor.* Retrieved January 08, 2014, from https://www.osha.gov.

Rodrigues, C. C., & Simmons, R. J. (2012). Development of an Engineering-based Master's Degree Program in HSE for the Petroleum Industry. *SPE Middle East Health, Safety, Security, and Environment Conference and Exhibition* (pp. 1-10). Abu Dhabi, UAE: Society of Petroleum Engineers.

Sandoe, E. (2012, Febuary 1). *How to build a strong safety culture*. Retrieved December 17, 2012, from Smart Business Network Inc: http://www.sbnonline.com.

Snow, N. (2010). National scientific academies criticize Macondo well procedures. *Oil & Gas Journal* , 18-21.

Venables, M. (2010, August 25). Analysis: Deepwater drilling in deep trouble. *Engineering & technology* , 14-15.

Wiegmann, D. A., & Shappell, S. A. (2012). *The human factors analysis and classification system.* Surrey, United Kingdom: Ashgate Publishing.

SECTION

2. CONCLUSION

The petroleum industry needs to reevaluate the current accident causation, risk assessment and mitigation strategies to prevent, or mitigate, major industrial accidents. The research focuses on investigating the validity of introducing different tools to address hazards and risks from different perspectives. Hence, when considering the current accident causation models, STAMP exceeds conventional accident causation methods by pinpointing the reasons of human performance and component failure and takes it to another level of investigation. The model goes beyond acknowledging these factors and adds organizational hierarchy, working practices, and the roles and responsibility of each staff member in the organization.

Due to the availability of organizational structure, industry standards, and industrial professional guidelines and best practices, STAMP was simple to apply in the oil industry case study above without the need for special analytical skills or expertise. Accordingly, each scenario was analyzed according to the corresponding industry standard or best practice to identify the safety violations resulted in the catastrophe.

Accordingly, the impact of accidents on different scales urged the petroleum industry to innovate new risk assessment tools to prevent future failure from occurring. Risk in Early Design (RED), a product risk assessment tool, was applied to identify different failure modes that might interrupt operation in the oil and gas industry, especially in the design phase. The tool successfully identified the failure modes for different historical major accidents as they impact the integrity of the selected component. The results of the RED analyses were verified by the corresponding official accident reports. Hence, the tool is a supporting tool and compliments other Process Hazard Analysis (PHA) tools currently used in the industry.

However, RED is advantageous in generating a list of prelude risk assessment based on cataloged historical product failure record. The proposed new method aspires in assisting both novice engineers and designers lacking the necessary experience. The tool provides preliminary risk assessments and potential failure mode identification leverages for electromechanical products based on archived knowledge of past failures. The archived knowledge used to generate the RED risk results is mathematically associated to product function. This relationship to product function provides designers the ability to project failures related to their product's function as early as the conceptual design stages and identify consequent mitigation strategies.

Consequently, Generated Risk Event Effect Neutralization (GREEN) proposes common mitigation strategies. These strategies can aid the end user to minimize the likelihood and/or consequence of the potential failure modes that can negatively impact process operations. GREEN analysis was utilized to examine potential risk mitigation strategies in the petroleum industry. The analysis successfully identified, via RED's analysis of potential failure modes, the possible strategies to control these failures. In addition, the GREEN analysis was successful in providing the most common mitigation strategies utilized to minimize the likelihood and consequences, accordingly.

The tool is advantageous in producing a list of prelude risk assessment based on cataloged historical product failure record, and their corresponding control strategies. Hence, the tool can assist novice engineers and decision makers in the upstream industry in recognizing potential failure modes in the process system and how to, accurately, mitigate their likelihood and consequence especially in the design conceptual design stages.

Table 1 compares the currently used risk assessment and mitigation strategy selection tools in the petroleum industry with the tools addressed in this research. Hence, the end user is able to compare and contrast each tool to fit his/her need when assessing potential risks and hazards in the facility, especially in the design phase.

Table 1. Risk assessment tools comparison

Technique	Advantages	Limitation
Fault Tree Analysis (FTA)	– Depicts the cause and effect relationship between the root cause events – Qualitative and quantitative results – Focuses on single failure at a time	– Difficult to failures related to human behavior – Time consuming and lengthy – Latent hazards are not addressed – Requires an expert to identify potential risks
Failure Mode and Effect Analysis (FMEA)	– Efficient when applied to overall system – Structured and detailed approach – Prioritizes product/process deficiencies – Identifies and eliminates potential failure modes early in the development phases approximation	– Difficulty to construct with multiple components – Only considers hazards arising from single point failure modes rather than combinations of failures – Relies on people with detailed system knowledge. – Does not recognize failures due to operations. – Time consuming and lengthy – Expensive – Does not consider human relater failures
Bow Tie Analysis	– Graphical representation to various systems – Clear links between management systems and safety are shown	– Lengthy and complicated; especially for complex systems – Cannot identify how effective safeguard is – Need of user can oversee potential risks – Organizational procedures cannot be incorporated
Layers of Protection Analysis (LOPA)	Identifies risks encountered in the entire system, broader approach - Easy to apply and very effective in exposing systemic problems - Accounts for human error - Semi quantitative - Takes less time to evaluate complex systems qualitatively	– The quantified output is an approximation - Requires experience in approximation of risk numbers excessive for simple or low-risk decisions – Relatively slow progress compared to other methods – Not so easy to perform as a team exercise – Time consuming – Not so visual.

Table 1. Risk assessment tools comparison (cont.)

Hazard and Operability Analysis (HAZOP)	– The team approach to a HAZOP makes it a multidisciplinary study – Systematic and rigorous. – Involves interaction of views from multidisciplinary experts. – Can be applied to a wide range of types of system. – Creates a detailed and auditable record of the hazards identification process	– Requires a considerable amount of preparation. – Can rely heavily on the skills of the HAZOP Chairman – Can be time consuming and therefore expensive. – Can inhibit imaginative thinking and so certain kinds of hazards – No means to assess hazards involving interactions between different parts of a system or process – No risk ranking or prioritization capability – No means to evaluate effectiveness of current proposed safeguard – May need to interface HAZOP with other risk management tools
Risk in Early Design (RED)	– Utilizes historical knowledgebase to produce potential risks – Well-suited for novice engineers – Identifies risk in the early design phase – User friendly – Graphical illustration	– Potential risk may be over or under quantified – Does not account for human error
Generated Risk Event Effect Neutralization (GREEN)	– Wide spectrum of mitigation strategies for single failure mode – Ease of strategy selection based on likelihood/consequence reduction calculations	– user interface needs to be improved – No link to RED's failure mode identification – Cataloged data needs periodic update – Implementing human-system interaction

Table 1. Risk assessment tools comparison (cont.)

System Theoretic Accident Model and Processes (STAMP)	– Pinpointing the reasons at human performance and component failure – Adds organizational hierarchy, working practices, and the roles and responsibility of each staff member – Simple to apply – No need for special analytical skills or expertise – Identifies the violations against the existence safety constraints – More focused on enforcing safety constraints behavior in systems rather than preventing failures. – Accidents are viewed as a result of inadequate safety control – Assist in recognizing scenarios, inadequate controls, the dysfunctional interaction, and the incorrect process models	– Must have access organization's hierarchy, Policies, standards, and regulations. – Roles and responsibilities of each staff members not always available – Organization flow of communication flow not documented

On the other hand, investing in human capital is another tool to mitigate potential human errors and to be fully incorporated with design parameters since human-system interaction is part of the petroleum industry. In order to establish such investment, the first step to bench mark the current knowledge base and safety attitude in students. Hence, the analyses of the survey results show that science students in college workshops and laboratories receive informal safety training prior to either participating in laboratory experiments or design teams' machine shops. The outcome of this is often ineffective, where accidents in university laboratories or machine shops still occur. This is an indication that these types of training sessions do not always assure positive safety attitude or safety performance. As a result, the frequent neglect of minimum safety requirements in machine shops or laboratories can result in avoidable accidents and losses. In addition, the survey showed that the young engineers' knowledge of five domains of the OSHA guidelines: PPE, lockout/tagout, MSDS, machine guarding, and emergency action plan was insufficient. Lack of knowledge in these minimum essential domains can cause undesired consequences when accidents occur and the students fail to adhere to the proper safety guidelines. Consequently, the lack of overall safety attitude is reflected in their attitude toward risk associated with their shop projects and class assignments. Hence, the students underestimate the potential consequences when positive safety attitude is not part of their work ethic behavior to execute assigned tasks safely. Therefore, adequate training provided with skilled professionals shall enhance the implementation of safety culture; an essential to implement such culture for novice engineers in their college education.

In addition, implementing an effective safety culture is essential to protect employees as well as enhancing the students' safety awareness. Students need to be able to identify hazards, assess the risk associated with them, and respond to an emergency situation if the occur. Therefore, The proposed launch of Health, Safety, and Environment focus area in the Petroleum Engineering Department at Missouri University of Science and Technology will boost the credentials of both the department and the university as pioneers in that in that field within the South Central region. Students will be exposed to different HSE topics, besides enhancing their communications skills, safety awareness, ethical responsibilities, and most importantly, creating safety culture by exposing HSE awareness and knowledge to cater for the oil and gas industry. Collaborating with experts in the HSE field, to sponsor the program while sharing their knowledge and expertise with the students to gain the utmost from this course will promote safety culture within young engineers. Moreover, enhance awareness in decision making, especially when it comes to understanding potential consequences ad associated risks.

Currently, the petroleum industry is incorporating Enterprise Risk Management (ERM) system in as part of its integral corporate governance to mitigate different aspects of risk and to achieve targeted objectives. The system look into different aspects of risks in terms of operational, financial, compliance, and governance. Hence, encompassing such trend within corporate strategic plan to ensure potential risks are reduced accordingly. In addition, implementing an asset integrity management system to assure the mechanical/electrical integrity of equipment is necessary to mitigate potential failures.

On the overhand, the human aspect of operational safety is essential when designing any system. Hence, combining all these risk assessment tools and investing in the human capital is the aim of bridging potential gaps between academia and the industry. Hence, the petroleum industry would benefit from a new breed of engineer and scientist with safety culture and awareness ingrained in them. Today's young engineers are future decision makers and managers. Therefore, creating a safety-awareness environment, and exposing them to real accident case studies, will impact their thinking process toward decision-making and risk management. Training them in college can shape their safety attitude positively and influence organizational culture as they are promoted in the professional ladder. As a result, their decision paradigm shall be more tailored toward possible consequences that can affect operations. Thus, their commitment towards safety have the potentials to make a great impact creating a safer working environment for the operating facility's surrounding community, workforce and stakeholders, respectively.

VITA

Dr. Mohammad Abdulhameed AlKazimi is a Senior Reliability and Equipment Support Engineer at Kuwait Oil Company in Kuwait. He holds a bachelor degree in mechanical engineering (1998) and a masters degree in Industrial Engineering (1999); both earned at the University of Toledo in Ohio. As part of professional development program by the oil sector in Kuwait, he was one of the first of employees to be selected to peruse his higher degree. He joined the petroleum engineering program in 2009 where he started his PhD program with focus area in risk assessment and mitigation in the petroleum industry. During his course of studies, he earned his masters degree in petroleum engineering (2011) along with certificated in Safety Engineering, Leadership in Engineering Organizations, and Project Management, respectively.

He held several leadership positions as the president of The Council of Graduate Students at Missouri S&T (2012-2013) and the International Students Concerns Committee (ISCC) Chair for the National Association of Graduate and professional Students (NAGPS) (2013-2014). In addition, he served by representing the graduate student body at Missouri S&T as board and committee member, respectively.

In addition, Dr. AlKazimi is a member of multiple professional societies, including but not limited to, Pi Epsilon Tau (the national petroleum engineering honor society), Alpha Epsilon Lambda (the national honor society for graduate and professional school students), American Society of Mechanical Engineers (ASME), Society of Petroleum Engineers (SPE), American Society for Engineering Education (ASEE), American Society of Engineering Management (ASEM), American Society of Safety Engineers (ASSE), Institute *of* Industrial Engineers (IIE), and Kuwait Society of Engineers, respectively.