Fall 2013

Risk analysis: comparative study of various techniques

Hanan Mohammad Altabbakh

RISK ANALYSIS: COMPARATIVE STUDY OF VARIOUS TECHNIQUES

by

HANAN MOHAMMAD ALTABBAKH

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

ENGINEERING MANAGEMENT

2013

Approved by

Susan Murray, Advisor
Katie Grantham
Steven Corns
Hong Sheng
Nick Lockwood

PUBLICATION DISSERTATION OPTION

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

1. Pages 4 to 23 "Applying the Swiss Cheese Model of Accident Causation." Is in the style required by the Annual International Conference of the American Society for Engineering Management. The citation is: Altabbakh, Hanan, and Susan L. Murray, "Applying The Swiss Cheese Model of Accident Causation", *Annual International Conference of the American Society for Engineering Management*, Curran Associates, Inc. (October 2011), pp. 301-307.
2. Pages 24 to 62 "Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster." Is in the style required by Engineering Management Journal. The citation is: Hanan Altabbakh, Susan Murray, Katie Grantham, and Siddharth Damle, "Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster." *Engineering Management Journal*, 25:2 (June 2013), pp. 13-24.
3. Pages 63 to 99 "STAMP - Holistic System Safety Approach or Just Another Risk Model?" Is in the style required by Journal of Loss Prevention in Process Industries. It has been submitted and is under review.
4. Pages 100 to 110 "Toward Quantifying the Safety Cognition in the Undergraduate Engineering Student." Is in the style required by American Society of Mechanical Engineers.

ABSTRACT

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 being faced that needed to be assessed and addressed. Managers and engineers face the challenge to choose from the vast amount of techniques available and utilize the correct one. Indeed, new or improved risk assessment tools that can address these complexities are needed.

One of the most important steps in assessing risk is first to categorize it. There are risks associated with product component failure, human error, operational failure, environmental disasters, etc. So far, however, there has been little discussion about how do managers choose between the available risk assessments tools, which this considered the first step in risk analysis. In this research, risk assessment tools have been investigated, analyzed, categorized, and then applied to case studies in different industries. A pathway for researchers has been paved to overcome the difficulties in choosing risk assessment tools.

ACKNOWLEDGMENTS

I would like to express the sincere gratitude to my committee Advisor, Dr. Susan Murray, for her contentious support, trust, and persuasion to achieve my goal. She contributed an inordinate amount of time structuring this project. Her excellent editing skills, knowledge, patience, and sense of humor were irreplaceable.

Special thanks to Dr. Grantham, who served as a significant resource and was of marvelous support and I thank her for all her effort on my behalf. In addition, I would like to thank Dr. Steven Corns, Dr. Hong Sheng and Dr. Nick Lockwood, for serving as committee members for their direction, dedication and invaluable contribution for this project.

I am especially thankful to my beloved husband, Mohammad AlKazimi, for standing by me in times of need and his love and support to persuade my goal. My children (Malak, Abdullah, and Jana) for understanding, patience, and nonstop love and care as they were my ultimate reason to earn my degree. Also, I can't forget my mother who always kept me in her prayers and surrounded me with her never ending love and encouragement.

Also, I would like to extend my gratitude to my friends and colleagues for standing by me in times of need and their motivation to reach my goal.

TABLE OF CONTENTS

Page

PUBLICATION DISSERTATION OPTION iii

ABSTRACT iv

ACKNOWLEDGMENTS v

LIST OF ILLUSTRATIONS x

LIST OF TABLES xi

SECTION

1. INTRODUCTION 1

PAPER

I. APPLYING THE SWISS CHEESE MODEL OF ACCIDENT CAUSATION 4

Abstract 4

Introduction 5

Background 5

The Swiss Cheese Model in Aviation 8

The Swiss Cheese Model in Medicine Management and Health Care 10

The Swiss Cheese Model in Engineering Management Perspective 12

The Space Shuttle Challenger Incident 13

Unsafe Acts 13

Psychological Precursors of Unsafe Acts 14

Line Management Deficiencies 14

Fallible Decisions 15

Summary of The Space Shuttle Challenger Incident 16

The Exxon Valdez Oil Spill Incident 16

Unsafe Acts 17

Psychological Precursors of Unsafe Acts 18

Line Management Deficiencies 19

Fallible Decisions 19

Summary of The Exxon Valdez Oil Spill Incident 20

Conclusion 21
References 22
II. VARIATIONS IN RISK MANAGEMENT MODELS: A COMPARATIVE STUDY OF THE SPACE SHUTTLE CHALLENGER DISASTER 24
Abstract 24
Introduction to Risk Assessment 25
Space Shuttle Challenger Disaster 27
Types of Risk Assessment Tools 30
Product-Based Risk Assessment Tools 30
Failure Mode and Effects Analysis 31
Fault Tree Analysis 32
Risk in Early Design 34
Using RED to Analyze the Space Shuttle Challenger Disaster 34
Product-Based Risk Assessment Tool Summary 37
Process-Based Risk Assessment Tools 37
Layer of Protection Analysis 38
Using LOPA to Analyze the Space Shuttle Challenger Disaster 40
Human Factors Analysis and Classification System and the Swiss Cheese Model 45
Using the Swiss Cheese Model to Analyze the Space Shuttle Challenger Disaster 49
Productive Activities 50
Preconditions 50
Line Management 51
Decision Makers 51
Process-Based Risk Assessment Tool Summary 53
Conclusion 54
References 59
III. STAMP – HOLISTIC SYSTEM SAFETY APPROACH OR JUST ANOTHER RISK MODEL? 63

Abstract 63
1. Introduction 64
2. Hazard Analysis 64
2.1 Failure Mode and Effects Analysis 66
2.2 Fault Tree Analysis 66
2.3 Event Tree Analysis 67
2.4 Hazard and Operability Analysis 67
3. System Theoretic Accident Model and Processes - Introduction 68
3.1 STAMP Analysis 71
4. Applying STAMP to an accident in the Oil and Gas Industry 76
4.1 The Accident 77
4.2 Proximity of events: 79
4.3 Hierarchical Control Structure 80
Pipeline Mechanical Integrity 81
Assistant Facility Operators 82
Facility (B) Operator 83
Facility (B) Supervisor 83
Senior Maintenance Engineer 84
Maintenance Engineers: 85
Foremen 86
Operations and Maintenance Manager 87
5. Recommendation 88
6. Conclusion 91
References 93
IV. TOWARDS QUANTIFYING THE SAFETY COGNITION IN THE UNDERGRADUATE ENGINEERING STUDENT 100
ABSTRACT 100
INTRODUCTION 101
LITERATURE REVIEW 102
METHODOLOGY 103

RESULTS AND ANALYSIS 105
Goal one: Evaluate the amount of safety training of Missouri S&T design team members 106
Goal two: Evaluate the student design team members' safety knowledge . 106
Goal three: Evaluate the student design team members' safety attitude 106
Goal four: Evaluate the student design team members' safety consciousness 106
CONCLUSION 107
REFERENCES 109
SECTION
2. CONCLUSION 111
VITA 114

LIST OF ILLUSTRATIONS

Page

Paper 1

Exhibit 1. The Swiss Cheese Model 7
Exhibit 2. First Version of The Swiss Cheese Model 8
Exhibit 3. The Swiss Cheese Model in Aviation 8
Exhibit 4. The Swiss Cheese Model of Error in Medicine Management 11
Exhibit 5. Generic Organizational Accident Model Applied to Health Care System 12

Paper 2

Exhibit 1: The Consequences Classification System 32
Exhibit 2: RED Results for SRB Analysis 36
Exhibit 3: Examples from the detailed RED report 36
Exhibit 4: Protection Layers 39
Exhibit 5: LOPA Model for Challenger Disaster 41
Exhibit 6: Layer Definitions and Flow 42
Exhibit 7: Adapted from Reason's Swiss Cheese Model 47
Exhibit 8: The HFACS framework 49
Exhibit 9: Summary of Risk Assessment Tools 57

Paper 3

Figure 1: Classification of Control Flaws Leading to Hazards 73
Figure 2: Classification of Control Flaws Leading to Hazards 74
Figure 3: Accident Causal Factor of Provincial Governments - the Walkerton Water Contamination Accident 75
Figure 4: Layout of crude oil processing facilities (A) and (B) 77
Figure 5: Oil leak and in Facility (B) 77
Figure 6: Hierarchical Level Control Structure of Company XYZ 81

LIST OF TABLES

Page

Paper 4

Table 1 The Goal Question Metric Survey Model 104

1. INTRODUCTION

It is amazing how our world is advancing everyday with more technologies and inventions. The advancement in technologies merged with different industries. For example, the medical field utilizes nano technology to perform complex procedures. The communication had its share of success where the Internet bridged the gap as information is transferred in fractions of a second from one location to another. Software became more complex in solving mathematical models, and it is used in sophisticated manufacturing processes as well. In fact, these technologies became more interrelated to introduce new products and services to mankind. However, such progress introduced new types of challenges due to the complexity of both organizations and processes. As a result, new types of risks need to be identified. Risk is "a characteristic of a situation or action wherein two or more outcomes are possible, the particular outcome that will occur is unknown, and at least one of the possibilities is undesired" (Covello and Merkhofer, 1993). The technologies with its advancement have become so complex that these new risks need new risk assessment tools.

"Risk assessment is the process of identification, evaluation, acceptance, aversion, and management of risk" (Eccleston, 2011). Researchers faced the challenge to develop new risk assessment techniques to overcome the shortage in the conventional ones available. Managers and engineers face the challenge to choose from the vast amount of techniques available and utilize the correct one. One of the most important steps in assessing risk is first to categorize it. There are risks associated with product component failure, human error, operational failure, environmental disasters, etc. So far, however,

there has been little discussion about how do managers choose between the available risk assessments tools, which this considered the first step in risk analysis. One of the most significant questions that will arise when assessing risk is, which tool should be used in this scenario? In this research, risk assessment tools have been investigated, analyzed, categorized and then applied to case studies in the aviation and oil and gas industry. A pathway for researchers has been paved to overcome the difficulties in choosing risk assessment tools.

The overall structure of the dissertation takes the form of six sections, including this introductory section. Section two begins by a conference paper that was presented and published at the Annual International Conference of the American Society for Engineering Management 2011, "Applying the Swiss Cheese Model of Accident Causation." The paper introduces the Swiss Cheese Model of accident causation, which was developed by James Reason, explores it, and applies it to two case studied to test its applicability and validity. The third section is a journal article that was published in the Engineering Management Journal Special Issue –Risk Analysis June 2013, "Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster." The article is addresses more risk assessment tools such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Risk in Early Design (RED), Layer of Protection analysis (LOPA), and Swiss Cheese Model of Accident Causation.

It identifies the advantages, limitations and applicability of each tool and utilizes the Space Shuttle Challenger as a case study. Section four presents a journal article that was submitted and is under review in the Journal of Loss Prevention in Process Industries**,** "STAMP - Holistic System Safety Approach or Just Another Risk Model?"

The article introduces a relatively new risk assessment model that has not been evaluated in the literature. Moreover, the article identifies the advantages and disadvantages of the model and applies it to a case study in the oil and gas industry to validate its applicability.

Section five is an article that won first place in the 2012 Student Safety Innovation Challenge for the American Society of Mechanical Engineer's Safety Engineering and Risk Analysis Division (SERAD), "Toward Quantifying the Safety Cognition in the Undergraduate Engineering Student." This article analyzes a survey that conducted to measure the Safety knowledge and attitude of young engineering students in an effort to improve safety and prevent accidents in labs and workshops. Finally, in section six, the conclusion provides a brief summary and critique of the findings.

PAPER

I. APPLYING THE SWISS CHEESE MODEL OF ACCIDENT CAUSATION

Hanan Altabbakh

Susan Murray, Ph.D.

Missouri S&T

Abstract

This paper shows how utilizing the Swiss Cheese Model of accident causation can aid engineering managers in understanding how errors might occur and how they can be prevented. Human error is an issue of concern for every system. Engineering managers need a structured approach to identify system gaps that fail to address potential human errors. The model considers different levels of human error including unsafe acts, preconditions for unsafe acts, unsafe supervision, and organizational influences.

Examples of past incidents including the Space Shuttle Challenger and the Exxon Valdez oil spill that resulted in catastrophic outcomes will be analyzed using the Swiss Cheese Model to identify potential hazards, safeguards, and shortcomings that resulted in loss of human lives, financial ruin, environmental damages and other impacts.

Introduction

The Swiss Cheese Model has been used for different types of accidents; it has most commonly been adopted in health care and aviation safety. In this paper we will compare how each of these industries define their perspectives of the Swiss Cheese Model. Furthermore, we will explore a new model for industrial application from an engineering management perspective. First we will define the model and proceed with examples from aviation and health care. Then we will introduce the new sequenced defensive layers for our examples the Space Shuttle Challenger and the Exxon Valdez oil spill incidents. The Space Shuttle Challenger disaster demonstrated a valuable example of human error and incorrect decision-making at an organizational level. The Exxon Valdez oil spill incident shows different prospective of error causation, where all levels of the organization contributed to the incident, including the crewmembers in direct contact with the system.

Background

The Swiss Cheese Model was developed by James Reason to address accidents in complex systems where many components interact with each other. Reason (2008), presented multiple human error accident examples in aviation systems, which include component aircrafts, runways, control towers, communication tools and equipment, luggage transport and handling systems. These components interact with each other to form a complex system, which function as a whole. Moreover, each component works independently by rules and policies set as a single system and interacts with other components to function as part of a whole system following different additive rules and

policies. Considering the variety of components, policies, rules and environments, these systems are complex, which makes it harder for analysts to assess risk mitigation, human potential error, and accident prevention. Many of the current risk assessment tools do not go far enough. Some of them only identify technical aspects of the adverse event, pointing the finger toward the operator's actions without tracing back to the origin of the accident and its circumstances.

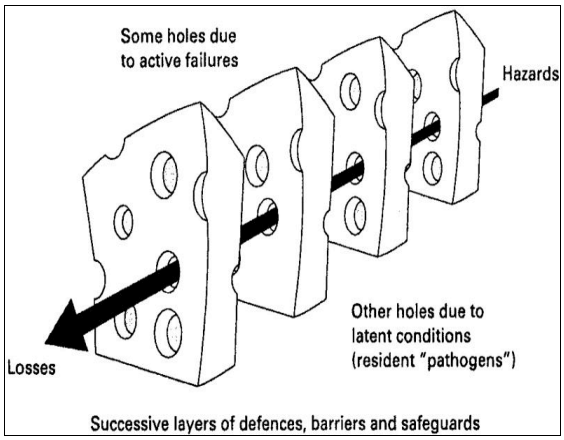
The Swiss Cheese Model was proposed to overcome such dilemma by introducing a model that tracks accident causation in different levels of the organization without blaming individuals. "We cannot change the human condition, we can change the conditions under which humans work" (Reason, 2000).

James Reason presented his model as stacked slices of Swiss cheese, where the slices represent the defenses and safeguards of the system and the holes represent *active failures* (i.e. unsafe acts) and *latent conditions*. Unsafe acts occur when a human is in direct contact with the system such as during the Chernobyl accident where the operator wrongly violated the plant procedures and switched off successive safety system. On the other hand, latent condition can occur at any level of the organization or any system and it is harder to detect such as lack of training, poor design, and inadequate supervision, unnoticed defects in manufacturing (Reason, 1997). Latent conditions considered the source of ignition of any accident or error (Reason, 2000).

The holes in the model are not static. They move from one position to another, may open or close, and change in size continuously depending on the situation and the climate of the system. According to Sidney Dekker (2002), it is the investigator's job to find out the position, type, source, and size of each hole and identify the cause of these

changes. Finally, the investigator must determine how the holes line up to produce accidents since all holes must align through all the defensive layers for the trajectory to pass through and cause the adverse event as shown in Exhibit 1.

Exhibit 1. The Swiss Cheese Model

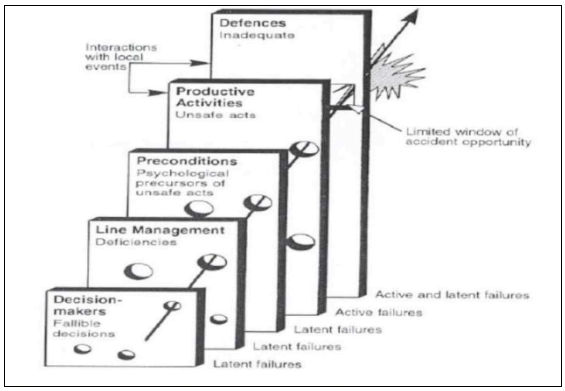


In contrary to the latest version where the layers are not specified, Exhibit 2 shows the previous version of the model, where it consisted of five layers as follows:

- Fallible decisions
- Line management deficiencies
- Psychological precursors of unsafe acts
- Unsafe acts
- Inadequate defenses

The current version is not limited to certain numbers of defensive layers nor have they been labeled or specified. Thus, a variety of layers of defenses and safeguards can be adapted to this model from different organizational environments depending on the amount of risk involved.

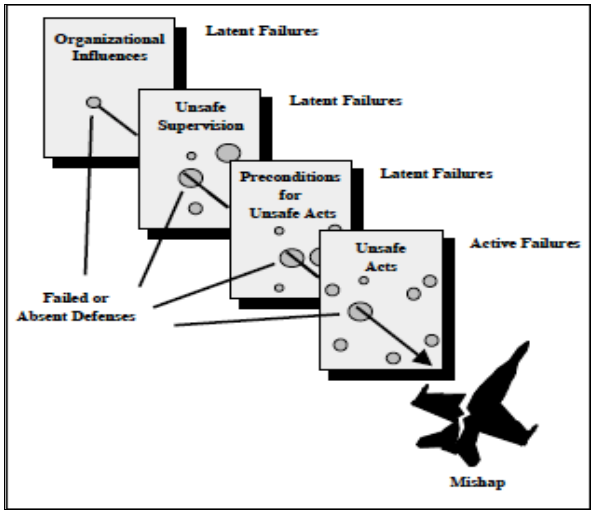
Exhibit 2. First Version of The Swiss Cheese Model



The Swiss Cheese Model in Aviation

Wiegmann and Shappell (2003) conducted a study to identify the holes and safeguards of the aviation system. They were able to precisely target each defensive layer and classify its holes (i.e. unsafe acts and latent conditions). They categorize the layers into four levels of human failure where each layer influenced the succeeding one as shown in Exhibit 3.

Exhibit 3. The Swiss Cheese Model in Aviation



Each of the following bullets represents a defensive layer in the model:

- Unsafe acts
    - Errors
        - Decision
        - Skill-based
        - Perceptual
    - Violations
        - Routine
        - Exceptional
- Preconditions for unsafe acts
    - Substandard conditions for operators
        - Adverse mental states
        - Adverse physiological states
        - Physical/mental limitations
    - Substandard practices of operators
        - Crew resource mismanagement
        - Personal readiness
- Unsafe supervision
    - Inadequate supervision
    - Planned inappropriate operations
    - Failed to correct problem
    - Supervisory violations
- Organizational influences

- Recourse management
- Organizational climate
- Organizational process

Under each bullet, they identified whether the corresponding potential error was an active or a latent failure.

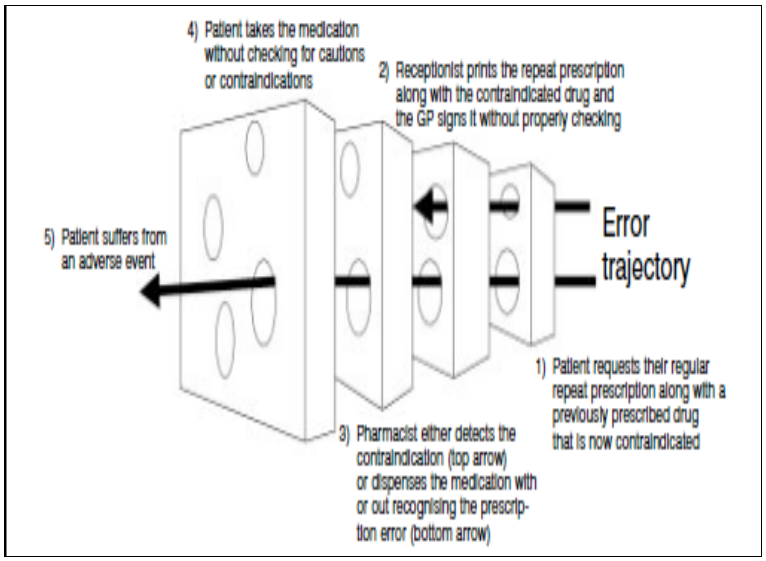
The application of the Swiss Cheese Model for aviation was successful to an extent. Several modifications were made to the original model to make it specific to aviation. Over 300 naval aviation accidents were assessed to identify the holes and defensive layers that are specific to the aviation industry. The Swiss Cheese Model for Aviation cannot be applied successfully to other industries because of its specificity.

According to (Reason, et al., 2006, 9) "The model was intended to be a generic tool that could be used in any well defended domain—it is for the local investigators to supply the local details".

The Swiss Cheese Model in Medicine Management and Health Care

Avery et al. (2002) adapted the Swiss Cheese Model for management of medicine. Errors in the process of medicine management are considered an important cause of induced harm in health care. For example, a patient suffered an adverse event after using a previously prescribed medicine without considering its current contraindications with his/her developing health situation. The slices of cheese, (i.e. the defensive layers), were introduced and both active failures and latent conditions were classified. The following model shown in Exhibit 4 was then generalized to be used in primary care risk management.

Exhibit 4. The Swiss Cheese Model of Error in Medicine Management



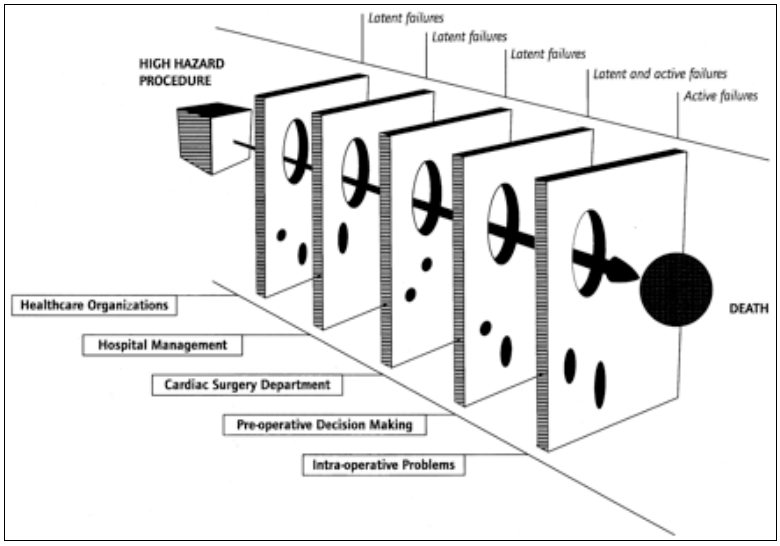
Other representations of the model were adapted for use in health care institutions and hospitals. Carthey et al. (2001) demonstrated the use of this model for determining cardiac surgery accident causation as shown in Exhibit 5.

They classified the defensive layers into five categories:

- Health care organization
- Hospital management
- Cardiac surgery department
- Preoperative decision making
- Intraoperative problems

In their paper, they illustrated some examples of the active failures and latent conditions in relation to each defensive layer and safeguard.

Exhibit 5. Generic Organizational Accident Model Applied to Health Care System (Carthey et al., 2001)



In the previous applications, the investigators discussed brief examples of the latent conditions and active failures without identifying the location of holes and their sizes. In contrast to the aviation model, which can be generalized to the whole aviation industry, the previous health care models were limited to each specific branch of the health care industry; models for medicine management would not apply to cardiac surgery and vice versa.

The Swiss Cheese Model in Engineering Management Perspective

For the rest of this paper, we will illustrate how to classify and adapt the Swiss Cheese Model into engineering management applications.

The Space Shuttle Challenger Incident

In 1986 the Space Shuttle Challenger, exploded 74 seconds after launch killing seven astronauts including the teacher in space. Technically, the main cause of the disaster was the O-ring designs. According to the presidential commission report (1986), the cause of the accident was the failure, due to improper design, of the pressure seal in the aft field joint of the right solid rocket booster. Top management, line managers, engineers, companies, and the organizational climate contributed to the disaster. We will examine the Challenger and classify the errors made according Reason's Swiss Cheese Model (1990).

Unsafe Acts

Errors in the launch of the Space Shuttle Challenger were unintentional. Blame cannot be attributed to a pilot, crewmember, operator, or controller. The incident was due to poor decision-making at the upper management level, which constitutes an unsafe act under the decision error type (Orasanu, 1993). The commander and pilot flying the shuttle are considered the direct operators, but in the Challenger disaster it was not their choice whether or not to launch; it was the decision maker's. Therefore, the *unsafe act* defensive layer might not be applicable in the case of the Challenger, thus this layer would be removed from the model. However, according to the Swiss Cheese Model, it takes both active failure and latent condition to cause an accident, so removing an essential layer might invalidate the model.

Psychological Precursors of Unsafe Acts

The weather on the day of the launch was threatening, thus introducing latent failure. For a successful reseal of the O-ring, the environmental temperature should be ≥ 53°F. According to Thiokol, low temperature would jeopardize the capability of the secondary sealing of the Solid Rocket Motor (Kerzner, 2009). Communicating that issue was complicated by the fact that engineers use technical jargon that is not always understood by upper management. Moreover, the ice on the launch pad introduced additional risk factors to the launch operation. The ice also covered the handrails and walkways surrounding the shuttle, which presented hindrances to emergency access. In addition, availability of spare parts, physical dimension, material characteristics, and effects of reusability were other factors that may have contributed to the disaster.

Line Management Deficiencies

Line management did not adequately enforce a safety program (Kerzner, 2009). As a result, all risks were treated as anomaly and that became the norm in the NASA culture. An escape system during launch was not designed due to overconfidence in the reliability of the space shuttle and that having a plan would be cost effective. A latent failure introduced an unsafe act which violated the most important factor; the safety of the crew. Pressure to launch on the designated schedule due to competition, politics, media, and congress issues made it hard for line managers to communicate the engineers concerns and reports to top decision makers and administrators. Problems that were discussed internally at Thiokol and NASA were not adequately communicated between

the two organizations due to lack of problem reporting procedures. The lack of communication introduced a latent failure.

Fallible Decisions

Budget was a major constraint at NASA at that time. Consequently, top management at NASA approved the design of the solid rocket motor in its entirety, including the O-ring joint, even when this meant changing the research direction at a great cost. Risk was accepted at all levels since calculated safety projections were favorable. A NASA position for permanent administrator was empty for four months prior to the accident, and turnover rate of upper management was considerably high, which resulted in a breakdown in communication from the top down. Moreover, lack of communication between NASA's top decision makers and Thiokol's technical engineers introduced a gap where problem reporting remained in house. Concerns never reached top officials in NASA for fear of job loss. Moreover, bad news was generally downplayed to protect the interests of higher officials. In general, there was no accepted standard for problem reporting that transected all levels of either NASA or Thiokol.

There was no clear recommendation from Thiokol not to launch under the cold weather condition (Kerzner, 2009). According to (The Presidential Commission on the Space Shuttle Challenger Accident Report 1986, 82) regarding the launch decision, "Those who made that decision were unaware of the recent history of problems concerning the O-rings and the joint and were unaware of the initial written recommendation of the contractor advising against the launch at temperatures below 53 degrees Fahrenheit and the continuing opposition of the engineers at Thiokol after the

management reversed its position. They did not have a clear understanding of Rockwell's concern that it was not safe to launch because of ice on the pad. If the decision makers had known all of the facts, it is highly unlikely that they would have decided to launch 51-L on January 28, 1986". The general lack of communication both between NASA and Thiokol, and internally within each organization, functions as a latent condition.

Summary of The Space Shuttle Challenger Incident

The Space Shuttle Challenger's holes were not identified in sufficient time for safeguards to be implemented to prevent such catastrophic loss. Moreover, there was no active failure involved in the front end layer of defense; all decisions were made from the top management level of the organization. With the miscommunication that occurred between NASA and Thiokol, the administrators at NASA were not aware of the potential risk that was involved with the launch decision. As a result, the *unsafe acts* layer of defense was discarded, resulting in a critical flaw in the Swiss Cheese Model—without the provisions to counteract or override unsafe acts, the model is inadequate for accident prevention. Further investigation is needed to determine whether another model may be more successful in addressing complex systems such as the NASA space shuttle launch, in terms of identifying risk factors and predicting potential accidents.

The Exxon Valdez Oil Spill Incident

The Exxon Valdez oil spill disaster will demonstrate how active failures and latent conditions merge to cause a catastrophic adverse event that could have been avoided. The incident occurred on Mach 24, 1989, when the vessel ran aground on Bligh

Reef its way to transport crude oil from Alaska to California. Approximately 10 million gallons of crude oil were spilled into the Prince William Sound, Alaska, after eight cargo tanks were ruptured. The incident caused a huge environmental issue, and the cost of cleaning the water exceeded $2 billion in addition to the costs of vessel damage and the various lawsuits from the environmental agencies, fishermen and other affected parties were filed (Harrald, et al., 1990). Human error contributed greatly to the accident. Errors were made from all levels of the organization. We will next utilize the Swiss Cheese Model of Accident Causation to analyze this incident and its contributed factors.

Unsafe Acts

The holes in this layer of the model were essential to cause the accident along with the latent condition that existed:

- The crew did not get enough time to rest before departing the port. Which is considered a violation of the amount of sleep required before being able to go on a cargo watch task. As a result, the crewmembers suffered fatigue due to the impaired task performance (National Transportation Safety Board, 1990).
- The crew also violated the procedures of consuming alcohol before and while on mission on the vessel. Evident showed that the master, the captain and the other mates on the vessel were intoxicated.
- The captain violated the navigation rules by travelling outside the normal shipping lanes in an attempt to avoid ice. Violating the procedures of slowing down to a minimum speed in the original shipping lane and passing the ice.

- The captain also violated procedures by not being accurate and precise in reporting position and speed of the vessel on time.
- Incorrect procedure was taken by crewmember to maneuver the vessel to avoid ice.
- The crew violated the Exxon Shipping Company Navigation and Bridge Organization Manual by reducing the number of officers required on the bridge. For the specific situation on the vessel, two navigating officers were required to attend on the bridge. Unfortunately only one was there since the captain was absent.
- The captain engaged the vessel on autopilot violating the regulation set by the USCG. Also violating the standing orders of the Exxon Shipping Company that steering should always be manual if navigating near the shore or shallow banks (Alaska Spill Oil Commission, 1990).

Psychological Precursors of Unsafe Acts

Some of the major latent conditions that factored in the accident:

- The presence of the icebergs
- Crewmembers fatigue condition due to lack of sleep
- The alcohol-impaired captain on board
- Inadequate training on vessel maneuvering
- Reduced number of manpower in the port, the bridge and on vessel
- Lack of procedures with regards to hours-of-service (National Transportation Safety Board, 1990)

The previous latent conditions represent the weaknesses in the safeguards of the system of the Exxon Valdez. If these were detected in proper time, the accident would not have happened.

Line Management Deficiencies

Inadequate supervision at the port and on board vessel was the main cause of generating the holes on this defensive layer:

- The captain did not request to stay longer at the port for the crew to get enough rest.
- Failing to correct the shortage of officers and crewmembers required in port and on vessel that caused impaired task performance
- Lack of problem reporting communication between the vessel and the port
- Inadequate instructions were communicated to crewmembers with regards to procedures in maneuvering the vessel.
- Lack of feedback when problems were reported to the captain
- Incorrect procedures with regards to navigating the vessel through ice
- The master did not provide an adequate watch over the vessel due to alcohol-impairment.

Fallible Decisions

The weakness of this defensive layer demonstrated how inadequate regulations and supervisions resulted in catastrophic accident:

- Lack of contingency plans

- Limitation of the technology available and required equipment in case of such accident (Harrald et al., 1990)
- Lack of resources; i.e. crewmembers
- Lack of procedure regarding crew members safety and drug tests
- Lack of training for crewmembers
- Poor utilization of safety plans and communication equipment - There is evidence that the radar on the port was not working effectively at the time the vessel was navigating (Leveson, 2005).
- Assigning a master before proofing his alcohol problem was under control.

Summary of The Exxon Valdez Oil Spill Incident

The Exxon Valdez oil spill incident's demonstrated how all levels of the organization can contribute to the cause of a catastrophic disaster. Blame cannot be pointed to the crewmembers alone in this incident due to the lack of regulations and the norm of organizational behavior, where violating the procedures were practiced to overcome obstacles and meet schedules. The holes in the Exxon Valdez oil spill were identified in each layer. The holes lined up in the stacked weak defensive layer, and the trajectory of accident breach causing the unfortunate disaster, which could have been avoided if these unsafe acts and their related latent conditions were identified in the proper time.

Conclusion

Human errors have caused numerous catastrophic disasters over the past decades. Tracking the causes of these error will reveals contributing factors to these errors. The Swiss Cheese Model of accident causation suggested that in order for an accident to occur all the safeguards in the organization have to be breached with a trajectory that passes through all the holes, which includes unsafe acts and latent conditions. Identifying and characterizing these holes and preparing the corresponding defensive safeguards early in the system will make it almost impossible for a trajectory to pass through every layer. Unfortunately, Reason did not specify how to apply the Swiss Cheese Model. He suggested the theory and handed it over to the investigators to identify all the holes and defensive layers. However, it is unclear how to allocate the holes and measure their sizes, or how to relate each of the active failures to the corresponding latent condition. The Swiss Cheese Model was not successfully utilized in the Space Shuttle Challenger incident due to the lack of one vital defensive layer; the *unsafe act*. However, the model was valid for the Exxon Valdez oil spill incident. Both accidents were caused mainly by human error and were operating as a complex system. After examining the previous engineering management applications, it turned out that not all complex accidents could be investigated using the Swiss Cheese Model. Further instructions and modifications are needed by investigators to be able to apply the model.

References

Alaska Oil Spill Commission. *Spill: the Wreck of the Exxon Valdez, Implications for Safe Transportation of Oil: Final Report*. Junea: the Commission, (1990).

Avery AJ, A. Sheikh, B. Hurwitz, L. Smeaton, Y-F Chen, RL Howard, J. Cantrill, and S. Royal, *Safer medicines management in primary care.* Br J Gen Pract (2002), 52(Suppl):S17–22.

Carthey J, MR de Leval, JT Reason, *The human factor in cardiac surgery: errors and near misses in a high technology medical domain*. Ann Thorac Surg (2001), 72:300 –5.

Harrald, J. R., H. S. Marcus, and W. A. Wallace, The *EXXON Valdez: An assessment of crisis prevention and management systems*. Interfaces, (October, 1990), Vol. 20(5), pp.14–20.

Kerzner, Harold. *Project Management: Case Studies*, (2009), Wiley & Sons. New Jersey, pp. 425-461.

Nancy G. Leveson "Software System Safety". Ocw.mit.edu, (July 2005), pp. 18–20. Retrieved 2010-07-30.

Orasanu, J.M., *Decision-making in the cockpit*. In E.L. Wiener, B.G. Kanki, and R.L. Helmreich (Eds.), Cockpit resource management, (1993), San Diego, CA: Academic Press. pp. 137-72.

Reason J. *Human error,* (1990), New York: Cambridge University Press.

Reason J. *Human error: models and management*, BMJ, *(*2000), 320:768–70.

Reason, J., E. Hollnagel, and J. Paries. *Revisiting the Swiss cheese model of accidents*, (2006) Eurocontrol, EEC Note no. 13/06.

Reason J. T., *The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries*. (2008), Ashgate Publishing.

Sidney Dekker. *The Field Guide to Human Error Investigations*, (2002), pp. 119-120.

The National Transportation Safety Board*, Safety recommendation, Exxon Valdez report*, (September 18, 1990), in reply to M-90-26 through -3.

U.S. Presidential Commission, *Report on the Space Shuttle Challenger Accident*, (1986), http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html.

Wiegmann, Douglas A., and Scott A. Shappell, *A human error approach to aviation accident analysis, The human factors analysis and classification system*, (2003), Burlington, VT: Ashgate.

II. VARIATIONS IN RISK MANAGEMENT MODELS: A COMPARATIVE STUDY OF THE SPACE SHUTTLE CHALLENGER DISASTER

Hanan Altabbakh, Susan Murray, Katie Grantham, Siddharth Damle

Missouri University of Science and Technology

Abstract

Managers seeking to assess risk within complex systems face enormous challenges. They must identify a seemingly endless number of risks and develop contingency plans accordingly. This study explores the strengths and limitations of two categories of risk assessment tools: product assessment techniques including Failure Mode and Effect Analysis (FMEA) and Risk in Early Design (RED) and process assessment techniques, such as Layer of Protection Analysis (LOPA) and the Swiss Cheese Model (SCM). A NASA case study is used to evaluate these risk assessment models. The case study considers the January 1986 explosion of the Space Shuttle Challenger, 73 seconds after liftoff. This incident resulted in the loss of seven crew members and consequently grave criticisms of NASA's risk management practices. The paper concludes with comparison and recommendations for engineering managers on selecting risk assessment tools for complex systems.

Introduction to Risk Assessment

Risk exists in our everyday activities from getting out of bed in the morning to the most complicated task in any complex system. Managers need to consider a wide range of risks, including risks related to products' component failure, human error, and operational failure. There are a variety of assessment tools for each of these risk types.

The Human Systems Integration Handbook (Booher, 2003) lists 101 techniques available for evaluating safety in complex systems. Even with this wealth of tools, or perhaps because of them, mitigating risks remains a daunting task. Various authors have generated definitions of risk. According to Covello and Merkhofer, risk is defined as "a characteristic of a situation or action wherein two or more outcomes are possible, the particular outcome that will occur is unknown, and at least one of the possibilities is undesired" (Covello & Merkhofer, 1993). NASA defines risk as the chance (qualitative) of loss of personnel capability, loss of system, or damage to or loss of equipment or property (National Research Council, 1988). Another definition of risk was founded by the Occupational Health and Safety Assessment Series (OHSAS), which states "Risk is a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury or ill health that can be caused by the event or exposure(s)" (OHSAS, 2007).

Taxonomies of risk have been established in the literature where some risks were categorized according to their source, for example, political, environmental, and economic risk sources. Risks can also be categorized according to industry or service segment or according to their order of significance from the user's perspective. These classifications might limit engineers and managers to existing taxonomies only, avoiding

investigation for further risk classification, or even omitting unidentified ones. In that case, engineers and managers must have risk assessment tools as part of their risk management programs available in hand along with the existing taxonomies to evaluate a design for risks (Letens, Van Nuffel, Heene, & Leysen, 2008).

"Risk assessment is the process of identification, evaluation, acceptance, aversion, and management of risk" (Eccleston, 2011). A study conducted by interviewing 51 project managers proved that experience alone does not contribute to risk identification among engineers and managers as much as the level of education, information search style, and training (Maytorena, Winch, Freeman, & Kiely, 2007).

Murray developed a generic risk matrix that can be adapted by project management to quickly identify potential risk, probability, and impact (Murray, Grantham, & Damle, 2011). After identifying risks and quantifying their magnitude, the next step in risk assessment is to evaluate the associated decisions to be made and their impact. There are various risk assessment tools for different risk environments such as nuclear reactors, chemical plants, health industry, construction, automotive industry, project management, financial industry, and others. In general, they all address three issues: the adverse event, its likelihood, and its consequences. Reducing the probability of failure and its consequences has been the major goal of reliability and safety analysis.

Failures can cause loss of life, significant financial expenses, and environmental harm (Henley & Kumamoto, 1981). Determining the appropriate assessment tool(s) is the first step in risk analysis. These can include simple, qualitative, quantitative, and hybrid assessment approaches (National Research Council, 2007). The purpose of this paper is to investigate the advantages and shortcomings of various product and process-based risk

assessment tools to assist engineers, managers, and decision makers in selecting the proper tools for the specific situation. The Space Shuttle Challenger Disaster is used to demonstrate the differences among the techniques.

Space Shuttle Challenger Disaster

On January 28, 1986 the Space Shuttle Challenger took off for the last time. Its flight lasted just over a minute when the Space Shuttle exploded resulting in the loss of all its seven crew members. The Challenger was the most anticipated launch for NASA and was supposed to be a milestone for more than one reason. The technical cause for the accident was determined to be the erosion of the o-ring on one of the solid rocket boosters, which allowed the passage of hot gases. This caused the release of hydrogen into the external tank, which deflagrated and caused the shuttle to blow up.

Unfortunately, this technical glitch was just one of the factors attributed to the failure of this high profile space mission.

Over the next three months, a presidential commission led by former Secretary of State William P. Rogers and a NASA team investigated the accident (Damle & Murray, 2012). The commission concluded that there was a serious flaw in the decision making process leading up to the launch. A well structured and managed system emphasizing safety would have flagged the rising doubts about the solid rocket booster joint seal. Had these matters been clearly stated and emphasized in the flight readiness process in terms reflecting the views of most of the Thiokol (a subcontractor responsible for the solid rocket boosters (SRBs)) engineers and at least some of the Marshall Space Center engineers, it seems likely that the launch of 51-L might not have occurred when it did.

Apparently, Thiokol was pressured into giving a go ahead for the launch by NASA.

Reasons for the disaster (Damle & Murray, 2012):

1. Faulty o-ring – The o-ring sealing in the solid rocket boosters eroded and let hot gases pass through causing an explosion.
2. Application beyond operational specifications – The o-rings had been tested at 53^0F before, but were never exposed to launch day temperatures of 26^0F.
3. Communication – Thiokol and NASA were geographically away from one another and travel for meetings was not feasible. This led to communication issues between the two organizations.
4. Management pressure – The engineers at Thiokol knew about the o-ring's poor performance at low temperatures, but management forced them to let go of technical issues citing "broader picture."
5. Risk management – Proper risk management methods were not in place at NASA. The criticality of the o-ring problem had been downgraded without sufficient evidence. Also, it had become a norm to issue waivers against problems to meet the schedule requirements of flights.
6. Global competition – The European Space Agency had started competing for the commercial satellite business. Also, NASA had to beat the Russians at deploying a probe into Haley Comet from the same launch station, which meant the Challenger had to be launched as per schedule.

7. Budget pressure – NASA was tight on budget and hence had to curb many of its research and development activities. Also, it had to launch a large number of flights that year to justify expenditure on the Space Shuttle program.
8. Political pressure – President Reagan was supposed to announce the inclusion of a school teacher on the Challenger mission at his State of Union Speech. This put additional pressure on NASA to launch the spacecraft as scheduled. This also attracted excessive media attention on this mission and NASA felt its reputation was at stake.

Prior to the Challenger accident in 1986, NASA emphasized quantitative risk analysis such as Fault Tree Analysis. The low probability of success during the Apollo moon missions intimidated NASA from persuading further quantitative risk or reliability analysis (Stamatelatos, Vesely, Dugan, Fragola, Minarick, & Railsback, 2002). More recently NASA moved from a preference for qualitative methods such as FMEA in assessing mission risks to an understanding of the importance of the probabilistic risk assessment such as FTA (Stamatelatos, et al., 2002). Process-based risk assessment techniques were not common prior to the Challenger Disaster. It was not until the early 1990s that the first process safety risk assessment techniques were introduced (Center for Chemical Process Safety, 2001). Cost was a factor in NASA's preference for qualitative over quantitative risk assessment. Gathering data for every single component of the shuttle to generate statistical models that are the backbone of probabilistic assessment tools was time consuming and expensive (Kerzner, 2009).

Types of Risk Assessment Tools

This paper considers risk assessment tools in two broad categories: product-based tools and process-based tools. Product-based tools concentrate on failures at the component level, including product design shortcomings and failures. This paper introduces FMEA, FTA, and Risk in Early Design (RED) in this category. These tools, in spite of being comprehensive, fail to address systemic issues, mainly relating to human error, decision making errors, culture issues, external pressures on decision making process, and inadequate user training. Many of these issues were encountered in the Challenger accident. This paper also considers process-based risk assessment including Layer of Protection Analysis (LOPA) and the Swiss Cheese Model. These methods strive to consider the system as a whole, with due consideration to organizational issues and human error causes. Detailed descriptions of the methods and their application to the Challenger accident follow.

Product-Based Risk Assessment Tools

Product risk assessment tools investigate risks associated with the system from the component level and the product design. Product-based risk assessment tools are categorized into qualitative and quantitative tools, where the probabilities of failure occurrence are quantified in the latter one. Both of these types of risk assessment tools can be used throughout the product life cycle, even simultaneously, to identify potential risks. Product-based risk assessment tools do not consider the human factors due to the complexity of human minds and behaviors.

Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is a very structured and reliable bottom-up method to classify hardware and system failures. Applying FMEA can be easy even in a complex system due to the simplicity of the method. FMEA increases design safety by identifying hazards early in the product lifecycle when improvements can be made cost effectively (Dhillon, 1999). In spite of the fact that FMEA is very efficient, if it is applied to the system as a whole, it may not be as easy if the system consists of a number of components with multiple functions (Stamatis, 2003). FMEA only considers hazards that lead to failure. It does not address potential hazards that result from normal operations (NASA, 2001). Other negative aspects of the detailed FMEA format include being very time consuming and expensive, due to its detailed nature.

A significant concern for complex systems with human interaction is that FMEA does not consider failures that could arise due to human error (Foster, et al., 1999). NASA used FMEA on the overall Space Shuttle program, also known as the Space Transportation Systems (STS), the Ground Support Equipment (GSE), and individual missions to identify the Critical Item List (CIL). This list consists of failure modes sorted according to their severity starting with the worst (National Research Council, 1988). Exhibit 1 explains the consequence classification system at NASA where critical items are classified according to their effect on the crew, the vehicle, and the mission (Kerzner, 2009).

Exhibit 1: The Consequences Classification System (Kerzner, 2009)

Level	Description
Criticality 1 (C1)	Loss of life and/or vehicle if the component fails
Criticality 1R (C1R)	Redundant components exist; the failure of both could cause loss of life and/or vehicle
Criticality 2 (C2)	Loss of mission if the component fails
Criticality 2R (C2R)	Redundant components exist; the failure of both could cause loss of mission
Criticality 3 (C3)	All others

In 1982 (four years before the Challenger explosion), FMEA revealed that the Space Shuttle's o-ring seal had a criticality rating of 1 (Winsor, 1988). However, it was only one of over 700 criticality 1 classified components that existed in 1985 (Kerzner, 2009). During this time period, C1 risk items were considered acceptable risks and waivers were issued by managers.

Fault Tree Analysis

Fault Tree Analysis (FTA) is a top-down probabilistic risk assessment technique. It is a deductive method that investigates the factors and conditions that contribute to adverse events in a system. It utilizes logic gates and graphical diagrams to identify the failures in the system, subsystem, and components. The FTA starts with a critical root event and proceeds with determining all the possible potential causes, parallel and sequential, that contribute to the top adverse event and represents it as a cause-and-effect relationship (Ireson, Coombs, & Moss, 1995). There is no single correct way to construct

a fault tree. Different people can come up with different fault trees for the same root event. FTA is a probabilistic risk assessment tool that can be quantitatively evaluated using the rules of Boolean algebra between its gates.

The strength of the FTA is that it is a visual model that clearly depicts the cause-and-effect relationship between the root cause events to provide both qualitative and quantitative results (Bertsche, 2008). Another benefit of the FTA is that it concentrates on one particular failure at a time. The detailed, structured approach also has the advantage of requiring the analyst to study the system in great detail in an organized manner, which can reduce the danger of overlooking risk factor(s) (Dhillon, 1999).

This technique suffers from a few limitations. A fault tree might not be able to capture all the error causes that are related to humans due to the complexity of human behavior. Accounting for human error in fault trees can make the analysis too complicated and unmanageable (Kirwan & Ainsworth, 1992). For every top-level hazard that is identified, a thorough fault tree must be constructed which is time consuming and lengthy. Some large fault trees may not fit into a reliability report due to their size and complexity. Latent hazards may not be identified during the construction of a fault tree.

In January 1988, after the Space Shuttle Challenger Disaster, the Shuttle Criticality Review and Hazard Analysis Audit Committee recommended that NASA apply probabilistic risk assessment (PRA) methods to the risk management program (Stamatelatos & Dezfuli, 2011). According to NASA "No comprehensive reference currently exists for PRA applications to aerospace systems. In particular, no comprehensive reference for applying FTA to aerospace systems currently exists." (Stamatelatos, Vesely, Dugan, Fragola, Minarick III, & Railsback, 2002).

Risk in Early Design

The Risk in Early Design (RED) theory was developed in 2005 by Grantham et al. to assist engineers in risk assessment by automatically generating lists of potential product risks based on historical information (Grantham, Stone, & Tumer, 2009). With given product function as inputs, RED generates the historically relevant potential failure modes of those functions and ranks them by both their likelihood of occurrence and the consequence, ranking from one as least severe to five as most severe of those failures.

Unlike FMEA and FTA, which require experts to identify potential failure modes, RED utilizes a historical knowledgebase to produce the potential risks. This feature is beneficial for novice engineers who do not have substantial experience predicting failures; it is also beneficial for newer systems that can benefit from the performance of older products while determining potential failures. While it is highly recommended by the developers that experts review the RED output and assess its relevance to the system under study, a drawback of this risk assessment method is potential risk over or under quantification. Further, the method is only as good as the knowledgebase used to generate the risks.

Using RED to Analyze the Space Shuttle Challenger Disaster

The first step in applying RED to identify and analyze risks is to select the functions performed by components of the product from the provided list of electromechanical functions from the RED software tool, http://idecms.srv.mst.edu/ide/.

For the Challenger Disaster, a “human centric, subsystem level” risk analysis of only the solid rocket boosters (SRBs) was performed. Twenty-one functions were

selected that represented the functionality of the SRBs. From those 21 functions, 402 risks were identified (7 high risks–upper right hand region, 130 moderate risks-middle region, and 265 low risks-left/lower-left hand region). The risk fever chart produced by RED is shown in Exhibit 2. The examples from the detailed report are included in Exhibit 3. Referring to Exhibit 3, of the seven high risks identified, five were suggested to fail due to high cycle fatigue, and the remaining two were suggested to fail due to brittle fracture. This is interesting because at the cold temperatures of the Challenger launch, the material used for the o-rings took on more brittle characteristics. Also, the functions most closely associated with the o-ring, "stop gas" and "stop liquid," generated interesting risks related to the Challenger Disaster. For example, "stop gas" was linked with the following potential failure modes and likelihood-consequence pairs: brittle fracture (likelihood-1, consequence-4) and thermal shock (likelihood-1, consequence-4), which are both low risks. Similarly, "stop liquid" was linked with the following potential failure modes and likelihood-consequence pairs: brittle fracture (likelihood-2, consequence-5) and thermal shock (likelihood-1, consequence-5), which are both medium risks. The classification of the risks is due to the low likelihood rating of the failures on the risk fever chart. However, the consequence ratings represent the severity of the event, where (consequence = 4) indicates total malfunction of the SRBs and (consequence = 5) indicates loss of life. The risk ratings produced by RED are consistent with the expectations that cold weather is not likely at a Space Shuttle launch; however, should it occur, devastating consequences can be expected.

Exhibit 2: RED Results for SRB Analysis

Likelihood						
	5	0	0	0	0	3
	4	0	0	0	0	1
	3	0	0	0	5	3
	2	0	0	0	1	35
	1	0	3	64	198	89
		1	2	3	4	5
		Consequence				

	High risk
	Low Risk
	Moderate Risk

Exhibit 3: Examples from the detailed RED report

Risk Level	Function	Failure Mode	Likelihood	Consequence
High	Change Electrical Energy	High Cycle Fatigue	5	5
High	Stop Solid	High Cycle Fatigue	5	5
High	Store Solid	High Cycle Fatigue	5	5
High	Change Solid	High Cycle Fatigue	4	5
High	Stop Solid	Brittle Fracture	3	5
High	Store Solid	Brittle Fracture	3	5
High	Export Gas-Gas Mixture	High Cycle Fatigue	3	5
Med	Export Gas-Gas Mixture	Stress Corrosion	3	4
Med	Change Solid	Stress Corrosion	3	4
Med	Stop Solid	Stress Corrosion	3	4
Med	Change Electrical Energy	Stress Corrosion	3	4
Med	Store Solid	Stress Corrosion	3	4

Product-Based Risk Assessment Tool Summary

FMEA, FTA, and RED have their limitations and merits, and they complement each other well. FMEA is used to identify the potential failure modes of the system components; this was done by NASA to generate the critical items list for the Space Shuttle program. FTA, on the other hand, evaluates each of the critical items to find its cause(s). Both can be used repeatedly throughout the system design cycle. FTA and FMEA are standard risk assessment techniques for product components but they share the shortcomings that they do not include human error and hostile environment (Qureshi, 2008). RED identifies and assesses risk in the early design phase, which aids managers and decision makers in minimizing the subjectivity of the likelihoods and consequences. Due to the simplicity of RED, managers with less experience in risk assessment can easily adapt the tool and apply it at the conceptual phase. These risk assessment tools aid the engineering manager in identifying a variety of hazards and associated causes at a component level.

Process-Based Risk Assessment Tools

Process-based risk assessment tools use a system-wide approach. Instead of identifying risks related to component and product design, these tools identify risks that can be encountered in the entire process, including those related to humans, organization, management, and decision making. Hence, risks involved with all entities concerned with the product are considered. The following process-based models consider risk on a broader system level, thus, widening the scope of risk assessment compared to the product-based risk tools.

Layer of Protection Analysis

Among the various existing risk management techniques being used today, Layer of Protection Analysis (LOPA) is widely used in the process industry (Center for Chemical Process Safety, 2001). It is a semi-quantitative analytical tool to assess the adequacy of protection layers used to mitigate risk (Summers, 2002). LOPA is a process hazard analysis (PHA) tool. The method utilizes the hazardous events, event severity, initiating causes, and initiating event likelihood data developed during the hazard and operability analysis (HAZOP). The LOPA method allows the user to determine the risk associated with the various hazardous events by utilizing their severity and the likelihood of the events being initiated. LOPA identifies the causes of each adverse event and estimates the corresponding initiating event likelihood. Then, it determines the independent protection layers (IPL) for each pair of cause-consequence scenarios and addresses the probability of failure on demand (PFD) accordingly. To quantify the mitigated event frequency for each IPL, LOPA multiplies each initiating event frequency by the PFD, then compares the result to the criteria for tolerable risk (Dowell, 1999).

LOPA focuses on one cause-consequence scenario at a time. Using corporate risk standards, the user can determine the total amount of risk reduction required and analyze the risk reduction that can be achieved from various layers of protection (Frederickson, 2002). IPLs, as shown in Exhibit 4, are simply safety systems that meet the following criteria (Summers, 2002) –

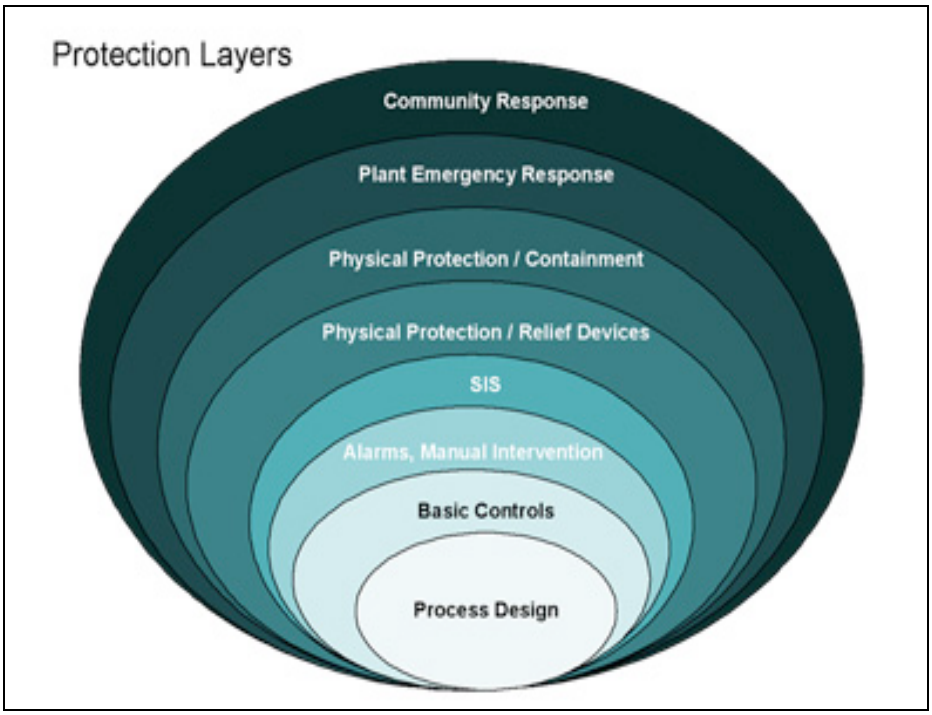
1. Specificity - The IPL should be capable of mitigating the identified initiating event.

2. Independence – An IPL should be independent of any other IPL or of the initiating event. This way, failure of one does not affect performance of any other IPL.

3. Dependability – The IPL reduces the risk by a known amount with a known frequency.

4. Auditability - IPL should allow for regular validation.

Exhibit 4: Protection Layers (General Monitors, 2011)



The IPLs perform three main functions of prevention (to reduce the probability of accident), protection (to detect the initiating cause and neutralize it) and mitigation (to control/reduce the accident severity) (Markowski & Mannan, 2010). LOPA has significant advantages over other fully quantitative methods. It takes less time to analyze

scenarios that are too complex to be qualitatively evaluated, compared to a regular quantitative risk method. It proves to be very effective in resolving disagreements in decision making since it provides a clear, simple, and concise scenario structure to estimate risk. The output of LOPA is vital to assign safeguards during different situations such as operation and maintenance to assure safety of employee, assets, environment and organization. Also, by design, LOPA deals with general decision making in risk assessment; it is not intended to be used for detailed decision making (Center for Chemical Process Safety, 2001). A valuable feature of LOPA is that the quantified output of the analysis can reduce the uncertainty about residual risk levels (Gulland, 2004). The primary disadvantage of the method is that the numbers generated are only an approximation and, hence, its application requires a certain degree of experience while evaluating and assessing scenarios.

Using LOPA to Analyze the Space Shuttle Challenger Disaster

In the case of the Space Shuttle Challenger, the system under consideration is the Solid Rocket Boosters (SRB) o-ring sealing, which eventually blew up due to the o-ring's failure to contain hot gases. Different layers can be designed to capture this problem at an initial stage, as per the LOPA model (Damle & Murray, 2012). Exhibit 5 and Exhibit 6 show the layers developed for the Challenger Disaster.

Exhibit 5: LOPA Model for Challenger Disaster (Damle & Murray, 2012)

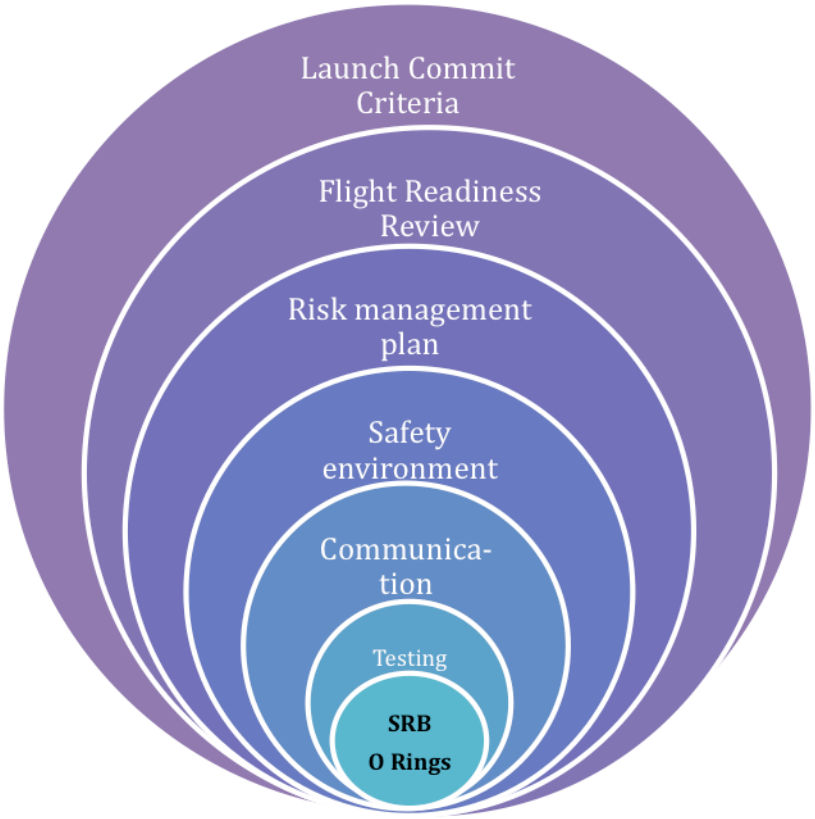


Exhibit 6: Layer Definitions and Flow (Damle & Murray, 2012)

The following demonstrates how NASA could have applied the LOPA technique to the Space Shuttle.

Layer 1 – Testing

Each component going into the Space Shuttle is tested prior to delivery at the vendor's location. In this case, SRBs have to be tested as per test plans by NASA. Any conditions beyond the testing specifications should be deemed risky and retesting at new parameters has to be carried out before any decision is made.

Layer 2 – Communication

Any observation made during testing should be documented and clearly communicated to all persons involved. Any discrepancy or non-conformity should be immediately flagged and necessary actions should be recommended through two-way communication with the end user (NASA). Any phone calls should also be logged so that they can be referred to in the future, in case issues arise later.

Layer 3 – Safety Environment

There needs to be an inherent safety environment within the organization. Any problem, when detected should be brought to the notice of immediate superiors, while critical issues should be escalated before it is too late in the process. With a safety environment, every employee is safety concerned and works towards making the entire system as safe as possible. The voice of every employee regarding safety matters should be given due attention.

Layer 4 – Risk Management Plan

There is usually a risk management plan in place. The most crucial aspect of the plan is to adhere to the severity definitions and the risk matrix. Risk assessment should be carried out using a comprehensive method for identifying potential failures and a specific quantitative methodology should be used to assess safety risks (National Research Council, 1988). The criticality of any risk should not be downgraded, especially when human life is at stake. Waivers should only be issued under extremely special conditions and should need to have multiple signatories including top management. It should not be a norm to issue waivers for small issues, which might eventually lead to bigger problems. As recommended by the presidential committee, all contractors should review high

criticality items and improve them prior to flight. An audit panel should verify the adequacy of the report and report directly to the Administrator of NASA (U.S. Presidential Commission, 1986).

Layer 5 - Flight Readiness Review

The Flight Readiness Review (FRR) is a meeting of all teams and management to check if all components are in place for a launch. This also includes confirming that the parts are manufactured to specifications. Managers provide evidence that all work to prepare a Space Shuttle for flight was done as required. This is a crucial meeting and the FRR should be used to escalate issues if they were not addressed by immediate supervisors. Considering the criticality of the risk involved, there should be no concessions on specifications or quality of work. Lack of sufficient test data for the given conditions should not be interpreted as a go ahead for application.

Layer 6 – Launch Commit Criteria

This is the final check before any Space Shuttle takes flight. A formal prelaunch weather briefing is held two days prior to launch (NASA, 2010). This includes weather data specifications including temperature, winds, cloud ceilings, and thunderstorms. These criteria specify the weather limits at which launch can be conducted. These criteria should be strictly followed, and no waivers should be allowed based on pressures from external factors. Launching in spite of bad weather conditions is a decision that most certainly increases the risk of a major disaster.

The Probability to Fail on Demand (PFD) is difficult to determine at this stage. In the Challenger case, loss of life is the consequence. Thus, the severity of consequence is very high and criticality is maximal. But, there are no typical initiating event frequencies,

as there is no historical data. The frequency of the consequence occurrence depends on probability to fail on demand (PFD) of every protection layer. For the cases considered, the protection layers are not engineering systems or devices. Hence, their PFDs cannot be determined in a manner prescribed in LOPA methodology.

Human Factors Analysis and Classification System and the Swiss Cheese Model

The Human Factors Analysis and Classification System (HFACS) was developed to analyze the U.S. Navy's aviation accidents. It uses James Reason's Swiss Cheese Model for its basic structure. Early in the 1990s, the U.S. Navy was undergoing a high rate of accidents, and 80% of the accidents were due to human error (Shappell & Wiegmann, The Human Factors Analysis and Classification System - HFACS, 2000).

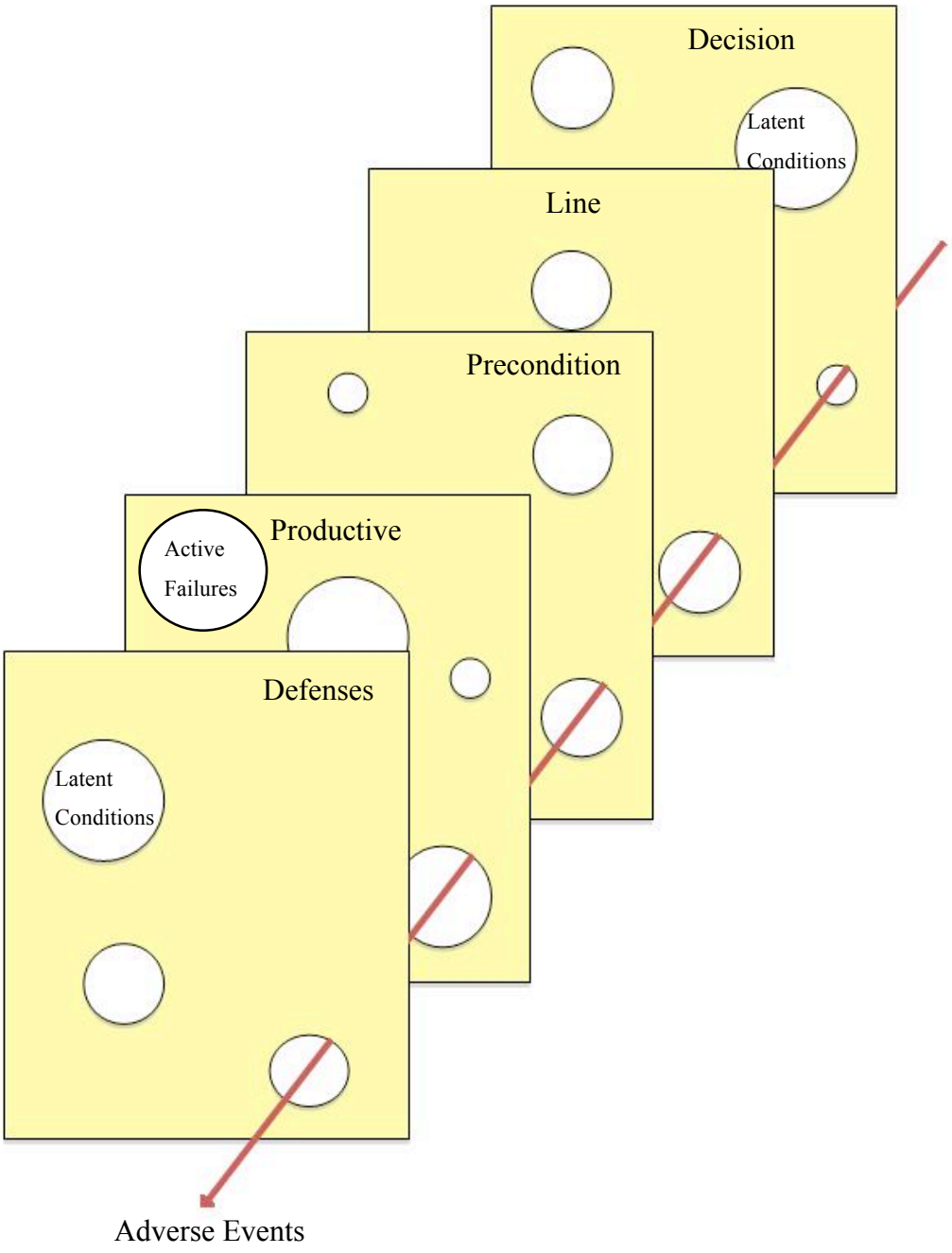
Human error is a significant cause of catastrophic accidents in many industries (Hollywell, 1996). Investigating why human errors occur can be essential to find an accident's roots cause(s). The more general form of this process-based tool, the Swiss Cheese Model, will be used for the discussion and application in this paper.

The Swiss Cheese Model was developed by James Reason (1997) to address accidents in complex systems where many components interact with each other. The model tracks accident causation at different levels of the organization without blaming individuals. The Swiss Cheese Model determines the true causes of an accident by linking different contributing factors into a rational sequence that runs bottom-up in causation and top-down in investigation (Reason, Managing the Risks of Organizational Accidents, 1997). Reason presents his model as stacked slices of Swiss cheese, where the slices represent the defenses and safeguards of the system, and the holes represent *active*

failures (i.e., unsafe acts) and *latent conditions*. Unsafe acts occur when a human is in direct contact with the system, such as during the Chernobyl accident where the operator wrongly violated the plant procedures and switched off successive safety systems. Latent conditions can occur at any level of the organization or any system and are harder to detect. Examples of latent conditions include lack of training, poor design, inadequate supervision, and unnoticed defects in manufacturing (Reason, 1997). Latent conditions are considered the source of ignition of any accident or error (Reason, 2000).

The holes in the model are not static. They move from one position to another, and they may open or close and change in size continuously depending on the situation and the system climate. According to Dekker, it is the investigator's job to find out the position, type, source, and size of each hole and identify the cause of these changes (Dekker, 2002). Finally, the investigator must determine how the holes line up to produce accidents since all holes must align through all the defensive layers for the trajectory to pass through and cause an adverse event. Exhibit 7 shows the original version of the model containing five layers, namely decision makers, line management, preconditions, productive activities, and defenses.

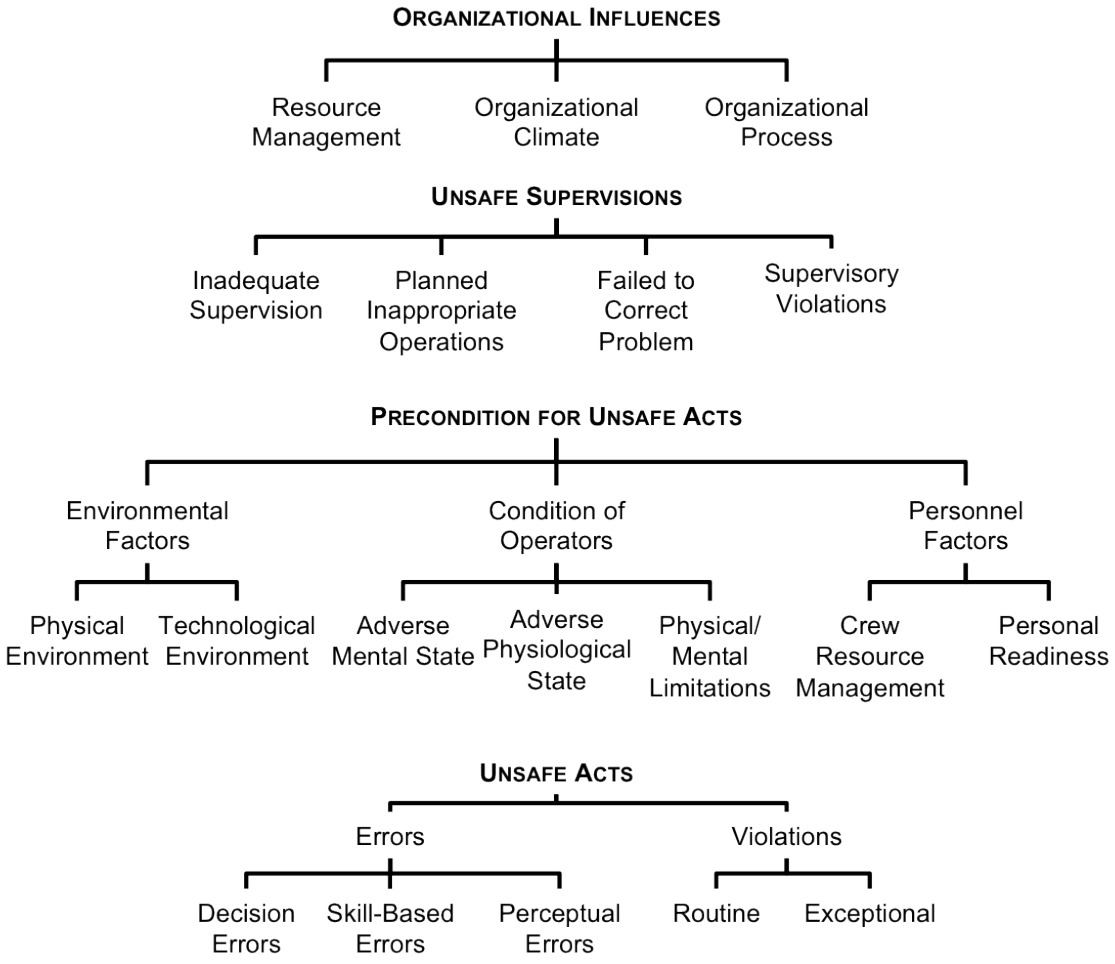
Exhibit 7: Adapted from Reason's Swiss Cheese Model



The enhanced version of the model is not limited to certain numbers of defensive layers nor are they labeled or specified by Reason. Thus, a variety of defense layers and

safeguards can be adapted to this model from different organizational environments depending on the amount of risk involved. Unfortunately, the model does not specifically explain the relationship between the various contributing factors, which may result in unreliable use of the model (Luxhoj & Kauffeld, 2003). Wiegmann and Shappell (2003) conducted a study to identify the holes and safeguards for an aviation system. They were able to precisely target each defensive layer and classify its holes (unsafe acts and latent conditions). They categorize the layers into four levels of human failure where each layer influenced the succeeding. Exhibit 8 illustrates the HFACS model with proposed defensive layers for the aviation industry.

Exhibit 8: The HFACS framework (Shappell, Detwiler, Holcomb, Hackworth, Boquet, & Wiegmann, 2007)



Using the Swiss Cheese Model to Analyze the Space Shuttle Challenger Disaster

To examine the Challenger Accident using Reason's Swiss Cheese Model (1990), the "layer of cheese" must first be identified.

Productive Activities

Errors in the launch of the Space Shuttle Challenger were unintentional. Blame cannot be attributed to a pilot, crewmember, operator, or controller. The incident was due to poor decision-making at the upper management level, which constitutes an unsafe act under the decision error type (Orasanu, 1993). The commander and pilot flying the Space Shuttle are considered the direct operators, but in the Challenger Disaster, it was not their choice whether or not to launch; it was the decision of leaders not on board the shuttle.

Therefore, the unsafe act defensive layer might not be applicable for the Challenger Accident. This layer would be removed from the model for this application. However, according to the Swiss Cheese Model, it takes both active failures and latent conditions for the trajectory to pass through the defensive layers and cause an accident.

Therefore, removing an essential layer might invalidate the model since the error was not made at the operational level.

Preconditions

Preconditions are the latent conditions/failures that contributed towards occurrence of an accident, such as the poor weather conditions on the day of the launch. For a successful reseal of the o-ring, the environmental temperature should be $\geq 53^{\circ}$F.

According to Thiokol, low temperature would jeopardize the capability of the secondary sealing of the Solid Rocket Motor (Kerzner, 2009). Communicating that issue was complicated by the fact that engineers use technical jargon that is not always understood by upper management. Moreover, the ice on the launch pad introduced

additional risk factors to the launch operation. The ice also covered the handrails and walkways surrounding the Space Shuttle, which presented hindrances to emergency access. In addition, availability of spare parts, physical dimensions, material characteristics, and effects of reusability were other factors that may have contributed to the disaster.

Line Management

Line management did not adequately enforce the safety program (Kerzner, 2009). As a result, all risks were treated as anomaly and that became the norm in the NASA culture. An escape system during launch was not designed due to overconfidence in the reliability of the Space Shuttle and a belief that having an escape plan would be cost prohibitive. A latent failure introduced an unsafe act, which violated the most important factor: the safety of the crew. Pressure to launch on the designated schedule due to competition, politics, media, and Congressional issues made it hard for line managers to communicate the engineers' concerns and reports to top decision makers and administrators. Problems that were discussed internally at Thiokol and NASA were not adequately communicated between the two organizations due to lack of problem reporting procedures. The lack of communication introduced a latent failure.

Decision Makers

Budget was a major constraint at NASA at the time. Consequently, top management at NASA approved the design of the solid rocket motor in its entirety, including the o-ring joint, even when this meant changing the research direction at a great

cost. Risk was accepted at all levels since calculated safety projections were favorable. A NASA position for permanent administrator was empty for four months prior to the accident, and turnover rate of upper management was relatively high; this added to the communication breakdown from the top down. Moreover, the lack of communication between NASA's top decision makers and Thiokol's technical engineers introduced a gap where problem reporting remained in house. Concerns never reached top officials in NASA for fear of job loss. Moreover, bad news was generally downplayed to protect the interests of higher officials. In general, there was no accepted standard for problem reporting that transected all levels of either NASA or Thiokol. There was no clear recommendation from Thiokol not to launch under the cold weather condition (Kerzner, 2009). According to the U.S. Presidential Commission, (1986) regarding the launch decision, "Those who made that decision were unaware of the recent history of problems concerning the o-rings and the joint and were unaware of the initial written recommendation of the contractor advising against the launch at temperatures below 53 degrees Fahrenheit and the continuing opposition of the engineers at Thiokol after management reversed its position. They did not have a clear understanding of Rockwell's concern that it was not safe to launch because of ice on the pad. If the decision makers had known all of the facts, it is highly unlikely that they would have decided to launch 51-L on January 28, 1986." The general lack of communication, both between NASA and Thiokol and internally within each organization, functions as a latent condition.

Process-Based Risk Assessment Tool Summary

The layers of LOPA clearly expose the problems with launching the Challenger Shuttle. It can be seen that management pressures and external political pressures forced decisions to be made by violating systems and risk management measures that were in place. In spite of the pressure situation, the decision makers at NASA should have followed the risk management plan and taken into account issues raised by engineers regarding safety of the Space Shuttle. Focusing only on technical safety without consideration of decision making and human errors, can cause catastrophes, as was the case with this accident. To reduce such incidents in future, the role of human factors in system safety should not be neglected, but instead, should be addressed with priority.

When closely examining the output of LOPA, this model can be effective in identifying the key high risk stages and mitigating the problem at an early stage, with the incorporation of control points, procedural checks, regulations at different stages, and finally consequence response guidelines. Once the challenge of determining the probabilities can be overcome through acceptable assumptions, LOPA can be a powerful tool for project managers and risk managers in reducing the chances of a hazard occurrence.

From the Swiss Cheese Model, the Space Shuttle Challenger's holes (active failures) were not identified in sufficient time for safeguards to be implemented to prevent such catastrophic loss. Moreover, there was no active failure involved in the front-end layer of defense; all decisions were made from the top management level of the organization. With the miscommunication that occurred between NASA and Thiokol, the administrators at NASA were not aware of the potential risk that was involved with the

launch decision. As a result, the unsafe acts layer of defense was discarded, resulting in a critical flaw in the Swiss Cheese Model—without the provisions to counteract or override unsafe acts, the model is inadequate for accident prevention. Further investigation is needed to determine whether another model may be more successful in addressing complex systems such as the NASA Space Shuttle launch, in terms of identifying risk factors and predicting potential accidents. The Swiss Cheese Model was applied successfully to the Exxon Valdez Oil Spill Incident (Altabbakh & Murray, Applying The Swiss Cheese Model of Accident Causation, 2011). Both active failures and latent conditions combined and caused a catastrophic adverse event. The active failures were due to multiple front line operators including the captain of the vessel and the crew members. Unsafe acts were considered both error and violations in the Exxon Valdez Oil Spill Incident (Altabbakh & Murray, Applying The Swiss Cheese Model of Accident Causation, 2011).

Conclusion

After a comprehensive evaluation of the different risk management models applied to the Space Shuttle Challenger Disaster, we can conclude that these techniques are effective for a given scope of risk identification and varying times during the system lifecycle. While FMEA, FTA, and RED address risks at the component and sub-system level, the Swiss Cheese Model addresses risks related to human system interaction. LOPA considers the system in its entirety and designs defense layers to protect the system from an undesirable consequence.

FMEA strives to identify all possible failure modes and identifies a critical item list based on the criticality definitions. This can be used at an initial design phase to prevent the occurrence of failure modes and take measures according to the occurrence/severity ratings. RED can assist designers in identifying the potential risks associated with the product at the conceptual phase based on a historical stored data, which reduce the subjectivity of the decision made with regards to the likelihood and the consequences of failure modes. FTA considers all possible causes leading to an adverse event. Engineering managers can check their system stability to make sure all causes have been addressed. The logic gates make FTA an effective visual tool. However, FTA is dependent on the individual constructing the FTA, and there can be multiple ways of doing so. FMEA does not consider any failure modes resulting from normal operation. Both FMEA and FTA fail to consider human error as a probable cause of failure.

Managers need to be aware that these techniques can be fairly time consuming and lengthy and hence demand more resources and longer working time frames.

If design changes are not feasible due to financial, technical, or other restrictions, managers can explore the possibility of using risk management models, which consider risks in a broader perspective. The Swiss Cheese Model has a specific set of identified defenses designed to expose the shortcomings within the system when human system interaction is involved. It gives considerable weight to human errors and human factors when identifying risks. The most valuable contribution of this model is that it also considers precursors to unsafe actions, which can help in identifying problems with the inherent system construction and hierarchy. The holes in the defenses change according to the system or industry under consideration. This model can be used at a later stage

during operation of the system. Since it has pre-specified defenses, this model may not be applicable to certain systems. It also fails to identify a cause that is unrelated to the system (involving human) under consideration.

Layer of Protection Analysis (LOPA), a process risk management technique, uses identified hazards to build defensive layers around the system under consideration. It is easy to deploy because of its scenario-based approach. This technique allows managers to not only prevent and protect a system, but also to mitigate the effects of a consequence.

No other model considers designing defenses for a post-disaster scenario to control the after-effects of the undesirable event. LOPA can be used to include not just component risks, but risks related to organizational issues and human factors. It can guide or provide a best practice context, when considering generic projects. Managers need to note that LOPA requires pre-identified hazards to begin the analysis. The model does not consider basic component risks, but is broader, encompassing system/organization wide issues. A primary drawback is that it is project-specific, and there are no existing references of past applications. The application of this model requires experience due to its semi-quantitative nature.

Engineering managers should note that there is no one single perfect model for risk assessment. Exhibit 9 summarizes the risk assessment tools discussed in this article by identifying the pros and cons of each tool/method. The manager has to use sound judgment in deciding which method is appropriate for the project. The factors that can affect the decision to select a particular model include industry type, phase in the product/system lifecycle, time and resources available for risk assessment, and scope/level to which risks need to be identified. If risk is to be assessed at the core

component level, FMEA, FTA, and RED are useful. If human errors and organizational shortcomings need to be captured, the Swiss Cheese Model or/and LOPA are useful. If overall safety of the system needs to be ensured, then LOPA is a useful technique to use.

Exhibit 9: Summary of Risk Assessment Tools

Risk Assessment Tool	Advantages	Disadvantages
Failure Mode and Effects Analysis	- Very efficient if applied to the system as a whole - Structured, detailed approach - Prioritizes product/process deficiencies - Identifies and eliminates potential failure modes early in the development phases	- Not easy to build if the system consists of a number of components with multiple functions - Only considers hazards that lead to failure, does not consider hazards that result from normal operations - Time consuming, expensive to build and very detailed - Does not consider failures resulting from human error
Fault Tree Analysis	- Visual, depicts the cause-and-effect relationship between the root cause events - Provides Both qualitative and quantitative results - Concentrates on one particular failure at a time	- Does not capture all failure related to human due to the complexity of human behavior - Time consuming and lengthy - Latent hazards are not addressed - Requires an expert to identify potential risks
Risk in Early Design	- Utilizes historical knowledgebase to produce potential risks - Well-suited for novice engineers - Identifies risk in the early design phase	- Potential risk may be over or under quantified - Does not account for human error

Layer of Protection Analysis	- 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
Swiss Cheese Model	- Tracks accident causations at different levels of the organization - Does not blame individuals	- Applicable only when human interacts with the system - Does not expose component level issues

References

Center for Chemical Process Safety, *Layer of Protection Analysis - Simplified Process Risk Assessment.* New York: Center for Chemical Process Safety/AIChE, (2001).

Altabbakh, Hanan, & Murray, Susan L., Applying The Swiss Cheese Model of Accident Causation, *Annual International Conference of the American Society for Engineering Management*, Lubbock: Curran Associates, Inc., (October 2011), pp. 301

Bertsche, Bernard, *Reliability in Automotive and Mechanical Engineering,* Berlin: Springer, (2008).

Booher, Harold R., *Handbook of Human Systems Integration,* New York: John Wiley and Sons, (2003).

Covello, Vincent T., & Merkhofer, Miley W., *Risk Assessment Method: Approaches for assessing health and environmental risks,* New York: Plenum Press, (1993).

Damle, Siddharth B., & Murray, Susan L., Using LOPA to Analyze Past Catastrophic Accidents Including 2008 The Mortgage Market Crises and Space Shuttle Challenger Disaster, submitted *to The Journal of Loss Prevention in the Process Industries*, (January 2012).

Dekker, Sidney, *The Field Guide to Human Error Investigations.* Burlington, VT: Ashgate, (2002).

Dhillon, Balbir S., *Design Reliability: Fundamentals and applications,* Boca Raton: CRS Press, (1999), pp. 128.

Dhillon, Balbir S., *Design Reliability: Fundamentals and applications,* Boca RAton: CRC Press, (1999), pp. 147.

Dowell, Arthur M., Layer of Protection Analysis and Inherently Safer Processes, *Proces Safety Progress , 18* (4), (1999), pp. 214-220.

Eccleston, Charles H., *Environmental Impact Assessment: A guide to best professional practices,* Boca Raton, FL: CRC Press, (2011).

Foster, Mollie, Beasley, James, Davis, Brett, Kryska, Paul, Liu, Eddie, McIntyre, Andy, Sherman, Mike, Stringer, Brett, Wright, James, *Hazards Analysis Guide: A Reference Manual for Analyzing Safety Hazards on Semiconductor Manufacturing Equipment.* International SEMATECH, www.sematech.org/docubase/document/3846aeng.pdf, (1999).

Frederickson, Anton. A., *The Layer of Protection Analysis (LOPA) method,* Retrieved 20-February 2012 from www.jlab.org/accel/ssg/safety/lopa.pdf, (April 2002).

General Monitors, Retrieved 20-February 2012 from Protection Layers: http://www.gmsystemsgroup.com/sil/sil_info_lopa.html, (July 2011).

Grantham, Katie L., Stone, Robert, Tumer, Irem Y., The Risk in Early Design Method, *Journal of Engineering Design, 20*:2 (2009), pp. 155-173.

Gulland, G. William, Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons. *Proceedings of the Safety-Critical Systems Symposium* , (February 2004), pp. 105-122.

Henley, Ernest J., & Kumamoto, H., *Reliability engineering and risk assessment,* New Jersey: Prentice-Hall, (1981).

Hollywell, Paul D., Incorporating human dependent failures in risk assessments to improve estimates of actual risk, *Safety Science, 22* (1996), pp.177-194.

Ireson, W. Grant, Coombs, C. F., & Moss, R. Y, *Handbook of Reliability Engineering and Management second Edition,* New York: McGraw-Hill, (1995).

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

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

Letens, Geert L., Van Nuffel, Lieve, Heene, Aime, & Leysen, Toward a Balanced Approach in Risk Identification, *Engineering Management Journal, 20*:3 (January 2008), pp. 3-9.

Luxhoj, James T., & Kauffeld, Kimberlee, *Evaluating the Effect of Technology Insertion into the National Airspace System,* Retrieved 20-February 2012 from The Rutgers Scholar: http://rutgersscholar.rutgers.edu/volume05/luxhoj-kauffeld/luxhoj-kauffeld.htm, (2003).

Markowski, Adam S., & Mannan, M. Sam, ExSys-Lopa for the Chemical Process Industry, *Journal of Loss Prevention in the Process Industries , 23*:6 (2010), pp. 688-696.

Maytorena, Eunice, Winch, Graham M., Freeman, Jim, & Kiely, Tom, The Influence of Experince and Information Search Style on Project Risk Identification Performance, *Engineering Management Journal, 54*:2 (2007), pp. 315-326.

Murray, Susan L., Grantham, Katie, & Damle, Siddharth B., Development of a Generic Risk Matrix to Manage Project Risks, *Journal of Industrial and Systems Engineering, 5*:1 (2011), pp. 320-336.

NASA, *Preparing Hazard Analyses - Safety test operation division.* Houston: National Aeronautics and Space Administration, (2001).

NASA, Space Shuttle Weather Launch Commit Criteria and KSC End of Mission Weather Landing Criteria, (2010).

National Research Council, *Challenger Evaluation of Space Shuttle Risk Assessment and Management.* Washington, DC: National Academy Press, (1988).

National Research Council, *Human-System Integration in the System Development Process: A New Look.* Washington, DC: The National Academies Press, (2007).

National Research Council, *Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management,* (S. A. Committee on Shuttle Criticality Review and Hazard Analysis Audit, Ed.) Washington, DC: The National Academic Press, (1988).

OHSAS, *18001:2007*, Occupation Health and Safety Assessment Series, (July 2007).

Orasanu, Judith M., *Decision Making in the Cockpit. In E.L. Wiener, B.G. Kanki, and R.L. Helmreich (Eds.), Cockpit resource management,* San Diego, CA: Academic Press, (1993).

Qureshi, Zahid H., *A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems,* Edinburgh, Australia: Defence Science and Technology Organization, (2008).

Reason, James, Human Error: Models and Management, *BMJ , 320*:7237 (2000), pp. 768-770.

Reason, James, *Managing the Risks of Organizational Accidents,* Burlington, VT: Ashgate, (1997), pp. 15-18.

Reason, James, *Managing the Risks of Organizational Accidents,* Burlington, VT: Ashgate, (1997), pp. 9-11.

Shappell, Scott A., & Wiegmann, Douglas A., *The Human Factors Analysis and Classification System – HFACS,* Washington, DC: Federal Aviation Administration, (2000).

Shappell, Scott A., Detwiler, Cristy, Colcomb, Kali, Hackworth, Carla, Boquet Albert, & Wiegmann, Douglas A.,Human Error and Commercial Aviation Accidents: An Analysis

Using the Human Factors Analysis and Classification System, *The Journal of the Human Factors and Ergonomics Society,* 49:2 (April 2007), pp. 227-242.

Stamatelatos, Michael, & Dezfuli, Homayoon, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,* NASA, Washington DC: NASA, (2011).

Stamatelatos, Michael, Vesely, William, Dugan, Joanne, Fragola, Joseph, Minarick III, Joseph, & Railsback, *Fault Tree Handbook with Aerospace Application,* NASA, (January 2002).

Stamatis, Dean H., *Failure Model Effect Analysis,* Milwaukee: ASQ, (2003).

Summers, Angela E., Introduction to Layer of Protection Analysis, *Mary Kay O'Conner Process Safety Center Symposium*, (October 2002).

U.S. Presidential Commission, *Report on the Space Shuttle Challenger Accident,* http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html, (1986).

Wiegmann, Douglas. A., & Shappell, Scott. A., *A Human Errorr Approach to Aviation Accident Analysis: The Human Factors Analysis and Classififcation System*, Burlington, VT: Ashgate, (2003).

Winsor, Dorothy A., Communication failures contributing to the Challenger accident: an example for technical communicators, *IEEE Transactions on Professional Communication, 31*:3 (1988), pp. 101-107.

III. 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 Systems

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.

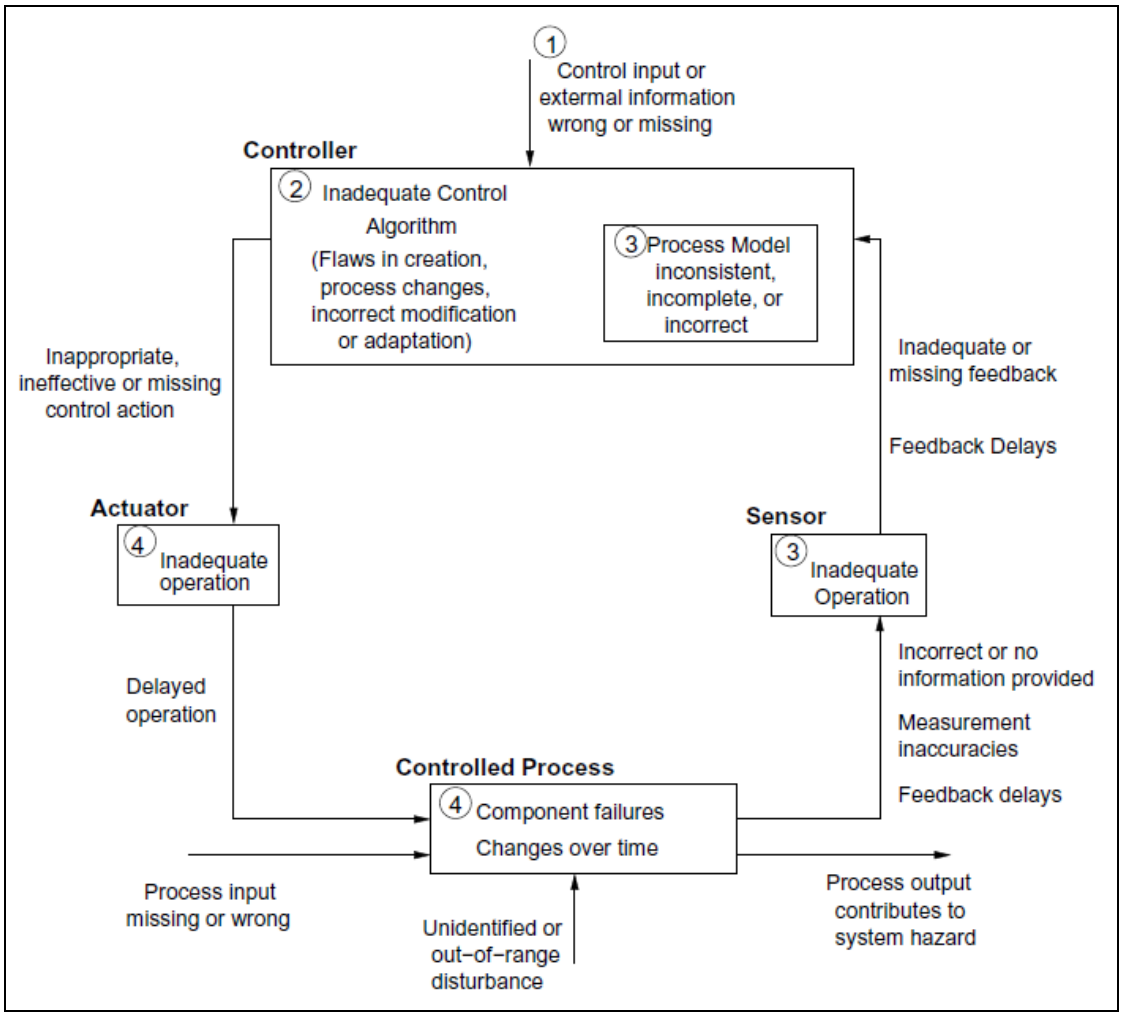


Figure 1: Classification of Control Flaws Leading to Hazards (Leveson, 2012).

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.

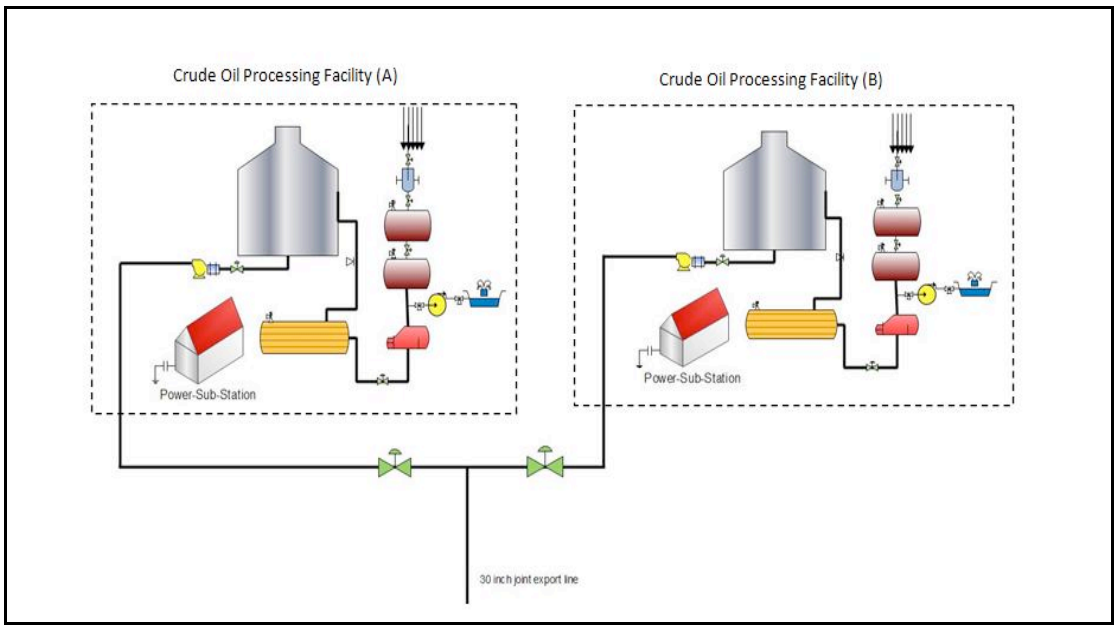


Figure 4: Layout of crude oil processing facilities (A) and (B)

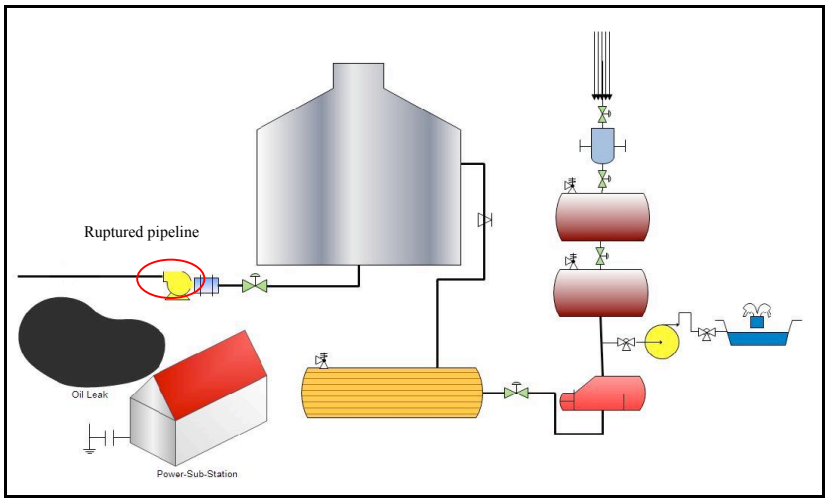


Figure 5: Oil leak and in Facility (B)

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.

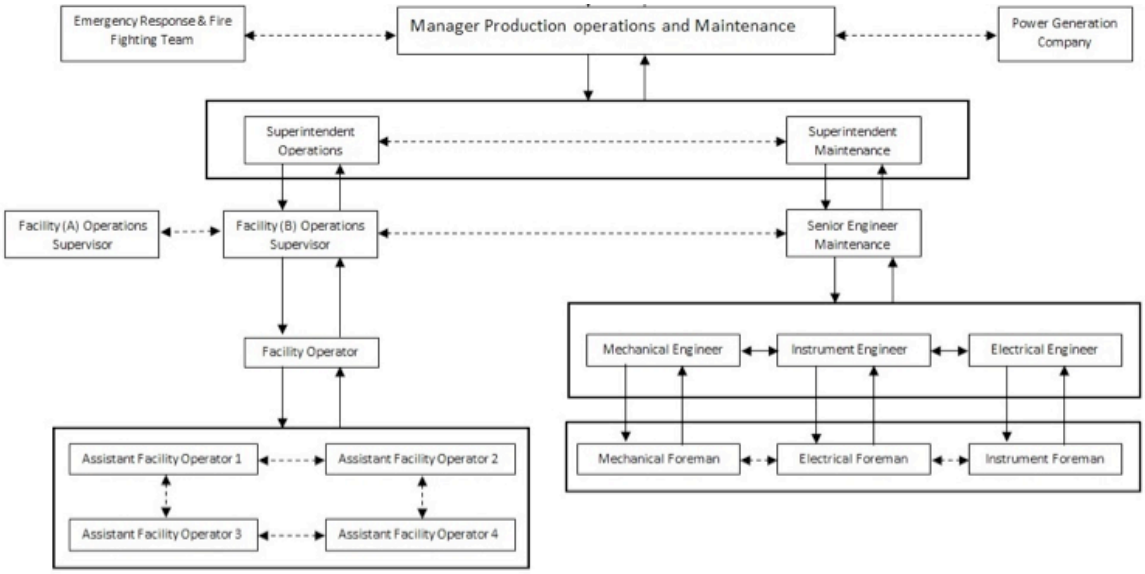


Figure 6: Hierarchical Level Control Structure of Company XYZ

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: Asource 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.

IV. TOWARDS QUANTIFYING THE SAFETY COGNITION IN THE UNDERGRADUATE ENGINEERING STUDENT

Hanan Altabbakh
Missouri S&T
Rolla, MO, USA

Dr. Katie Grantham
Missouri S&T
Rolla, MO, USA

ABSTRACT

Accidents among young engineers in school's workshops and labs are relatively frequent, among which were severe injuries and tragic fatalities. Students participate in various engineering design competition teams where they spend time in labs and/or workshops and other hazardous environment. Consequently, underestimating the safety mindset, which is essential in various phases of any project. These engineers will be part of a task force and progress in ranking within the organization and inherit a safety culture for the younger engineers to pursue. In an effort to prevent such accidents and improve safety cognition in young engineers, this study examines the training exposure and knowledge within engineering competition teams from the students' perspectives. A survey targeting different OSHA safety areas was conducted to measure safety attitudes of these young engineers. The paper, also, explores potential causes that can prevent these engineers from making appropriate decisions from a safety prospective.

INTRODUCTION

Young engineers who participate in various design teams spend time in their workshops where they encounter different types of hazardous and flammable materials, machines, and other hazardous environment. In addition, other young scientists undergo lab experiments as part of their curricular. However, without the adequate amount and utilizing of safety knowledge, these young engineers are vulnerable to avoidable tragic accidents. In the past decade, there have been great concern regarding the frequency of academic laboratory accidents occurring across the country, among which were severe injuries and deaths. A graduate student lost three fingers, burned his hands and face, and injured one of his eyes at a chemistry lab at Texas Tech university (U.S. Chemical Safety and Hazard Investigation Board, 2010). Another 23 year old female student died of second and third degree burns over 43% of her body while doing a research experiment in the UCLA lab (Christensen, 2009). An unfortunate student died of asphyxiation due to neck compression when her hair got caught in one of Yale University's shop's lathe machine (Henderson, Rosenfeld, & Serna, 2012). Moreover, Four students from the University of Missouri were severely injured during hydrogen explosion in June, 2010 (U.S. Chemical Safety and Hazard Investigation Board, 2010). There are few examples of recent tragic accidents that resulted in injuries, fatalities, and financial losses, not to mention school reputation.

Such examples of fatal accidents, along with other non-fatal ones, indicate that perhaps young college students lack the safety awareness that could prevent such tragedies.

These young engineers are part of future US workforce where employment reached 19.5 million young worker (between the age of 16 and 24 years old) in July 2012 that is 2.1 million increased compared to 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. Further more, 7.9 million nonfatal injuries treated in emergency departments (Centers for Disease Control and Prevention (CDC), 2010). In order to identify the lack in safety training within students, a survey was conducted to measure safety training, knowledge and attitude of these young engineers.

LITERATURE REVIEW

Researchers have indicated that young workers are more at 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 prefer activities with higher sensation- seeking than adults (Zuckerman, 1979). Numerous research have discussed the variables that account for such behavior in emerging adults. Immaturity in decision-making in young adults might be categories to cognitive and psychosocial factors (Steinberg & Cauffman, 1996). Theories have tackled the risk taking behavior in emerging adults and adolescents and they all revolve around three essential forms. First, biological based on hormonal effects, asynchronous pubertal timing, or generic predispositions. Second, psychological or cognitive deficiencies in self-esteem, cognitive immaturity, affective disequilibrium, or high sensation seeking. Third, environmental causes that focus on social influence related to family and peer interactions, or community and societal norms (DiClemente, Hansen, & Ponton, 1995). Based on that, it

is essential to measure the safety knowledge and attitude of these young engineers and identify any safety training deficiencies to prevent undesired outcomes.

METHODOLOGY

In order to measure safety training, knowledge and attitude of young engineers, a survey was constructed based on the Goal Question Metric approach with reference to OSHA Guidelines 54 Fed Register #3904-3916. The GQM method required a top down methodology in constructing the survey. First, goals need to be specified and focused on.

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 24 items together with four demographic questions was used to collect the data. The goal of the survey as depicted in Table 1, was to determine the amount of training the student have on OSHA procedures, his/her knowledge of general safety procedures they think they have versus what they actually do, their safety attitude and consciousness. Five questions were asked about the amount of training that the young engineers had on personal protective equipment (PPE), lockout/tagout, material safety data sheets, machine guarding and evacuation in case of an emergency based on 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 the labs or workshops. Finally one question to discuss their safety consciousness as a self-assessment.

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?	
	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

RESULTS AND ANALYSIS

A total of 93 questionnaires were returned including responses that have answered some of the survey questions. 68% of the respondents were male, 31% were female, and 1% preferred not to answer. The majority of the respondents' were undergraduate students ranging between 32% seniors, 25% juniors, 18% freshman, and 17% sophomore, where the others were 3% Alumni and 3% graduate students with 95% of the total students majoring in Engineering. 95% of the students were either involved in one or more design teams in the present or have been involved in the past and only 5% were never involved in any design team. 97% of the students responded positively with regard to receiving any types of safety training during college education or job safety training such as OSHA 10 hour training, first aid CPR and AED, high school shop training, etc.

Goal one: Evaluate the amount of safety training of Missouri S&T design team members

When analyzing the students feed back 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. This shows that the majority of these young engineers have been working in the labs or workshops without the proper training, which makes them vulnerable to make unfortunate accidents.

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

The amount of knowledge these young engineers have is insignificant. Less than 50% of the students recognized the correct procedures of safety in the workshops and labs, which is evidence that their students lack the basic safety procedure knowledge.

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

About 30% of the respondents would often follow safety procedures while they are in workshops or labs working on their projects. The majority of students would either follow the procedures occasionally or only when forced to.

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

The respondents were requested to evaluate their self-consciousness toward overall safety; one can predict the response reading the analysis above. 58% of the respondents find themselves as safety conscious when self-asses themselves, 25% find themselves very conscious, 14% are neutral, and 3% are very conscious.

CONCLUSION

There are some remarkable findings that were attained from this survey. Most of the findings show that young engineers have been receiving informal training. Informal safety training are often ineffective and does not always assure positive safety attitude or safety performance, it actually can lead to death, injury, pain and economic loss (Whiles, 1999). Training should be conducted through educational institutes 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. It is noticed that 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). A strong safety culture is required to protect employees but is especially important in protecting students and in developing students' skills and awareness of safety. Thus, students will acquire the skills to recognize hazards, to assess the risk of exposures to those hazards, to minimize the risk of exposures to hazards, and to be prepared to respond to laboratory emergencies (Committee on Chemical Safety, 2012).

The findings of this survey showed that the respondents' knowledge of five domains of the OSHA guidelines was inadequate specifically with regards to PPE, LOTO, MSDS, Machine guarding, and Emergency action plan. Consequently, it reflected on their attitude toward the risk that might come from their areas of occupational safety and health. For young engineers and scientist in the work force, the technical promotion ladder places them within future management and decision-making

positions. (Allen & Katz, 1986). Engineers with high-potentials rapidly rise within their organizations to positions of great distinction and leadership and they are competent in transforming their acquired educational knowledge and skills into successful entrepreneurial ventures (Hissey, 2000). Those young engineers are the future managers of the organizations. Thus, training them at younger age would shape their safety attitude positively to be inherited within the organization once they rank higher. Managers and supervisors play an essential role in creating a safety climate within the organization the safety culture that the managers and supervisors create within the organization have a great impact perceptions of safety climate, which in return will influence the employees' safety performance (Thompson, Hilton, & Witt, 1998). Safety is a positive value – it prevents injuries, saves lives, and improves productivity and outcomes. When safety is actively practiced, and is regarded as a critical core value by organizational leaders, it bestows a sense of confidence and caring in all working there (Committee on Chemical Safety, 2012).

REFERENCES

- Allen, T. J., & Katz, R. (1986). The dual ladder: motivational solution or managerial delusion? *R & D management* , 185-197.

- 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.

- 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/

- Hissey, T. (2000). Education and careers 2000. Enhanced skills for engineers. *PROCEEDINGS OF THE IEEE* , *88*, pp. 1367-1370.

- 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.

- 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.

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

- 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.

SECTION

2. CONCLUSION

The different risk management models utilized in the case studies showed their competency in identifying potential risks of the system's lifecycle. FMEA, FTA, and RED address risks at the component and sub-system level, the Swiss Cheese Model focus on risks related to human system interaction. Moreover, LOPA contemplate the system in its entirety and designs defense layers to protect the system from an adverse outcome.

Finally, STAMP is a holistic model that identifies the reason why those safety constraints in place were not effective in the first place.

The phase of risk identification dictates the different risk management models discussed in the paper. For example, FMEA, with its capability in identifying failure modes, is suitable in the preliminary design phase to prevent such failures by taking the necessary cautiousness based on occurrence/severity ratings. RED can identify potential failures of a product, as early as the conceptual phase, throughout the historical database imbedded in the software. This is advantageous as RED can minimize any decision making preconceptions. FTA considers all potential causes resulting in undesired consequences. All these causes can be evaluated to assure the stability of the system where engineering managers lead these evaluation sessions. However, and regardless of their potential in risk identification, both FTA and FMEA are time and recourses consuming and they lack the ability to target human errors as potential cause of failure.

The Swiss Cheese Model is beneficial when human system interaction is involved in identifying risks. The model constructs defensive layers in the system and focuses on human errors and human factors when assessing risk. The model suggest that in order for an accident to occur all the safeguards in the system have to be breached with a trajectory that passes through all the holes, which includes unsafe acts and latent conditions. Thus, Swiss Cheese Model will not be applicable if one of the defensive layers is missing.

Layer of Protection Analysis (LOPA) utilizes the known risk to construct defensive layers to protect the designated system. LOPA is a scenario-based approach, which allows the managers to address probable mitigation tools to reduce undesired consequences, including both human and organizational factors, which makes it unique among other models. Yet, LOPA is project specific, which requires past knowledge and experience since it not generic to all systems.

System Theoretic Accident Model and Processes recognizes the violation against the existence safety constraints at each level of the hierarchy of any system. The model main concern is why these safety controls were not effectively enforced if they have adequately been designed at the first place. However, in order to utilize this model, system hierarchy of the accident and accident report must be available for investigators to successfully apply the model.

There is no risk assessment model that is able to identify all potential risks. Engineering managers need to address and weigh their options when deciding which method is appropriate for the project. Industry type, product/lifecycle phase, scheduling, available recourses, and risk level identifications are important factors to consider in selecting the proper risk assessment model. FMEA, FTA, and RED can be utilized at the

core component level. Swiss Cheese Model and/or LOPA can trigger human errors and organizational shortcomings. However, LOPA and STAMP is a beneficial technique to use if overall safety of the system is the aim of the evaluator.

VITA

Hanan Altabbakh was born in Kuwait. She received her Bachelor of Science degree in Industrial and Management Systems Engineering from Kuwait University in 2005. She worked at the ministry of education – Kuwait as an Industrial Engineer specialized in building safety. After that she transferred to building maintenance department where her expertise was utilized in construction quality assurance.

She started her Masters of Science program with Engineering Management Department at Missouri University of Science and Technology in August 2009. She received her Masters In Engineering Management in December 2010.

Hanan Altabbakh entered the PhD program in Engineering Management at Missouri University of Science and Technology in the January of 2011. Her main area of research is Risk Assessment and Safety. She received her PhD in December 2013.

Hanan Altabbakh worked as a graduate research assistant for three years in the Engineering Management Department at the Missouri University of Science and Technology. She is a member of Tau Beta Pi; National Engineering Honor Society, as well as the American Society of Engineering Management.