Fall 2012

Analyzing risk and catastrophic accidents: using LOPA and human factors to improve safety in generic projects

Siddharth B. Damle

Department: Engineering Management and Systems Engineering

ANALYZING RISK AND CATASTROPHIC ACCIDENTS: USING LOPA AND HUMAN FACTORS TO IMPROVE SAFETY IN GENERIC PROJECTS

by

SIDDHARTH B. DAMLE

A DISSERTATION

Presented to the Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

ENGINEERING MANAGEMENT

2012

Approved by:

Susan Murray, Advisor
Katie Grantham
Elizabeth Cudney
Steven Corns
Neil Book
Sam Mannan

PUBLICATION DISSERTATION OPTION

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

(1) Pages 8 to 35 "*Development of a Generic Risk Matrix to Manage Project Risks*" is in the style required by the Journal of Industrial and Systems Engineering (JISE). It has been accepted and published. The citation is:
Murray S., Grantham K., Damle S. (2011). Development of a Generic Risk Matrix to manage project risks. Journal of Industrial and Systems Engineering, Volume 5, No.1, Spring 2011. Pg 320-336.

(2) Pages 36 to 62 Damle S., Murray S. "*Using LOPA to analyze past catastrophic accidents including the 2008 Mortgage Market Crisis and Space Shuttle Challenger Disaster*" is in the style required by Journal of Loss Prevention in Process Industries. It is an invited article. It has been submitted and is under review.

(3) Pages 63 to 93 Altabbakh H., Murray S., Damle S., Grantham K. "*Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster*" is in the style required by Engineering Management Journal. It has been accepted for publication in the special issue on Risk.

The Introduction, Literature Review, Conclusions, and Appendix have been added to maintain the flow of the dissertation.

ABSTRACT

Risk assessment and identification in the early stages of any project is critical to the success of that project from time, budget and cost prespective. Identifying unacceptable risks and making provisions to mitigate those, can reduce the uncertainty in the project and ensure its smooth completion and closure. Various techniques have been developed over time to identify and quantify risks. Inspite of all the available research on risk management tools, accidents continue to happen and projects consistently fail.

The objective of this study is to first, determine the generic risks that can be encountered by a project. A list of generic risks will be prepared and validated by surveying managers from various industries. These risks will be prioritized to provide managers with a generic risk matrix which can be readily applied to cross-industry projects. The second part of the study involves the use of Layers of Protection Analysis (LOPA), to analyze two past catastrophic accidents. The financial industry and the Space Shuttle program will be considered to produce the required analysis. LOPA models will be created to expose shortcomings in the failed projects and provide lessons to be learned in order to avoid future disasters. This research will provide a unique direction and a new tool for project managers to deploy this technique of building protection layers to prevent, protect and/or mitigate risks encountered by their system/project. The dissertation includes three journal papers, one published in the Journal of Industrial and Systems Engineering, one accepted in Engineering Management Journal and one under review.

ACKNOWLEDGMENTS

Throughout my stay here at Missouri University of Science and Technology, several people have supported me both academically and personally inspired me. I owe my deepest gratitude to Dr. Susan Murray, who gave me an opportunity to conduct research under her supervision. Dr. Murray has helped me in several ways at times when I needed support. I have to thank her for believing in me and allowing me to conduct research in my field of interest under her able guidance. Without her direction and persistent help this dissertation would not have been possible.

I would also like to thank my committee members Dr. Katie Grantham, Dr. Elizabeth Cudney, Dr. Steven Corns, Dr. Neil Book and Dr. Sam Mannan who helped me with my research through the years of my PhD. I want to take this opportunity to thank MKOPSC (Texas A&M University) for supporting my research idea.

In addition, I want to thank Department Chairs and Professors Dr. William Daughton and Dr. David Enke for their direct and indirect support in completing this work.

I am grateful to all the professors and staff who have helped build my overall profile over the years through coursework and projects. I appreciate their support and valuable suggestions in accomplishing my tasks.

I would not miss this opportunity to express gratitude to my family for showing faith in me and supporting me in all my big decisions. It was their love and efforts that I could make it successfully to this day though all the ups and downs. I would also express my heartfelt thanks to my aunt, uncle and cousins, without whom higher studies in the US might not have been possible.

I cannot thank my friends enough, who made my life so much easier while being away from family. My life in Rolla has been memorable owing to all my friends who supported me all through my years at MST and made my student life all the more enjoyable.

TABLE OF CONTENTS

Page

PUBLICATION DISSERTATION OPTION iii
ABSTRACT iv
ACKNOWLEDGMENTS v
LIST OF ILLUSTRATIONS ix
LIST OF TABLES x
SECTION
1. INTRODUCTION 1
1.1 BACKGROUND 1
1.2 RESEARCH OBJECTIVES 2
1.3 RESEARCH METHODS 3
1.4 RESEARCH CONTRIBUTION 4
1.5 DISSERTATION OUTLINE 5
2. LITERATURE REVIEW 6
PAPER
I. Development Of A Generic Risk Matrix To Manage Project Risks 8
Abstract 8
1. INTRODUCTION 9
2. RELATED WORK 10
2.1. Risk Identification Techniques 10
2.2. Risk Assessment Techniques 13
3. GENERIC RISK MATRIX APPROACH 16
3.1. GRM Risk Categories 17
3.2. GRM Probability and Impact Assessment 18
3.3. GRM Survey 20
3.4. Survey Results 21
4. CASE STUDY 28
5. CONCLUSIONS AND DISCUSSION 31
REFERENCES 32

II. USING LOPA TO ANALYZE PAST CATASTOPHIC ACCIDENTS INCLUDING 2008 MORTGAGE MARKET CRISIS AND SPACE SHUTTLE CHALLENGER DISASTER 36
Abstract 36
Introduction 37
LOPA Method 38
Case I- Mortgage Market Crisis 41
Secrutization- Collateralized Debt Obligations 43
Credit Default Swaps 45
The Model 47
How the Layers Failed 52
Case II- Space Shuttle Challenger Disaster 54
LOPA Model 55
Estimating Probability to Fail on Demand (PFD) 58
Conclusion 59
References 61
III. VARIATIONS IN RISK MANAGEMENT MODELS: A COMPARATIVE STUDY OF THE SPACE SHUTTLE CHALLENGER DISASTER 63
Abstract 63
Introduction to Risk Assessment 63
Space Shuttle Challenger Disaster 65
Product Based Risk Assessment Tools 67
FMEA 67
FTA 68
RED 70
Using RED to Analyze the Space Shuttle Challenger Disaster 70
Findings 71
Process Based Risk Assessment Tools 72
LOPA 72
Using LOPA to Analyze Space Shuttle Challenger Disaster 74
Human Factors Analysis & Classification System (HFACS) 76

Using Swiss Cheese Model to Analyze the Space Shuttle Challenger Disaster 78

Findings 80

Conclusion 81

References 83

SECTION

3. CONCLUSIONS 94

3.1 SUMMARY 94

3.2 FUTURE RESEARCH 96

APPENDIX 98

BIBLIOGRAPHY 116

VITA 117

LIST OF ILLUSTRATIONS

Figure Page

Paper 1

1. Simplified Risk Matrix 19
2. Impact-Risk Combinations with Weights 20
3. Project Size 22
4. Use of Risk Management 22

Paper 2

1. Protection Layers 39
2. LOPA Process 40
3. Subprime Lending 42
4. CDO Structure 45
5. CDS Block Diagram 46
6. LOPA Model for Mortgage Market 48
7. Layer Definitions 49
8. LOPA Model for Challenger Disaster 56
9. Layer Definitions and Flow 56

Paper 3

1. The Consequences Classification System 87
2. RED Results for SRB Analysis 87
3. Examples from detailed RED report 88
4. Protection Layers 89
5. LOPA Model for Challenger Disaster 90
6. Layer Definitions and Flow 91
7. Adapted from Reason's Swiss Cheese Model 92
8. The HFACS framework 93

LIST OF TABLES

Table Page

Paper 1

1. Previous Studies Categorizing Risks in Specific Projects 14
2. Risks Ranked 24
3. Risks Rated for Probability and Impact 26
4. Generic Risk Matrix 28
5. Case Study Results 30

1. INTRODUCTION

1.1 BACKGROUND

Risk identification, assessment, management, and communication are phases of risk analysis. Risk management (RM) is an important aspect for improving project performance and successfully completing projects on schedule and within cost. Since every project is unique in terms of risk, assessing risks in terms of probability and impact is challenging and time consuming (Murray, Grantham & Damle, 2011). Risk management is one of the most important aspects of corporate and project management. Managing risk at an early stage can avert occurrence of undesirable consequences. There needs to be some amount of risk to make the project/program attractive in its returns. Risk can be both positive and negative. Positive risk is the one which when undertaken can yield in positive consequences and increase the returns from the project.

The first step is risk identification. It is necessary to identify most risks associated with the project as the beginning. Risks which are not identified cannot be assessed. An unidentified risk can cause problems with the progress and success of the project. Risks can be identified using a number of methods including historical data, expert opinions and market surveys. These methods can help in making a list of most severe and/or common risks as well as industry specific risks.

The next step is risk assessment. Assessing risks involves ascertaining the likelihood and severity of the impact of the risks that have been identified. This process also needs some expertise. An organization needs to develop a specific risk matrix which outlines the firm's risk tolerance level. Accordingly the likelihood-impact matrix can show the risks that are not tolerable and appropriate actions need to taken to eliminate the risk or mitigate the severity of the consequence. Some techniques use the risk factor number which a product of probability of occurrence and consequence severity. The first paper, published in the Journal of Industrial and Systems Engineering, describes a

Generic Risk Matrix (GRM) technique to assess risks in most common projects. It provides a list of risks along with their likelihood and severity estimates taken from surveying industry project managers.

Risk analysis can be performed by quantitative tools like Failure Mode Effect Analysis (FMEA), Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). As useful as these techniques are, they are more time consuming and can also require a lot of resources. The next paper introduces a relatively new technique known as Layer of Protection Analysis (LOPA) which is a semi-quantitative risk assessment technique used by the chemical process industry. It discusses the application of this technique to the past disasters to expose safety shortcomings. This tool can be successfully applied to projects from other industries with the help of historical data and suitable assumptions.

1.2 RESEARCH OBJECTIVES

The first objective of this research is to develop a generic risk matrix. This will include a list of most common risks encountered by project managers. These risks will then need to ranked based on their importance in terms of probability of occurrence and severity of consequence. The result would be a ready-to-use risk matrix which managers can use on their projects in addition to their own project specific risks.

The second objective is to study the Layer of Protection Analysis (LOPA) which is used in the chemical process industry. The goal of the research is to test the feasibility of application of this technique to generic projects for managing risks. Past accidents will be analyzed using LOPA to check if the tool is effective in exposing problems that caused the disasters. This part of the research will focus on providing a solution to avoid similar disasters in future. This paper was presented at the Mary Kay O'Connor Process Safety Center's (MKOPSC) 2011 Annual Symposium at Texas A&M and invited to the Journal of Loss Prevention in Process Industries.

The next goal is to model the mortgage market using LOPA. The financial industry being fragile since the market crisis of 2008, this model should help protect the

system through deployment of protection layers. A quantifiable risk reduction should be achieved with available historic data and suitable assumptions. A set of system level recommendations for improvements will be made in line with the model. A journal paper will be submitted to a finance journal.

Another objective of this research is to compare three risk assessment techniques by applying them to the Space Shuttle Challenger Disaster. This case study will give an insight into the use of RED, Swiss Cheese and LOPA at varying levels during a project. The effectiveness as well as the shortcomings of each of these tools will be discussed. This paper is submitted to the Engineering Management Journal's special issue on Risk Management.

1.3 RESEARCH METHODS

For the development of a generic risk matrix, a literature review will be conducted to get a list of risks currently faced by managers from various industries. The list will then be narrowed and the surveying technique will be used to develop a matrix. A survey will be designed to rank the importance the risks and get an industry perspective with regards to their probability and impact. The survey will be deployed to project managers from a variety of industries. Their responses will be recorded and the risks weighted, to rank them in order of their importance. A case study will be presented to validate the application and use of this matrix in managing project risks.

Since LOPA is new to non-process industries, the study will involve basic literature review on its fundamentals and methods to apply it to manage risk. Two past catastrophes will be considered, one the Space Shuttle Challenger Disaster and the 2008 Mortgage Market Crisis. Further literature review will be conducted to study the causes of these accidents and inquiry reports. LOPA guidelines will be used to model these disasters with a view of risk management and safety.

1.4 RESEARCH CONTRIBUTION

The initial contribution of the research is to provide project managers with a ready-to-use tool for risk analysis. A set of generic risks ranked according to their importance gives managers a head start at managing and taking actions to prevent applicable risks. The manager then has to consider project specific risks if they do not fall under one of the generic categories presented in this research. The generic risk matrix considers the probability and impact of each of the chosen risks and gives the manager a guideline towards prioritizing actions to prevent/mitigate these risks.

One of the most important contributions of this research is to apply LOPA to ensure safety of systems with a broad industry wide approach. LOPA is an evolving risk assessment technique and its use was restricted to the chemical process industry until now. It is a simple intuitive tool that can be used to enhance the safety of systems to avoid disasters/accidents. The deployment of layers of protection ensures a huge reduction in the frequency of occurrence of the undesired consequence. This research provides an example of application to LOPA to the finance industry, which can be extremely useful considering the current global financial turmoil. Besides such applications, LOPA can also be used to manage risks in big programs like the Space Shuttle program to reduce the chances of accident occurrence.

The research contributes by providing methods to extract failure data. Most industries do not have documented failure data. Even if data is available, few assumptions need to be made regarding time span of historical data, interpretation of data, etc. Once the technique is widely used and evolved, data can be collected and standards can be written for specific industries. With a reference for the probability values, a quantified risk reduction can be easily achieved and the use of this technique can be strongly justified.

1.5 DISSERTATION OUTLINE

The dissertation is presented as a publication option, which consists of three journal articles, which are presented as sections. Following the Introduction, the first paper “Development of a Generic Risk Matrix for Managing Project Risks” is presented. This is followed by “Using LOPA to Analyze Past Catastrophic Accidents including the 2008 Mortgage Market Crisis and Space Shuttle Challenger Disaster” and “Variations in Risk Management Models: A Comparative Study of the Space Shuttle Challenger Disaster” papers. Section 6 summarizes the findings and implications of the dissertation and concludes with future research.

2. LITERATURE REVIEW

This literature review introduces topics that form the basis of the three articles. Additional literature review is presented for each manuscript.

Risk assessment is carried out using many techniques today. A major percentage is done using qualitative analysis, very few instances use the full quantitative risk assessment (QRA). About 5-10% of cases need the semi-quantitative approach (Bridges & Clark, 2009) since qualitative methods are not adequate enough and fully quantitative methods consume too much time and resources.

Layers of Protection Analysis falls in the semi-quantitative category. This technique is a simplified process of quantitative risk assessment, using the order of magnitude categories for initiating cause frequency, consequence severity, and the likelihood of failure of independent protection layers to analyze and assess the risk of a particular accident scenario. LOPA requires applying the qualitative hazard evaluation methods to identify accident scenario including initiating causes and pertinent safeguards (Markowski & Mannan, 2009). LOPA is not just another hazard assessment or risk assessment tool. It is an engineering tool used to ensure that process risk is successfully mitigated to an acceptable level. LOPA is a rational, defensible methodology that allows a rapid, cost effective means for identifying the Independent Protection Layers (IPLs) that lower the frequency and/or the consequence of specific hazardous incidents. LOPA provides specific criteria and restrictions for the evaluation of IPLs, eliminating the subjectivity of qualitative methods at substantially less cost than fully quantitative techniques (CCPS, 2001).This method has been used in the chemical process industry to protect systems from hazards. Over the years, a lot of research has been put into perfecting the method and also incorporating human error into the assessment. It is generally believed that 50-90% of the process accidents can be attributed to human failures (Baybutt, 2002).

There seemed to be no existing literature on application of LOPA beyond the chemical process industry. This gave the idea of attempting to model a generic accident to check feasibility of application. Many catastrophic incidents were reviewed which could be used for this research. The 2008 mortgage market crisis and Space Shuttle Challenger disaster were chosen to be modeled. These represented two entirely new industries and related disasters which would prove feasibility of LOPA.

The analysis of the 2008 mortgage market crisis reveals systemic issues. The Challenger case also exposes decision making flaws and poor safety culture within the organization. The literature related to the two cases has been presented in the respective journal papers.

PAPER

I . Development of a Generic Risk Matrix to Manage Project Risks

Susan L. Murray[1], Katie Grantham[2], Siddharth B. Damle[3]

[1]Engineering Management and Systems Engineering (EMSE) Department, Missouri University of Science & Technology, U.S.A (murray@mst.edu)

[2]EMSE Department, Missouri University of Science & Technology, U.S.A (kag@mst.edu)

[3]EMSE Department, Missouri University of Science & Technology, U.S.A (sbdkxc@mst.edu)

Abstract

A generic risk matrix is presented for use in identifying and assessing project risks quickly and cost effectively. It assists project managers with few resources to perform project risk analysis. The generic risk matrix (GRM) contains a broad set of risks that are categorized and ranked according to their potential impact and probability of occurrence. The matrix assists PMs in quickly identifying risks and can serve as a basis for contingency planning to minimize cost and schedule overruns. It is suitable for a wide variety of projects and can be modified for specific types of projects using historical data or expert opinion. An R&D project case study is included to demonstrate how the GRM is applied for a specific project.

Key Words: Risk Management, Project Management, Risk Matrix, Contingency Planning

1. INTRODUCTION

Risk identification, assessment, management, and communication are phases of risk analysis. Risk management (RM) is an important aspect for improving project performance and successfully completing projects on schedule and within cost. Since every project is unique in terms of risk, assessing risks in terms of probability and impact is challenging and time consuming. A project manager (PM) could find similar projects and analyzes the occurrence of risks associated with his or her project Henselwood et al, (2006). When risks are identified early, a risk matrix can be used by a project manager to develop a risk control and contingency plan. A risk matrix is used to rank risks and is considered a semi-quantitative approach to risk assessment Dyke et al, (2002).

The goal of this study is to develop a generic risk matrix (GRM). The matrix is used to identify and assess project risks quickly in a cost effective manner. The GRM will assist PMs who have not typically done risk analysis due to a lack of resources, a lack of emphasis on contingency planning, or an uncertainty about how to approach project risk analysis. The generic risk matrix (GRM) contains a broad set of risks that are categorized and ranked according to their potential impact and their general probability of occurrence. The generic risk matrix is suitable for a wide variety of projects. It can be modified for specific types of projects if the project manager has historical data or input from subject matter experts to customize the matrix. The matrix assists PMs in quickly identifying risks and directs that focus of contingency planning to minimize cost and schedule overruns. The risk matrix was created by considering the impact and probability of various risks within numerous industrial and government organizations based on inputs from 13 project managers. An R&D project case study is included to demonstrate how the generic risk matrix can be modified and applied for a specific project.

During literature survey, it was found that categorization of risks is often according to the project area like construction or governmental projects. No consistent set of risks was found, developing general risk categorizations was challenging. A survey was performed to identify which risks should be included in generic risk matrix and which could impact projects. An online survey was used to gain the opinion of

respondents from a variety of organizations and fields. Potential risks came from a literature review, a preliminary project risk survey, and subject matter expert opinions. Once these materials were compiled the potential generic risk categories were incorporated into the final survey. After the risk categories are formed, the assessment of risks based on impact and probability for each risk is done. Then the generic risk matrix is formed, with the various risks and their prioritization.

2. RELATED WORK

Wang et al (2000) define risk as generally arising because of uncertainty. Another definition of risk defined by Cooper et al (2005) is "It is exposure to the impacts of uncertainty." Lansdowne (1999) define risk as "The possibility that a program's requirements cannot be met by available technology or by suitable engineering procedures or processes." Hillson et al (2004) define risk as "An uncertainty that if it occurs could affect one or more project objectives." Risk is different from uncertainty. Risk arises when uncertainty has the potential to affect objectives and can be defined as "Any uncertain event or set of circumstances that, should it occur, would have an effect on one or more objectives" Simon et al., (2004). There are uncertainties that do not significantly affect objectives and which therefore are not classified as risks. Risks can occur at any stage of the project and so risk identification and analysis is important in project management for successfully completing the project on cost, within budget, and on schedule.

2.1 Risk Identification Techniques

The goal of risk identification is to identify risks before they become problems. Chapman and Ward (2003) conclude that risk identification is both important and difficult. They recommend risk identification techniques including brainstorming, interviewing with individual and groups, and using checklists. Lyons et al (2003) also concludes that brainstorming is the most common risk identification technique. A risk identification process should be comprehensive so as many risks as possible, can be captured. Risks that are not identified cannot be assessed. If unidentified risk occurs

during some stage of the project, they can hinder the overall success of the project. Risk identification can be done by using information from historic data, empirical data, or the opinions of experts such as project stakeholders. Risk identification can be done using various techniques including brainstorming, checklists, Delphi technique, interviewing, scenario analysis, work breakdown structure analysis, surveys, and questionnaires to collect information from similar projects. In some special scenarios, event tree analysis and/or fault tree analysis can be used for project risk identification (Cooper, 2005).

Brainstorming is an interactive team based approach where risks are identified based on the experience and knowledge of the team. Participants are asked to list all of the potential project risks that can, no matter how unlikely they are to occur. This technique is done as a group because as one person identifies a risk it will often trigger another person to identify additional related risks. This technique is useful for the initial identification of wide range of risks. (McInnis, 2001)

Similar to brainstorming, the Delphi technique gains information from experts about the likelihood of risks occurring. However, the technique eliminates bias and prevents any one expert from having undue influence on the others, which can occur with brainstorming. Group meetings can suffer from "leader following" or collective thinking tendencies and result in resistance to stated opinions. The Delphi technique is based on the Hegelian Principle of achieving oneness of mind through a three-step process of thesis, antithesis, and synthesis. This technique is an iterative process, where experts express their opinions anonymously, which are complied, and the entire group reviews the results and responds until a consensus is achieved. In this approach participants tend to accept ownership of the results and develop a consensus. The drawback is that this technique can be labor intensive and time consuming (Shen et.al., 2008).

Another meeting based risk assessment technique is interviewing. In this approach, face-to-face meetings with project participants, stakeholders, subject-matter experts, and/or individuals with similar project experience are used to gain information about risks occurring during past projects or potentially occurring in the new project. This

approach is more structured than the brainstorming. It is faster than the Delphi technique; however, it can be affected by groupthink. (Chapman & Ward, 2003)

A checklist analysis includes a listing of potential risks that is typically developed over time from historical information or lessons learned (Chapman and Ward, 2003 and Cross, 2001). The Risk Breakdown Structure (RBS) can also be used as a checklist for project risk analysis. Hillson (2002) used an RBS framework similar to a work breakdown structure to identify risks. A risk identification breakdown structure with several levels in hierarchical order for specific projects are discussed in Trummala et al (1999), Chapman (2001) and Miller et al (2001). Abdou et al (2005) identified various risk factors and events, which could occur in health care projects. Checklists are not comprehensive and other techniques may be used to complete the lists of risks. They are generally useful for routine projects and can be a hindrance to non-standard or unique projects because the items in the pre-developed checklists may not apply to these new projects.

Diagramming techniques, such as system flow charts, cause-and-effect diagrams, and influence diagrams have been commonly used to identify risks in production operations. Cause and effect diagrams or fish bone diagrams are used to find the causes of risk or errors. Flow charts show the interrelationship between processes or elements in a system. Influence diagrams show influences between input and output variables. According to the PMBOK Guide, (2008), they show risks or decisions, uncertainties or impact and their influence on each other. This technique however, calls for resources and expertise in risk management. It can be very time consuming and requires considerable effort to be completed.

Surveys can also be used to determine which risks can impact various projects (Cooper, et.al, 2005). List of questions are developed and data is collected in a survey format to identify potential risks in a project. One drawback to this technique is that surveys are not always completed or answered in the anticipated way. They are subjective in nature so gathering the required information is sometime cumbersome and elusive. The questions should be focused and the answers should be given according to the asked

questions for this technique to be successful. It is critical that the individuals completing the surveys understand the scope of the particular project. For projects dealing with new technology or research efforts, this can be particularly difficult.

2.2 Risk Assessment Techniques

While the tools and techniques used for risk identification are designed to help a project manager gather information which can impact a project's objectives, scope, and budget; risk assessment provides an insight concerning how likely something is to go wrong (likelihood) and what the associated impact will be (Wang et al, 2000). There are many different terms used to describe risk impact. Some studies have used categories such as "catastrophic", "critical", "marginal", and "negligible" (Standard Practice for System Safety, 2000) or "critical", "serious", "moderate", "minor", and "negligible" (Lansdowne, 1999) or "catastrophic", "major", "moderate", "minor", and "insignificant" (Cooper et al, 2005). Likewise, for defining the extent of probability, some authors have used "frequent", "probable", "occasional", and "remote" (Rosenburg et al., 1999) or "very likely", "probable', and "improbable" (Department of Defense, 2000) or "almost certain", "likely", "possible"," unlikely", "rare" (Cooper et al, 2005).

Ranking the risks based on product of likelihood (P) and consequence (c) gives a risk factor (RF) (Cooper, 2005). This can be stated mathematically as RF = P * C, where P and C are not restricted between zero and one. The significant disadvantage in this method is that high consequences and low probabilities may result in a low risk factor. Even though the risk has a low value due to the low probability, the PM may still want to manage the risk due to its high consequence. An example of this logic is the home owner who buys flood insurance even though the probability of a flood is very, very low. Another recommended method of calculating a risk factor is RF = P + C - (P*C) where the values of P and C are restricted between zero and one. This is based on the probability calculation for disjunctive events: prob (A or B) = prob(A) + prob(B) - prob(A) * prob(B). There are a variety of other risk assessment techniques that provide unique risk calculations including scenario analysis, risk assessment matrices, failure modes and

effects analysis, fault tree analysis, and event tree analysis.

Scenario analysis is commonly used technique for analyzing risks. Each risk event is analyzed for it potential undesirable outcome. The magnitude or severity of the event's impact, chances of the event occurring, and the time when that event can occur during the project's life is determined. The values can be qualitative or quantitative. Quantitative analysis is generally not done because real data availability is limited. (Gray et al, 2005).

The risk assessment matrix method allows for categorization of different risk types. Risks can be classified into different types including internal and external project risks, (Cleland et al, 2010) risks caused by natural and human risks (Bowen et al, 1999). Wideman (1992) used classifications including external unpredictable, external predictable, internal non-technical, technical, and legal risks. Previous researchers have developed risk categories for specific project types, such as underground rail projects (Ghosh et al., 2004) and public health care projects (Abdou et al., 2005). Previous studies have chosen categories according to the project's type (Nielsen, 2006). Table 1 summarizes some studies done on risk identification in project management.

Table 1. Previous Studies Categorizing Risks in Specific Projects

Author	Risk Categories
Stamatis, 2003	Competition, Safety, Market Pressure, Management Emphasis, Development of Technical Risk, Public Liability, Customer Requirements, Warranty, Legal, Statutory Requirements
Ghosh et al., 2004	Financial and Economic Risk, Contractual and Legal Risk, Subcontractors related Risk, Operational Risk, Safety and Social Risk, Design Risk, Force Majeure Risk, Physical Risk, Delay Risk
Abdou et al., 2005	Financial and Economic Risk, Design Risk, Operational and Managerial Risk, Political Risk
Nielsen, 2006	Delivery/ Operational Risk, Technology Risk, Financial Risk, Procurement Risk, Political Risk, Environmental Risk, Social Risk, Economic Risk
Condamin, 2006	Financial Risks: Banking Risk, Liquidity Risk, Foreign Exchange Risk, Interest Rate Risk, Investment Risk; Non-Financial Risks: Health Risk, Military Risk, Weather Risk
Thomset, 2004	Business Risk, Production System Risk, Benefits System Risk, Personal Risk

Table 1. Previous Studies Categorizing Risks in Specific Projects (contd.)

Henselwood et al, 2006	Geographic Risk, Societal Risk
Hall et al, 2002	Management Risk, External Risk, Technology Risk

Failure mode and effects analysis (FMEA) is another risk analysis technique. It is used to evaluate a system or design for possible ways in which failures can occur. Failure can be defined as a problem, concern, error, or challenge (Stamatis, 2003). Failure mode is defined as physical description of the manner in which a system component fails. The potential failure causes can then be defined. As an example, a failure could be loss of power to a motor. The cause of this failure could include a short circuit, disconnected power cord, or loss of electricity. The effect of failure is then determined. For example this could be stopping the motor. Due to the complexity of systems today, FMEA is performed by a team with widely ranging expertise. For each failure three values are established probability of occurrence, severity of the failure, and how the failure would be detected. A risk priority number (RPN) is generated which is the product of occurrence, severity, and detection. High RPN failures are addressed first; if the failures have same RPN, high severity as compared to detection is chosen. The impacts of these failures are investigated and a bottom-up approach to examine their impact is used. This is a proactive approach commonly used before a design or process is implemented (Lansdowne, 1999, Nielsen, 2006 and PMBOK®, 2008). The disadvantage of FMEA is that it is time consuming, complex, and may not include failures caused by a combination of events. The FMEA risk priority number is subjective. The standards for rating severity, occurrence, and detection vary from organization to organization. FMEA is effective for systems with components that can potentially fail. It is not well suited for projects where failures are not connected with specific component failures and the uniqueness of each project makes it difficult to determine the impact of failures.

Fault Tree Analysis (FTA) was developed by Bell Labs in 1961. The FTA diagram graphically shows the various combinations of conditions that may result in a failure. Fault trees are constructed using logical connections including “AND” gates and

"OR" gates. FTA may include a quantitative evaluation of the probabilities of various faults or failure events leading eventually to calculation of probability at the top event, the system failure (Wang et al, 2000). The main advantages of FTA is that it helps in visualizing the analysis, considering combinations of failures, and determining occurrence probability for complex failures. The FTA risk assessment can be done qualitatively or quantitatively. The main disadvantage is that the failure trees can become very large and complicated especially for complex and large systems. Event tree analysis is similar to FTA. The ETA describes the possible range and sequence of outcomes that may arise from an initiating event. Event trees are a forward logic technique, which attempts to see all possible outcomes of an initiating event (Rausand, 2003). An advantage of ETA is that multiple failures can be studied. The main disadvantage of ETA is that initiating events are studied as independent events and the technique does not work well with parallel sequences. It would be difficult to use ETA for project management since it is often challenging to foresee the impact of various potential events due to the complexity and uniqueness of most projects.

3. GENERIC RISK MATRIX APPROACH

The goal of this paper is to construct a high-level risk identification and assessment tool broad enough for use with a wide variety of project types. The proposed GRM risk assessment approach uses a risk identification tool based on an industrial survey. The survey results were used to develop risk categories that populate the rows of the GRM. Risk probability and impact attributes are included as columns on the GRM for the user to enter data based on their specific project. The GRM allows a PM to make quick risk identification similar to completing a checklist. The risk assessment for the identified risks can be based on the generic impact and probability values or can be specific for the project with weights and data collected from project stakeholders.

3.1 GRM Risk Categories

From an extensive review of the literature, including the papers listed in Table 1, nine categories were identified. Respective risks determined for each category. The

categories and associated risks are as follows.

(1) Technological and Operational Risk is sub-divided into operational, engineering, and performance risk. Operational risk includes lack of communication and coordination in the project, labor productivity and improper project planning. Engineering risk includes inadequate engineering designs, incomplete project scope, inadequate specifications, and differences between actual values and engineering assumptions. Performance risk includes technology limits and quality.

(2) Financial and Economic Risk is sub-divided into credit default, budget constraint/ scope creep, foreign exchange, inflation and interest rate, insurance, and funding risk. It includes credit fraud, changes in inflation or interest rates, and changes in the price of raw materials. For international projects, changes in exchange rates can cause budget pressures leading to cost overruns and/or decreases in the project performance or scope.

(3) Procurement and Contractual Risk is sub-divided into raw material procurement and subcontractor procurement risk. Raw material procurement risk is the delay due to market competition. Contractual risk involves issues or concerns associated with procurement through contractor.

(4) Political Risk is sub-divided into political instability and customer requirement risk. Political risk can be due to revisions in policies and rules, slow approvals, unstable governments, or other bureaucratic hurdles. The political environment can impact projects during the implementation phase. Customer requirement risks can be caused by changes to customer technical or aesthetic requirements, which often lead to scope creep.

(5) Environmental Risk is sub-divided into weather and pollution risk. Risks to the project due to weather conditions such as rain, snow, or reduced sunlight are considered weather risks. Pollution risk is considered when the project affects the environment by generating pollution and vice versa. Generating pollution can result in delays and fines. Working in a polluted environment may affect the project’s performance or cause additional effort to successfully complete the project.

(6) Social Risk is sub-divided into cultural relationship and society impact risk. Society impact risk occurs when a project has an effect on society. An example of social risk is the construction of a dam that could disturb the ecological balance of the region.

Cultural relationship risk is often associated with global projects. In these situations misunderstanding the needs and sensitivities of the customer can impact the scope and operation of the projects.

(7) Regulatory and Legal Risk is risk sub-divided into litigation and non-compliance with codes and laws. Rules and regulations vary by country and industry sector. Changing regulations can impact a projects' budget and/or schedule. The risk of litigation is great if rules are not properly followed.

(8) Safety Risk includes security risk. Security risk can be caused by many factors, such as acts of God, fire, theft, terrorism, and war. For example, floods or fire can drastically impact construction projects but they can influence any type of project if deliveries are impacted.

(9) Delay Risk is sub-divided into project delay and third party delay risk. Project delay risk can be caused by plan approval delays or other constraints. Third party delay risk is caused by delays by sub-contractors, suppliers, or vendors.

3.2 GRM Probability and Impact Assessments

Once the generic risk categories were developed, it was necessary to create a risk assessment classification scheme to complete the GRM. The interpretation of probability and risk impact is not consistent throughout various industries. To address these inconsistencies, a simplified risk matrix approach was chosen. Figure 1 shows the levels of probability and impact that were selected. Both impact and probability use the values of "low", "medium" and "high". Using only three values limits the amount of information for the PM to work with. This simplifies the process of completing the matrix for a specific project but also reduces the detail in the results. Given the limited information available to a PM concerning probabilities, this is a reasonable level of detail for an initial risk assessment.

	Probability		
Impact	Low	Medium	High
Low	LI-LP	LI-MP	LI-HP
Medium	MI-LP	MI-MP	MI-HP
High	HI-LP	HI-MP	HI-HP

Figure 1. Simplified Risk Matrix

For the development of the GRM in this study, each risk was divided into LI-LP (low impact & low probability), LI-MP (low impact & medium probability), LI-HP (low impact & high probability), and similarly MI-LP, MI-MP, MI-HP, HI-LP, HI-MP and HI-HP. These nine different combinations, as shown in Figure 1, were defined in the form of "economic function" definitions (Condamin, 2006) for this work. Such definitions facilitate the ease of use of the GRM. It defines the implications of impact-probability combinations on the project planning and budgeting. In this way, a PM can take a particular course of action depending on what level the risks fall into. The LI-LP implies little practical significance to the project's performance and these factors can be addressed if and when they occur. They do not justify additional planning or monitoring. LI-MP might require some judgment or budget provisions. The LI-HP implies that contingency budgeting should be performed. The MI-LP and MI-MP indicate that the impact of the risk could be considerable and contingency planning at the minimum should be done. HP risks will often need allocated amounts in the budget, since the chances of the risk occurring are maximum. HI-LP and HI-MP imply that if the event occurs external funding may be necessary or insurance should be purchased. If the risk affects resources the PM should consider identifying potential additional resources and possibly even reserving them. MI-HP and HI-HP implies that the PM should plan for the risk event to occur. This might include budgeting additional funds or additional slack time to associated tasks to either avoid or minimize the impact of the event.

In order to rank the risk elements a weighting scheme was applied to the nine simplified risk matrix categories. The impact and probability attributes were given a weight of 1, 2 and 3 corresponding to "low", "medium" and "high" values. The impact and probability values are then multiplied to get a combination weight. For example, LI-

LP combination will generate factors (1 and 1) that are multiplied together giving a combined risk value of 1. Similarly LI-HP and HI-LP resulted in a risk value of 3 and HI-HP results in a risk value of 9. The risk matrix with weights is shown in Figure 2. However, one caveat to this approach is that weighing impact and probability attributes in this manner may not be detailed enough or can be misleading. Using this balanced approach, MI-HP and HI-MP are both given the same value of six. These two combinations may not be of equal concern for some projects. The weights can be adjusted by the PM for projects that warrant it.

		Probability		
	Impact	Low	Medium	High
Weights		1	2	3
1	Low	LI-LP (1)	LI-MP (2)	LI-HP (3)
2	Medium	MI-LP (2)	MI-MP (4)	MI-HP (6)
3	High	HI-LP (3)	HI-MP (6)	HI-HP (9)

Figure 2. Impact –Risk Combinations with Weights

3.3 GRM Survey

A survey was designed to find the frequency of use of risk management techniques in project management and to rank various business risks. The survey consisted of 55 questions for PMs. The A section of the survey contained demographic questions about the respondent's employer and PM experiences. The second section contained impact and probability assessments of each of the identified risks. The available choices for the risk impact questions were critical, serious, moderate, minimal, negligible and not applicable. The probability options given to the respondents were 0-20%, 20-40%, 40-60%, 60-80%, 80-100% and not applicable. The response data was converted into the simplified impact-probability matrix as follows –

Critical & Serious – High Impact - 60-80% & 80-100% - High Probability
Moderate – Medium Impact - 40-60% - Medium Probability
Minimal & Negligible – Low Impact - 0-20% & 20-40% - Low Probability

3.4 Survey Results

All of the survey participants were in technical and/or managerial positions in their organization with extensive project management experience. A total of 13 useable responses were used in the analysis. Many respondents were involved with construction projects; however other types of projects including R&D and military programs were represented in the survey. Respondents were currently working on an average of two to three projects. The average project size was $100,000 to $1,000,000 (See Figure 3). The majority did use some kind of risk management techniques; however a significant portion, nearly 28% of respondents, had seldom or never used risk management techniques in their organizations (See Figure 4). The survey asked respondents about the type of risk matrix being used for risk management in the question “Is the risk matrix approach company or project based?” Of the organizations doing risk management, the majority used a company-wide risk matrix, while few used project-specific ones. This may be due to the number of ongoing projects as an organizational-based generic risk matrix would be more likely for those doing numerous projects or it could be due to a lack of available generic matrices. Some comments from those using a risk matrix highlighted their usefulness including: “It minimizes the risk exposure and keeps the project on schedule. The schedule is for convenience, planning and costs” and “It is a good way to ID tasks”

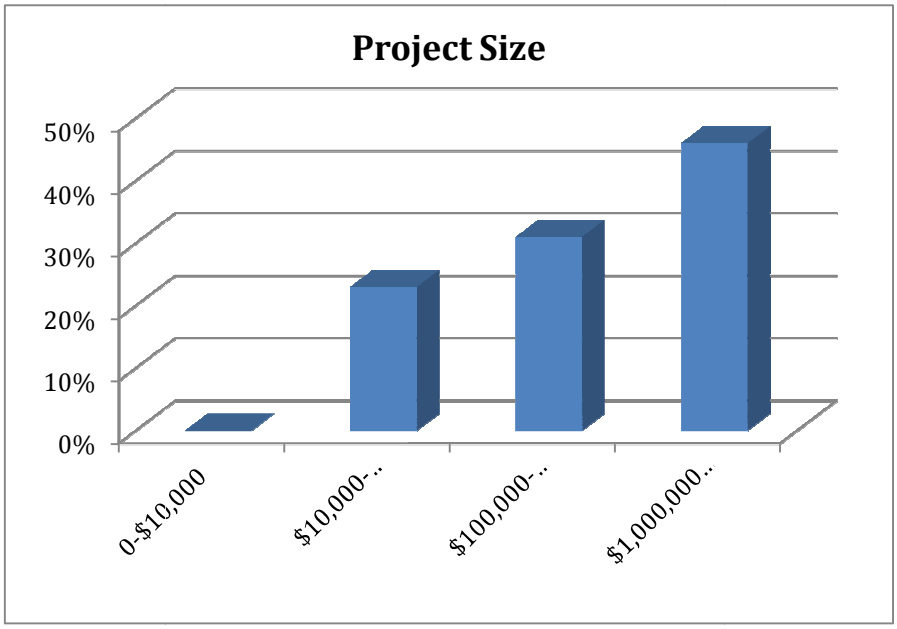

Figure 3. Project Size

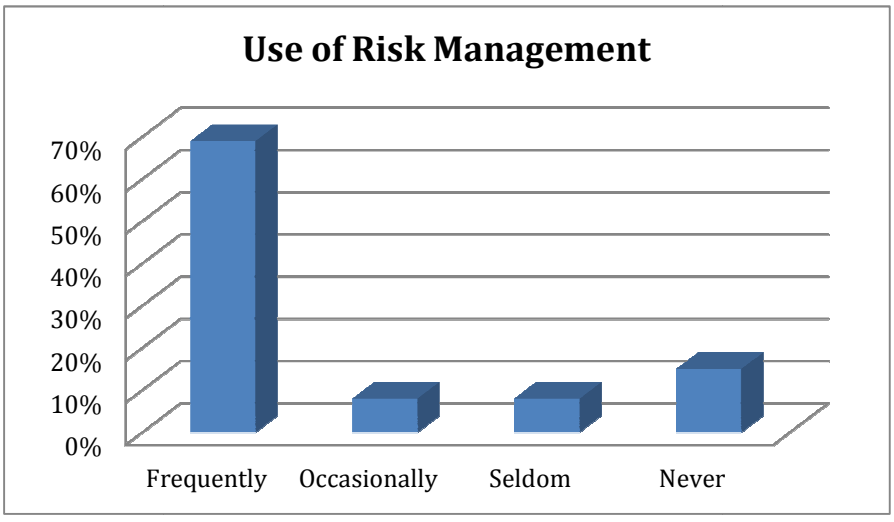

Figure 4. Use of Risk Management

Risk Ranking –

To prioritize the risks the survey responses were converted to risk ranking parameters. The analysis is based on 13 responses to the survey. The individual responses to impact and probability of each risk is combined and classified in one of the nine types, namely LI-LP, LI-MP, LI-HP, MI-LP, MI-MP, MI-HP, HI-LP, HI-MP and HI-HP. The responses for each of the nine types were totaled and converted into a percentage value. For example, in Table 2, one response falls under LI-LP, giving it a value of 7.69% (1/13*100). These percentage values were then multiplied by the associated weights (as per Figure 2) and summed together row-wise. The resultant total weighted value is used in ranking the risks. The column showing N/A or not applicable is the percentage of respondents finding that specific risk not applicable to their projects. It has a weight of zero and does not influence the total weighted values.

Consider another example, in Table 2, credit/default risk has values of 30.77, 0, 0, 23.08, 0, 0, 7.69, 7.69, 7.69, and 23.08 for the impact-probability combinations respectively. These values are multiplied by respective weights of 1, 2, 3, 2, 4, 6, 3, 6 and 9. Summing the resultant values will result in a value of 215.38. This value is used to rank the risks. Thus, credit risk gets a rank of 14 as shown in Table 2. Risks having identical weighted values are given the same rank. Operational Risk and Customer Requirement risk are the top two most important risks that a PM should consider in risk management of projects in general.

Table 2. Risks Ranked

	Weight -->	LI-LP 1	LI-MP 2	LI-HP 3	MI-LP 2	MI-MP 4	MI-HP 6	HI-LP 3	HI-MP 6	HI-HP 9	N/A 0	Weighted Importance	Rankings from most to least importance
	Types of Risk												
1	**Technological and Operational risk**												
	Operational risk	7.69	0.00	0.00	0.00	0.00	59.17	30.77	30.77	15.38	7.69	778.11	1
	Engineering risk	7.69	0.00	0.00	7.69	0.00	0.00	30.77	30.77	15.38	7.69	438.46	5
	Performance risk	7.69	0.00	0.00	7.69	15.38	0.00	7.69	46.15	0.00	15.38	384.62	7
2	**Financial and Economic risk**												
	Credit risk/ Default risk	30.77	0.00	0.00	23.08	0.00	0.00	7.69	7.69	7.69	23.08	215.38	14
	Budget Constraint/ Scope creep risk	0.00	0.00	0.00	15.38	15.38	7.69	7.69	23.08	15.38	15.38	438.46	5
	Foreign Exchange risk	38.46	0.00	0.00	0.00	0.00	0.00	15.38	0.00	0.00	46.15	84.62	17
	Inflation and Interest rate risk	53.85	0.00	0.00	23.08	0.00	0.00	0.00	0.00	7.69	15.38	169.23	15
	Insurance risk	30.77	0.00	0.00	23.08	0.00	0.00	15.38	15.38	0.00	15.38	215.38	14
	Funding risk	15.38	0.00	0.00	7.69	15.38	0.00	30.77	15.38	7.69	7.69	346.15	8
3	**Procurement and contractual risk**												
	Raw material procurement risk	15.38	0.00	0.00	23.08	7.69	7.69	0.00	23.08	7.69	15.38	346.15	8
	Subcontractor procurement risk	7.69	7.69	0.00	15.38	0.00	0.00	23.08	23.08	15.38	7.69	400.00	6
4	**Political risk**												
	Political instability risk	38.46	0.00	0.00	7.69	0.00	0.00	7.69	23.08	7.69	15.38	284.62	10
	customer requirement risk	15.38	0.00	0.00	0.00	7.69	7.69	7.69	30.77	23.08	7.69	507.69	2
5	**Environmental risk**												
	Weather risk	15.38	0.00	7.69	7.69	0.00	7.69	0.00	46.15	7.69	7.69	446.15	4
	Pollution/ environmental risk	23.08	0.00	0.00	23.08	7.69	0.00	0.00	23.08	7.69	15.38	307.69	9
6	**Social risk**												
	Cultural relationship risk	38.46	7.69	0.00	0.00	0.00	7.69	0.00	7.69	7.69	30.77	215.38	14
	Society impact risk	30.77	0.00	0.00	15.38	15.38	0.00	0.00	0.00	0.00	38.46	123.08	16
7	**Regulatory and legal risk**												
	Litigation risk	7.69	0.00	0.00	30.77	0.00	0.00	23.08	23.08	0.00	15.38	276.92	11
	Non-complaince of codes and laws risk	30.77	0.00	0.00	15.38	0.00	0.00	23.08	23.08	0.00	7.69	269.23	12
8	**Safety risk**												
	Security risk	30.77	0.00	0.00	0.00	0.00	0.00	53.85	7.69	0.00	7.69	238.46	13
9	**Delay risk**												
	Project delay risk	0.00	0.00	0.00	0.00	23.08	7.69	7.69	53.85	0.00	7.69	484.62	3
	Third party delay risk	0.00	0.00	0.00	15.38	15.38	7.69	7.69	46.15	0.00	7.69	438.46	5

The results of Table 2 are used as a baseline to rank the risks with the Generic Risk Matrix. The weighted importance values provide a quick assessment of impact and probability of each risk. The impact and probability ratings were used to determine generic impact and probability values for the GRM. The low, medium and high impact survey responses were summed and the results are shown in Table 3. The same was done

for the probability responses. For example, Operational Risk in the first row has 7.69% for LI-LP, 0% for LI-MP and 0% for LI-HP which is summed up for impact attribute to generate a value of 7.69% for low impact. Similarly, for low probability of Operational Risk, the values of 7.60% for LI-LP, 0% for MI-LP and 30.77% for HI-LP are summed to get 38.46%. The aggregate of impact and probability values for each risk has been marked an “X”. A conservative approach has been used, when identical values were found, the maximum of the two was considered. For example, the values for Insurance Risk under impact are 30.77% for low as well as high impact. Here, the risk has been marked as high impact. This table allows for a quick assessment just by looking at the concerned columns. The risk ranks have been retained from the previous calculations in Table 2.

Table 3. Risks Rated for Probability and Impact

		Probability			Impact			Probability			Impact			Rankings from most to Least important
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	
	Types of Risk													
1	**Technological and Operational risk**													
	Operational risk	38.46	30.77	74.56	7.69	59.17	76.92			X			X	1
	Engineering risk	46.15	30.77	15.38	7.69	7.69	76.92	X					X	5
	Performance risk	23.08	61.54	0.00	7.69	23.08	53.85		X				X	7
2	**Financial and Economic risk**													
	Credit risk/ Default risk	61.54	7.69	7.69	30.77	23.08	23.08	X			X			14
	Budget Constraint/ Scope creep risk	23.08	38.46	23.08	0.00	38.46	46.15		X				X	5
	Foreign Exchange risk	53.85	0.00	0.00	38.46	0.00	15.38	X			X			17
	Inflation and Interest rate risk	76.92	0.00	7.69	53.85	23.08	7.69	X			X			15
	Insurance risk	69.23	15.38	0.00	30.77	23.08	30.77	X					X	14
	Funding risk	53.85	30.77	7.69	15.38	23.08	53.85	X					X	8
3	**Procurement and contractual risk**													
	Raw material procurement risk	38.46	30.77	15.38	15.38	38.46	30.77	X				X		8
	Subcontractor procurement risk	46.15	30.77	15.38	15.38	15.38	61.54	X					X	6
4	**Political risk**													
	Political instability risk	53.85	23.08	7.69	38.46	7.69	38.46	X					X	10
	customer requirement risk	23.08	38.46	30.77	15.38	15.38	61.54		X				X	2
5	**Environmental risk**													
	Weather risk	23.08	46.15	23.08	23.08	15.38	53.85		X				X	4
	Pollution/ environmental risk	46.15	30.77	7.69	23.08	30.77	30.77	X					X	9
6	**Social risk**													
	Cultural relationship risk	38.46	15.38	15.38	46.15	7.69	15.38	X			X			14
	Society impact risk	46.15	15.38	0.00	30.77	30.77	0.00	X				X		16
7	**Regulatory and legal risk**													
	Litigation risk	61.54	23.08	0.00	7.69	30.77	46.15	X					X	11
	Non-compliance of codes and laws risk	69.23	23.08	0.00	30.77	15.38	46.15	X					X	12
8	**Safety risk**													
	Security risk	84.62	7.69	0.00	30.77	0.00	61.54	X					X	13
9	**Delay risk**													
	Project delay risk	7.69	76.92	7.69	0.00	30.77	61.54		X				X	3
	Third party delay risk	23.08	61.54	7.69	0.00	38.46	53.85		X				X	5

The probability and impact columns, marked with an “X” in Table 3, are the basis of the GRM. They provide a quick overview that a PM can use to identify risks when managing a project. These results are particularly useful when a PM has little insight into the project and potential challenges that may arise during the life of the project. However,

PMs and others in the organization often have some insight into the potential problems the project can face. Blank columns were added to the GRM to allow the PM to use knowledge and judgment about a specific project to customize the risk matrix. The PM can rate the risks for impacts and probabilities for any or all of the risks listed. Thus the generic rankings shown in the GRM in Table 4 gives the PM a baseline value to work from. The PM can then customize it to suit a specific project. This same methodology could be used to generate a matrix for a specific project type or even to generate a company-wide matrix for a particular industry.

Table 4. Generic Risk Matrix

		Generic							Specific						
		Probability			Impact			Generic	Probability			Impact			Specific
		Low	Medium	High	Low	Medium	High	Rankings	Low	Medium	High	Low	Medium	High	Rankings
	Types of Risk														
1	**Technological and Operational risk**														
	Operational risk			X			X	1							
	Engineering risk	X					X	5							
	Performance risk		X				X	7							
2	**Financial and Economic risk**														
	Credit risk/ Default risk	X			X			14							
	Budget Constraint/ Scope creep risk		X				X	5							
	Foreign Exchange risk	X			X			17							
	Inflation and Interest rate risk	X			X			15							
	Insurance risk	X					X	14							
	Funding risk	X					X	8							
3	**Procurement and contractual risk**														
	Raw material procurement risk	X				X		8							
	Subcontractor procurement risk	X					X	6							
4	**Political risk**														
	Political instability risk	X					X	10							
	customer requirement risk		X				X	2							
5	**Environmental risk**														
	Weather risk		X				X	4							
	Pollution/ environmental risk	X						9							
6	**Social risk**														
	Cultural relationship risk	X			X			14							
	Society impact risk	X				X		16							
7	**Regulatory and legal risk**														
	Litigation risk	X					X	11							
	Non-compliance of codes and laws risk	X					X	12							
8	**Safety risk**														
	Security risk	X					X	13							
9	**Delay risk**														
	Project delay risk		X				X	3							
	Third party delay risk		X				X	5							

4. CASE STUDY

To illustrate the practicality of the generic risk matrix, it was applied to a project with a two-year span and a one million dollars budget. This was a research and development (R&D) project for the Department of Defense (DoD). This case was chosen to illustrate that the generic matrix could be applied to an R&D project. The risk ranking

developed in this paper was based on respondents from a variety of industries. We suspected that some potential risk factors, the Foreign Exchange risk for example, might not apply to a DoD R&D project.

A blank risk matrix without generic rankings was given to three PMs with significant experience on military research projects. The blank matrix listed all the generic potential risks. The PMs were asked to rate the impact and probability of each risk for the two year, one million dollar project. The PMs did not know specifics of the case study project, but based their responses on their prior experiences with government research projects. The results were compiled and the specific ranked risks averaged as shown in Table 5.

Table 5. Case Study Results

	Types of Risk	Rankings from most to least important (1-22) Respondent-1	Rankings from most to least important (1-22) Respondent-2	Rankings from most to least important (1-22) Respondent-3	Rankings Average	Avearge Rankings from most to least important (1-22)
1	**Technological & Operational risk**					
	Operational risk	1	6	12	6.333	5
	Engineering risk	2	13	6	7.000	6
	Performance risk	3	14	5	7.333	7
2	**Financial & Economic risk**					
	Credit risk / Default risk	10	7	20	12.333	10
	Budget constraint/ Scope creep risk	4	1	2	2.333	1
	Foreign exchange risk	11	15	22	16.000	17
	Inflation & interest rate risk	12	16	13	13.667	12
	Insurance risk	13	17	19	16.333	18
	Funding risk	14	18	14	15.333	15
3	**Procurement & Contractual risk**					
	Raw material procurement risk	5	2	4	3.667	2
	Subcontractor procurement risk	7	3	3	4.333	4
4	**Political risk**					
	Political instability risk	15	19	21	18.333	21
	Customer requirement risk	16	20	15	17.000	20
5	**Environmental risk**					
	Weather risk	17	21	11	16.333	19
	Pollution / environmental risk	18	22	16	18.667	22
6	**Social risk**					
	Cultural relationship risk	19	8	18	15.000	14
	Society impact risk	20	9	17	15.333	16
7	**Regulatory & Legal risk**					
	Litigation risk	21	10	8	13.000	11
	Non-compliance of codes and laws risk	22	11	9	14.000	13
8	**Safety risk**					
	Security risk	8	12	7	9.000	9
9	**Delay risk**					
	Project delay risk	6	4	1	3.667	3
	Third party delay risk	9	5	10	8.000	8

These rankings come purely from each PM's perspective. There is some variability in the values due to their subjective nature, but there is general agreement on many values. Budget constraint/scope creep was ranked 4, 1, and 2 for an average value of 2.3, which is the highest priority risk for this type of research project. As expected some risks such as political and environmental have low priority since they do not typically apply to R&D projects. A construction project, however, would typically rate these to be significant concerns. Many of the risks did have ranking approximately similar to the results for the generic risk matrix shown in Table 2. The generic matrix provides the R&D PM with a good set of categorized risks for contingency planning. Seeking input from PMs with related experience provides further refinement. The PM will still need to consider the various risks based on the project's parameters and project to-date, but the GRM has given the PM much needed structure for the risk analysis process.

5. CONCLUSIONS AND DISCUSSION

Twenty three percent of the PMs surveyed are not using risk management frequently. This could be due to a lack of an easy-to-use process for risk assessment. The generic risk matrix developed in this paper provides a quick approach to guide project managers in contingency planning. This matrix identifies risks and prioritizes them with minimal resources required of the PM. In the GRM approach, the use of nine different risk areas can be a first step to standardization of risk identification process in an organization. This reduces the subjectivity in defining risks and more importantly can aid discussions about risks across projects. The GRM approach attempts to reduce the subjectivity and remain simple to use by limiting values to either low, medium, or high.

A project manager can use the GRM as is for a quick start on risk planning or can call on personal experience or the expertise of other PMs in the organization and customize the matrix. The contingency planning can be as basic or as elaborate as warranted. It is critical that project managers consider the wide variety of things that can go wrong on a project; the GRM gives the PM a tool to do this. As with project management in general, planning and monitoring the project for a variety of risk factors is key to having a successful project.

In order to take this research further, there could be a few opportunities to consider other risk factors in the analysis. PMBOK 4th edition mentions the inclusion of ‘positive risks’ in the project planning stage. Positive risks are opportunities which can be capitalized on, resulting in a favorable outcome. These risks have a probability of a positive outcome and are usually initiated by the project manager. Such risks can be considered in future for conducting this analysis. Positive risks can be ranked according to perception of its importance among respondents and project managers. Such risks might be industry specific, but the survey results might prove ability of managers to consider such risks as well as how much importance would be given to those.

REFERENCES

1. A guide to the project management body of knowledge (PMBOK®), (2008) Newtown Square, PA, US: Project Management Institute, Fourth edition.

2. Abdou, A., Alzarooni, S. & Lewis, J. (2005). Risk identification and rating for public health care projects in the United Arab Emirates. Proceeding of the Queensland University of Technology Research Week International Conference, Brisbane, Australia.

3. Chao LP, Ishii K. (2003) Design Process Error-proofing: Failure Modes and Effects Analysis of the Design Process. Proceedings of ASME Design Engineering Technical Conferences, IL, U.S.A.

4. Chapman, R.J, (2001) "The Controlling Influences on Effective Risk Identification and Assessment for Construction Design Management," International Journal of Project management, Vol. 19, No. 3, pp. 147-160.

5. Chapman C. & Ward S. (2003) Project Risk management: Processes, Techniques and Insights, 2nd Edition, England: John Wiley & Sons.

6. Clemens, P.L. (2002) Fault Tree Analysis, 4th ed., Tullahoma, TN: Jacobs Sverdrup.

7. Condamin Laurent, Louisot Jean-Paul and Naiim Patrick (2006) "Risk Quantification: Management, Diagnosis and Hedging," John Wiley & Sons, Ltd.

8. Cooper Dale F., Grey Stephen, Raymond Geoffrey & Walker Phil (2005) "Project Risk Management Guidelines," John Wiley & Sons, Ltd.

9. Department of Defense: Standard Practice for System Safety. (2000). MIL-STD-882-D.

10. Dyke, Frederick T and Ozog, Henry (2002) "Designing an Effective Risk Matrix," An ioMosaic Corporation Whitepaper.

11. Ghosh, S. & Jintanapakanont, J. (2004) "Identifying and Assessing the Critical Risk Factors in an Underground Rail Project in Thailand: a Factor Analysis Approach," International Journal of Project Management, Vol. 22, 8, 633-643.

12. Jonassen D.H., Tessmer M., Hannum W.H. (1999), Task analysis methods for instructional design, Psychology Press.

13. Gray, Clifford and Larson Erik (2005) "Project Management: The Complete Guide for Every Manager," Mc-Graw Hill Publishing Company, Edition 2nd.

14. Hall, D.C., & Hulett, D.T, (2002) “Universal Risk Project-Final report” Available from PMI Risk SIG website.

15. Henselwood, Fred, Phillips, Grey (2006) “A Matrix-based Risk Assessment Approach for Addressing Linear Hazards such as Pipelines,” Journal of Loss Prevention in the Process Industries, Vol. 19, pp. 433-441.

16. Hillson DA, Hulett DT. (2004) Assessing Risk Probability: Alternative Approaches. Proceedings of Project Management Institute Global Congress, Prague, Czech Republic.

17. Hillson, D. (2002). Use of Your Risk Breakdown Structure to Understand Your Risks. Proceedings of the Project Management Institute Annual Seminars & Symposium, San Antonio, Texas, USA.

18. Hillson, D. A. & Hulett, D. T. (2004). Assessing Risk Probability: Alternative Approaches. Proceedings of PMI Global Congress, Prague.

19. Hillson, David (2002) “The Risk Breakdown Structure (RBS) as an Aid to Effective Risk Management,” Proceedings of the Fifth European Project Management Conference, France

20. Karuppuswamy, P., Sundararaj, G. Devadasan, S. R., Elangovan, D. (2006) “Failure Reduction in Manufacturing Systems through the Risk Management Approach and the Development of a Reactive Maintenance Model,” International Journal of Risk Assesment and Management, Vol. 6, No. 4/5/6.

21. Lansdowne, Z. F. (1999). “Risk matrix: an approach for prioritizing risks and tracking risk litigation progress”. Proceedings of the 30th Annual Project Management Institute Seminars & Symposium.

22. Lyons Terry and Skitmore Martin (2004) “Project Risk Management in Queensland Engineering Construction Industry: A Survey”, International Journal of Project Management, Vol. 22, pp. 51-61.

23. Leung P, Ishii K, Abell J, Benson J. (2005) Global Failure Modes and Effects Analysis: A Planning Tool for Global Product Development. Proceedings of ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, CA, U.S.A.

24. Miller, R., & Lessard, D. (2001) “Understanding and Managing Risks in Large Engineering Projects” International Journal of Project Management, Vol. 19, No. 8, pp.437-443.

25. Murray, S., Alpaugh, A., Burgher, K., Flachsbart, B., and Elrod, C. (2010) "Development of a Systematic Approach to Project Selection for Rural Economic Development: A Case Study of Vienna, Missouri, USA," Journal of Rural and Community Development, Vol. 5, No. 2.

26. Nielsen, K. R. (2006) "Risk Management: Lessons from Six Continents," Journal of Management in Engineering, Vol. 22, 2, 61-67.

27. Rafele, C., Hillson, D. & Grimaldi, S. (2005) "Understanding project risk exposure using the two-dimensional risk breakdown matrix". Proceeding of PMI Global Congress, Edinburgh, Scotland.

28. Cleland D.L., Ireland L. (2010), Project Managers Portable Handbook 3/E, McGraw-Hill Prof Med/Tech, 464 pages

29. Rausand M, Hoyland A. System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, 2nd Edition, 2003.

30. Rosenburg, L., Hammer, T. & Gallo, A. (1999). Continuous risk management at NASA. Proceeding of Quality Week Conference, San Francisco, California.

31. Shen G., Feng J. & Xu K (2008) "Identification of Essential Risk Factors in Software Projects by using an 'Information Content' based Reasoning Approach", Computing and Information Systems Journal, Vol.12, Issue 2, pp.29-36.

32. Simon PW, Hillson DA, Newland KE. (2004) Project Risk Analysis & Management (PRAM) guide. High Wycombe, Buckinghamshire, UK: APM Group, 2nd edition.

33. Stamatis DH. (2003) Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press, 2nd Edition.

34. Telford, T. (2005). Risk Analysis and Management for Projects (RAMP). Institution of Civil Engineers (ICE), Faculty of Actuaries, Institute of Actuaries, London, 2nd edition.

35. Tummala, V.M.R, & Burchett J.F. (1999) "Applying a Risk Management Process (RMP) to Manage Cost risk for an EHV Transmission Line Project," International Journal of Project Management, Vol. 17, No.4, pp. 223-235.

36. Thomsett, R. (2006) "Risk in Projects-The Total Tool Set," online website: www.thomsett.com.au

37. McInnis A. (2001). The New Engineering Contract: A legal commentary, Thomas Telford Publishing, London.

38. Wang John X and Roush Marvin L. (2000). “What Every Engineer Should Know About Risk Engineering and Management”, Marcel Dekker Inc.

39. Ward, S.C. (1999). Assessing and Managing Important Risks. International Journal of Project Management, Vo. 17, No. 6, pp 331-6.

40. Wideman, R. M. (1992) “Risk Management: A Guide to Managing Project Risks and Opportunity. Project and Program,” Project Management Institute, Pennsylvania.

II. USING LOPA TO ANALYZE PAST CATASTROPHIC ACCIDENTS INCLUDING THE 2008 MORTGAGE MARKET CRISIS AND SPACE SHUTTLE CHALLENGER DISASTER

Siddharth Damle and Susan Murray, Ph.D

Engineering Management & Systems Engineering department
Missouri University of Science & Technology
223 Engineering Management
600 W. 14th St.
Rolla, MO 65409-0370
E-mail: sbdkxc@mst.edu

Abstract

It has been established in the chemical process industry that Layer of Protection Analysis (LOPA) is a helpful tool in analyzing systems safety. It is an effective semi-quantitative risk assessment and mitigation technique which involves independent layers of protection to maximize safety and minimize risk. LOPA has not yet been liberally applied to other industries outside the chemical process industry. Can the contributions of LOPA to the process industry be extrapolated to other industries? Is there a generic approach that could be used to analyze a broader assortment of hazardous situations?

This paper will apply LOPA to past catastrophic accidents and will evaluate the effectiveness of this application. The two major accidents considered are the 2008 mortgage market crisis and the space shuttle *Challenger* disaster. This research will attempt to analyze these events within the LOPA framework. This might result in designing new layer(s) and looking into the aspects of culture, organizational structure issues, ethics and human errors. In case of the *Challenger* disaster, the primary reason for the occurrence of the accident was poor decision making on the part of the management. An attempt will be made to incorporate such issues into the layers and try to maintain their independence. The probabilities for these layers might be difficult to ascertain, yet an attempt will be made to provide a method of determining the same. The generic model

will help project managers to predict safety shortcomings and to take proactive actions to maintain and achieve relevant independent layers of protection.

Introduction

Risk management comprises both risk analysis and risk assessment. Risk analysis broadly involves hazard identification, consequence prediction, and frequency estimation. Risk assessment is the process of determining if the risk is tolerable as per industry standards or if more protection is required for further mitigation. The primary steps in performing risk analysis include hazard recognition, system description, scenario identification, incident analysis, consequence analysis, likelihood evaluation and risk estimation [1]. It is advantageous to have a simple and less time consuming method for such exhaustive risk analysis. Amongst the various existing risk management techniques being used today, Layer of Protection Analysis (LOPA) is widely used in the process industry. It is a semi-quantitative analytical tool to assess the adequacy of protection layers used to mitigate risk [2]. LOPA method is a process hazard analysis (PHA) tool. The method utilizes the hazardous events, event severity, initiating causes and initiating 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. 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 [3].

Process hazard analysis incorporates various tools like HAZOP, Failure Mode and Effect Analysis, Fault Tree Analysis, Event Tree Analysis; which help identifying potential hazards in the system and its operations. While some of these like HAZOP are qualitative, others like FTA and ETA are quantitative. LOPA lies somewhere in the middle of the spectrum and provides a good balance of subjectivity and quantification. LOPA assists in evaluating the risk of the hazard scenarios which have already been identified and compares the safety levels with industry standards.

LOPA has been used exclusively in the risk management of process industry applications. This paper explores the use to this technique in other applications and projects. In order to analyze generic events from a LOPA perspective, this paper uses past catastrophic accident cases including the 2008 mortgage market crisis. An attempt will be made to model such events using the LOPA method, and explore the possibility of better prediction of disasters in future applications.

LOPA Method

LOPA is a simplified risk assessment method, which is generally used when the scenario is too complex or the consequence is too severe for decision-making during HAZOP. It utilizes the hazardous events, event severity, initiating causes and its likelihood data from the HAZOP stage [4]. This method is used to identify the protection systems, safeguarding against an adverse incident, that meet CCPS criteria [2]. CCPS (Center for Chemical Process Safety) is a not-for-profit, corporate membership organization that identifies and addresses process safety needs within the chemical, pharmaceutical, and petroleum industries [5]. The Independent Protection Layers (IPLs) are safety systems which meet the following criteria [2]-

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

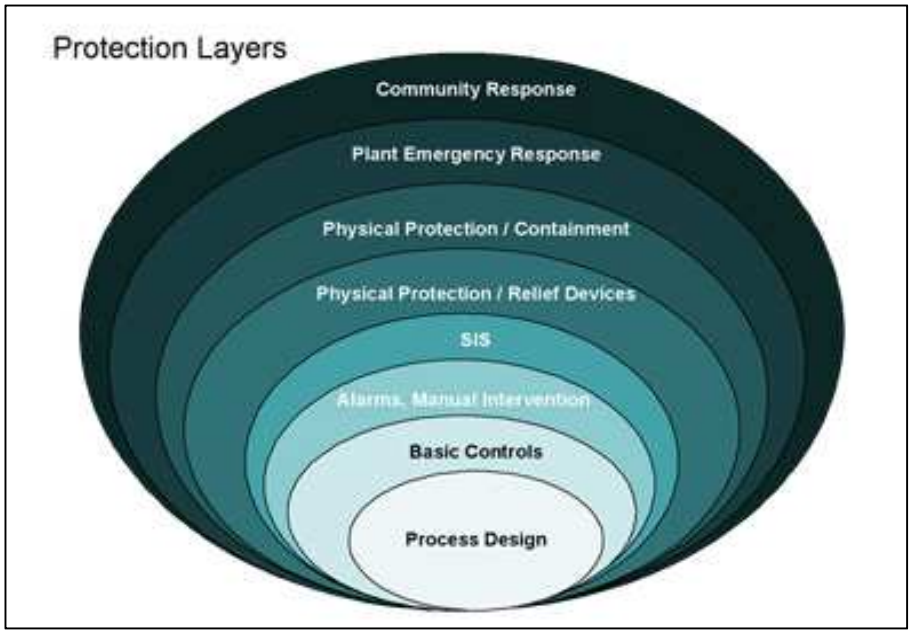

Figure 1 - Protection Layers [6]

As shown in figure 1, the process design system is to be protected, by using seven layers. The first layer is the basic controls which can prevent the undesirable event. It is followed by alarms and manual intervention, where an operator can take action to control the parameter that caused the alarm. If the problem still goes undetected, the safety instrumented systems (SIS), and physical protection like relief devices can normalize or shutdown the system. After this layer, the remaining layers are for containment and work towards safety of the plant and surrounding community through emergency response procedures. These layers are independent of one another and hence the failure of one layer will not affect performance of the following layers.

The IPLs perform three main functions [7] –

1. Prevention - to reduce the probability of accident
2. Protection - to detect the initiating cause and neutralize it
3. Mitigation - to control/reduce the accident severity

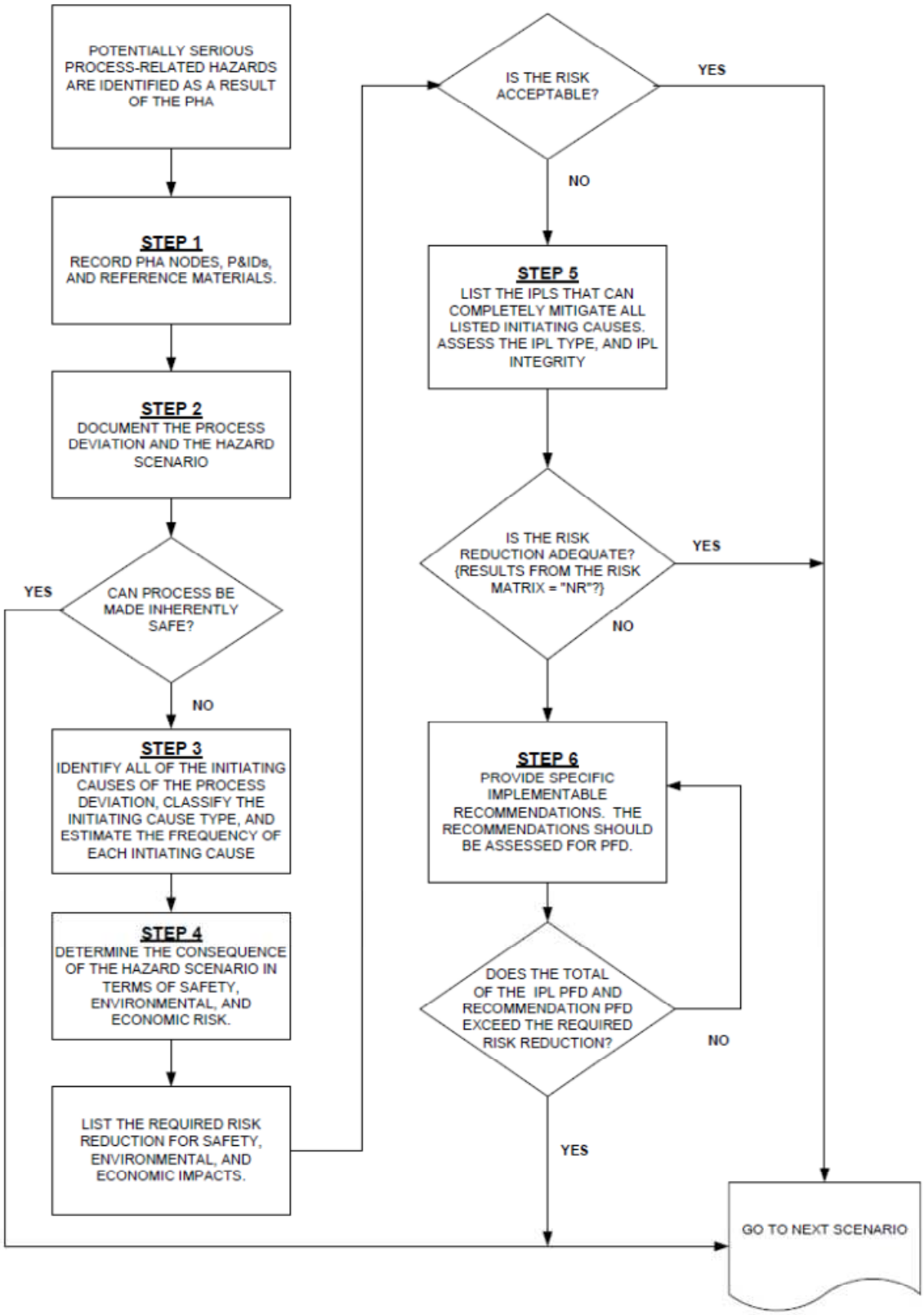

Figure 2 - LOPA Process [2]

Figure 2 shows the main steps in a LOPA process [2]-

1. Record all documentation, reports, design documents, etc
2. Document the hazard scenario under consideration
3. Identify all initiating causes for the incident and determine the frequency of occurrence of each of them
4. Determine the consequence of the scenario under consideration. From the frequency and consequence, develop a risk matrix and check if the risks are acceptable. Assess if additional risk reduction is required.
5. List all IPLs that can achieve risk reduction/mitigation of all initiating causes. For each IPL determine the Probability to Fail on Demand (PFD)
6. Provide feasible recommendations. Select the best option with considerations to ease of implementation and cost.

Case I - Mortgage Market Crisis

In late 2008, the US faced a huge market crisis which not only affected the local economy but also had a big impact on the global economy. The high sub-prime lending and repackaged Collateralized Debt Obligations (CDOs) led to a big mortgage market crash. CDOs are generally used to redistribute risk, such that the risk of defaulting loans is transferred to the CDO investor. A big disadvantage of CDO is that lower grade mortgages can be repackaged and sold as attractive investment options in the secondary markets. A similar scenario happened to be one of the prime causes of a market crisis in 2008, followed by a recession in the economy.

There were a few specific factors which eventually turned out to be responsible for the market collapse. These are two major ones.

1. Monetary Policy

   This was one of the primary causes of the crisis. The government came up with an expansive monetary policy to urge more consumers to buy houses. It wanted to see an increase in homeownership since 2001. The decrease in interest rates

coupled with the policy accommodating more and more subprime lending, the housing rates began to fall and were destined to eventually bust. The Fed was slow to tighten the monetary policy until finally in 2004 when it increased the rates by 25 basis points [8]. The demand for houses was stimulated by offering benefits for homeownership. Fannie Mae and Freddie Mac were created and were urged to increase their purchase of mortgages going to borrowers of low to moderate incomes. These organizations were given targets like 50 percent of their mortgage financing should go to borrowers with incomes below the regional median [8]. This also allowed the government to subsidize low income housing. Thus, homeownership was expanded at the expense of good-credit lending. Figure 3 shows the gradual increase in the subprime share of total mortgages from 2001 to 2006.

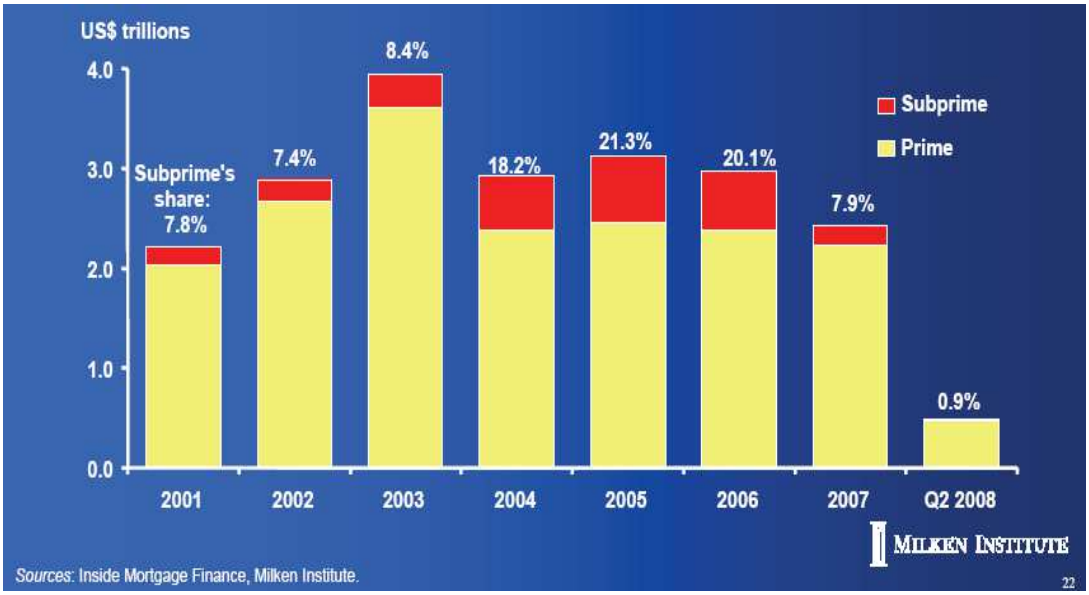

Figure 3 - Subprime Lending [9]

2. Securitization and financial innovations

Securitization means combining a pool of illiquid assets or contractual debts and transforming them into securities through the use of financial engineering. Though it was an interesting innovation, it had some drawbacks. Securitization helped shift the risk from the original lender to various other investors through

complex systems. Instead of spreading the risk, it ended up diluting it. The second drawback was that these were extremely difficult to price as they had a highly complex design. Even the rating agencies were incapable of determining the price of the security. They assigned high ratings to securities without focusing on the individual mortgages underlying these derivative products. Insurance companies also provided insurance to such securities and thus more and more institutions got involved with the high risk products. Firms traded Credit Default Swaps (CDS) as a means of protection against loan default. They also took opposite positions to secure themselves. This caused a further spread of the risk and involvement of not only local, but global firms. This was sure to create a domino effect as soon as a mortgage payment defaulted. Finally when foreclosures grew and banks had large number of illiquid assets in their possession, a market crisis was imminent.

Securitization – Collateralized Debt Obligations

Today's mortgage market is quite complex, not only because of changing interest rates, but also because of the large number of derivative products that can be designed and offered. These derivatives highly depend on the interest rates, the timely payback capability of the mortgage payer and the credit risk associated with it. In the past few years, the financial industry has seen many intelligently designed derivative products. They help in making the economy robust, but at times can be more risky than equities. One such product is Collateralized Debt Obligation (CDO).

Collateralized Debt Obligations (CDO) is a type of the structured asset backed security (ABS), whose payments are derived from the underlying fixed-income assets. They are sophisticated financial tools that take various individual loans and package them together to design a product which can be sold on the secondary market. The underlying could be corporate debt, credit card debt, loans, mortgages, etc. CDOs were initially designed with a view of providing more liquidity to the economy. It acts as an instrument for banks or corporations to sell off their debt. This in turn allows them more capital to work with, be it investing or loaning. There are a few downsides to it too. The originators

of the loans might not be keen in collecting due installments since the loans are now owned by some investors. This increases the chances of default. Another disadvantage of CDOs is that they are too complex, and often banks do not reveal the underlying assets that are embedded in them. Thus, investors do not have enough access to information for researching the product. They have to solely rely on the bank for returns on investment.

CDOs have a complex architecture. They are split into different risk classes called tranches. The upper tranches are safer with a high credit rating, while the lower ones are more risky. A CDO pays fixed cash flow to its investor based on what it receives from the pool of assets. CDOs are often termed according to the underlying loan. In this paper, CDOs with underlying mortgage backed securities have been considered.

Mortgage backed securities are based upon mortgage payments. The ones having residential mortgages as underlying assets are called Residential Mortgage Backed Securities (RMBS). A pool of residential mortgage payments forms one RMBS. Each RMBS also has tranches of varying level of risks. The higher tranches have lower risk while the bottom tranches have higher risks associated with higher returns as well. The upper tranches are paid first depending on the receipt of payments of the underlying mortgages. Every tranche has a credit rating, issued by the credit rating agencies. AAA is the topmost rating while BB- or ‘unrated’ is the lowest on the credit risk scale. Thus, instead of all the investors sharing the fund’s return in proportion to their investment, investor returns are also determined by the seniority of the CDO tranches they purchase [10].

As shown in the figure 4, the structure has a three stepped design. The first is individual mortgage payers, second is a pool of such individual payers (RMBS) and the third is a pool of all such RMBS (CDO). There can be another level of a pool of CDOs called CDO squared which is more complex in nature.

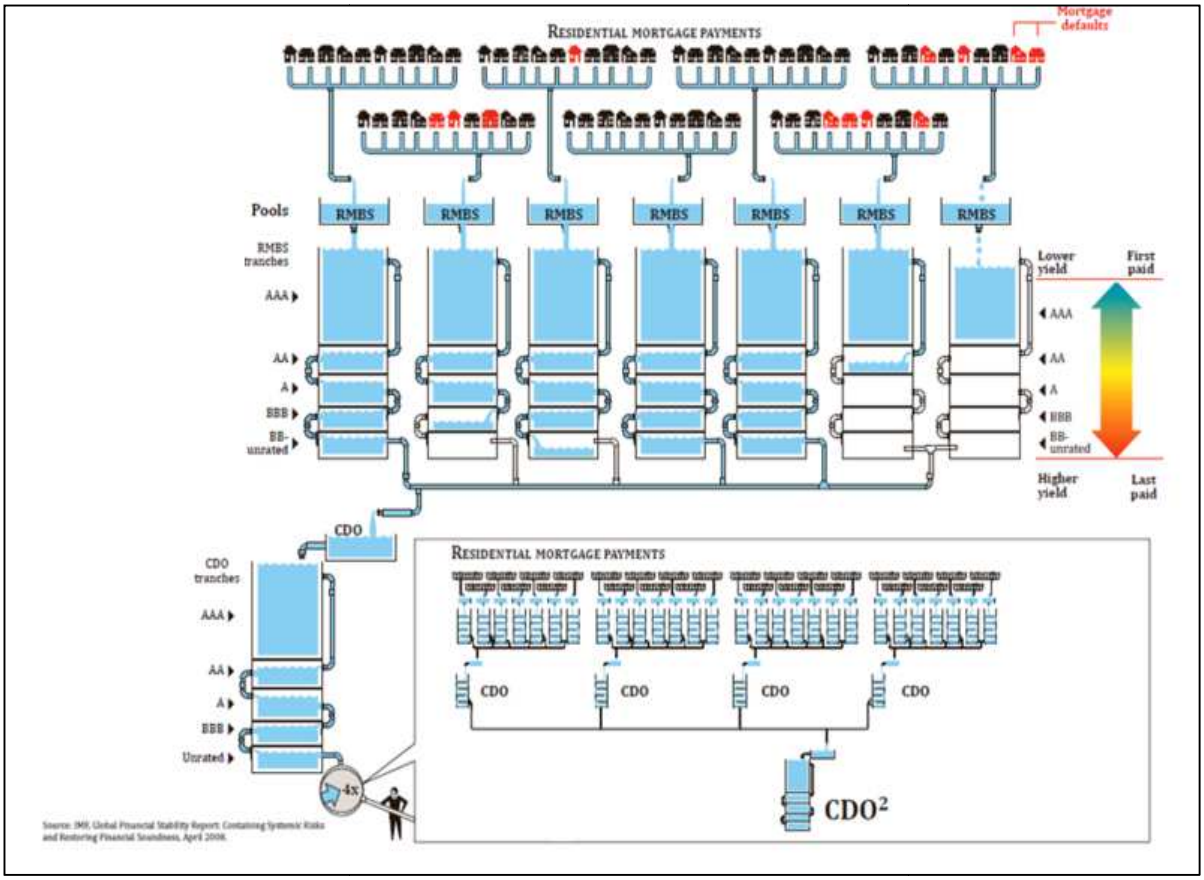

Figure 4 - CDO Structure [11]

Credit Default Swaps (CDS)

Credit Default Swaps are a type of insurance. The buyer of a CDS gets insured against default of the underlying asset and in turn pays the seller a premium or a fee. If the underlying defaults as per terms mentioned in the contract, the seller has to compensate the buyer with the fair market value of the asset. The premium is usually known as CDS spread and is quoted in annual percentage of the notional amount [12]. Depending on the credit rating of the insurer, it is required to maintain some form of collateral to the contract. In cases of high credit rating like AAA, there is no need to maintain a collateral. The most notable feature of a CDS is that the buyer does not need to own the asset. Buyer can essentially bet on an asset price movement even without owning it. This way, the price movement or default of a single asset can affect any

number of investors who are associated with that underlying asset. CDS gained huge popularity and by 2007, the CDS market was worth almost $62 trillion [13], double the size of the US stock market!

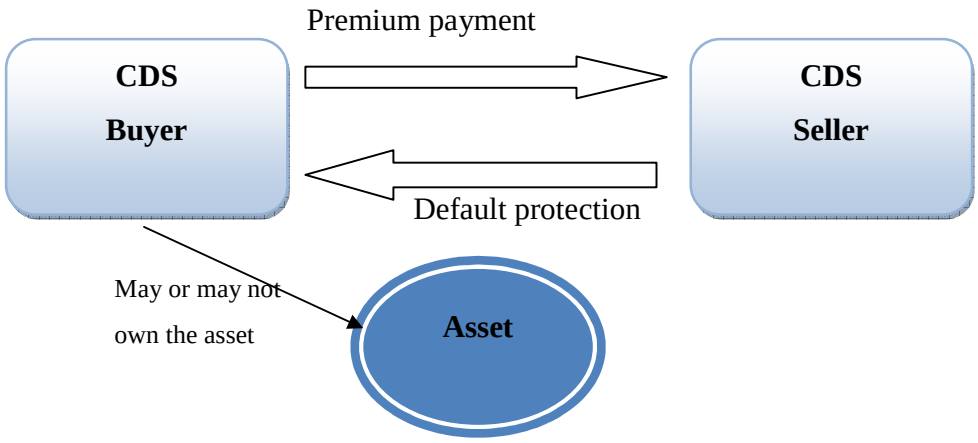

Figure 5 - CDS Block Diagram

There are three primary purposes of CDS –

I. Risk hedging – The main purpose of a CDS is to provide protection for one's investment. If the investor thinks the asset is too risky, the risk can be hedged by buying a CDS. If the asset defaults, the seller will pay the investor with the contractual amount. If the asset performs well, the investor ends up losing just the premium for the CDS.

II. Speculation – An investor or institution can purchase a CDS contract over an asset which it thinks or forecasts will default. The striking aspect of CDS is that the asset need not be owned by the buyer. It is a form of betting on the movement of the price of an asset.

III. Arbitrage – If an asset's value increases or decreases slower than the market signals, there is an arbitrage opportunity for the CDS parties.

The Model

This study will attempt to the model the mortgage market crisis using LOPA method. The system under consideration would be the mortgage market (can be more specific to cover securitization – CDOs). Various layers would be designed around this system to prevent a catastrophe or a crash from occurring. The problem, if detected at any of those layers, can be avoided or its consequence severity can be mitigated. This model is challenging because the independence of the layers needs to be maintained and it has to follow the general rules of the LOPA method. An attempt will be made to provide a method to ascertain probabilities (to fail on demand) of these layers. Figure 6 shows a LOPA model developed for the finance industry.

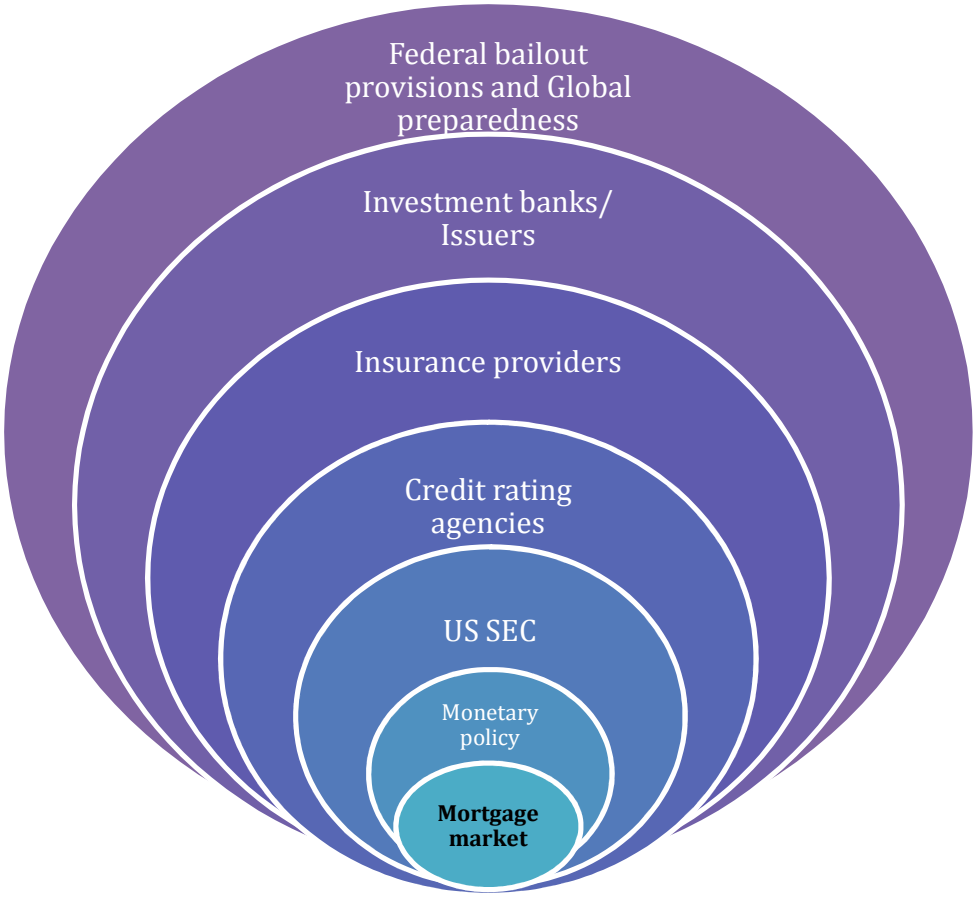

Figure 6 – LOPA for Mortgage Market

Applicable steps in LOPA process (refer figure 2) –

Step 1 – System definition and documentation

The mortgage market is considered to be the system which needs to be protected. The hazard is a market crash. The hazard scenario and all reference material are documented.

Step 2 –Initiating event

The initiating event is the high level of subprime lending. Subprime lending results in increased number of low grade tranches of mortgage payments. These tranches form the CDO and eventually a market crash occurs. The frequency of this event is difficult to determine and might require complex quantitative analysis.

Step 3 – Consequence of hazard scenario

The consequence of this hazard is mainly in terms of economic losses. The estimation of losses depends on the market indicator which is used. In any case, the losses are catastrophic and the severity falls under the high criticality region of the risk matrix.

Step 4 – Designing and listing the IPLs

Protection layers need to be designed to mitigate the consequence occurrence and also to control the initiating event. In this case the first layer needs to control event of high subprime lending. These layers have to be carefully designed to ensure their independence from one another and the initiating event.

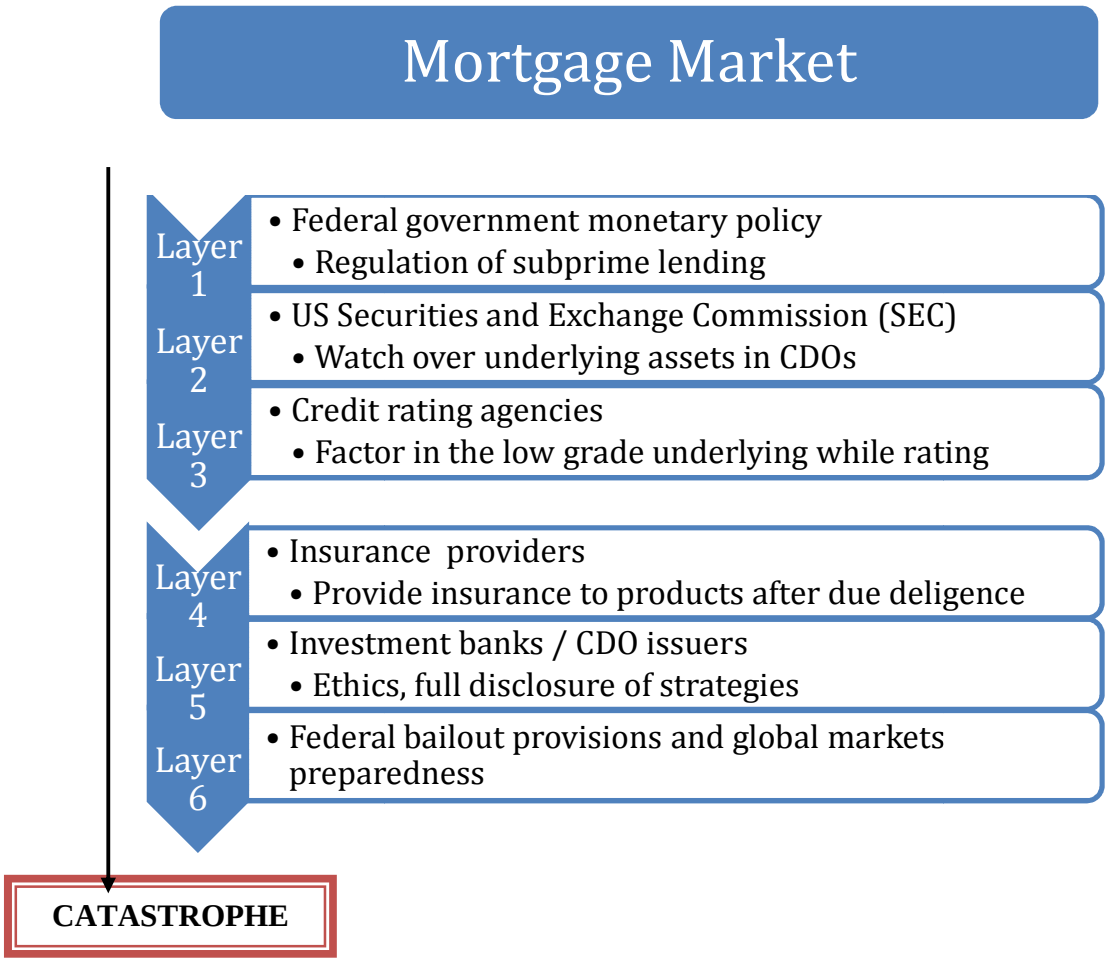

Figure 7 – Layer Definitions

Figure 7 shows the layers in order of their actions and their definitions for the mortgage market system.

Layer 1 – Federal Monetary Policy

The first step towards curbing higher subprime lending is to have a tight monetary policy. The government should restrict the percentage of subprime lending. In a view to provide homes to people with bad credit, the government might risk an eventual market collapse. The policy must include a regulation which includes more checks and examination while lending sub-prime.

Layer 2 – US Securities and Exchange Commission (SEC)

The SEC acts as a watchdog over the stock market. It needs to focus its efforts more towards CDO products. When a CDO enters the market, the SEC should investigate the roots of the CDO. It needs to ensure that the repackaging of mortgages does not only include low grade tranches in the system. There should be an SEC regulation which governs the design of these CDOs with underlying as mortgage backed securities (MBS). This regulation should include a cap on the percentage of lower grade assets used while forming the CDO. The SEC also should track the activities of market makers like investment banks when they launch complex derivative products.

Layer 3 - Credit Rating Agencies (CRAs)

Credit rating agencies are one of the most important factors in the market. Investors tend to rely on the ratings provided by these agencies to make sound investing decisions. CRAs like Standard & Poor's, Moody's Investor Services and Fitch Group issue ratings to various investment products including CDOs. These agencies use different statistical methods to derive ratings for investment products, which in turn inform the investor of the associated risk with the product. These agencies need to examine deeper into complex products like CDOs to check the ratings of the individual mortgage pools and accordingly assign a cumulative rating. Ratings should not be assigned based on the issuer's (like investment banks) reputation or its track record in the market or any other such

factors. This is one of the most sensitive layers of the model, since these agencies have a huge scope for criticism. Their ratings can be biased by firm reputation, they have strong relationships with company upper managements, they are slow in responding to events and downgrading ratings, etc. A lowering of the score can result in deep impacts for any firm, as it causes higher interest rates on borrowing and can force bankruptcy.

Layer 4 – Insurance Companies

Insurance companies provide insurance on loans and are also involved in products like credit default swaps. While engaging in credit default swaps (CDS) on CDOs, these companies need to investigate the CDO product to its roots and estimate the risk in accordance with the lower rated loans in the pool of underlying assets. In cases where CDOs have lower grade underlying loans, the premium for selling credit default swaps should be considerably higher. In the event that they have to pay for defaulted loans, there is a high chance of liquidity crisis. In many cases the issuer, which is a reputed investment bank, can cause an insurance firm to provide protection through CDS without thorough risk analysis.

Layer 5 – Investment Banks, CDO issuers

Large investment banks and other investment product issuers need to be more risk averse when packaging low grade mortgages into their CDOs. Even if they do design a product with sub-grade tranches, they have to explicitly disclose the structure of the CDO to the investors. Ethics is an important aspect for these investment banks. Such firms ethically cannot sell investment products and then take a position in the market which bets on the failure of those same products. They have to disclose their entire strategy to the investors.

Layer 6 – Federal bailout provisions/Global market preparedness

The government needs to have a federal bailout provision in place and should have proactive measures in the policy. This can help in mitigating the effects of a recession. Once the earlier layers are in place, they would help in regulating the

markets to an acceptable level. The global markets also need to have respective policies to reduce dependence on a single market. Their governments should have a recession response policy in place to avoid the domino effect.

How the Layers Failed

The causes of the 2008 recession have been discussed earlier in this paper. Now, we look at how the failures occurred with respect to the layers in the model. This will make it easier to analyze them and avoid such a collapse in future.

The expansive government policy which promoted home buying also encouraged increased sub-prime lending [14]. The government was not being considerate about the fact that such lending practices could eventually lead to a housing bubble burst once the number of foreclosures increased. Government organizations like Fannie Mae and Freddie Mac had their sub-prime lending targets revised and more percentage of their lending began to come from sub-prime lending. A little foresight and restricted lending policy could have reduced the size of the bubble.

The second layer was the SEC, which failed to realize the potential danger which was created by the Collateralized Mortgage Obligations. The sub-prime lending led to more and more risky mortgages, whose payments were not assured. Investors seeking high risk high returns were looking at investing in products which had such loans. These packaged and re-packaged mortgages eventually formed the CDOs and no one knew exactly how to price them and what their value was. The SEC could have stepped in and regulated the issuers from packaging all low grade loans. There could have been a policy in place indicating a method to calculate the true value of the product. The CDS market was also de-regulated, and hence the transactions were restricted to the two parties in the contract. No one knew exactly how large the CDS market was getting and how many investors were speculating the movement of any particular asset. SEC should have had a regulatory policy on the CDS contracts.

The next to be blamed were the credit rating agencies. These agencies gave high ratings to CDOs based on the reputation and good relationship with top banks. The agencies also were clueless regarding the exact pricing of CDOs and CDO squared. They ignored the fact that these products contained risky low grade/junk status loans inside them. They understated the default from falling house prices and failed to anticipate the extent of these falling prices [15]. The agencies should have rated those with respect to the percentage of low grade loans packaged in the product. The top management of these agencies had good relations with most of the top managers of leading investment banking firms. This added to the biasing of the ratings.

The next layer to fail was the insurance firms. These firms provided insurance to CDOs, again relying on the reputation of large investment banks. The insurance was provided mainly through Credit Default Swap (CDS). These firms were insuring products that had a high likelihood of defaulting. In 2008, the rating agencies dropped AIG's rating which forced AIG to maintain collateral on CDS. By that time it was involved in so many contracts that it was impossible to generate such collateral amount and AIG was on the verge of bankruptcy [16]. The failure of the largest insurance company in the world caused a huge domino effect not only on the CDO market but also on global economy.

Large investment banks were responsible for packaging dodgy loans into investment products and selling them without revealing the details and strategies behind them. According to the lawsuit filed by SEC against Goldman Sachs, the largest investment bank on Wall Street, Goldman packaged bad loans and sold the CDO, while its hedge fund betted against the same product by predicting a default on those same loans [17]. The senate hearing that followed raised this as a serious ethics issue, but Goldman refused to accept the fact that they had done wrong and pointed out that it was not a contractual obligation to reveal its hedge fund managers and their strategies to the investors [18].

Case II – Space Shuttle *Challenger* Disaster

On 28 January, 1986 the Space Shuttle Challenger took off and its flight lasted just over a minute when it exploded resulted 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 project.

Over the next three months, a presidential commission led by former Secretary of State William P. Rogers and a NASA team investigated the accident [19]. 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 engineers and at least some of the Marshall 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 [19] –

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-rings poor performance at low temperatures, but the 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 a lot 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.

LOPA Model –

In case of the Challenger, the system under consideration would be the Solid Rocket Boosters (SRB) O-ring sealing, which eventually blew up due to O-ring failure to contain hot gases. Different layers can be designed to capture this problem at an initial stage. The challenge in applying the LOPA model for this case is that the problem was detected before the launch, but was neglected due to various reasons. An attempt will be made to use LOPA as an effective method in ensuring that the criticality of the problem is taken into account before proceeding and eventually necessary actions can be taken.

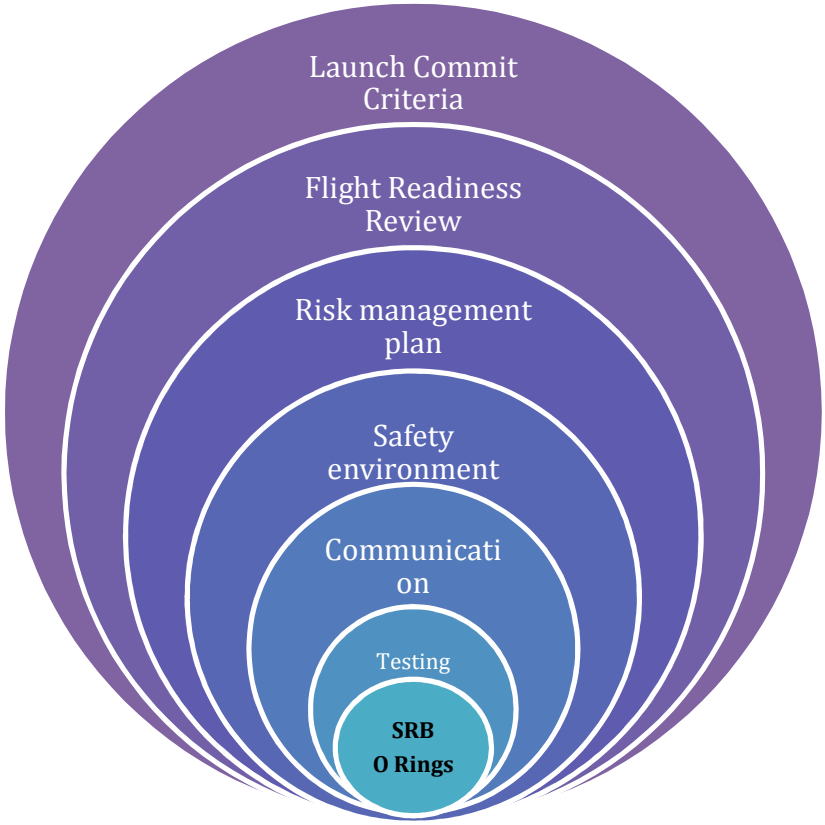

Figure 8 - LOPA Model for *Challenger* Disaster

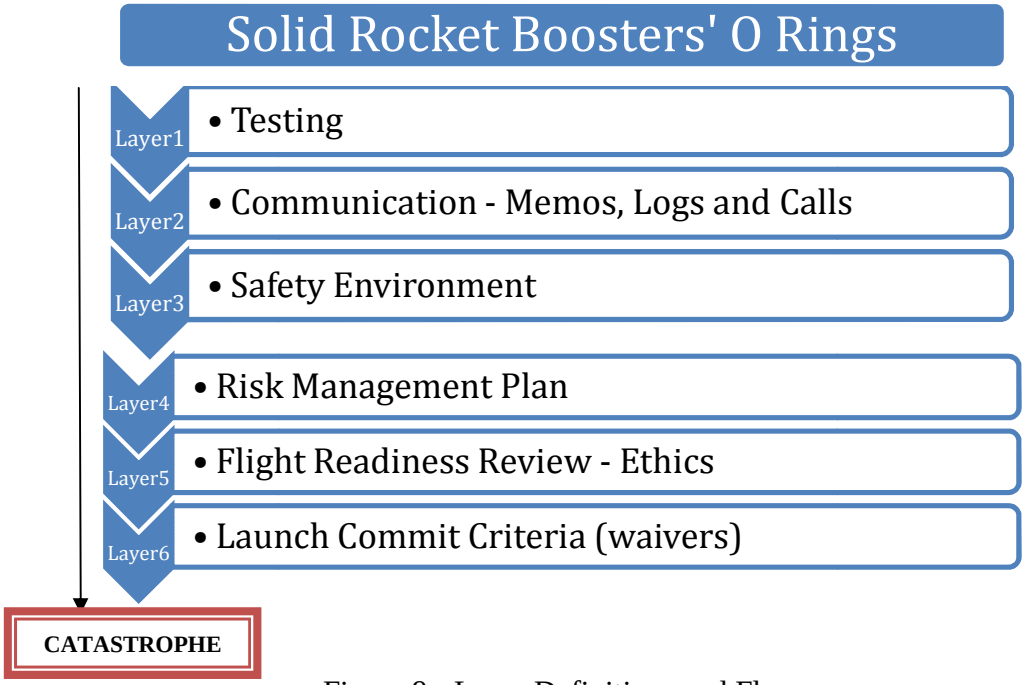

Figure 9 - Layer Definitions and Flow

Figure 8 and Figure 9 show the layers developed for the *Challenger* disaster.

Layer 1 – Testing

Each component going into the 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 re-testing 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 to and fro communication with the end user (NASA). Any phone-calls should also be logged so that they can be referred in future, in case an issue arises.

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 the immediate superiors, while critical issues should be escalated before it is too late in the process. With 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 [20]. 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 the top management. It should not be a norm to issue waivers for

little issues, which might eventually sum up to a bigger problem at hand. 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 [20].

Level 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 shuttle for flight was done as required. This is a crucial meeting and the FRR should be used to escalate issues if they had not been 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.

Level 6 – Launch Commit Criteria

This is the final check before any shuttle takes flight. A formal prelaunch weather briefing is held two days prior to launch [21]. This mainly includes weather data specifications like 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 inspite of bad weather conditions is most certainly taking the shuttle towards disaster.

Estimating Probability to Fail on Demand (PFD)

The most challenging aspect of application of LOPA is the estimation of risk and frequency of occurrence of the consequence. The consequence in the first case study is a market crash, which has huge economic implications and affects the entire economy. In the *Challenger* case, loss of life is the consequence. Thus, in both cases 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. The challenges in estimating PFDs include –

1. LOPA has not been used in the past for applications beyond the process industry.
2. There are no industry standards or historical data on failure of layers.
3. There are no standard SILs (safety integrity levels).
4. Layers involving aspects like ethics cannot be quantified.
5. Certain industry acceptable assumptions need to be made to compute those values.

One study mentions the use of historical data such as failure of a relief valve to open being 1 in 100 challenges. That gives it a PFD of 1×10^{-2} [22]. The study also states a generic estimation, called LOPA credits, for the generic protection layers which can be applied to any chemical process application [22]. Some layers in this paper can use historical data, like the credit rating agencies. We could track their ratings against performance of financial products over the past 10 years. But failure has to be defined in terms that are acceptable and fair to the agencies. Most layers in this study face the problem of defining failure. Hence, quantifying PFDs for these layers becomes a huge challenge. Quantifying PFDs for the layers might require extensive research.

Conclusion

The analysis of the two case studies in this paper shows that protection layers can be designed under the LOPA framework. The LOPA methodology can be applied effectively to analyze past accidents and prevent future catastrophes. The layers seem to be a success in mitigating the consequence occurrence, by controlling and trying to prevent the initiating event from leading to a disaster. The application of LOPA gives a clear understanding of what exactly went wrong and what improvements can be made to

avoid a repeat occurrence. The model shows that the problem can be trapped in at least one of the protection layers. The goal of LOPA to achieve risk reduction can be seen in the applications in this paper, though the reduction is purely qualitative at this stage. It is difficult to estimate the risk involved using the LOPA calculations. Though the layers can be qualitatively stated, their respective probabilities to fail on demand are difficult to ascertain. There are too many variables involved while attempting to calculate frequency of occurrence of the initiating event as well as PFDs for the layers. For layers that involve qualitative aspects like ethics, it is extremely challenging to compute probabilities. With the absence of industry standards like SIL levels and PFD data, the computation calls for further research in each of the fields that comprise the layers. The probability of organizations and decision-makers defaulting is a tricky estimation. This study might need a generic industry standard in determining such challenging quantities in future.

This LOPA model can be extended to be applied to most projects. With the incorporation of control points, procedural checks, regulations at different stages and finally consequence response guidelines, this mode can prove to be effective in identifying the key high risk stages and mitigating the problem at an early stage. An independent LOPA model can be designed for each industry, so that it can be applied to all scenarios pertaining to that industry. There needs to be an industry standard or at least a set of assumptions for estimating failure probabilities. 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.

References

1. First, K., *Scenario Identification And Evaluation for Layer of Protection Analysis*, in *MKOPSC 12th Annual Symposium*. 2009: Texas A&M University.

2. Summers, A.E., *Introduction to Layer of Protection Analysis*, in *MKOPSC Symposium*. 2002: Texas A&M University.

3. Frederickson, A., *The Layer Of Protection Analysis (LOPA) Method*.

4. Babu, J.R., *Layer of Protection Analysis – As effective tool in PHA*. 2007, Cholamandalam MS Risk Servics Ltd.

5. AIChE. Retrieved from: http://www.aiche.org/CCPS/About/index.aspx.

6. *Protection Layers*. July 2011, Retrieved from: http://www.gmsystemsgroup.com/sil/sil_info_lopa.html.

7. Adam S Markowski, M.S.M., *ExSys-LOPA for the chemical process industry* in *MKOPSC 12th Annual symposium*. 2009: Texas A&M University.

8. Schwartz, A.J., *Origins of the Financial Market Crisis of 2008*. Cato Journal, 2009. **29**(1): p. 5.

9. Michael Lea, O.H., Marja Hoek-Smit, *Lessons Learned From the US Mortgage Market Crisis*. 2008, Wharton School of Business.

10. Douglas J. Lucas, L.S.G., Frank J. Fabozzi, *Collateralized Debt Obligations and Credit risk transfer* Yale International Center for Finance, 2007. **Working paper 07-06**.

11. IMF, *Global Financial Stability Report*. 2008.

12. Mengle, D., *Credit Derivatives: An Overview*, in *Atlanta Fed's Financial Markets Conference*. 2007.

13. *ISDA market survey*. 2010. Retrieved from: http://www.isda.org/statistics/pdf/ISDA-Market-Survey-annual-data.pdf.

14. Alec Klein, Z.A.G., *The Bubble*, in *The Washington Post*. 2008.

15. Jaffee, D., *The U.S. Subprime Mortgage Crisis: Issues Raised and Lessons Learned*. 2008, University of California, Berkeley.

16. Davidson, A., *AIG And The Trouble With 'Credit Default Swaps'*. 2008, NPR.

17. Grier, P., *Goldman Sachs hearing pulls back curtain on bankers' ethics*, in *The Christian Science Monitor*. 2010.

18. *Wall Street and the Financial Crisis: the Role of Investment Banks*, in *Senate Permanent Subcommittee on Investigations*. 2010.

19. Siddharth Damle, L.V., Julian Smith, Raymond J. Kaminski, *The Space Shuttle Challenger Disaster*, D. Dow, Editor. 2009, Missouri S&T.

20. Committee on Shuttle Criticality Review and Hazard Analysis Audit, S.A.B., Commission on Engineering and Technical systems, National Research Council *Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management* 1988.

21. NASA, *Space Shuttle Weather Launch Commit Criteria and KSC End of Mission Weather Landing Criteria*, F. Kennedy Space Center, Editor. 2010, NASA.

22. Freeman, R., *Using Layer of Protection Analysis to Define Safety Integrity Level Requirements*, in *AIChE Spring 2006 National Meeting*. 2006: Orlando, FL.

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

Hanan Altabbakh, Susan Murray, Siddharth Damle and Katie Grantham

Engineering Management & Systems Engineering department
Missouri University of Science & Technology
223 Engineering Management
600 W. 14th St.
Rolla, MO 65409-0370

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 risks 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 et al 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 hybrids 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 28 January 1986 the Space Shuttle Challenger took off and its flight lasted just over a minute when it 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 project.

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) 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 pressurized into giving a go ahead for the launch by NASA.

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

1. Faulty o-ring – The o-ring seal 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 the 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 III, & 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, Vesely, Dugan, Fragola, Minarick III, & Railsback, 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 of qualitative over the 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).

Product Based Risk Assessment Tools

Product risk assessment tools investigate risks associated with the system from the component level and the product design. The product based risk assessment tools are categorized into qualitative and quantitative risk assessment 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 to identify the potential risk in a preferred order or even simultaneously. Product based risk assessment tools do not consider the human factors due to the complexity of human minds and behaviors.

FMEA

Failure Mode and Effects Analysis (FMEA) is a very structured and reliable bottom up method to classify hardware and system failures. Applying FMEA to a system can be easy 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, it may not be as easy if the system consists of a large 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 were classified according to their effect on the crew, the vehicle, and the mission (Kerzner, 2009).

Insert Exhibit 1.

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.

FTA

Fault tree analysis is a top-down probabilistic risk assessment technique. It is a deductive method that investigates the factors and conditions that contribute to the adverse events in the system. It utilizes logic gates and graphical diagrams to identify the failures in the system, subsystem, components, and others. The fault tree analysis 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 respective fault trees for the same root event. Fault trees analysis is a probabilistic risk assessment tool that can be quantitatively evaluated using the rules of Boolean algebra between its gates.

The strength of the fault tree analysis 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 fault tree analysis 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 B. S., 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 human 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 tree could not fit into a reliability report due to their size and complexity. Latent hazards are not accepted in constructing fault trees. Hazards must be known.

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 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).

RED

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). When given product function as input, RED generates the historically relevant potential failure modes of those functions and ranks them by both their likelihood of occurrence and the consequence 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 don't have substantial experience to predict failures as well as newer systems that can borrow from the experience of older products for their potential failures. While it is highly recommended by the developers that experts review the RED output and assess its relevance to the system understudy, a drawback of this risk assessment method includes 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 case, 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 –red colored, 130 moderate risks-yellow colored, and 265 low risks-green colored). 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 indicate total non-functioning of the SRBs (consequence = 4) and loss of life (consequence = 5). 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.

Insert Exhibit 2.
Insert Exhibit 3.

Findings

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 in the Challenger example. 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 of analyzing complex systems that include human error and hostile environment (Qureshi, 2008) along with RED. RED identifies and assesses risk in early design phase, which aid the managers and decision makers in minimizing the subjectivity of the likelihoods and consequences in the early stage of the design. 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 indentifying 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 identify risks that can be encountered in the entire process, including humans, organization, management, decision making, etc. Hence, risks involved with all entities concerned with the product are considered. The following models will consider risk on a broader system level, thus widening the scope of risk assessment.

LOPA

Amongst 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 method 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 scenario 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 PDF 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). Independent Protection Layers (IPLs) are simply safety systems, which 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.

Insert Exhibit 4.

The IPLs perform three main functions (Markowski & Mannan, 2010) –

1. Prevention - to reduce the probability of accident
2. Protection - to detect the initiating cause and neutralize it
3. Mitigation - to control/reduce the accident severity

The advantages of LOPA are:

- It takes less time to analyze scenarios that are too complex to be qualitatively evaluated, compared to a regular quantitative risk method.
- 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.
- LOPA is designed to deal with general decision making in risk assessment, it is not intended to be used for detailed decision making (Center for Chemical Process Safety, 2001).
- The quantified output of the analysis can reduce the uncertainty about residual risk levels (Gulland, 2004).

The disadvantages of LOPA are:

- The numbers generated by the method are only approximation and not precise. Since it is a semi-quantitative tool, its goal is to give a general idea about the scenarios with regards to potential risk carried.
- Requires experience in approximation of risk numbers.

Using LOPA to Analyze the Space Shuttle Challenger Disaster

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

Insert Exhibit 5.

Insert Exhibit 6.

Exhibit 5 and Exhibit 6 show the layers developed for the Challenger Disaster. The following demonstrates how NASA could have applied the LOPA technique to the space shuttle.

Layer 1 – Testing

Each component going into the 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 in 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 the immediate superiors, while critical issues should be escalated before it is too late in the process. With 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 the top management. It should not be a norm to issue waivers for small issues, which might eventually sum up to a bigger problem at hand. 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 shuttle for flight was done as required. This is a crucial meeting and the FRR should be used to escalate issues if they had not been 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 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.

The Human Factors Analysis and Classification System (HFACS)

One of the major causes of catastrophic accidents in many industries is human error. “Human errors have become widely recognized as a major contributing cause of serious accidents in a wide range of industries” (Hollywell, 1996). Therefore investigating why human errors occur in the first place is very essential to find the roots of any accident.

The Human Factors Analysis and Classification System was developed to analyze the United States Navy’s aviation accidents using James Reason’s Swiss Cheese Model. Early in the 1990s the U.S. Navy was undergoing a high rate of accidents and 80% of them were due to human error (Shappell & Wiegmann, 2000).

The Swiss Cheese Model was developed by James Reason 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 the accident by linking different contributing factors into a rational sequence that runs bottom-up in causation and top-down in investigation (Reason, 1997). 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 systems. On the other hand, latent conditions can occur at any level of the organization or any system and are harder to detect, such as 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, they may open or close and change in size continuously depending on the situation and the system climate. According to Sidney 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 the adverse event. Exhibit 7 shows the original version of the model with five layers comprising of Decision makers, Line management, Preconditions, Productive activities and Defenses.

Insert Exhibit 7.

The current version is not limited to certain numbers of defensive layers nor have they been 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). Since the author did not mention where the holes are, what they consist of and why they constantly move in size and position, it is the investigator's job to fill all these gaps and find out how all these holes line up to cause an adverse event (Dekker, 2002).

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, in detail, the proposed defensive layers for the aviation industry.

Insert Exhibit 8.

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

We will examine the Challenger Accident and classify the errors made according to Reason's Swiss Cheese Model (1990).

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 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 makers'. Therefore, the unsafe act defensive layer might not be applicable in the case of the Challenger Accident, thus this layer would be removed from the model. However, according to the Swiss Cheese Model, it takes both active failure and latent condition 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 -

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 $\geq 53^{\circ}$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 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 -

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 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 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, 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 (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 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.

Findings

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 prospect, 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 Swiss Cheese Model was applied successfully to the Exxon Valdez Oil Spill Incident (Altabbakh & Murray, 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, 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 historical stored data, which reduce the subjectivity of the decision made with regards to the likelihoods and the consequences of the failure modes. FTA considers all possible causes leading to an adverse event. However, FTA is dependent on the individual constructing it 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. 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. 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, not only to 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 become a guide to best practices when considering generic projects. Managers need to note that it 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 prefect model for risk assessment. The factors that can affect the decision in choosing one of these models include industry type, phase in the product/system lifecycle, time and resources available for risk assessment, 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, 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. LOPA can help in proactively managing risks and ensuring safety of the system in its entirety.

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.

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

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

Exhibit 2: RED Results for SRB Analysis

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

Exhibit 3: Examples from the detailed RED report

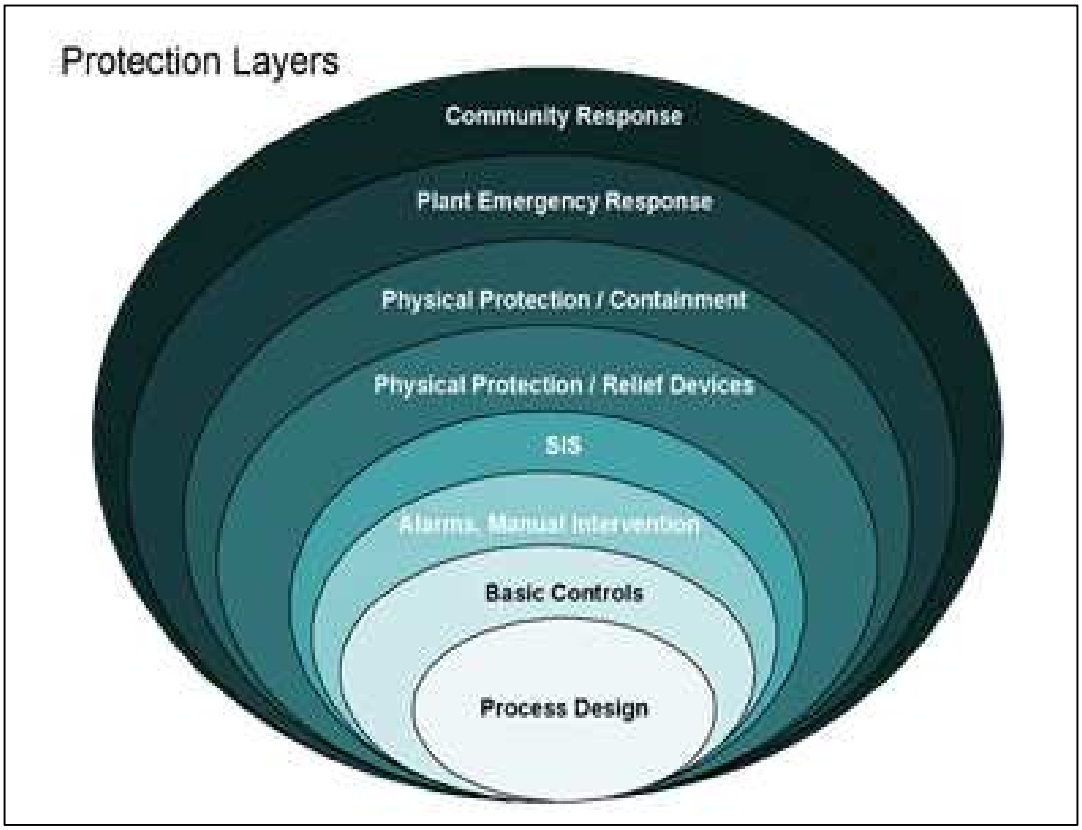

Exhibit 4: Protection Layers (General Monitors, 2011)

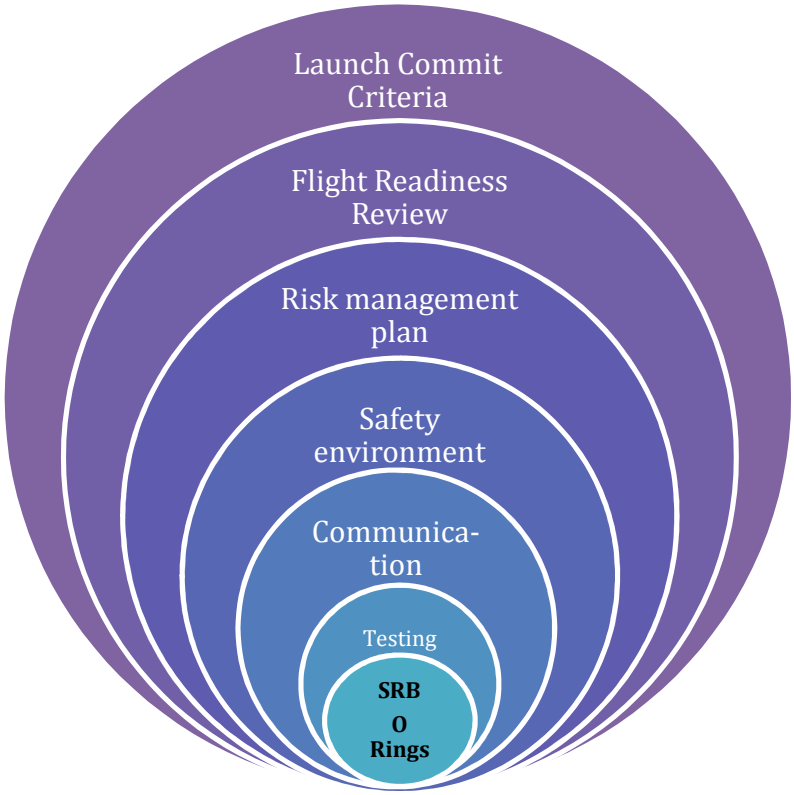

Exhibit 5: LOPA Model for Challenger Disaster (Damle & Murray, 2012)

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

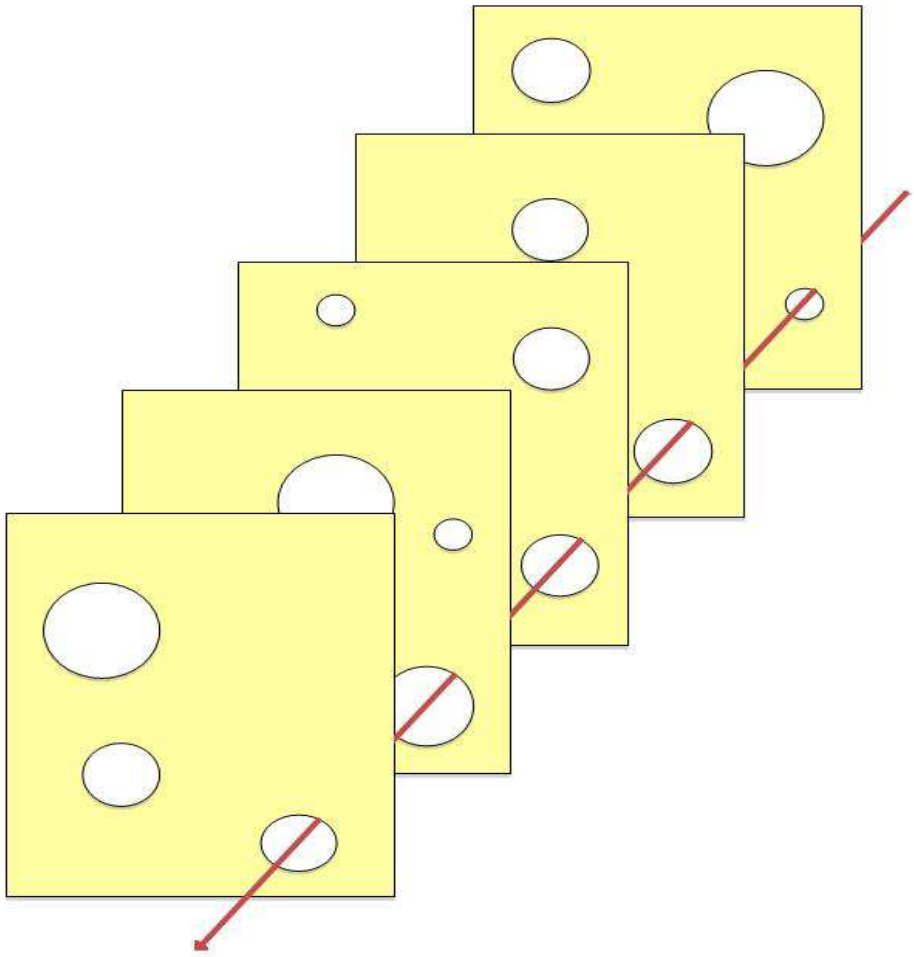

Exhibit 7: Adapted from Reason's Swiss Cheese Model

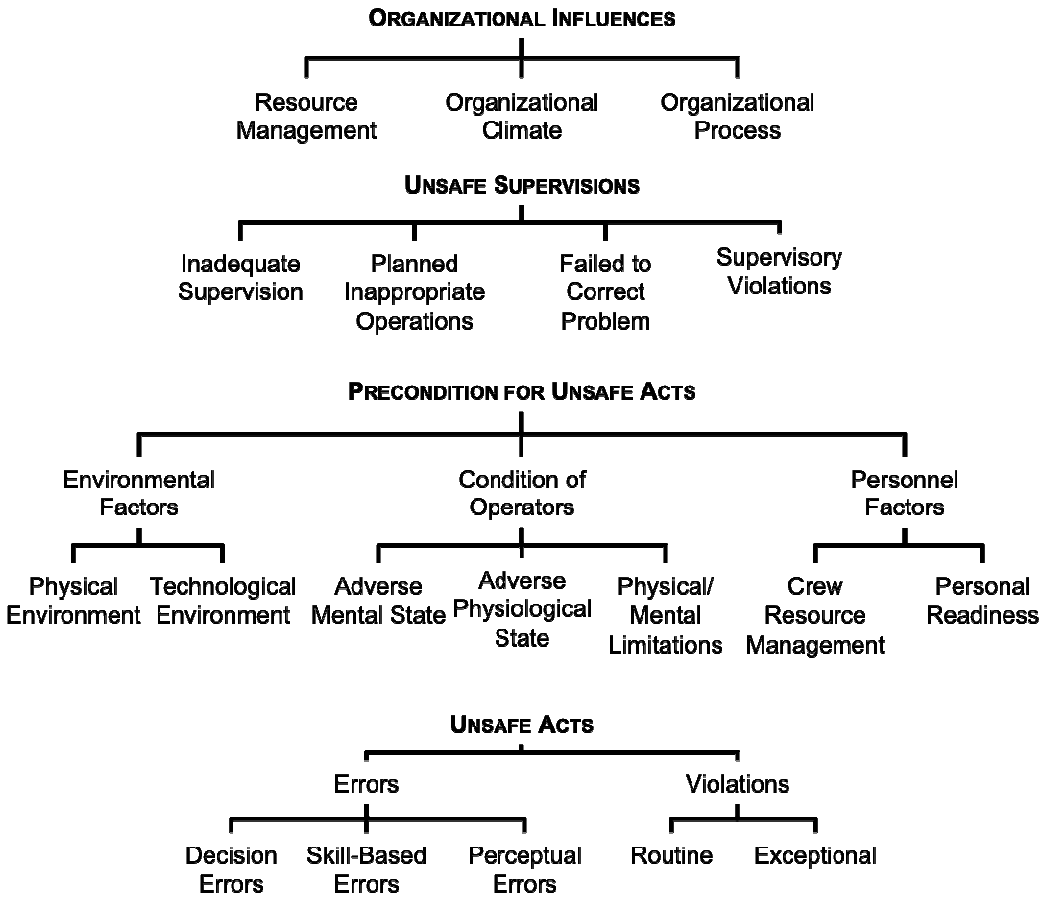

Exhibit 8: The HFACS framework (Shappell, Detwiler, Holcomb, Hackworth, Boquet, & Wiegmann, 2007)

SECTION

3. CONCLUSIONS

3.1 SUMMARY

Risk management is an essential part of any project irrespective of size. Various existing tools are used for the purpose. Inspite of pre-existing risk management procedures, accidents continue to happen. More and more research is being carried out in this field. With a view to make risk assessment easier, the generic risk matrix is useful to the project manager. It provides a set of most common and important risks to start with. Most of these risks exist in any generic project and the fact that they are ranked according to importance also gives a headstart at risk assessment.

Layer of Protection Analysis (LOPA) is being effectively used in the chemical process industry to manage risk and ensure safety of systems. This tool can now also be used to manage risks in generic projects. It gives a broad system wide approach to risk management and safety. Once independence of layers is achieved, LOPA proves to be very simple and effective in exposing and managing systemic problems. It 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, not only to 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 become a guide to best practices when considering generic projects. Managers need to note that it 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.

The analysis of the mortgage market crisis does reveal some inherent systemic risks. The entities that form a part of the financial system are largely interconnected and non-independent leading to a domino effect when one of them collapses. The LOPA model helps in identifying key recommendations which could help avoid a similar market crash in future. The model demands for the entities to be independent according to LOPA guidelines. Without independence, the model would not effectively manage systemic risks. A new set of reforms are required along with ethical behavior by the investment banks. A full disclosure of strategies is needed to help investors make wise decisions. Sub prime mortgages need to form just a small part of the total mortgage portfolio. The leverage ratios need to be capped by the Federal Reserve. Insurance companies and rating agencies need to have thorough diligence when evaluating mortgage backed securities. These recommendations, if implemented, can help reduce the systemic risk in the mortgage market. This novel method of applying LOPA to the financial industry can prove effective in reducing risk to an amount that falls under an acceptable risk range. Though there is no sufficient historical performance data, some failure probabilities can be assumed with sufficient reasoning. In this way, we can at least get a risk reduction value to start with. Further research and data collection can help in providing a better approximation of the assumed values.

The analysis of the space shuttle Challenger disaster reveals the problems within the organization with respect to decision making and culture. There were various reasons for the explosion of the Challenger. LOPA helps to build protection layers around the system under consideration. These protection layers recommend firm testing policies, effective communication, presence of safety culture, strong risk management plan without issuing waivers and changing criticality definitions and finally precedence of ethics over other pressures when launching the shuttle. Based on historical failure rates, the layer probabilities can be determined and remaining risk can be deemed acceptable or unacceptable based on the risk matrix. Implementing the model will assure a reduction in chances of occurrence of another similar disaster.

The quantification of risk is the biggest challenge when applying LOPA to generic projects. The chemical process industry has standards in place and there exist historical failure data maintained over the years. In other industries though, there is no specific historical failure data. Hence, some assumptions need to be made and probability values need to be assumed to start with. A set of procedures need to be laid down to collect data for future reference. Some quantification techniques can be used as suggested by some studies in the chemical process industry domain. Issues like ethics and human errors are difficult to quantify. Various studies have attempted to predict and quantify human error; currently most research is directed towards operator errors in a process plant/manufacturing plant setting, which are not directly applicable to human errors in generic projects.

To conclude, the study introduces a new risk management tool to the project risk domain. Firstly it lays out a risk matrix which can be readily used at the start of any project. The new tool, LOPA, is simple, less time consuming, easy to implement and intuitive. It proves to be effective in analyzing systemic issues with any organization handling big projects. It can be applied to an entire industry to design reforms and recommendations to avoid future disasters. Since this is the first time such research has been conducted, there are avenues for improvement. Continuous research is necessary to perfect the tool for generic applications. Once risk is reasonably quantified, the application of this tool can be sufficiently justified.

3.2 FUTURE RESEARCH

LOPA, for application to generic projects and other industries is in its nascent stages. As stated earlier, further research is required to perfect the study. The effective use of LOPA in the process industry is a result of years of industry specific research and continuous improvement studies. In future, an attempt can be made at collecting as much relevant historical data as possible to use for risk reduction calculations. Performance metrics for the industry entities can be determined. Annual reports can be used to quantify performance. Different ways can be explored to numerically express PFDs. A

set of procedures and guidelines can be written to apply and implement this tool in as many generic cases as possible. Models can be designed for major industries to address systemic issues. It is still a challenge to control and predict human actions, but research can be carried out to deal with issues like ethics, culture and communication. In future, this risk management tool holds promise and would prove to be extremely useful in preventing disasters, by learning from past mistakes.

APPENDIX

GENERIC RISK MATRIX SURVEY RESULTS

Risk Management Survey

Response Status: Completed

Hello, you are invited to participate in this risk management survey. This survey is to analyze the potential risks in construction projects and to generate a risk matrix. Your participation will help identify and prioritize the risks in various areas of construction projects. Participation is voluntary and there is no right or wrong answer to the survey questions. Your responses to this survey will be completely confidential. If you know of others that are well-suited to also take this survey, please feel free to forward the link to them. This survey should only take 10-15 minutes to complete. Thank you for your participation and support of this endeavor. If you have any questions please contact Amy Jacks at amj139@umr.edu.

1. What type of position do you hold within your company or organization?		
Technical	3	23%
Management	4	31%
Both	5	38%
Other	1	8%

2. Average Size of Projects		
$0 - $10,000	0	0%
$10,000 - $100,000	3	23%
$100,000 - $1,000,000	4	31%
$1,000,000 and above	6	46%
Total	13	100%

3. What type of projects do you typically work on? (i.e. bridges)
13 Responses

4. How many projects are you currently working on?
12 Responses

5. How many projects have you worked on as Project Manager?
13 Responses

6. Does your company do risk management? (Risk Management is the process of measuring and assessing risk then developing strategies to manage the risk)		
Frequently	9	69%
Occasionally	1	8%
Seldom	1	8%
Never	2	15%
Total	13	100%

7. Does your company utilize risk matrices for risk identification and mitigation? (Risk Matrix provides a structured way to identify, prioritize, and manage the impact of key risks on programs)		
Yes	5	38%
No	3	23%
Don't Know	5	38%
Total	13	100%

8. Is the risk matrix approach helpful? Yes, No, Why?
10 Responses

9. Is the risk matrix approach Company or Project Specific?		
Company Specific	4	31%
Project Specific	2	15%
Don't Know	2	15%
N/A	5	38%
Total	13	100%

Please mark the risk factors encountered in your projects or company ranking the impact and the the probability.

10. The impact of Operational Risk (i.e. lack of communication and coordination in project, labor productivity etc.)		
Critical	8	62%
Serious	3	23%
Moderate	1	8%
Minimal	1	8%
Negligible	0	0%
NA	0	0%
Total	13	100%

11. The probability of Operational Risk (i.e. lack of communication and coordination in project, labor productivity etc.)		
0% - 20%	5	38%

20% - 40%	3	23%
40% - 60%	1	8%
60% - 80%	2	15%
80% - 100%	1	8%
NA	1	8%
Total	13	100%

12. The impact of Engineering Risk (i.e. inadequate engineering designs, incomplete project scope, inadequate specifications etc.)		
Critical	7	54%
Serious	4	31%
Moderate	1	8%
Minimal	1	8%
Negligible	0	0%
NA	0	0%
Total	13	100%

13. The probability of Engineering Risk (i.e. inadequate engineering designs, incomplete project scope, inadequate specifications etc.)		
0% - 20%	6	50%
20% - 40%	3	25%
40% - 60%	1	8%
60% - 80%	1	8%
80% - 100%	1	8%
NA	0	0%
Total	12	100%

14. The impact of Performance Risk (i.e. technology limits and maturity, quality etc.)		
Critical	3	23%
Serious	5	38%
Moderate	3	23%
Minimal	1	8%

Negligible	0	0%
NA	1	8%
Total	13	100%

15. The probability of Performance Risk (i.e. technology limits and maturity, quality etc.)		
0% - 20%	3	23%
20% - 40%	7	54%
40% - 60%	1	8%
60% - 80%	0	0%
80% - 100%	0	0%
NA	2	15%
Total	13	100%

16. The impact of Credit Risk / Default risk		
Critical	2	15%
Serious	1	8%
Moderate	3	23%
Minimal	2	15%
Negligible	2	15%
NA	3	23%
Total	13	100%

17. The probability of Credit Risk / Default risk		
0% - 20%	9	69%
20% - 40%	0	0%
40% - 60%	0	0%
60% - 80%	1	8%
80% - 100%	0	0%
NA	3	23%
Total	13	100%

18. The impact of Budget Constraint / Scope Creep risk		
Critical	3	23%
Serious	4	31%
Moderate	5	38%
Minimal	0	0%
Negligible	0	0%
NA	1	8%
Total	13	100%

19. The probability of Budget Constraint / Scope Creep risk		
0% - 20%	3	23%
20% - 40%	4	31%
40% - 60%	1	8%
60% - 80%	1	8%
80% - 100%	2	15%
NA	2	15%
Total	13	100%

20. The impact of Foreign Exchange risk		
Critical	0	0%
Serious	1	8%
Moderate	2	15%
Minimal	4	31%
Negligible	2	15%
NA	4	31%
Total	13	100%

21. The probability of Foreign Exchange risk		
0% - 20%	6	46%
20% - 40%	1	8%
40% - 60%	0	0%
60% - 80%	0	0%
80% - 100%	0	0%
NA	6	46%
Total	13	100%

22. The impact of Inflation & Interest Rate risk		
Critical	0	0%
Serious	1	8%
Moderate	3	23%
Minimal	4	31%
Negligible	4	31%
NA	1	8%
Total	13	100%

23. The probability of Inflation & Interest Rate risk		
0% - 20%	10	77%
20% - 40%	0	0%
40% - 60%	0	0%
60% - 80%	1	8%
80% - 100%	0	0%
NA	2	15%
Total	13	100%

24. The impact of Insurance Risk		
Critical	2	15%
Serious	3	23%
Moderate	3	23%
Minimal	1	8%
Negligible	4	31%
NA	0	0%
Total	13	100%

25. The probability of Insurance Risk		
0% - 20%	9	69%
20% - 40%	2	15%
40% - 60%	0	0%
60% - 80%	0	0%
80% - 100%	0	0%
NA	2	15%
Total	13	100%

26. The impact of Funding Risk		
Critical	3	23%
Serious	4	31%
Moderate	3	23%
Minimal	2	15%
Negligible	0	0%
NA	1	8%
Total	13	100%

27. The probability of Funding Risk		
0% - 20%	7	54%
20% - 40%	2	15%
40% - 60%	2	15%
60% - 80%	0	0%
80% - 100%	1	8%
NA	1	8%
Total	13	100%

28. The impact of Raw Material Procurement risk (i.e. delay due to market competition)		
Critical	4	31%
Serious	1	8%
Moderate	5	38%
Minimal	1	8%
Negligible	2	15%
NA	0	0%
Total	13	100%

29. The probability of Raw Material Procurement risk (i.e. delay due to market competition)		
0% - 20%	5	38%
20% - 40%	4	31%
40% - 60%	0	0%
60% - 80%	1	8%
80% - 100%	1	8%
NA	2	15%
Total	13	100%

30. The impact of Subcontractor Procurement risk		
Critical	4	31%
Serious	5	38%
Moderate	2	15%
Minimal	2	15%
Negligible	0	0%
NA	0	0%
Total	13	100%

31. The probability of Subcontractor Procurement risk		
0% - 20%	6	46%
20% - 40%	3	23%
40% - 60%	1	8%
60% - 80%	2	15%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

32. The impact of Political Instability risk (i.e. change in policies and rules, slow approvals, instable government)		
Critical	2	15%
Serious	3	23%
Moderate	1	8%
Minimal	4	31%
Negligible	1	8%
NA	2	15%
Total	13	100%

33. The probability of Political Instability risk (i.e. change in policies and rules, slow approvals, instable government)		
0% - 20%	7	54%
20% - 40%	1	8%
40% - 60%	2	15%
60% - 80%	1	8%
80% - 100%	0	0%
NA	2	15%
Total	13	100%

34. The impact of Customer Requirement risk (i.e. change in customer requirements)		
Critical	3	23%
Serious	6	46%
Moderate	2	15%
Minimal	2	15%
Negligible	0	0%
NA	0	0%
Total	13	100%

35. The probability of Customer Requirement risk (i.e. change in customer requirements)		
0% - 20%	3	23%
20% - 40%	4	31%
40% - 60%	1	8%
60% - 80%	4	31%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

36. The impact of Weather risk		
Critical	3	23%
Serious	5	38%
Moderate	2	15%
Minimal	2	15%
Negligible	1	8%
NA	0	0%
Total	13	100%

37. The probability of Weather risk		
0% - 20%	3	23%
20% - 40%	2	15%
40% - 60%	5	38%
60% - 80%	1	8%
80% - 100%	1	8%
NA	1	8%
Total	13	100%

38. The impact of Pollution / Environmental risk		
Critical	3	23%
Serious	2	15%
Moderate	4	31%
Minimal	0	0%
Negligible	3	23%
NA	1	8%
Total	13	100%

39. The probability of Pollution / Environmental risk		
0% - 20%	6	46%
20% - 40%	4	31%
40% - 60%	0	0%
60% - 80%	0	0%
80% - 100%	1	8%
NA	2	15%
Total	13	100%

40. The impact of Cultural Relationship risk		
Critical	2	15%
Serious	0	0%
Moderate	2	15%
Minimal	3	23%
Negligible	3	23%
NA	3	23%
Total	13	100%

41. The probability of Cultural Relationship risk		
0% - 20%	5	38%
20% - 40%	2	15%
40% - 60%	0	0%
60% - 80%	2	15%
80% - 100%	0	0%
NA	4	31%
Total	13	100%

42. The impact of Society Impact risk (i.e. dam construction disturbs eco-balance)		
Critical	0	0%
Serious	1	8%
Moderate	4	31%
Minimal	2	15%
Negligible	3	23%
NA	3	23%
Total	13	100%

43. The probability of Society Impact risk (i.e. dam construction disturbs eco-balance)		
0% - 20%	6	46%
20% - 40%	2	15%
40% - 60%	0	0%
60% - 80%	0	0%
80% - 100%	0	0%
NA	5	38%
Total	13	100%

44. The impact of Litigation risk		
Critical	3	23%
Serious	4	31%
Moderate	4	31%
Minimal	1	8%
Negligible	1	8%
NA	0	0%
Total	13	100%

45. The probability of Litigation risk		
0% - 20%	7	54%
20% - 40%	3	23%
40% - 60%	1	8%
60% - 80%	0	0%
80% - 100%	0	0%
NA	2	15%
Total	13	100%

46. The impact of Non-compliance of codes and laws risk		
Critical	5	38%
Serious	2	15%
Moderate	2	15%
Minimal	3	23%
Negligible	1	8%
NA	0	0%
Total	13	100%

47. The probability of Non-compliance of codes and laws risk		
0% - 20%	9	69%
20% - 40%	2	15%
40% - 60%	1	8%
60% - 80%	0	0%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

48. The impact of Security risk (i.e. acts of god, fire, theft, terrorism, war etc.)		
Critical	4	31%
Serious	5	38%
Moderate	0	0%
Minimal	3	23%
Negligible	1	8%
NA	0	0%
Total	13	100%

49. The probability of Security risk (i.e. acts of god, fire, theft, terrorism, war etc.)		
0% - 20%	11	85%
20% - 40%	1	8%
40% - 60%	0	0%
60% - 80%	0	0%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

50. The impact of Project Delay risk (i.e. plan approval delay, delay due to other constraints)		
Critical	5	38%
Serious	4	31%
Moderate	4	31%
Minimal	0	0%
Negligible	0	0%
NA	0	0%
Total	13	100%

51. The probability of Project Delay risk (i.e. plan approval delay, delay due to other constraints)		
0% - 20%	1	8%
20% - 40%	9	69%
40% - 60%	1	8%
60% - 80%	1	8%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

52. The impact of Third Party Delay risk (i.e. sub-contractors, suppliers, vendors etc.)		
Critical	5	38%
Serious	3	23%
Moderate	5	38%
Minimal	0	0%
Negligible	0	0%
NA	0	0%
Total	13	100%

53. The probability of Third Party Delay risk (i.e. sub-contractors, suppliers, vendors etc.)		
0% - 20%	3	23%
20% - 40%	4	31%
40% - 60%	4	31%
60% - 80%	1	8%
80% - 100%	0	0%
NA	1	8%
Total	13	100%

54. Would you like to add any additional risk factors other than suggested above?

7 Responses

55. Comments

4 Responses

BIBLIOGRAPHY

Adam S Markowski, M.S.Mannan., "ExSys-LOPA for the chemical process industry in MKOPSC 12th Annual symposium". 2009: Texas A&M University.

Babu, J.R., "Layer of Protection Analysis – As effective tool in PHA. 2007", Cholamandalam MS Risk Servics Ltd.

Baybutt, P., "Layer of Protection Analysis for Human Factors (LOPA-HF)", Process Safety Progress, Vol.21., No.2, pps. 119-129, June 2002.

Bridges, W., Clark, T., "Key Issues with Implementing LOPA (Layer of Protection Analysis) –Perspective from One of the Originators of LOPA" – 5th Global Congress on Process safety, 11th Plant Process Safety Symposium, American Institute of Chemical Engineers, 2009.

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

First, K., "Scenario Identification And Evaluation for Layer of Protection Analysis", in *MKOPSC 12th Annual Symposium*. 2009: Texas A&M University.

Sawyer, M. "LOPA Lessons from Past Process Plant Accidents". 12th Annual Symposium, MKOPSC, Texas A&M, October 2009.

Summers, A.E., "Introduction to Layer of Protection Analysis", in *MKOPSC Symposium*. 2002: Texas A&M University.

VITA

Siddharth Damle was born in Pune, Maharashtra, in the western part of India. He received his Bachelor of Engineering degree in Mechanical Engineering from P.V.G's College of Engineering and Technology – Pune, India in July 2004. He worked with Burckhardt Compression (I) Pvt. Ltd. (formerly Sulzer India Ltd.) – Pune, India as Assistant Manager- Sales & Marketing, from August 2004 to July 2007.

He started his Master of Science program with Engineering Management Department at Missouri University of Science and Technology in August 2007. His primary areas of interests are in Risk Management, Corporate Finance, Financial Engineering and Project Management. He received his Masters in Engineering Management in December 2008.

Siddharth Damle entered the PhD program in Engineering Management at Missouri University of Science and Technology in the Fall of 2009. His main area of research is in Finance, Risk Management and Safety. He received his Ph.D. in December 2012.

Mr. Siddharth Damle worked as a research assistant for four years in the Engineering Management Department at the Missouri University of Science and Technology. He was an instructor for graduate level Engineering Economics (EMGT308) in Fall 2012.