

Copyright Warning & Restrictions

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be “used for any purpose other than private study, scholarship, or research.” If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of “fair use” that user may be liable for copyright infringement,

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

Please Note: The author retains the copyright while the New Jersey Institute of Technology reserves the right to distribute this thesis or dissertation

Printing note: If you do not wish to print this page, then select “Pages from: first page # to: last page #” on the print dialog screen

The Van Houten library has removed some of the personal information and all signatures from the approval page and biographical sketches of theses and dissertations in order to protect the identity of NJIT graduates and faculty.

ABSTRACT

SUPPLY CHAIN RISK MITIGATION

by
Roshan R Pai

In recent years, especially post 9/11, there has been an increasing awareness for securing business supply chains against probable disruptions. With globalization and lean inventories, the efficiency of supply chain has greatly enhanced over the years, but at the expense of new vulnerabilities. Supply chain vulnerabilities have resulted in disruptions to the economic stability and security. As a result, risk analysis and mitigation has now grown to become one of the key links to business stabilization. To ensure business continuity, it is necessary to identify key assets (physical and operational) within the supply chain and secure them against probable threats.

This study proposes a methodology to examine risks within supply chain and analyze their consequences to recommend the most effective and cost efficient safeguards to mitigate consequences. Supply chain risk management and mitigation has been broadly classified into two stages – vulnerability and risk assessment and risk mitigation through implementation of safeguards.

The vulnerability and risk assessment stage aims at the identification of the most probable threats to an organization by analyzing the related vulnerabilities to threats. Bayesian probabilistic approach has been proposed to derive inference and model the causal simulations. The risk mitigation stage aims at continuous monitoring and analyzing risk associated with the system, evaluate alternate safeguards associated with

each threat/asset pair and suggest the most effective safeguard, which would mitigate the threat consequences and occurrences.

The main objective of risk mitigation is to reduce the overall probable loss from an adversary threat. The cost of implementing countermeasures should therefore be less than the loss from a risk. Fuzzy game payoffs have been used to derive utility of safeguards and evaluate alternative safeguards available. The safeguard selected should not only be cost efficient but also provide the desired level of security to one or more supply chain elements. The level of security provided by the safeguard forms the feedback to the risk assessment stage and updates the risk levels until they are below a pre-specified acceptable range.

The risk management and mitigation system would thus enable supply chain managers to ensure sustainability of business through detection of high-risk elements, reliable identification of cost effective safeguards and continuous monitoring of these high-risk elements within the supply chain.

SUPPLY CHAIN RISK MITIGATION

by
Roshan R Pai

A Thesis
Submitted to the Faculty of
New Jersey Institute of Technology
In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Industrial Engineering

Department of Industrial and Manufacturing Engineering

May 2004

APPROVAL PAGE

SUPPLY CHAIN RISK MITIGATION

Roshan R Pai

Dr. Reggie Caudill, Thesis Advisor Date
Executive Director, Multi-Lifecycle Engineering Research Center and
Professor of Industrial and Manufacturing Engineering, NJIT.

Dr. Paul Ranky, Committee Member Date
Professor of Industrial and Manufacturing Engineering, NJIT

Dr. Mengchu Zhou, Committee Member Date
Director of Discrete Events Laboratory and
Professor of Electrical and Computer Engineering, NJIT

Blank Page

BIOGRAPHICAL SKETCH

Author: Roshan R. Pai
Degree: Master of Science
Date: May 2004

Undergraduate and Graduate Education:

- Master of Science in Industrial Engineering
New Jersey Institute of Technology, Newark, NJ, 2004.
- Bachelor of Science in Mechanical Engineering
Manipal Institute of Technology, Karnataka, India, 2001.

Major: Industrial Engineering

Presentations and Publications:

R. Pai, V. Kallepalli, R. Caudill and M. Zhou, “Methods Toward Supply Chain Risk Analysis”, Proceedings of 2003 IEEE International Conference on Systems, Man & Cybernetics, Washington D.C., USA

This thesis is dedicated to my beloved family and friends.

ACKNOWLEDGEMENT

I would like to first thank my research advisor, Dr. Reggie J. Caudill for his unwavering guidance, encouragement and support that greatly enhanced my graduate school education at New Jersey Institute of Technology. His expertise in the field of supply chain management and his valuable suggestions made my research work extremely enjoyable and rewarding.

I would also like to thank Dr. Paul Ranky and Dr. Mengchu Zhou, for serving as members of the thesis committee. Mr. Najeeb Alli, Systems Manager, MERC, deserves a special note of appreciation for his assistance and guidance. Special thanks to Mr. Donald Yee and Mr. Bob Goldberg fro Picattiny Arsenal, United States Army Armament Research, Development and Engineering Center, for providing the case study.

I am grateful to Multi-Lifecycle Engineering Research Center for providing the necessary infrastructure and support to carry out the research work. I would also like to acknowledge my lab mate, Venkata Kallepalli, whose knowledge and encouragement helped me in my crucial times.

This thesis is dedicated to my family for whom I would like to express my love and gratitude, who kept me focused and encouraged me to do my best. I also wish to express my gratitude to everyone who assisted in completing my thesis work.

TABLE OF CONTENTS

Chapter		Page
1	INTRODUCTION.....	1
1.1	Overview.....	1
1.2	Problem Review.....	2
1.3	Envisioned System.....	3
1.4	Research Needs.....	5
1.5	Objective.....	8
1.6	Outline.....	9
2	BACKGROUND RESEARCH.....	10
2.1	Terminology.....	11
2.2	Risk Management and Vulnerability Assessment.....	11
2.3	Literature Review.....	14
2.3.1	Risk Management Software.....	15
2.3.2	Decision Tools.....	24
2.4	Summary.....	37
3	SUPPLY CHAIN RISK ANALYSIS.....	39
3.1	Risk Analysis.....	39
3.2	Supply Chain Risk Assessment.....	41
3.2.1	Asset Identification.....	42
3.2.2	Asset Screening.....	42
3.2.3	Activity Identification.....	43
3.2.4	Threat Identification.....	43

TABLE OF CONTENTS
(Continued)

Chapter	Page
3.2.5 Threat Assessment.....	44
3.2.6 Risk Quantification	49
4 SUPPLY CHAIN RISK MITIGATION.....	51
4.1 High Risk Threat/Asset Identification	51
4.2 Safeguard Identification	52
4.3 Safeguard Assessment.....	53
4.3.1 Level of Protection	54
4.3.2 Value of Asset/Activity	54
4.3.3 Cost of Safeguard	56
4.3.4 Reliability of Safeguard.....	56
4.3.5 Probability of Intent.....	57
4.4 Utility Calculation	57
4.5 Safeguard Analysis	58
4.5.1 Payoff Calculation.....	59
4.5.2 Safeguard Selection.....	60
4.5.3 Safeguard Implementation.....	62
5 CASE STUDY	64
5.1 Background	64
5.2 Supply Chain Description	65
5.2.1 Operational Parameters	66
5.2.2 Risk Matrices	69

TABLE OF CONTENTS
(Continued)

Chapter	Page
5.3 Case Study – Stage 1.....	71
5.3.1 Safeguard Identification	71
5.3.2 Safeguard Analysis.....	74
5.4 Case Study – Stage 2.....	84
5.5 Case Study – Stage 3.....	88
6 DISCUSSION AND SCOPE FOR FUTURE RESEARCH.....	92
APPENDIX A SYSTEM ARCHITECTURE.....	95
APPENDIX B SUPPLY CHAIN RISK ANALYSIS AND MANAGEMENT SYSTEM METHODOLOGY.....	97
REFERENCES.....	99

LIST OF TABLES

Table		Page
3.1	Assigned Values for Frequency of Occurrence.....	42
3.2	Assigned Values for Severity of Consequences.....	42
4.1	Assigned Values for Level of Protection of Safeguard	54
4.2	Assigned Values to Value of Asset	56
4.3	Assigned Values to Increase in Value of Asset.....	58
4.4	Payoff Matrix for a Normal Game.....	61
5.1	Supply Chain Operations	67
5.2	Threat/Asset Listing for Factory	67
5.3	Threat/Asset Listing for Factory Storage.....	67
5.4	Threat/Asset Listing for CONUS Storage	68
5.5	Threat/Asset Listing for Logistics Link from Factory to Factory Storage	68
5.6	Threat/Asset Listing for Logistics Link from Factory to CONUS by Rail.....	68
5.7	Threat/Asset Listing for Logistics Link from Factory to CONUS by Truck...	69
5.8	Risk Matrix for Factory.....	69
5.9	Risk Matrix for Factory Storage.....	69
5.10	Risk Matrix for CONUS Storage.....	70
5.11	Risk Matrix for Logistics Link from Factory to Factory Storage	71
5.12	Risk Matrix for Logistics Link from Factory to CONUS by Rail.....	71
5.13	Risk Matrix for Logistics Link from Factory to CONUS by Truck.....	71
5.14	Listing of Causes for High Risk Elements	72
5.15	Listing of Safeguards Identified for Mitigating Risk	73

LIST OF TABLES
(Continued)

Table	Page
5.16 Level of Protection of Safeguards Proposed.....	76
5.17 Asset Value Listing.....	76
5.18 Listing of Safeguard Implementation Costs.....	77
5.19 Listing of Reliability of Safeguards.....	78
5.20 Listing of Probability of Intent against Safeguards	79

LIST OF FIGURES

Figure		Page
1.1	Overview of Scrams Architecture	4
3.1	Factors Contributing to Risk	41
4.1	Payoff Matrix for a Normal Game.....	59
5.1	DPICM Cartridge Supply Chain for Case Study.....	65
5.2	Threat/Asset Listing for Case Study – Stage 1.....	73
5.3	Screenshot of Utility Calculation Table – Stage 1	80
5.4	Screenshot of Payoff Calculation Table – Stage 1	82
5.5	Screenshot of Payoff Matrix – Stage 1	83
5.6	Updated Threat/Asset Listing for Case Study – Stage 2.....	85
5.7	Screenshot of Updated Utility Calculation Table – Stage 2	86
5.8	Screenshot of Updated Payoff Matrix – Stage 2	87
5.9	Threat/Asset Listing with Evidence for Case Study – Stage 3	89
5.10	Screenshot of Updated Utility Calculation Table – Stage 3	90
5.11	Screenshot of Updated Payoff Matrix – Stage 3	91

CHAPTER 1

INTRODUCTION

1.1 Overview

A supply chain is a complex network of facilities and distribution operations that perform the functions of procurement of materials from vendors, transformation of these materials into intermediate and finished products, and the distribution of these finished products to customers. Supply chains exist in both service and manufacturing industries, although the complexity of the chain may vary greatly from industry to industry.

Though the concept of supply chain can be dated back to the origin of trade and commerce, it was not until the 19th century that the industry realized the due significance of the concept. In the latter half of the 19th century, practitioners began to comprehend the inter-relationships between warehousing and logistics functions that were involved in physical distribution. The integration of these functions resulted in significant inventory-reduction benefits. With faster warehouse handling and optimized logistics, response times shortened and accuracy of forecasts increased. Improved data communication and analysis techniques led to increased ability to make complex decisions.

The next stage saw the addition of the manufacturing procurement, order management functions, and the integration of chain functions. These additions, aided by electronic data interchange, worldwide communications, growing availability of computers, electronic data, and computerized decision support systems, revolutionized the business supply chains. This new generation of the supply chain is driven by advanced communication, adoption of more user-friendly decision support systems, and

availability of shared information to all participants in the supply chain. Advances in information technology sustains continual development of supply chain management through the availability of more accurate global information, as well as the continual discovery of tools to aid the analytical process making it possible to deal with the growing complexity of supply chains.

1.2 Problem Review

The concept of supply chain has now grown beyond being a simple succession of supplier, manufacturer and customer to being a complex network of interdependent business chains. In today's connected world it is difficult for supply chain managers to identify the location of risk, the damage it can inflict and ways to mitigate the risk effects. Power outages, natural disasters, terrorism and bad management can all severely disrupt supply networks.

Over the last decade, globalization and increased competition has led to low profit margins, resulting in heavy cost mitigation measures. Organizations outsourced globally to focus on core competencies, and seek out technical innovation and low cost resources, resulting in large, complex and unstructured supply networks. The businesses focused more on efficiency rather than on sensitivity leading to adoption of Just-In-Time (JIT) philosophy. Due to the highly volatile nature of the market demand, the implementation of JIT policies enhanced efficiency and enabled significant cost reductions. The low inventory levels lowered the risk of product design obsolescence. This, however, increased system vulnerabilities and any small disruption along the supply chain could interrupt the functionality of the entire supply chain. Unintentionally, organizations have

created, or become part of, supply networks that are increasingly vulnerable to a large number of risks.

Until a few years ago, the costs involved in risk mitigation measures were not justified, even though the supply chain was vulnerable to disruptions. Moreover, since the probabilities associated with the chances of disruption of supply chain were more or less negligible, the awareness was not strong enough to motivate the study and implementation of safeguards to mitigate the risk.

The heavy disruptions in the continuity of the supply chain posed by September 11 attacks on the World Trade Center and the 11-day strike-induced shutdown of 29 West Coast ports in the US completely changed the outlook of the business industry towards contingency issues and aroused a sense of urgency towards the issue of risk mitigation. Managing supply chain vulnerabilities and mitigating the inherent risk has been realized to be the key to ensuring business continuity. The economic instability due to the rare events resulted in disruptive supply chain instabilities and the lack of awareness led to increased recovery times. The concern for these instabilities now outweighed the relatively low probabilities of their occurrence and mitigating the effect of these has now become the primary objective for survival in the market.

1.3 Envisioned System

A new decision tool, Supply Chain Risk Analysis and Management System (SCRAMS) is envisioned, which would be capable of evaluating risk impacts in business supply chains and mitigating consequences of risk elements by implementing effective safeguards. The system would perform detailed examination including risk assessment,

risk evaluation, and risk management to understand the nature of undesirable, negative consequence events leading to loss of to human life, health, property, or the environment.

The SCRAMS architecture is shown in Figure 1.1.

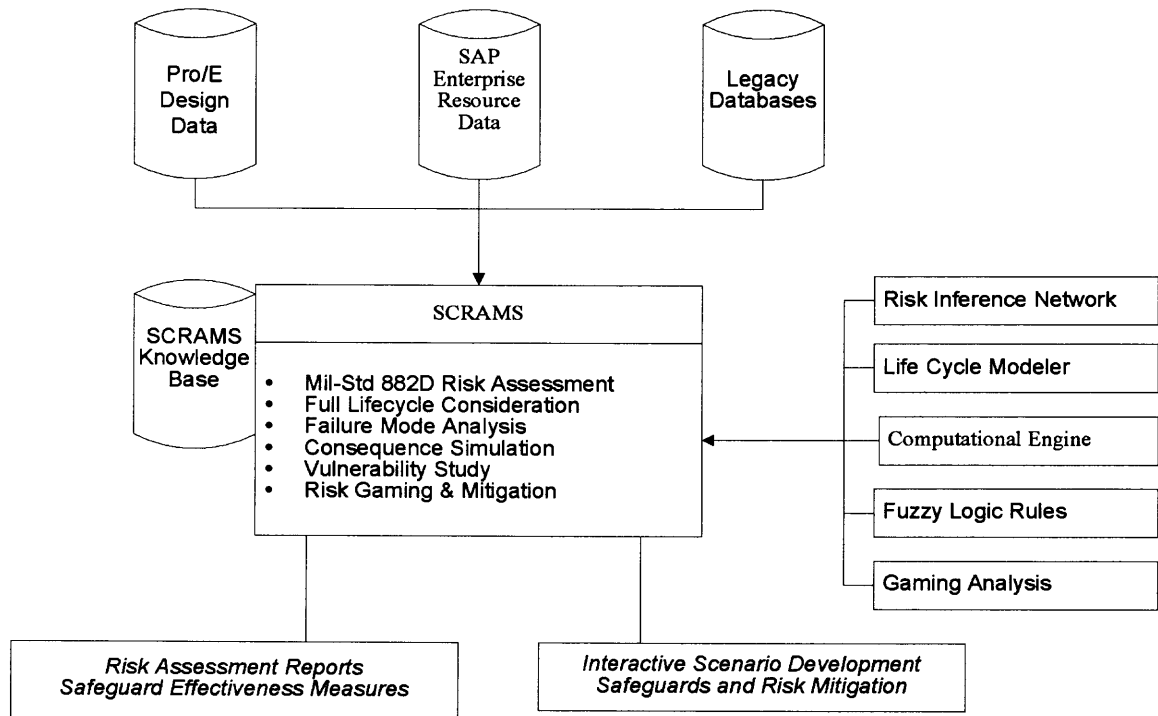


Figure 1.1 Overview of SCRAMS Architecture.

The primary objective of the Supply Chain Risk Analysis and Management system is to evaluate business risks and their mitigation alternatives in the supply chain environment. The tool will be channeled by the MIL-STD-882D guidelines and driven by a rule-based structure to better understand vulnerabilities and assess risks. The analysis framework will be developed using a responsive and intelligent inference tool capable of learning from prior assessments. The SCRAMS system will be designed to interface and extract information from the Enterprise Resource Planning software and other legacy database modules.

The architecture of the system identifies three distinct, but interdependent phases - data extraction, risk assessment and risk mitigation. This thesis will focus on addressing the risk mitigation phase, by developing a methodology to identify and evaluate safeguards required to secure supply chain elements against plausible threats. However, risk mitigation cannot be performed without risk assessment, as there is a certain degree of overlap between the two phases. Hence, this thesis will provide a brief overview of the risk assessment process to enable clear comprehension of the risk management.

1.4 Research Needs

Risk management and mitigation is the process of identifying and analyzing the key threat elements within the supply chain, evaluating their consequences on the supply chain assets and implementing safeguards to mitigate the level of risk that the threats pose. Risk management can be applied to a variety of fields ranging from insurance risk to environmental risk. However, the basic risk management approach to most functional fields is more or less the same, the only difference being the threats that pose the risk.

Conventional risk management methodology is generally applicable to static elements, for example, a factory or a nuclear storage facility, which have fixed boundaries for risk influence and is mostly a one-time assessment. Moreover, the traditional risk assessment approach does not account for external interdependencies and dynamics of the real time variations in operational and physical elements. The very structure of the supply chain is based on independencies and the existence of non-static logistic elements pose a distinctive dimension to the risk management and mitigation approach. This also creates a challenge to the risk assessment managers. The continuous

logistics and information flow along the supply chain limits the application of otherwise one-time risk identification and assessment methods.

The most significant aspect of risk management is risk mitigation, or in other words, reducing the occurrences or consequences of the identified risks. The identification of supply chain risks unless backed up by a strong risk mitigation plan that focuses on mitigating the risks, does not add value to the process of risk management. Risk mitigation renders a wider ambit to the risk management process. While many firms successfully implement strategic countermeasures for minimizing financial risk, they fail to develop strategies for operational ones leading to a passive approach to operational risk management. When a firm is indifferent to this risk, it focuses on minimizing cost without regard to the risk this strategy creates. In this case, a firm might source 100% of its raw material from a single vendor because it is the cheapest alternative, and therefore fail to have contingencies if that vendor interrupts service. Many firms subjectively factor risk by applying qualitative or intuitive constraints to a supply chain problem. In this case a manufacturer might assume that making a product in only one plant exposes the firm to service and capacity risks, but it cannot quantify the relationship between cost and risk and therefore determine the best number of production facilities.

Hence, there is a dire need to supplement the risk assessment approach with a robust risk mitigation system which should factor and implement cost effective safeguards to mitigate the probable risks within the supply chain and secure business chains from disruptions. A high level of sophistication and a rigorous methodology is required to mitigate supply chain risk, which necessitates quantifying the relationship between cost and utility (change to underlying factors like the network, suppliers,

processes etc.) and generating scenarios that ultimately best balance cost minimization with overall risk. By deploying analytical risk mitigation, firms can diversify their risk with a nominal cost increase and deploy a strategy that will yield a low long-term cost. And by building risk analysis and mitigation into supply chain decision-making, firms can outline the risk potential and prepare the business chains to deal with disruptive threats.

Risk mitigation encompasses loss prevention, loss control, and claims management. The success of a business depends on the ability of the firm to protect its assets from threats varying from natural disasters through Internet attacks to simple human errors. The challenge is in balancing the value of the assets with the cost of protecting it such that there is no wastage of money by overprotecting it, or worse, risk everything by under protecting it. The concerns that arise in risk mitigation is that how much risk is acceptable and how can that risk be mitigated and at what cost. By identifying the threats and the risks they represent to the business chains, the business value of the asset could be used as the selection criteria to identify appropriate recovery solutions in each scenario. Risk mitigation demands expertise in managing networks, system, applications, and security. Mitigating risk in supply chains requires attention to and knowledge of risk mitigation research and processes in conventional and high reliability organizations, as well as an understanding the nature and behavior of business elements. Structured effectively, a risk mitigation program will prevent losses and reduce the cost of losses that do occur while creating a low risk business environment for the organizational elements within the supply chain.

Though there have been studies on assessment and identification of risk elements within a system there has been no clear cut methodology for the identification, assessment and implementation of safeguards to mitigate the effects of these risks. Identifying the most effective safeguard, which provides the best protection for less cost, is a challenge by itself. With arising awareness for business sustainability, there is a clear demand for a supply chain risk mitigation system that can help organizations of all sizes to better manage the risks that exist within their supply chain network.

1.5 Objective

Though the concept of risk assessment is widely used in the financial sectors like insurance and stock trade, the significance of risk mitigation adds a whole new dimension which otherwise renders risk assessment futile. Risk mitigation and its applicability to business continuity and contingency planning models have not yet been explored to its full potential yet.

This study aims at bridging some of these research gaps and focuses on addressing the issue of risk mitigation within supply chains by developing a systematic approach toward identification and mitigation of supply chain risk. A performance model, which is used to reflect the systemic structure of an underlying supply chain, is introduced and a risk mitigation methodology is proposed to analyze and manage the risk. The methodology focuses on assessment and identification of the best safeguard based on its utility, cost, reliability and system vulnerabilities. The best safeguard is then fed back into the supply chain model and the consequences reassessed to evaluate the risks. This methodology would enable the development of a robust and intelligent risk mitigation

tool, which would greatly enhance the capabilities of risk management systems and enable managers to better assess and engage in more effective risk mitigation strategies.

1.6 Outline

Chapter 2 reviews the foregoing and ongoing research in the field of supply chain risk analysis and mitigation and evaluates different tools used in the field for inferencing and decision-making. Chapter 3 outlines the risk assessment methodology adopted in SCRAMS process. Chapter 4 details the risk mitigation methodology being proposed in the thesis. Chapter 5 illustrates the application of the risk mitigation methodology using a case study. Chapter 6 summarizes conclusions of the study and outlines the scope for future work.

CHAPTER 2

BACKGROUND RESEARCH

Supply Chain Management is defined as the effective integration of information and material flows within the demand and supply process [1]. This integration would include the supplier, distributor, and customer logistics requirements into one cohesive process to include demand planning, forecasting, materials requisition, order processing, inventory management and the related logistic services. Though supply chain integration enhanced the efficiency, visibility and responsiveness of businesses, the resulting complexities have made supply chains more vulnerable to disruptions. Supply Chain Management is a fast paced field and advances in technologies and decision systems keep the field constantly evolving.

Risk Management has become relevant to all aspects of management, governance and professions. Technology and process are seen as key drivers in a race against time to establish new means of competitive edge and differentiation of services. The advent of World Wide Web and advanced computer technologies has unlocked the ability to do complex business risk analysis. Interactive systems can now harness the implausible intuition of the human mind to model complex risk solutions. Risk management has become a universal management process involving quality of thought, process and responsive action.

2.1 Terminology

Risk analysis is applicable to any field that relates to uncertainty. The following terminology is the most common set of definitions used by researchers in the field of risk analysis to describe the various elements and parameters involved in risk analysis.

- Risk – Any negative outcome of an activity due to an unwanted or unplanned activity.
- Acceptable Risk- That part of identified risk, which can be borne by the management without any significant business disruption.
- Asset – Any resource that adds value to a business.
- Activity – Analogous to an asset but is described as a physical transfer of material or information within the risk environment.
- Threat – an action or potential action with the propensity to cause damage.
- Vulnerability –A condition of weakness; if there were no vulnerabilities, there would be no concern for threat activity. [2]
- Expected loss – the anticipated negative impact to assets due to threat manifestation.
- Safeguard – anticipatory steps taken to mitigate the risks.
- Consequence – the resulting effect of an action or change
- Target - Combination of a threat/asset or threat/activity pair

2.2 Risk Analysis and Vulnerability Assessment

Risk Analysis is the identification and analysis of the most probable threats to a system, the significance of the system varying with size and function within the boundaries of the risk environment. In the 70's, the concept of risk analysis started to gain recognition having derived its origins from the insurance industry. Its early focus was on protecting against catastrophe and evolved to protecting unaffordable potential losses. Risk

management evolved from natural intuition and analytical thinking into a more formal process of communication of the controls in place to influence outcomes. Today, risk assessment and management is the key to ensuring sustainability [3]. The increased level of focus and formalization of risk management as a business process has created the opportunity for experienced practitioners and innovative thinkers to capitalize on the latest technology and break new barriers in developing business solutions.

With the growing popularity of risk analysis concepts, the terms threat and asset have become conventional expressions to the risk assessment manager. A threat is an unplanned or unwanted event, which can cause a negative outcome to an activity within the risk environment [4]. The asset is anything, which can relate to a monetary value for the system and could vary from being a single operational element within an organization or a significant link to a full-fledged global supply chain. Risk analysis incorporates the identification and analysis of threats relative to the physical and operational assets, estimating consequences of threats and calculating the amount of risk associated with each threat/asset pair.

Risks are a derivative of the system vulnerabilities and hence vulnerability assessment is an integral part of analyzing the risk. The US Department of Energy defines vulnerability assessment to consist of three stages - threat assessment (pre-assessment), target analysis (assessment), and prioritizing mitigation recommendations and safeguards (post assessment) [5]. The threat assessment stage aims at determining the potential threats, the effects and probable mode of damage. Target analysis determines the susceptibility of the asset to the modes of threats based on the functionality, value, importance to society etc.

The vulnerability of a target based on the following factors: [6]

- Level of visibility (awareness of target presence and visibility of the target)
- Level of criticality (usefulness to population, economy etc)
- Value of target (value associated with the asset)
- Access to target (ease with which the target can be entered)
- Level of hazard (based on presence and concentration of hazardous material)
- Population density (max no of individuals at given time)
- Potential for collateral damage

Supply chain vulnerability has been defined as an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain [7].

Business Contingency or Disruption Management

Business contingency plan is a proactive executive commanded crisis management program driven by business requirements and is defined as the preparedness of the management to an impending disaster that can result in disruption of business. Depending on the length or severity of the disruption, the survivability of the corporation depend on ability of the management to reinstate critical business functions and to accomplish this in a timely manner demands a well thought out plan in place ready to be executed.

A business contingency plan prepares a crisis management team authorized to control any interruptions of the business to have the capability of responding appropriately to any interruption, from the interruption of a single operation to a worst case scenario involving complete collapse of supply chain functionality. Each business function has to be critically analyzed to define the consequences of an outage of service in quantifiable financial terms, operational impacts, and legal or regulatory restrictions.

These consequences have to be assessed by management to define the acceptable consequence level, which becomes the recovery time frame. Each business function may have a separate recovery time frame. The management has to identify recovery alternatives that cost effectively restores critical business functions within an acceptable time frame.

The most crucial aspect to business contingency or disaster recovery planning is the ability to communicate to large groups of people in a quick, efficient and reliable manner in order to protect lives, reduce consequences, prevent or limit economic loss, and avoid misinformation. Emergency notification serves as the strategic and tactical bridge between response and recovery efforts. Disaster recovery and emergency planning is basically a post disaster planning. While this is effective to survive in case of a disaster, avoidance of consequences would be a more desirable approach to ensure business continuity.

2.3 Literature Review

There is considerable extent of research in supply chain management, however, the field of supply chain risk mitigation is still not been completely harnessed into risk management and the literature available in this field is limited. This chapter summarizes the foregoing and ongoing research in the field of risk analysis and management and identifies the research gaps that need to be bridged in order to develop an effective and robust methodology for risk analysis and mitigation.

2.3.1 Risk Management Software

There are several software packages in the market, which completely or indirectly address the issue of risk management. This section provides an overview of these software packages. Sandia National Laboratories, a government owned risk management firm, develops risk management techniques to assess security concerns in the energy sector, military operations and homeland security. They developed methods for probabilistic risk assessment using qualitative evaluations. The technique represents risk levels in the form of matrices with row and column fields - consequences of threats and frequency of threat occurrence. Each cell in the matrix gives the risk value corresponding to the consequence and frequency levels. Sandia's technique has been used by the National Department of Justice in developing a methodology for vulnerability assessment of chemical facilities. The technique begins with identification and evaluation of the facilities in an organization to identify high priority facilities. Activities in the high priority facilities are then identified and evaluated to identify high priority activities. The high priority activities are rigorously studied for possible threats, system vulnerabilities, existing safeguards and consequences to estimate the risk factor using the risk matrix [8].

The vulnerability due to a terrorism threat has been of special significance to military and customs and techniques like DSHARP and THREATCON were developed to evaluate the vulnerability associated with the assets. These methods, though useful in evaluating vulnerability, did not provide effective risk mitigation capabilities. The Department of Defense (DoD), in collaboration with Digital Sandbox, developed a tool called the Site Profiler for assessing the vulnerability of its establishments. However, the

Site profiler mainly aimed at dealing with antiterrorism threats and other security issues associated with an asset.

The Combating Terrorism Technology Support Office (CTTSO) uses the Site Profiler for the Joint Vulnerability Assessment Tool Program (JVAT), used by all DoD organizations and installations for anti-terrorism risk assessment and planning. Digital Sandbox, in collaboration with Booz Allen Hamilton, a management consulting firm, is using the Site Profiler to manage the bio-terrorism threats by tracking chemical transactions. They are also attempting to extend the application of the Site Profiler to track passenger and cargo to detect possible threats. [9,10]

The Site Profiler is available in two versions – The Site Profiler Enterprise Server and Site Profiler Assessor. The Site Profiler Enterprise Server (ES) is a Web-based system for emergency managers, security personnel, operations managers, and resource managers to provide them with an enterprise level platform to access secure information. The Enterprise Server was built for large organizations that need to get a big-picture view of all of their security information and functions to facilitate timely and informed decision-making. [11]

Site Profiler Assessor is a vulnerability assessment tool that enables professional vulnerability assessment teams to ensure a consistent, collaborative approach to physical asset vulnerability assessment. The Site Profiler Assessor was constructed based on generic application development environment that combines a dynamically generated object model, a Bayesian inference engine, a graphical editor for defining the object model, and persistent storage for a knowledge base of Bayesian network fragment objects. The Bayesian network generated allows users to manage threat/asset pairs. The

constructed networks combine evidence from analytic models, simulations, historical data and user judgments.

The working methodology of Site profiler can be summarized as below:

- Data collection – data from disparate sources – users, historical data, analytical models and simulation
- Prompts the user to describe the features of an asset
- Prompts the user to select possible modes of attacks
- Identifies the elements that affect risk and evaluating their interaction
- Constructs Bayesian objects and risk influence network
- Computation engine solves the network and computes the risk associated with each threat/asset pair using Bayesian network solution module
- Computes the consequences of a threat using plug-ins like blast analysis
- Checks for credibility of the model and if the evidence is not credible, then the program goes back to data collection module and prompts the user to enter data or to take a decision.
- Generates the report

The software, however, is applicable only to physical assets, which is assessed for vulnerabilities based on the blast model technique. Non-physical assets like information and non-static logistic elements cannot be assessed using this technique. The Site Profiler is more or less risk assessment or vulnerability assessment software and not risks management software. Risk mitigation, which is an integral part of the risk management approach, is not integrated into the risk assessment approach.

The Buddy System, a risk management package developed by Counter-Measures Incorporation, is designed to evaluate vulnerability of assets to threat not only from terrorism, but also those from accidental disruptive elements as well. Raytheon

Corporation is using the Buddy System in support of work related to Presidential Decision Directive (PDD) 63 for the National Communications System (NCS) and the Joint Program Office-Special Technologies Safeguards (JPO-STC). The JPO work is part of the Critical Infrastructure Protection (CIP) and Critical Asset Assurance Program (CAAP). [13]

The Buddy System identifies and deals with the risk associated in a system. The package uses quantitative and qualitative analysis methodologies to compute the risk associated in a system. The software, after determining the current level of vulnerability, suggests safeguards to mitigate the risks associated in the system. The software works on the assumption that implementing safeguards will reduce vulnerability. [2]

The systematic procedure adopted by the Buddy System to assess risk is given below:

1. Comprehensive survey to generate or update relational database
 - a. Survey preload feature completes 75% of survey by populating the database of previous surveys
 - b. User answers a series of questions and has a self configuring system to fit the environment being surveyed
2. Survey is imported into analysis module by analyst
3. Establishes logical relationship between two or more surveys
4. Initial vulnerability levels are represented on the screen
5. Acceptable levels of vulnerability are set based on data sensitivity or other factors established by survey
6. Determines level of vulnerability of the system and displays graphically in either average or worst case scenario
7. Finds out threat activity

8. Calculates risk and loss probability based on level of vulnerability
9. Offers counter-measures based on rules and regulations and Return on Investment
10. Generates formal Project level risk analysis report
11. Surveys are saved as closed loops and can be modified at any later point (need not do the entire survey again and again)

The Buddy System [13] identifies two types of safeguards – Required and Discretionary. The safeguards that can be traced to one or more written rules or regulations have been categorized as Required Safeguards. The sensitivity of operation or asset, determine which regulations apply, which in turn decides which safeguard to apply. Rules and regulations are usually available for operational and process elements. However, for a global supply chain, due to increasing complexity in network, there are very few rules and regulated policies that are based on the benefits of all the partnering organizations in the supply chains. Moreover, rules conforming to each and every activity in the supply chain may not be easy to obtain.

The other type of safeguards, which the buddy system defines, is Discretionary Safeguards, which are defined to be elective. When Required Safeguards do not reduce the level of vulnerability to acceptable levels, Discretionary safeguards are implemented. Discretionary safeguards are ranked by the Buddy System based on cost, using a Return on Investment (ROI) calculation. The ROI calculation formula takes into account the number of vulnerability areas any given safeguard will reduce. This would mean that a safeguard providing a low level of protection, with low implementation cost and which addresses many vulnerable areas will be preferred over a safeguard which secures not as many vulnerable areas, but has high level of protection and high cost, even though the

latter is more reliable. This, however, need not always provide the most effective solution to secure assets within supply chains. The vulnerabilities should be secured based on their significance. Since interdependencies are key drivers in supply chain, securing the asset with the highest vulnerability, even though at high cost, can result in the reduction of many related vulnerabilities within the system.

Return on investment is generally based on the amount of money that a company would lose provided the vulnerabilities were not secured by the safeguard. There are many other factors that need to be considered other than just the potential loss. The reliability of the safeguard would be a critical element in the selection of the safeguard. Also, the chances of disruption of the safeguard also cannot be ruled out.

The Cobre Group [14] has developed software, Helpmate, to simulate the supply chain elements for optimal resource planning. It does not provide any risk assessment capabilities, but creates a standardized platform to document and map the various process elements within the organization.

The company, E Team, Inc. [15] provides enterprise-level collaborative software to public agencies and corporations for use in emergency response management, facility and event security, disaster preparedness and recovery, and business continuity. In an event of disaster, the E Team solution deploys rapidly, enabling all users to communicate and collaborate in real time, and manage resources as the situation demands. E-Team provides a common enterprise level platform which helps coordinate and communicate effectively to help recover from a disaster.

At the Los Alamos National Laboratory, researchers have developed simulation tools to analyze certain key areas like transportation, epidemic breakouts and

infrastructure independencies. These simulations result in better understanding of key factors influencing an activity. For example, the simulation of the traffic system enables a better understanding of traffic bottlenecks and the traffic control can then be modified to avoid this. The simulations perform different iterations for different safeguards and show the relative effect of their implementation. The system by itself does not seem to suggest any safeguard but the simulations represented graphically can be interpreted better. [16]

Palisade's @RISK [17] is a financial risk analysis and Monte Carlo simulation add-in for Microsoft Excel. @RISK integrates with the excel spreadsheet, adding risk analysis to the existing models. @RISK uses Risk probability distribution functions to define uncertainties and displays all possible outcomes in a situation and their probabilities of occurrence. However, the software has no decision inference capabilities.

Vulnerability Assessment Process

B. D. Jenkins proposed a set of axioms to carry out the risk analysis procedure [2]:

1. The same population of threats exist for all systems and networks
The threats posed to a system are infinite in number and variety. Any threat can occur in any part of the system at an unpredictable and uncontrollable frequency. The only factor that can be estimated is the relative likelihood based on prior occurrences, for example the likelihood of Colorado and California being hit by an earthquake is higher than any other state in the US, but there is still a great deal of uncertainty associated with the occurrences.
2. The frequency of occurrence of a threat cannot be controlled.
3. The level of the vulnerability decreases as the safeguards increase.
Implementation of safeguards reduce the risk in the system, the extent of reduction in the risk depends on the safeguard implemented.
4. All safeguards have inherent vulnerabilities.
5. An acceptable level of vulnerability can be achieved through the implementation of safeguards.

Based on the above axioms and summarizing the procedures used by the other software packages in the market, a generic process is outlined below in the following steps:

- 1 Identify and evaluate the supply chain components and list its assets
- 2 Evaluate assets based on value, criticality, sensitivity or a mix of these
- 3 Identify threats within risk environment
- 4 Evaluate threats and determine consequences on the assets
- 5 Estimate risk associated with each threat/asset pair
- 6 Identify high risk elements
- 7 Identify safeguards to secure assets
- 8 Evaluate safeguards against each other for utility and cost
- 9 Identify best safeguard
- 10 Implement Safeguard
- 11 Generate Report

The risk analysis and mitigation report must document the threats posed to the system and the safeguards, which secure them. The report should recommend the safeguards to be taken in order to reduce vulnerability levels to an acceptable level. The report should ideally include the vulnerability level, the threats mitigated, threat interaction effects, residual risks, frequency, particulars of the operational environment, system connectivity, data sensitivity levels, residual risk and expected annual loss.

The main objective of risk mitigation is to reduce the overall loss from an attack by implementing safeguards. The cost of implementing safeguards should therefore be

less than the loss from a risk. In risk mitigation, though the cost of implementing and maintaining a security measure and the indicated loss from the threat are trade offs to retain the cost benefits, the expected utility that the safeguard provides often overrules its cost. In some cases the implementation of the safeguards maybe guided by the significance of the entity under consideration rather than costs alone.

Constraints in implementing risk mitigation plan [18]

- Costs
- Interference with ongoing programs
- Lack of expertise
- Lack in efficiency
- Lack in functionality or effectiveness

Currently, with disruptive uncertainties lingering around business supply chains, the industry calls for a risk analysis and management system specifically designed for supply chain risk mitigation. The software systems discussed above, although comprehensive in approach, do not pertain appropriately to supply chains. The Site Profiler deals only with vulnerability of static physical assets. The Buddy System, although detailed in approach, does not consider reliability factors for safeguards and focuses more on cost aspect than utility aspect of safeguards. Companies like the E-Team and Strohl Systems deal with post disaster recovery and management. Researchers at the Los Alamos National Laboratories developed simulation tools to analyze certain specific areas but the system does not incorporate more than one activity at a time nor the inter relationships between activities. There are many more software which relate to financial

risk assessment like the Palisade groups, @Risk, but all of them are very specific in their application.

2.3.2 Decision Tools

Risk analysis and management entails a certain degree of intelligence to be embedded within the methodology in order to develop a system which is robust in its functionality, reliability and consistency. The heart of any decision-making system is a good inference engine. The inference engine must be based on the requirements of the network structures and on the form of data available. Some of the inference techniques used in decision-making are Bayesian Networks, Fuzzy Logic Structures, Hybrid Networks and Game Theoretic Reasoning. Kathryn Laskey, a renowned researcher of decision support systems, used Bayesian inference to develop the Site Profiler [9]. David Heckerman, a researcher at Microsoft Inc., Washington, used the Bayesian approach to model the Microsoft Office Assistant [22]. Heping Pan from Australia is working in the area of Fuzzy Bayesian Networks [26]. There is no study, however, that has been conducted comparing the different inference techniques to decide which inference technique is best for a particular area.

Selecting the most appropriate inference engine would be crucial to the reliability of the system. At this point, no inference technique can be rated to be better than the other. But the choice of the inference techniques would depend on the system model and the behavior of the system variables and the form of data available. Bayesian Networks are based on probabilistic inference, while fuzzy logic uses a more linguistic terminology to define membership values that can manipulate between varying degrees of variable definitions. Hybrid Networks, use both the applications to combine the advantages of

probabilistic inference and membership functionalities. However, research of the applicability of hybrid networks is still in its beginning stages of research. Once the risk management system model has been generated and the behavior of the variables clearly understood, the appropriate inference engine could be selected.

2.3.2.1 Bayesian Networks. These are also called Belief Networks or Probabilistic Inference Networks. The idea of Bayesian networks was initially developed by Pearl (1988). Bayesian networks in the recent years have evolved as an excellent and powerful tool to handle uncertainty. The concept has become popular in the recent times due to tremendous increase in computational power and due to development of heuristics search techniques to find events with the highest probability.

Bayesian networks are based on the Baye's theorem, which was proposed by Thomas Baye in 1763. The theorem combines subjective beliefs and the evidence available to draw logical inference. Initially, Bayesian theorem did not find much application, as it is difficult to assign the full probability distribution manually. With the advances in computational power, network generation and data feeding, a new dimension was found to development and understanding of Bayesian networks. Much of development in Bayesian Networks has been attributed to the science of Artificial Intelligence. [19]

It was not until the late 80's that researchers discovered that Bayesian networks could be used to handle uncertain information. Horvitz and his two colleagues, at Microsoft, developed a Bayesian based network to could diagnose the condition of patients without turning to surgery. This method was effective and efficient in combining historical data and imprecise subjective beliefs of the experts in the field. [20]

Scott Musman, developed a network which could identify enemy missiles and aircrafts and recommend the best weapons to counteract the enemy. General electric developed a technique, which can locate emerging engine problems based on the information from sensors and from the expert opinion, which is encoded into the database. [21]

The basic idea of using Bayesian networks is to address the following

- Modular knowledge in the world - most events are conditionally independent of most other events.
- Adoption of a model that can use a local representation to allow interactions between events that only affect each other.
- Make distinction between unidirectional and bi-directional events in the model
- Define the causal relationship between events in a network.

A Bayesian Network can be viewed as an annotated directed acyclic graph that encodes probabilistic relationships among distinctions of interest in an uncertain reasoning problem. The representation rigorously describes the relationships using quantitative structure that facilitates good communication between the user and the probabilistic system model [22]. Bayesian updating provides a means of propagating probabilities. Bayesian networks are a rich and powerful way of building probabilistic models. The nodes in a Bayesian network is divided into three types –

1. Chance nodes – representing random variables
2. Decision nodes – the decision can be made from a choice of options
3. Utility nodes – represent the utility function

Dynamic Belief Networks are similar to the Bayesian Networks, but for their state variables, which are time dependant. These networks grow over time and can end up occupying a large section of the database memory. But this size is controlled by maintaining only two time slices of the network in the memory.

Bayesian Nets can be used for the following purposes : [23]

1. Calculating the belief in query variables given the values of evidence variables
2. Predicting values in dependent variables given values for independent variables
3. Decision making based on probabilities in the network and on influence diagrams
4. Sensitivity analysis to test the impact of changes in probabilities on decisions

Bayesian Networks are used in a variety of applications including medical diagnosis, forecasting, manufacturing control, fault tree diagnosis etc.

Avantages of Bayesian Networks

1. Forward and backward reasoning enabling assessment of overall influences [24]
2. For simple discrete Bayesian Networks with discrete nodes, the inference is solvable in linear time. [25]
3. Conditional interdependence allows efficient updating and the probabilities can be changed in wake of new evidence [26] [23]
4. Matches the real world where probability of one event is conditional on the probability of previous one [27]
5. Domains can give a correct idea of the interrelationships making it easier to comprehend [27]
6. Data can be dynamicaly combined with the network at the run time thereby enabling continious monitoring [28]

7. Elaborate research has been conducted in this field to tap the full potential of Bayesian networks [29]
8. Best and consistent method for reasoning under uncertainty [28][30][26]
9. Can be used on real large scale problems [28]
10. Can combine diverse data including subjective beliefs and empirical data [31]
[28]
11. Can reason with incomplete data [30][28][31]
12. Sensitivity analysis capabilities [28]
13. Visual reasoning that makes all assumptions and evidence explicit and auditable to the regulator [28]
14. Integration of multiple forms of data [28]
15. Bayesian Models are very robust due to the easy updating capabilities [30]
16. Can handle different kinds of variables like continuous and discrete [30]
17. Can be used for data mining and fault tree diagnosis [30]
18. Ability to decompose a probability distribution into a set of local distributions [32]

Drawbacks of Bayesian Networks

1. The events represented by each node has to be mutually exhaustive [29]
2. The number of conditional probabilities varies exponentially over the number of nodes [29] [24]
3. The Bayesian network inference is known to be NP-Hard (not solvable in polynomial time) and the inference drawn from the network is an approximation[33] [24]

4. Knowledge acquisition is difficult and requires a large and uniform dataset [29]
5. Bayesian Networks do not account for the vagueness in the variable states [29]
[23]
6. Exclude the possibility of an event that is neither completely true nor completely false [29]
7. Updating new information is difficult and time consuming [34]
8. Exceptions like “none of the above” cannot be represented [34]
9. Though discrete and continuous nodes can be incorporated separately, combinations of them cannot be used in one network [23]

2.3.2.2 Fuzzy Logic. Fuzzy logic is a superset of conventional Boolean logic with extensions to cater for imprecise information. Fuzzy logic permits vague information, knowledge and concepts to be used in an exact mathematical manner. Words and phrases such as 'fast', 'slow', 'very fast', 'quite slow', 'not very fast' are used to describe continuous, overlapping states. This enables qualitative and imprecise reasoning statements to be incorporated within rule-bases so producing simpler, more intuitive and better-behaved models.

Fuzzy logic is based on the principle that every crisp value belongs to all relevant fuzzy sets to various extents, called the degrees of membership. These range from 0 (definitely not a member) to 1 (definitely is a member) with values between generated by a membership function. This contrasts with conventional Boolean logic, where membership of a set is either false or true, i.e. 0 or 1. This graduation from zero to one enables us to smooth out and overlap the boundaries between sets. Unlike Boolean logic where sets are mutually exclusive, Fuzzy logic allows crisp values to belong to more than

one Fuzzy set. This means that in a Fuzzy system all rules are used, with each having some influence on the resulting output. This is more of a consensus approach to expert systems.

Fuzzy network is established through the subsets that are generated defining the mapping between elements and quantifying certain degrees of membership (between 0 and 1). Any system that runs on Fuzzy control incorporates the concept of Fuzzy variables, (like speed, temperature) and the concept of Fuzzy qualifiers (hot, cold, slow, fast). Applying a qualifier to a Fuzzy variable generates a Fuzzy set. For each Fuzzy set there is a membership function relating crisp to Fuzzy values, and which is defined in terms of its shape and location. Fuzzy logic also incorporates the function of Fuzzy modifiers (very, extremely, not very), often referred to linguistic hedges. These affect the membership function by intensifying or diluting its shape. Fuzzy rules define relationships between different Fuzzy sets as if-then rules. These rules can be grouped into matrices, commonly known as Fuzzy associative memory (FAM).

Pure Fuzzy logic has extremely limited applications and the only popularized application is the Sony Palmtop. The main use of Fuzzy logic is as an underlying logic system for Fuzzy expert systems. Fuzzy expert system is a collection of membership functions and rules that are used to reason about data.

Applications of Fuzzy Logic based systems

1. Robots and other automated control mechanisms
2. Camera aiming for live telecast (Omron)
3. Prediction Systems for early recognition of earth quakes
4. Archiving system for documents

5. Flight aid for helicopters
6. Simulation for legal proceedings
7. Improving safety of Nuclear reactors
8. Temperature control
9. Traffic Control
10. Environmental Analysis

Advantages of Fuzzy Systems

1. Accounts for the ambiguity or uncertainty in describing an event [29]
2. Represents better interpolation between states for variables [29]
3. Represents uncertainty of categorization [29]
4. Simplified and reduced development cycle [35]
5. User friendly and efficient performance [35]
6. Can reason with incomplete data

Drawbacks of Fuzzy Systems

1. There is no completeness in inference formalism i.e. there is no optimal method for drawing an inference. The inference can be drawn from a combination of different rules, but no specific combination of rules can be clearly identified as giving an optimal solution for a given problem. [29]
2. Basic functions like min and max, which are the core components in Fuzzy logic are not supported by evidence, but are assumptions [29]
3. Backward reasoning is not possible
4. Membership values do not change in the wake of new evidence. [36]

2.3.2.3 Game Theory. Game theory is the study of situations involving contending benefits, modeled in terms of the strategies, probabilities, actions, gains, and losses of opposing players in a game. Game theory can be applied to economics, political management and many other fields, in which, strategic decision making is involved. A crucial aspect of the specification of a game involves the information that players have when they choose strategies. The simplest games are those in which agents have perfect information, meaning that at every point where each agent's strategy conveys to take an action, and knows everything that has happened in the game up to that point. A board-game of sequential moves in which in which both players watch all the action, such as chess, is an instance of such a game. The more complex games are the imperfect information games, which mimic real life situations more appropriately than perfect information games.

An analysis of supply chain strategic decision-making can benefit from applying game theory concepts. Game theory attempts to model the results of interactions between people or groups whose motives are not identical, if not opposed and has become an essential tool in the analysis of supply chain strategies with multiple agents. This section surveys the applications of game theory to supply chain analysis and outlines game-theoretic concepts that have potential for future application. The section does not explore the implications of game theoretic analysis on supply chain management, but rather, emphasizes the means of conducting the analysis to keep the exposition short. Many of the useful theoretical tools are spread over dozens of papers and books, buried among other tools that are not as useful in supply chain management. [37]

A strategy can be thought of as the complete instruction that drives the actions to be made in a game. A player can choose a strategy without absolutely no knowledge of the other players strategy. The strategy choice by one player is not allowed to limit the feasible strategies of another player. In the normal form players choose strategies simultaneously and the counter-actions are adopted after strategies are chosen. As an alternative to the one-shot selection of strategies in the normal form, a game can also be designed in the extensive form. However, normal form games portray a better proximity to real life situation, where, the strategies are not chosen one after the other, but almost simultaneously.

The mathematical theory of games was invented by John von Neumann and Oskar Morgenstern [38]. Since the late 1970s game theory has gained significance and has proven to be a useful tool for situations in which rational decision-making depends on the expectations about the game environment. Despite the fact that game theory has been rendered mathematically and logically systematic only recently, game-theoretic insights can be found among philosophers and political commentators going back to ancient times. The study of the logic that governs the interrelationships among strategic interactions and outcomes has been fundamental in modern political philosophy, since centuries before anyone had an explicit name for this sort of logic. Since managers have a special concern for the logical justification of actions, game theoretic reasoning is gaining in confidence due to the facts that actions are justified by reference to their expected outcomes.

The gains of each player at different stages in a normal game is described by means of an abstract concept called utility. The numbers featuring in an ordinal utility

function do not measure any quantity of anything, in other words, the numbers are relative and not absolute.

Utility

Game theory can be interpreted as providing an explanatory account of strategic reasoning. This explanatory account which justifies the choice of a strategy is termed as the utility. Based on the utility function, games can be of two types – zero sum games and non zero sum games. Zero-sum games are games where the amount of resources or utility is fixed, and whatever one player gains, the other loses. This corresponds to a situation of pure competition. In realistic situations, zero sum games exist only in a situation of pure competition, where the interests of both players are common and all strategies are aligned toward those interests. This is however, not the case in real life situations. Players engaged in a non-zero sum conflict have some complementary interests and some interests that are completely opposed. Hence the gain of one player, would not be the same as the loss of other player. Therefore, in the remainder of this chapter only nonzero outcome, imperfect information normal form games are discussed.

Payoff Function

A payoff function is defined as a measure of gain that a strategy provides based on its utility. Payoffs are generally functions of the utility. A game is defined by the payoffs assigned to the players and a strategy is defined by the utility it provides. The concept of game theory assumes that players are economically rational and a player can assess payoffs to outcomes, determine paths to outcomes and choose actions that yield the most-preferred outcomes by maximising their payoffs.

Payoff Matrix

A payoff matrix is a $n \times m$ matrix which lists the payoff functions of each player's strategies against the other player's strategies. Each field in the payoff matrix can either consist of one or two fields depending on whether the game is a zero-sum or a non-zero-sum game, respectively. In relevance to supply chain and real world environments, only non-zero-sum games are applicable, and hence, the payoff matrix consists of two fields, which relate to the payoff functions to each player. Once a payoff matrix is generated for a game, the strategies can be evaluated based on the payoff functions depending on the objective of the game.

Over the last few years, game theory has proved to be a powerful tool with which to design decision environments, and to understand interactions in systems. Game theory, building on the assumption that agents are rational and self-interested, has been employed in the design of mechanisms and protocols for interaction, coordination, communication, negotiation, coalition formation, fair voting techniques, market-based resource management systems, and industrial-scale information economies. [39]

Rapid developments in technology, communication, industrial organization, economic integration, political reforms and international trade have made it increasingly imperative to recognize the causes and effects of strategic interdependencies and interactions. A strategic approach to decision-making is crucial in areas such as military and naval warfare, trade negotiations, capital accumulation and investment, market integration, regional cooperation, development and implementation of new technology, international resource extraction, network sharing, competitive marketing and in particular supply chain management. Since its inception, game theory has contributed

significantly to the foundations of decision-making. As socio-economic and political problems increase in complexity, further advances in methodology, techniques, empirical investigations and applications of game theory are called for. Probabilistic and logical inference techniques are being embedded into game theoretic models to generate more robust and adapt decision tools.

Qiumin Zhu and Junping Sun have studied the application of game theory and Bayesian probability integrated approach to configure a decision support system paradigm. Bayesian game theory has been used as a viable means for modeling uncertainties in decision support. The Bayesian game constructs information complete games from information incomplete games by introducing random events to occur before the players choose their strategies. The random event describes the cost functions completely and hence is assumed to completely describe the payoff function. However, each player will be assumed to know only his cost functions and utilities but not the opponents [40].

Yan-Qing Zhang and group developed the theory of fuzzy moves by incorporating fuzzy inference and precise inference within the classical game theoretic approach. Generally the game theoretic approach can locally make the player achieve a goal, but this goal is an absolute goal. However, the fuzzy based approach can make a player achieve relative goals, in the sense that, it would not only be advantageous to the player, but also disadvantageous for the opponent. [41]

2.4 Summary

The recent terrorist strikes, political instability in third world countries, the last year's shutdown of West Coast shipping docks and the 2003 Blackout have awakened supply chain managers as never before to supply chain risks, some of which had been introduced or heightened by the very actions companies had taken to drive costs out of their supply chains. Now that this inverse relationship between risk and efficiency has been realized, supply chain managers apprehend that they cannot focus on cost cutback alone, but on inherent vulnerabilities as well. Risks lurk along the entire length of supply chains, and are as diverse as political instability, exchange rates, carriage capacity, shelf life, natural disasters and customer demand.

To avoid potentially catastrophic events, inventory managers and logistics managers, among others, must manage risks, and not ignore them by balancing operating costs with supply chain risk. An analytical risk mitigation process enables firms to tie risk management into strategic and tactical analyses, thus reducing overall costs, avoiding service disruption, and better balancing capacity and demand. To manage supply chain risks effectively, firms should not treat optimization as a single mathematical exercise that chooses the right answer to reduce cost or risk, but employ a higher level of sophistication in managing supply chain risk-analytical risk mitigation.

There is a clear need for a risk management and mitigation system which can assess and evaluate risks, identify potential safeguards and evaluate safeguards against each other with an aim to implement the most effective safeguard. The effectiveness of the safeguard should not be driven by cost or utility alone, but by a combination of cost, utility, reliability and potential disruptive elements influencing safeguards. The challenge

is in realizing the limits of risk that an organization, operation or an asset can endure without any significant impact on business entities during an event of disruption.

The heart of any decision-making system is a good inference engine. The review of different inference and decision-making tools, despite providing a good understanding for the applicability to logical inferencing, does not provide any basis of judging their relative capabilities. The choice of the inference techniques would depend on the system model and the behavior of the system variables. Since most supply chain related events are interdependent and it is better to model the system behavior based on historical data than managerial perception, a Bayesian inference engine would be apt for generating logical inference for risk assessment and evaluation. Risk mitigation requires strategic evaluation of safeguards based on its utilities. Game theory has proved itself to be a powerful tool to weigh strategic outcomes and would be the right tool to evaluate safeguards against each other.

CHAPTER 3

SUPPLY CHAIN RISK ANALYSIS

This thesis is a part of an extensive research in progress at the Multi-Lifecycle Engineering Research Center (MERC) in the field of supply chain risk management. In order to enumerate the supply chain risk mitigation methodology, it is essential to illustrate the supply chain risk assessment approach. The first few sections provide a brief overview of the risk assessment methodology, which forms the basis for the risk mitigation methodology being proposed in the thesis.

3.1 Risk Analysis

In recent years, interest in risk assessment approaches that better describe and quantify uncertainty has increased in the scientific and regulatory communities. Faced with the necessity to characterize uncertainty explicitly in risk assessments, the challenge is to effectively identify, adequately quantify, and methodologically analyze all significant sources of uncertainty for estimates of risk. Frequently, alternatives to assumptions are not adequately considered, nor are the impact of specific alternatives on the final sensitivity estimates assessed. To characterize uncertainty satisfactorily, the overall structure of the risk assessment must be well defined, the alternatives within the structure that influence sensitivity estimates clearly specified and appropriately structured to incorporate and facilitate mitigation strategies.

Risk is defined as the quantitative or qualitative expression of possible loss incorporating both the probability that a threat and the consequences of that event. Risk estimates are typically based on two parameters - the frequency of occurrence and severity of consequences. The more frequent a threat activity, the more significant the likelihood of the threat occurring, higher the risk exposure.

The severity of consequences defined by the loss or disutility due to the adverse outcome, indicate the degree of probable risk. However, either of the above estimates cannot be used alone to quantify risk. An event with a high frequency of occurrence would not necessarily contribute to high risk if the consequences of the event are negligible. On the other hand, an event with low frequency of occurrence, but with high consequences can definitely escalate risk. Hence, risk is best estimated as the product of frequency of occurrence and severity of consequences.

$$\text{Risk} = \text{Frequency of Occurrence} * \text{Severity of Consequences} \quad (3.1)$$

The real challenge is to estimate the frequency of occurrence of the events and the degree of consequences that the threat imparts to the entities under consideration. Frequency of occurrence is generally obtained from the historical data or from prior estimates of the event. Severity of consequences are estimated based on simulations, prototype testing or from subjective knowledge based on the influences of the threats on the different factors contributing to risk within the system domain.

The frequency of occurrence and severity of consequences are derivatives of four parameters - probability of occurrence, consequences of the threat on the system, vulnerabilities associated and the effectiveness of the safeguards in place. The Figure 3.1 gives a pictorial representation the factors contributing to risk.

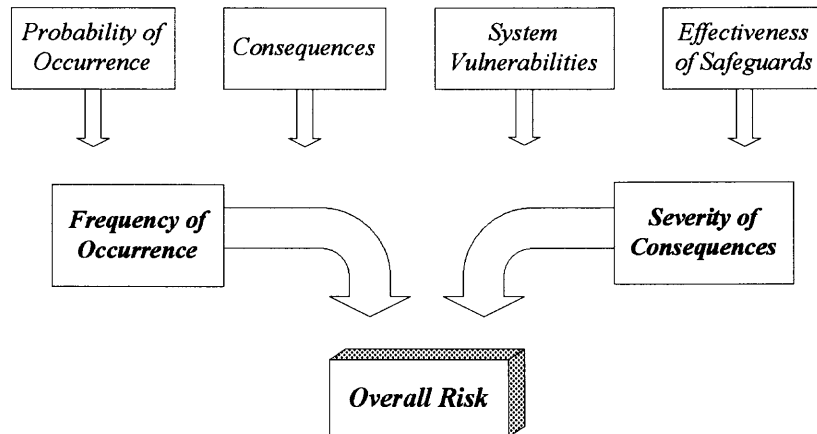


Figure 3.1 Factors contributing to risk.

3.2 Supply Chain Risk Assessment

Supply chain risk analysis is distinctively different from traditional risk analysis due the presence complex interrelationships among business entities. This section summarizes the supply chain risk assessment methodology developed as a part of the SCRAMS (Supply Chain Risk Analysis and Management System) architecture at the Multifecycle Engineering Research Center (MERC). The methodology is a derivative of the process proposed by the National Institute of Justice to assess vulnerability of chemical plants and Military Standard 882 D [13, 51]. National Institute of Justice developed a prototype model to assess the vulnerabilities in a chemical facility. Even though the methodology developed was for a chemical facility, the underlying concepts could be extended to a supply chain risk analysis. Risk analysis of a supply chain is classified as below:

- Asset Identification
- Asset screening
- Activity Identification

- Activity Screening
- Threat Identification
- Threat Assessment
- Risk Quantification

3.2.1 Asset Identification

An asset is defined to be an entity that has value to the organization, its business operations and their continuity. Assets include employees, manufacturing and distribution facilities, physical equipment, operational elements, stocks etc. Asset identification and categorization enables greater estimation of supply chain vulnerabilities.

The assets within a supply chain are classified to be under facility nodes or logistics links. Any physical static asset is defined as a facility node, whereas any transfer of material or information is defined to be logistics link. The logistics links typically interconnect or network the facilities across the supply chain.

3.2.2 Asset Screening

Each asset within the supply chain contributes toward the existence and continuity of the supply chain at varying degrees of significance. Gauging the assets based on their significance eliminates redundant assets, which may not require a risk assessment. Evaluating the assets may be based on several factors – the workforce employed within the asset, the physical and monetary value, and the significance of the asset to business continuity etc. These parameters may be determined based on objective values or subjective beliefs, based on the detailed availability of statistics. Based on the parameters, the assets are ranked to be under – high priority, medium priority, low priority and very

low priority asset. If the priority value is high or medium, then an assessment is recommended, however assessment for the assets with low and very low priority is not necessary.

3.2.3 Activity Identification

An activity is defined as any operation or process within an asset (facility node or logistics link), which generates value to the business. Every activity can be broken down into sub-activities; however, the desired level of reliability in risk assessment drives the depth of activity breakdown. The higher the reliability desirable, the more in-depth the activities must be defined. The priority of the activity is estimated based on the significance of the activity to the asset or business, its recognizability and accessibility and the amount of hazardous materials involved with the activity. The significance estimates for activity is listed below:

- Involvement of hazardous chemicals
- Amount of hazardous material involved
- Frequency of the activity
- Recognizability
- Accessibility

3.2.4 Threat Identification

Threat is defined as any potential cause of an unwanted event, intentional or unintentional, which may result in damage to an organization and its assets. Threats are generally associated with an asset or activity. A single threat may affect multiple assets or a single asset may have multiple threats. Hence, it is necessary to categorize the threats

and assets by forming threat asset pairs. This enables clear understanding of the consequences of each threat on each asset. Threats against assets could be infinite, and hence it is important to identify threats that relate to the risk associated with the entity under consideration. Threats can be broadly divided into three categories - intentional threats, accidental threats and natural hazards.

The underlying assumption which is made while determining the risk associated with accidental threats and natural hazards is that the frequency of threat can be predicted from prior rates of occurrence. Intentional threats, however, are completely random and complex to estimate. Hence, it is essential to ensure real time monitoring of intentional threats based on evidences. Information relating to adversary's intents, capabilities and beliefs is rarely presented, without which estimating the probability of occurrence would be a challenge. However, advances in efficient data mining, visibility of critical parameters and intelligent support systems, enable real time monitoring of threat levels.

3.2.5 Threat Assessment

Threat assessment deals with the estimation of the probabilities of occurrence the evaluation of consequences on the assets. This stage is critical to the sensitivity of the analysis. The estimates of the risk are based on the subjective and objective beliefs of the threat activities.

3.2.5.1 Frequency of Occurrence. The best technique to estimate the frequency of occurrence of an activity or event is by fault tree analysis. Fault trees can be used to determine the cause effect relationships between activities and estimate the source of threat. This analysis is particularly useful to identify causal relationships related to threat

activities enabling better identification of safeguards to mitigate risk. Fault trees are discussed in further detail in the following section of this chapter.

Frequency of occurrence of a threat disrupting an asset/activity can be estimated either qualitatively or quantitatively. Data pertaining to frequencies of occurrence is rarely available and hence it becomes imperative to use qualitative reasoning as opposed to quantitative evaluation. Moreover, it is easier to comprehend varying degrees of significance in linguistic terms rather than statistically. Qualitative estimates can then be discretely converted into quantitative values for performing risk calculations. As per the MIL STD, the frequencies of occurrence are classified to be under:

- Frequent: Likely to occur in the life of an asset or activity with a probability of occurrence greater than 10^{-1} .
- Probable: Probability of occurrence less than 10^{-1} but greater than 10^{-2} .
- Occasional: Probability of occurrence less than 10^{-2} but greater than 10^{-3} .
- Remote: Probability of occurrence less than 10^{-3} but greater than 10^{-6} .
- Improbable: Probability of occurrence less than 10^{-6} in that life.

The probability of occurrence is estimated based on subjective knowledge or intuitive beliefs to assign a probability value. An alternate approach to this is using fault trees. The use of fault trees extends the application of subjective beliefs to causal elements and enables reasoning and inference based on limited availability of data.

Fault tree analysis is a pertinent technique to estimate the frequency of occurrence of threat. This technique has been rigorously researched and brings in strong systems and reliability engineering concepts.

3.2.5.2 Fault Tree Analysis. Fault tree analysis is a risk management technique consisting of the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event, usually one which significantly contributes to risk within the system. Typically, it is a top-down approach to failure analysis starting with an undesirable event called a top event, such as a failure or malfunction and then determining all the ways it can happen. The analysis proceeds by determining how these top events can be caused by individual or combined lower level failures or events. Depending on the inference tool being used to generate the fault trees, backward inferencing is also feasible. This gives the system the flexibility to identify the root cause of an event as well as determine the trigger of events that a root event would generate.

A fault tree is constructed by relating the sequences of events, which individually or in combination, could lead to the top event. In other words, the tree is constructed by deducing in turn the preconditions for the top event and then successively for the next levels of events, until the basic causes are identified. Fault trees use boolean logic and inference is drawn with “AND” and “OR” gates.

Fault tree elements comprise of two types of nodes - gate and event nodes. Gates nodes have one or more successive nodes (child nodes) but event nodes are the independent whose occurrence does not depend on the occurrence of any other event. Events nodes are also known as leaf nodes and are the causal nodes. Gates nodes are of two fundamental types: “AND” and “OR” gates. At an “OR” gate the probabilities of an event get added to give the probability of the next event, whereas at an “AND” gate, the probabilities get multiplied. This is a powerful technique for identifying the failures that

have the greatest influence on bringing about the end event in a tree. The use of Boolean gates coupled with tree relationships makes the fault identification process simple but comprehensive in approach.

Incorporating bayesian inference to generate fault trees, extend a unique capability to inferencing in fault trees. The boolean true/false states can be extended to integrate intermediate states using this approach. Each event can now have more than two states and new evidence can be combined with the existing data to recalculate new probability value. Fault tree analysis is used to identify the causal events and to construct a network diagram. Bayesian networks deduct inference on the frequency of occurrence of the top event from the network structure. However, the use of traditional bayesian probabilistic approach increases the complexity of populating the conditional probability listing of each node. For a parent node with four children and five possible states for each node, 45 conditional probability values need to be entered. Generating logical inference rules, which replace the likelihood statistic with linguistic formulations, makes it easy to depict the causal relationships.

Clemens P. L. proposed logical rules to perform a qualitative fault tree analysis [52]. These rules have been adopted and modified to suit the problem in consideration.

Rules for calculating the frequency of occurrence

1. The frequency of occurrence of a “AND” gate is equal to the frequency of occurrence of the most probable child if no two other children are at the same level. Example: Probable, Occasional, Remote will be Probable.
2. The frequency of occurrence of an “OR” gate is equal to the frequency of occurrence of the least probable child if no two other children are at the same level. Example: Probable, Occasional, Remote will be Remote.

3. If an “AND” gate has three or more children having the highest level of probability of occurrence among all children then the probability of occurrence of the parent will be elevated to the next level. Example, Probable, Probable, Probable will be Frequent.
4. If an “OR” gate has three or more children having the highest level of probability of occurrence among all children then the probability of occurrence of the parent will be reduced by one level. Example, Probable, Probable, Probable is occasional.

3.2.5.3 Consequence Analysis. Consequence analysis is the assessment of any outcomes that become apparent as a result of a threat activity influencing the supply chain assets. The severity of consequences can be estimated through simulation, from prior data or through subjective beliefs, depending on resource availability. It is convenient to represent the consequences by translating it in terms of pecuniary functions. However, assessing the degree of consequence in certain cases like loss of employee lives or quantifying environmental damages is difficult. Consequences in supply chains are classified to be under three categories - monetary loss, personnel loss and environmental damage. To connote the varying degrees for the consequence parameters, the Mil Standard 88 D definitions have been adopted. The parameters have four degrees of consequence - catastrophic, moderate, marginal and negligible consequences. The definitions for these varying degrees are as below:

- **Catastrophic:** Death or permanent total disability of personnel, monetary loss exceeding 1 million US dollars or irreversible environmental damage violating laws and regulations
- **Critical:** Permanent partial disability, injuries or occupational illness resulting in loss of at least three personnel, monetary loss exceeding 200 thousand US dollars or reversible environmental damage violation laws and regulations
- **Marginal:** Injury or occupational illness resulting in one or more work days, monetary loss exceeding ten thousand, or mitigable environmental damage where restoration activities can be undertaken

- Negligible: Injury or illness not leading to loss of work days, loss exceeding 2000 US dollars, or minimal environmental damage without violating laws and regulations.

The statistics in the definitions are listed as per the military specification and need to be scaled to better configure the significance levels that exist in supply chains. The consequence of a threat j on an asset/activity i is denoted by Q_{ij}

3.2.6 Risk Quantification

Risk quantification is the final step in the risk assessment procedure. Risk associated with an asset i due to a threat j (R_{ij}) is calculated as the product of the frequency of occurrence, F_{ij} of the threat j for the asset i and the consequences C_{ij} of the threat j on asset i .

$$R_{ij} = F_{ij} * C_{ij} \quad (3.2)$$

The threat assessment stage estimates the frequency of occurrence and severity of consequences in qualitative terms. These qualitative terms are then discretely quantified to generate the risk associated with each threat/asset pairs. Table no 3.1 and 3.2 lists the values assigned to frequency of occurrence and severity of consequences. These values are not absolute and the significance level of the values indicates the relative level of risk. For example, a “Frequent” event (with value 0.1) is 100 times more likely to occur than “Probable” events (with value 0.001).

Table 3.1 Assigned Values for Frequency of Occurrence

Frequency of Occurrence	Numerical Value
Frequent	10^{-1}
Probable	10^{-3}
Occasional	10^{-5}
Remote	10^{-7}
Improbable	10^{-9}

Table 3.2 Assigned Values for Severity of Consequences

Severity of Consequences	Numerical Value
Catastrophic	10-1
Critical	10-3
Marginal	10-5
Negligible	10-7

The final risk values associated with the threat/activity pairs are organized in the form of a risk matrix to enable easy comprehension.

CHAPTER 4

SUPPLY CHAIN RISK MITIGATION

Risk mitigation is defined as the diminution of the probability or impact of a risk event through the implementation of safeguard strategies. Without a comprehensive analytical approach, risk mitigation decisions would be based purely on cost minimization or with only a subjective assessment of risk. These subjective, simplistic approaches of cost or risk minimization do not completely secure the business supply chain against impending threats. To manage supply chain risks effectively, optimization should not be the single mathematical exercise that chooses the right answer to reduce cost or risk. To balance highest profit strategies against the flexibility and responsiveness required to deal with real-world change or failure, a firm must balance mitigation costs with supply chain risk.

The risk mitigation methodology proposed in this thesis enables effective identification of high risk supply chain assets, generation of safeguards based on the fault tree analysis of the causal factors and evaluation of the safeguards against each other based on cost and level of security they impart to the assets. A game theoretic approach is proposed for evaluating the utility of safeguards and the cost of the implementing the security measure.

4.1 High Risk Threat/Asset Identification

The most critical aspect of risk management is determining the acceptable level of risk that the supply chain assets can endure without any significant impact on the business, provided any disruption occurs. Depending on the type of industry, the criticality of

supply chain assets and the fiscal constraints, the risk assessment manager can set the acceptable level of risk. Again, the acceptable level of risk is entirely relative to the risk values generated by the risk assessment system. The entire risk mitigation strategies will be based on the threshold risk level. The acceptable limit can be assigned based on the desirable levels of both frequency of occurrence of the event and severity of consequences. Absolute risk mitigation may not be always desirable, as certain business strategies may be based on risk prospects or gambles. Hence, it becomes a management decision as opposed to the risk manager's decision in setting the acceptable or permissible risk level.

Once an acceptable level of risk is established for each asset, the risk values associated with each threat/activity pair is compared to the acceptable level and high risk threat/activity pairs are identified. The high risk assets then have to be assessed for risk mitigation strategies.

4.2 Safeguard Identification

A safeguard is a process, procedure, technique, or strategy intended to mitigate the consequences of probable threats on the supply chain assets. Safeguard strategies are based on the asset under consideration, its significance and the cost associated with implementing the safeguard. It is imperative that the root cause of any disruption is identified prior to selecting the safeguard. This is achieved using fault tree analysis.

The activity associated with the high risk threat/activity pair is first identified and the root cause of it determined through fault tree analysis. The process starts with identification of the causal events that could lead to the top event and the safeguards in

place that prevent the occurrence of the unwanted event. The identified causal events are further studied to identify possible sub causes. The process is repeated until there are no further sub causes or the analyst is satisfied with the level of detail. Safeguards are now identified for the causal events which can mitigate the high risk threat/activity pairs. There can be multiple safeguards for one activity based on the causal events.

Safeguards secure the activities by either reducing the frequency of occurrence or by reducing the severity of consequences. Since risk is calculated based on the frequency of occurrence and severity of consequences, the safeguards can be identified based on the utility that the safeguard is expected to provide. For example, an event with high frequency of occurrence should be secured by a safeguard which reduces the frequency of occurrence of the threat.

4.3 Safeguard Assessment

Once the safeguards are identified, they have to be assessed to determine the utility and the cost of the safeguard. The assessment of safeguard is based on the following factors:

1. Level of Protection
2. Value of the Activity/Asset
3. Cost of the Safeguard
4. Reliability of Safeguard
5. Probability of Intent

4.3.1 Level of Protection

It is defined as the degree of protection rendered by the safeguard against the threat for a specific asset. Level of protection is denoted by $L_{i,j,k}$ and is read as the level of protection provided by safeguard k to asset or activity i against threat j . The level of protection provided by the safeguard is incorporated within the fault tree analysis to simulate the effect of implementing the safeguard. In the proposed method, the level of protection provided by the safeguard is defined as below:

- High: Provides complete protection and completely nullifies occurrence of an “Occasional” event
- Medium: Provides major protection, and nullifies the probability of occurrence of a “Remote” event
- Low: Provides few protection measures and nullifies occurrence of a “Improbable” event
- Very Low: Ineffective or no protection measures and events will occur with the same frequency irrespective of the safeguard.

For computational purposes, relative values are assigned to the different levels of protection, shown in Table 4.1

Table 4.1 Assigned Values for Level of Protection of Safeguard

High	0.75
Medium	0.5
Low	0.25
Very Low	0.1

4.3.2 Value of the Asset/Activity

The value of the asset is defined as the degree of significance that the asset/activity has to the business. It is denoted by V_i . In order to enable managers to identify the significance level of the assets/activity, eight critical parameters have been identified to estimate the

significance of a facility node. These parameters have varying degrees of significance and based on the expertise of the risk manager, the asset can be evaluated. The eight parameters are listed below.

- Inventory levels in the facility
- Number of vendors or suppliers
- Employees within the facility
- Geographical significance
- Significance to the business and supply chain
- Significance to the nation
- Recognizability

Priority value for a logistics link is also estimated based on eight parameters. They are as follows:

- Does the shipment cross national borders
- Attractiveness of goods to adversary
- Availability of alternate logistics routes
- Hazardous or explosive materials
- Shipment visibility or traceability
- Population density associated with the route
- Damage in the worst case scenario
- Significance to supply chain operations

The value of the asset/activity is an important criterion in determining the utility of the safeguard. In order to better comprehend the asset value, it is represented in four degrees of significance – high, medium, low and very low. For computation purpose,

each level is assigned a value (which is relative in significance and not absolute) shown in Table 4.2.

Table 4.2 Assigned Values to Value of Asset

High	0.75
Medium	0.5
Low	0.25
Very Low	0.1

4.3.3 Cost of Safeguard

The most significant factor relating to the constraints in implementation of safeguards is the cost of the safeguard. The cost of implementation of the safeguard is justified only if the utility of the safeguard exceeds its cost. The monetary loss that would be incurred to the firm in the absence of the safeguard should justify the implementation costs. The cost of implementation of safeguard k to secure asset i against threat j is denoted by $C_{i,j,k}$ and is based on

- Capital investment
- Cost of maintenance
- Salary to additional personnel employed
- Miscellaneous costs

4.3.4 Reliability of the Safeguard

This is defined as the probability that the safeguard will not fail, or in other words, the degree of dependability of the safeguard against the threat. Reliability of safeguard is categorized to be under five levels – very high, high, medium, low and very low. This factor is subjective and it is up to the manager to decide the level of reliability that a safeguard provides within the system under consideration. Generally, any increase in

reliability of safeguard increases the cost of the safeguard. For example, providing 10 security personnel to monitor a restricted area provides more reliability than 5 security personnel, but at higher costs. The reliability of safeguard is represented by $\alpha_{i,j,k}$ and is read as the reliability of safeguard k to secure asset i against threat j .

4.3.5 Probability of Intent

This is defined as the evidence of increase in the threat activity leading to failure of the safeguard. The Bayesian inferencing technique updates any increase in threat associated with any asset/activity. However, it is necessary to check for any evidence in likelihood of disruption of the safeguards. For example, if surveillance cameras are installed as a safeguard against security breaching, then the evidence of a thunderstorm would increase the probability of failure of the safeguard due to higher chances of surveillance disruption, leading to a higher probability of intent. This is represented by $\beta_{j,k}$ and read as the probability of intent of threat j against safeguard k .

4.4 Utility Calculation

Utility is defined as the measure of effectiveness of a safeguard in securing the asset/activity against plausible threats. In supply chain risk mitigation, the utility of the safeguard is dependent on the level of protection that the safeguard provides to the asset/activity and the value of the asset. Utility is denoted by $U_{i,j,k}$. The utility is computed as shown in Equation 4.1.

$$U_{i,j,k} = L_{i,j,k} * V_i \quad (4.1)$$

In some cases, the implementation of a safeguard increases the value of the asset due to increase in monetary value or increase in number of employees. This would reduce the utility of the asset and the net utility if formulated in Equation 4.2.

$$\text{Net } U_{i,j,k} = (L_{i,j,k} * V_i) - \text{increase in value of the asset } i \quad (4.2)$$

The increase in the value of the asset is expressed in varying degrees – high, medium, low, no and are quantified as shown in Table 4.3

Table 4.3 Assigned Values to Increase in Value of Asset

High	0.25
Medium	0.1
Low	0.01
No	0

4.5 Safeguard Analysis

The safeguards are now evaluated against each other to determine the most effective safeguard based on the cost of implementation and the utility it provides. A game theoretic approach is proposed to evaluate the safeguards against each other. The risk environment can be viewed as the setting for a two-player game. The one player would be the threat element trying to disrupt the high-risk asset/activity and the other player would be the risk manager implementing safeguards to mitigate the risk effects. This approach provides a comprehensive view of the risk environment. It enables identifying the prospective disruption elements and effective identification of safeguards that can mitigate these disruptions.

Game theory is the study of the ways in which strategic interactions among rational players produce outcomes with respect to the payoffs of the players. A normal game with imperfect information is defined in this methodology where both players are not aware of the moves planned by each other. The most crucial step in the generation of a game is the payoff function.

4.5.1 Payoff Calculation

A payoff matrix is defined as a table, which exhibits the payoffs ensuing from every possible action by each player for every possible action by the other player [42]. Typically, the payoff function comprises of two fields, the first field represents the payoff of the first player and the second the payoff of the other. The payoff function depends on the utility or the gain by each player.

Player one is defined to be the risk manager trying to overpower the threats by implementing safeguards and player two is defined to be the threat element driving disruptive actions against the high risk assets/activities.

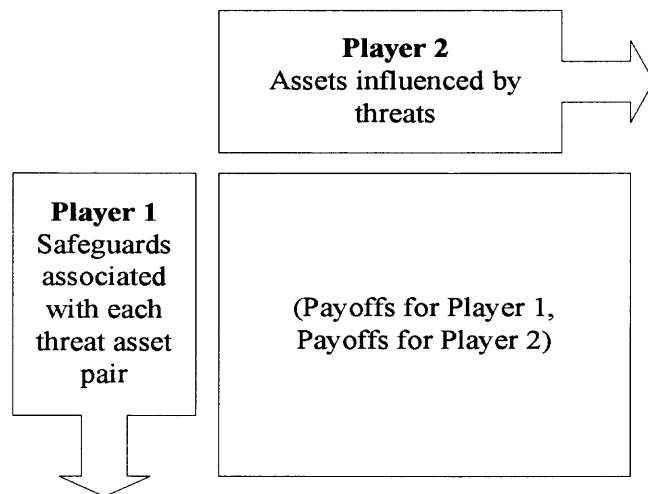


Figure 4.1 Payoff Matrix for the normal game.

The payoff for the safeguards (player 1) is denoted by $S_{i,k}$. It is read as the payoff for safeguard k securing asset i . It is generated as a function of cost and utility as shown in equation 4.4.

$$S_{i,k} = \alpha_{i,j,k} * \text{Net } U_{i,j,k} - (1 - \alpha_{i,j,k}) * C_{i,j,k} \quad (4.4)$$

The above equation incorporates both utility and cost within the same function, however, the higher the reliability of the safeguard, the lower would be the cost influence. As can be seen from Equation 4.4, the payoff function, $S_{i,k}$ would be higher for a safeguard with higher utility but same cost as another safeguard with relatively lower utility. Similarly, the payoff function will be higher for a safeguard with lower cost but same utility as another safeguard with higher cost. This relationship would enable the identification of both high reliability safeguards and low cost safeguards with ease. To bring both the cost and utility to the same significance level, they have been factored to fit the range from 0 to 1.

The payoff for the threats influencing the assets (player 2) is denoted by $A_{i,k}$. It is read as the payoff for asset i being secured by safeguard k . It is generated as a function of the consequences of threat and probability of intent as shown in Equation 4.5

$$A_{i,k} = \beta_{j,k} * Q_{i,j} \quad (4.5)$$

The above equation indicates the consequences that would result from failure of the safeguards. However, if for threat/activity pairs with same consequence, safeguards with higher probability of intent would generate higher payoffs indicating high vulnerabilities. Similarly, for safeguards with same probability of intent, high consequence threats would generate higher payoffs indicating higher vulnerabilities.

4.5.2 Safeguard Selection

Once the payoff matrix is generated, the game is set for analysis. The first step would be to check for dominance within the payoff matrix. Dominance can be defined as the state that exists when one strategy overpowers another strategy for the same player. For example, if all the payoffs for strategy 1 for the safeguards are more than all the payoffs for strategy 2 for the safeguards, then strategy 1 is understood to dominate strategy 2. In this case, strategy 2 can be eliminated from the payoff matrix because strategy 1 provides better payoff for any safeguard asset combination. Table 4.4 illustrates a typical payoff matrix.

Table 4.4 Payoff Matrix for a Normal Game

	Asset 1	Asset 2	Asset 3	Total Payoff for Safeguard
Safeguard 1	$(S_{1,1}, A_{1,1})$	$(S_{1,2}, A_{1,2})$	$(S_{1,3}, A_{1,3})$	ΣS_1
Safeguard 2	$(S_{2,1}, A_{2,1})$	$(S_{2,2}, A_{2,2})$	$(S_{2,3}, A_{2,3})$	ΣS_2
Safeguard 3	$(S_{3,1}, A_{3,1})$	$(S_{3,2}, A_{3,2})$	$(S_{3,3}, A_{3,3})$	ΣS_3
Total Payoff for Assets	ΣA_1	ΣA_2	ΣA_3	

The next step would be to identify the most vulnerable asset based on the highest total payoff for the assets. The first step toward safeguard selection would be to secure the most vulnerable asset using the most effective safeguard. For this purpose, the following methodology is adopted.

1. Identify the most vulnerable asset as the asset with highest value in the row "Total Payoff for Assets"
2. Identify safeguards, which secure the most vulnerable asset, obtained from the previous step.

3. Determine the most effective safeguard among the safeguards which secure the most vulnerable asset as safeguard with the highest value in the “Total Payoffs for Safeguard” column.
4. Select the safeguard.

4.5.3 Safeguard Implementation

The safeguard selected is now assessed to determine the type of protection it provides. The safeguard can either reduce the frequency of occurrence of a threat or reduce the severity of consequences. A safeguard that reduces the frequency of occurrence is fed back into the fault tree analysis. The selected safeguard now gets added to the fault tree structure and the probabilities of occurrence recalculated. To calculate the new probability value of an event (gate), the influence of the safeguards associated with it is ignored and the probability of occurrence is estimated. Then, all events in the fault tree are assumed to be a single node and the frequency of occurrence is recalculated with the safeguard in place. Logical inference rules are developed to incorporate the level of protection rendered by the safeguard into the fault tree analysis.

1. A safeguard providing “High” level of protection will reduce the frequency of occurrence by three levels. Example: If the event frequency is “High” and safeguard provides a high level of protection then the effective frequency of occurrence would be “occasional”.
2. A safeguard providing “Medium” level of protection will reduce the frequency of occurrence by two levels.
3. A safeguard providing “Low ” level of protection will reduce the frequency of occurrence by one level.
4. A safeguard providing “Very Low” level of protection will affect the frequency of occurrence.

Safeguards can also reduce the severity of consequences of a threat on an asset/activity. Logical inference rules are developed to incorporate the level of protection rendered by the safeguard into the consequence analysis.

1. A safeguard providing “High” level of protection will reduce the severity of consequence of a “Catastrophic” event by one level. Example: If the consequence level is “Catastrophic” and safeguard provides a high level of protection then the effective consequence would be “Critical”.
2. A safeguard providing “High” level of protection will reduce the severity of consequence of “Critical” and “Marginal” events to “Negligible”.
3. A safeguard providing “Medium” level of protection will reduce the severity of consequence by one level.
4. A safeguard providing “Low ” level of protection will not reduce the severity of consequence
5. A safeguard providing “Very Low” level of protection will not affect the consequences of a threat.

After the implementation of safeguards, the risk values are reassessed, safeguards identified and analyzed again to determine the most effective safeguard. This process is repeated till the risk levels of all the threat/asset pairs are below the acceptable risk level.

CHAPTER 5

CASE STUDY

This chapter aims at illustrating the risk mitigation methodology described in the previous chapter in the form of a case study. The pertinent supply chain information, necessary for simulating the case study has been provided by Picatinny Arsenal. The case study focuses on a section of the supply chain to make the depiction of the methodology easy to comprehend. The supply chain product is a dual-purpose improved conventional munitions (DPICM) cartridge. The case study simulation is done in Microsoft Excel using Macros in Visual Basic. The case study serves to better enumerate the risk mitigation methodology through the analysis and implementation of effective safeguards to mitigate the risk. The case study is divided into three stages.

- Stage 1 illustrates the risk mitigation methodology through the identification, assessment and evaluation of safeguards.
- Stage 2 simulates the implementation of the most effective safeguard
- Stage 3 illustrates the response of the methodology to change in degree of consequence for a threat/asset pair.

5.1 Background

The DPICM cartridge was developed for use in the howitzer gun to leverage light infantry divisions capabilities and to make them more lethal. When fired with a supercharge, the extended range DPICM cartridge permits mass fires across the division front and improves survivability of the troops. This cartridge also allows engagement of deep targets that was not possible with the previous cartridge.

The DPICM uses a supercharge to improve the projectile range. The cartridge contains a sub munitions payload of 42 Dual Purpose grenades. The projectile uses a one piece all steel carrier which is internally scalloped to contain the cargo without additional hardware. The grenades use a new Electronic Self Destruct Fuse. This fuse will reduce the number of DPICM duds on the battlefield and be reasonably safe for friendly maneuvering or advancing troops.

5.2 Supply Chain Description

The entire supply chain of the DPICM cartridge consists of nine facilities and twenty three logistics links. Though the methodology is applicable to the entire length of the supply chain, the case study has been limited to three facilities and three logistics links. The simple supply chain segment is as shown in Figure 4.1. The logistics links are represented by dotted lines and the activities within the facility are shown by solid lines.

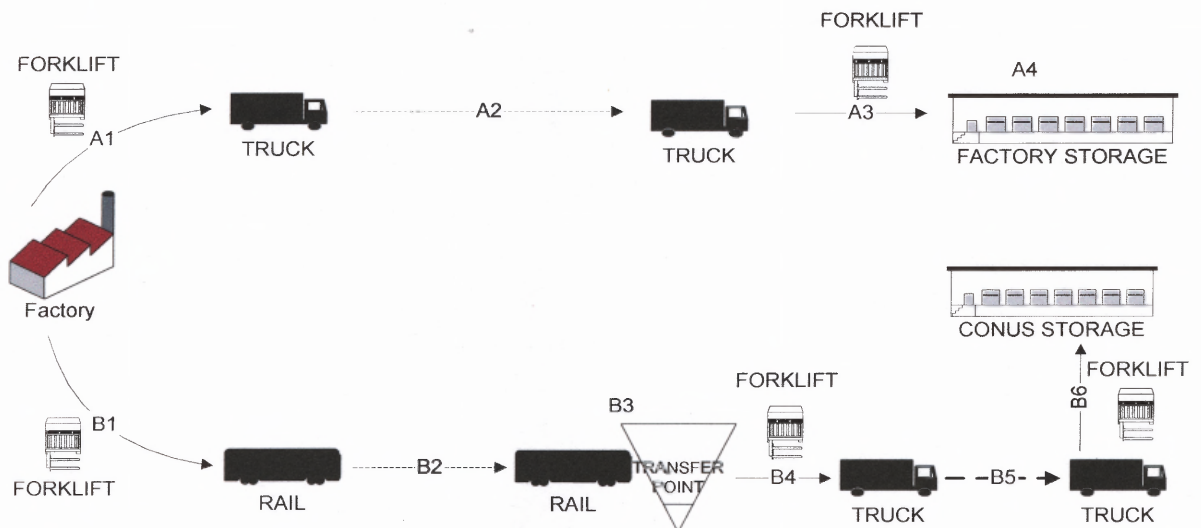


Figure 5.1 DPICM Cartridge Supply Chain Simulated in Case Study.

The supply chain structure shown in the Figure 5.1 has two distinct physical flows (chains) – one, from Factory to Factory Storage and other from Factory to CONUS Storage. The DPICM cartridge is manufactured at the Factory and is transferred to Factory Storage and CONUS Storage for further deployment when necessary. Facility nodes and logistics links associated with the Factory to Factory Storage chain is represented by asset/activities A1 to A4. Trucks are used to transport the manufactured product from the Factory to Factory Storage. At the Factory, the product is loaded in containers and loaded onto trucks using forklifts. The trucks then transport the product from the Factory to Factory Storage, where it is unloaded from the trucks using forklifts again and putaway into the storage facility until further deployment.

The other sub-chain of the model, Factory to CONUS Storage, is modeled by assets/activities B1 to B6. Rail transport is used to transport the DPICM cartridges loaded in containers. The manufactured product is first loaded onto the train using forklift and then transported to the transfer point where the product is loaded from the rail to truck using forklift. The truck then transfers it to the CONUS storage site, where the product is unloaded using forklifts and putaway for storage. The supply chain structure is modeled by the set of operations listed in Table 5.1.

5.2.1 Operational Parameters

The Tables 5.1, 5.2 and 5.3 list the various activities that are carried out, the duration of activities, the threats associated with each activity and the frequency of occurrence of the threat for each of the facilities – Factory, Factory Storage and CONUS Storage. Tables 5.4, 5.5 and 5.6 list the threat/activity pairs for the logistics links connection the factory to the storage facilities.

Table 5.1 Supply Chain Operation Description

Activity / Asset	Type of Network Element	Description
A1	Facility	Factory to Truck using forklift
A2	Logistics	Factory to Factory Storage
A3	Facility	Truck to Factory Storage using forklift
A4	Facility	Factory Storage
B1	Facility	Factory to Train using forklift
B2	Logistics	Factory to Storage Site
B3	Facility	Storage Site
B4	Facility	Storage Site to Truck using forklift
B5	Logistics	Storage Site to CONUS Storage
B6	Facility	Truck to CONUS Storage using forklift

Table 5.2 Threat/Asset Listing for Factory

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Forklift to Truck	1.5	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling
Forklift to Rail	0.9	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling

Table 5.3 Threat/Asset Listing for Factory Storage

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Forklift to Bunker	0.3	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling
Bunker Storage	720	Storage Auto ignition Battery Initiates Fire	Remote Event Remote Improbable	Storage

Table 5.4 Threat/Asset Listing for CONUS Storage

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Bunker Storage	61320	Auto ignition Battery Initiates Fire Storage Reaction with items	Remote Remote Remote Remote Remote	Storage
Forklift to Rail	0.3	Forklift Tines Puncture Container Pallet Falls	Probable Occasional	Material handling
Forklift to Truck	1.5	Forklift Tines Puncture Container Pallet Falls Detonation Pierside Fire	Probable Occasional Remote Remote	Material Handling
Forklift to Bunker	1.9	Forklift Tines Puncture Container Pallet Falls	Probable Occasional	Material Handling
Truck to Bunker	0.3	Truck Fire Detonation Bullet Puncture Truck Accident	Remote Remote Remote Remote	Material Handling

Table 5.5 Threat/Asset Listing for Logistics Link from Factory to Factory Storage

Activity	Duration	Threats	Frequency	Activity Type
Truck to Bunker	0.3	Truck Fire Detonation Bullet Puncture	Remote Remote Remote	Land Transportation

Table 5.6 Threat/Asset Listing for Logistics Link from Factory to CONUS Storage by Rail

Activity	Duration	Threats	Frequency	Activity Type
Rail to Conus	336	Rail Fire Detonation Bullet Puncture Rail Accident	Remote Remote Remote Remote	Land Transportation

Table 5.7 Threat/Asset Listing for Logistics Link from Factory to CONUS Storage by Truck

Activity	Duration	Threats	Frequency	Activity Type
Truck to Conus	168	Truck Fire Detonation Bullet Puncture	Remote Remote Remote	Land Transportation

5.2.2 Risk Matrices

The risk matrices pertaining to the threat/activity pairs were obtained from the risk assessment module of the SCRAMS system and the risk matrices for the case study are listed in Tables 5.8 through 5.13. This assessment was done using a risk assessment tool currently being developed as a part of the ongoing research investigating the risk analysis approach in supply chains. An acceptable risk level of 1.13×10^{-7} is assumed for all the assets/activities. Each asset can be assigned a unique acceptable risk level, however, for simplicity of understanding, a common acceptable risk level has been assumed.

Table 5.8 Risk Matrix for Factory

	Fork tines Puncture Container	Pallet Falls
Forklift to Rail	1.00E-12	1.00E-10
Forklift to Truck	1.00E-12	1.00E-10

Table 5.9 Risk Matrix for Factory Storage

	Auto ignition	Battery Initiates	Forklift Tines Puncture container	Pallet Falls	Storage	Fire
Bunker Storage	1.00E-07	1.00E-07	NA	NA	1.00E-10	1.00E-07
Forklift to Bunker	NA	NA	1.00E-12	1.00E-10	NA	NA

Table 5.10 Risk Matrix for CONUS Storage

	Auto ignition	Battery Initiates	Bullet Puncture
Bunker storage	1.00E-06	1.00E-06	NA
Forklift to Bunker	NA	NA	NA
Forklift to Rail	NA	NA	NA
Forklift to Truck	NA	NA	NA
Truck to Bunker	NA	NA	1.00E-10

	Detonation	Fire	Forklift Tines Puncture Container
Bunker Storage	NA	1.00E-10	NA
Forklift to Bunker	NA	NA	1.00E-12
Forklift to Rail	NA	NA	1.00E-12
Forklift to Truck	1.00E-10	NA	1.00E-12
Truck to Bunker	1.00E-10	NA	NA

	Pallet Falls	Pierside Fire	Reaction with items
Bunker Storage	NA	NA	1.00E-08
Forklift to Bunker	1.00E-10	1.00E-11	1.00E-08
Forklift to Rail	1.00E-10	NA	NA
Forklift to Truck	1.00E-10	NA	NA
Truck to Bunker	NA	NA	NA

	Storage	Truck Fire	Truck Accident
Bunker Storage	1.00E-10	NA	NA
Forklift to Bunker	NA	NA	NA
Forklift to Rail	NA	NA	NA
Forklift to Truck	NA	NA	NA
Truck to Bunker	NA	1.00E-07	1.00E-14

Table 5.11 Risk Matrix for Logistics link from Factory to Factory Storage by Truck

	Truck Fire	Detonation	Truck Accident	Bullet Puncture
Truck to Bunker	1.00E-07	1.00E-08	1.00E-12	1.00E-14

Table 5.12 Risk Matrix for Logistics Link from Factory to CONUS Storage by Rail

	Bullet Puncture	Detonation	Rail Fire	Rail Accident
Rail to CONUS	1.00E-12	1.00E-08	1.00E-08	1.00E-10

Table 5.13 Risk Matrix for Logistics Link from Factory to CONUS Storage by Truck

	Bullet Puncture	Detonation	Truck Fire	Truck Accident
Truck to Conus	1.00E-12	1.00E-08	1.00E-07	1.00E-12

5.3 Case Study - Stage 1

The first stage of the case study illustrates the safeguard pre-assessment and analysis methodology. The risk matrices corresponding to the supply chain model is obtained from the risk assessment process. The list of threat/activity pairs are listed in Figure 4.2. As can be seen from the figure, the high risk threat/activity pairs are highlighted in orange. The principle of the methodology is to bring the risk levels associated with the threat/activity pairs to or below the acceptable risk level.

5.3.1 Safeguard Identification

To identify safeguards to be implemented for mitigating the risk, the causal influences of the high risk threats need to be identified. This is accomplished through fault tree analysis. Once the causes are identified, safeguard identification becomes quite

straightforward. Table 4.14 lists the causes that have been identified which escalate risk for the activities under consideration.

Depending on the causes, safeguards are identified based on knowledge from prior assessments or based on expertise of the risk manager. Multiple safeguards are possible for the same threat asset pair. For example, for the threat/asset pair ‘truck fire’ for ‘A2’, three safeguards have been proposed – regular truck maintenance, driver training and providing cushions for pallets. The safeguards proposed to secure the assets/activities are listed in Table 5.15

Table 5.14 Listing of Causal Elements that Lead to Elevated Risk in System

Threat	Asset/Activity	Risk Value	Cause
Truck Fire	A2	1.00E-06	Mechanical Fault
Truck Fire	A2	1.00E-06	Abrupt Braking
Truck Fire	A2	1.00E-06	Impact
Storage	A4	1.00E-06	High Temp/Humidity
Storage	A4	1.00E-06	Proximity to other chemicals
Autoignition	A4	1.00E-06	High Temp/Humidity
Autoignition	A4	1.00E-06	Impact
Autoignition	A4	1.00E-06	Proximity to other chemicals
Battery Initiates	A4	1.00E-06	Fuse Trips
Rail Fire	B2	1.00E-05	Impact
Rail Fire	B2	1.00E-05	High Temp/Humidity
Rail Fire	B2	1.00E-05	Electrical Faults
Truck Fire	B4	1.00E-06	Mechanical Fault
Truck Fire	B4	1.00E-06	Abrupt Braking
Truck Fire	B4	1.00E-06	Impact
Storage	B6	1.00E-06	High Temp/Humidity
Autoignition	B6	1.00E-06	Electrical Faults
Autoignition	B6	1.00E-06	Impact
Battery Initiates	B6	1.00E-06	Fuse Trips

	Threats	Assets	Risk Values	Risk Status
Factory to Factory Storage	Forklift tines puncture container	A1	1.00E-08	Acceptable
	Pallet Falls	A1	1.00E-08	Acceptable
	Truck Fire	A2	1.00E-06	Not Acceptable
	Detonation of Cartridge	A2	1.00E-08	Acceptable
	Truck Accident	A2	1.00E-09	Acceptable
	Bullet Punctures container	A2	1.00E-08	Acceptable
	Forklift tines puncture container	A3	1.00E-08	Acceptable
	Pallet Falls	A3	1.00E-08	Acceptable
	Storage	A4	1.00E-06	Not Acceptable
	Autoignition	A4	1.00E-06	Not Acceptable
	Battery Initiates	A4	1.00E-06	Not Acceptable
	Fire	A4	1.00E-08	Acceptable
	Reaction with other items	A4	1.00E-08	Acceptable
	Factory to COMUS Storage (Rail)	Forklift tines puncture container	B1	1.00E-08
Pallet Falls		B1	1.00E-08	Acceptable
Rail Fire		B2	1.00E-05	Not Acceptable
Detonation		B2	1.00E-08	Acceptable
Bullet Punctures container		B2	1.00E-08	Acceptable
Rail Accident		B2	1.00E-09	Acceptable
Forklift tines puncture container		B3	1.00E-08	Acceptable
Pallet Falls		B3	1.00E-08	Acceptable
Truck Fire		B4	1.00E-06	Not Acceptable
Detonation		B4	1.00E-08	Acceptable
Bullet Punctures container		B4	1.00E-08	Acceptable
Truck Accident		B4	1.00E-09	Acceptable
Forklift tines puncture container		B5	1.00E-08	Acceptable
Pallet Falls		B5	1.00E-08	Acceptable
Storage		B6	1.00E-06	Not Acceptable
Autoignition		B6	1.00E-06	Not Acceptable
Battery Initiates		B6	1.00E-06	Not Acceptable
Fire		B6	1.00E-08	Acceptable
Reaction with other items	B6	1.00E-08	Acceptable	

Indicates Acceptable Level of Risk
 Indicates Risk Level Not Acceptable
Acceptable Risk Level 1.13E-07

Figure 5.2 Threat asset/activity listing for all activities in the case study.

Table 5.17 Asset Value Listing

High Risk Assets	Value of the Asset	Factored Value of Asset
A2	Medium	0.5
A4	Low	0.25
B2	High	0.75
B4	Medium	0.5
B6	Medium	0.5

5.3.2 Safeguard Analysis

Once the safeguards are identified, the next step would be to evaluate and analyze the safeguards. The safeguards are evaluated based on the level of protection that a safeguard provides to the asset against a threat, the value of the asset being secured, the cost of implementation of the safeguard, reliability of the safeguard and the probability of intent against the safeguard by threat activities. These evaluations are based on the judgment of the risk manager or from prior assessment knowledge. Tables 4.16 to 4.20 provide a listing of the five safeguard evaluation factors and their numerical values that have been used in the case study to evaluate the utility and the payoffs of the safeguards.

Table 5.15 Listing of Safeguards Identified for Mitigating Risk

Threat	Asset/Activity	Risk Value	Cause	Safeguard
Truck Fire	A2	1.00E-06	Mechanical Fault	Regular Truck Maintenance
Truck Fire	A2	1.00E-06	Abrupt Braking	Train Drivers
Truck Fire	A2	1.00E-06	Impact	Cushions for Pallets
Storage	A4	1.00E-06	High Temp/Humidity	Temp & Humidity Maintenance
Storage	A4	1.00E-06	Proximity to other chemicals	Periodic Inspection
Autoignition	A4	1.00E-06	High Temp/Humidity	Temp & Humidity Maintenance
Autoignition	A4	1.00E-06	Impact	Cushions for Pallets
Autoignition	A4	1.00E-06	Proximity to other chemicals	Proper Packaging
Autoignition	A4	1.00E-06	Proximity to other chemicals	Periodic Inspection
Battery Initiates	A4	1.00E-06	Fuse Trips	Safety Clips
Rail Fire	B2	1.00E-05	Impact	Cushions for Pallets
Rail Fire	B2	1.00E-05	High Temp/Humidity	Temp & Humidity Maintenance
Rail Fire	B2	1.00E-05	Electrical Faults	Periodic Inspection
Truck Fire	B4	1.00E-06	Mechanical Fault	Regular Truck Maintenance
Truck Fire	B4	1.00E-06	Abrupt Braking	Train Drivers
Truck Fire	B4	1.00E-06	Impact	Cushions for Pallets
Storage	B6	1.00E-06	High Temp/Humidity	Temp & Humidity Maintenance
Autoignition	B6	1.00E-06	Electrical Faults	Electrical Inspection
Autoignition	B6	1.00E-06	Impact	Proper Packaging
Autoignition	B6	1.00E-06	Impact	Cushions for Pallets
Battery Initiates	B6	1.00E-06	Fuse Trips	Safety Clips

Table 5.16 Level of Protection of Safeguards Proposed to Secure the Assets

High Risk Threats	High Risk Assets/ Activity	Safeguard	Level of Protection	Factored Level of Protection
Truck Fire	A2	Regular Truck Maintenance	Medium	0.5
Truck Fire	A2	Train Drivers	High	0.75
Truck Fire	A2	Cushions for Pallets	High	0.75
Storage	A4	Temp & Humidity Maintenance	Medium	0.5
Storage	A4	Periodic Inspection	Medium	0.5
Autoignition	A4	Temp & Humidity Maintenance	Medium	0.5
Autoignition	A4	Cushions for Pallets	Medium	0.5
Autoignition	A4	Proper Packaging	Low	0.25
Autoignition	A4	Periodic Inspection	Medium	0.5
Battery Initiates	A4	Safety Clips	High	0.75
Rail Fire	B2	Cushions for Pallets	Medium	0.5
Rail Fire	B2	Temp & Humidity Maintenance	Low	0.25
Rail Fire	B2	Periodic Inspection	Medium	0.5
Truck Fire	B4	Regular Truck Maintenance	High	0.75
Truck Fire	B4	Train Drivers	High	0.75
Truck Fire	B4	Cushions for Pallets	Medium	0.5
Storage	B6	Temp & Humidity Maintenance	Low	0.25
Autoignition	B6	Electrical Inspection	High	0.75
Autoignition	B6	Proper Packaging	Low	0.25
Autoignition	B6	Cushions for Pallets	Medium	0.5
Battery Initiates	B6	Safety Clips	High	0.75

Once the safeguards are assessed based on the five evaluation factors, the utility can be computed using the Equation 3.1 as the product of value of the asset and level of protection the safeguard provides. Figure 5.3 shows the utility values computed for the safeguards. The net utility is now computed using Equation 3.3.

Table 5.18 Listing of Implementation Costs of Safeguard
(the cost is factored based on the average cost of implementation of a safeguard)

High Risk Threats	High Risk Assets	Safeguard	Cost	Factored Cost
Truck Fire	A2	Regular Truck Maintenance	\$10,000	1.78
Truck Fire	A2	Train Drivers	\$6,000	0.60
Truck Fire	A2	Cushions for Pallets	\$5,000	0.50
Storage	A4	Temp & Humidity Maintenance	\$3,000	0.30
Storage	A4	Periodic Inspection	\$8,000	0.80
Autoignition	A4	Temp & Humidity Maintenance	\$3,000	0.30
Autoignition	A4	Cushions for Pallets	\$4,000	0.40
Autoignition	A4	Proper Packaging	\$1,500	0.15
Autoignition	A4	Periodic Inspection	\$7,000	0.70
Battery Initiates	A4	Safety Clips	\$8,000	0.80
Rail Fire	B2	Cushions for Pallets	\$6,000	0.60
Rail Fire	B2	Temp & Humidity Maintenance	\$4,000	0.40
Rail Fire	B2	Periodic Inspection	\$6,000	0.60
Truck Fire	B4	Regular Truck Maintenance	\$10,000	1.00
Truck Fire	B4	Train Drivers	\$9,000	0.90
Truck Fire	B4	Cushions for Pallets	\$6,000	0.60
Storage	B6	Temp & Humidity Maintenance	\$4,000	0.40
Autoignition	B6	Electrical Inspection	\$7,000	0.70
Autoignition	B6	Proper Packaging	\$1,500	0.15
Autoignition	B6	Cushions for Pallets	\$1,000	0.10
Battery Initiates	B6	Safety Clips	\$8,000	0.80

Table 5.19 Listing of the Reliability of Safeguards (α)

High Risk Threats	High Risk Assets	Safeguard	Reliability of Safeguard	Factored Reliability
Truck Fire	A2	Regular Truck Maintenance	High	0.75
Truck Fire	A2	Train Drivers	Very High	0.90
Truck Fire	A2	Cushions for Pallets	Medium	0.50
Storage	A4	Temp & Humidity Maintenance	Low	0.25
Storage	A4	Periodic Inspection	Medium	0.50
Autoignition	A4	Temp & Humidity Maintenance	Medium	0.50
Autoignition	A4	Cushions for Pallets	Medium	0.50
Autoignition	A4	Proper Packaging	Very Low	0.10
Autoignition	A4	Periodic Inspection	High	0.75
Battery Initiates	A4	Safety Clips	Very High	0.90
Rail Fire	B2	Cushions for Pallets	Very Low	0.10
Rail Fire	B2	Temp & Humidity Maintenance	Low	0.25
Rail Fire	B2	Periodic Inspection	High	0.75
Truck Fire	B4	Regular Truck Maintenance	Very High	0.90
Truck Fire	B4	Train Drivers	Very High	0.90
Truck Fire	B4	Cushions for Pallets	Very Low	0.10
Storage	B6	Temp & Humidity Maintenance	Medium	0.50
Autoignition	B6	Electrical Inspection	High	0.75
Autoignition	B6	Proper Packaging	Very Low	0.10
Autoignition	B6	Cushions for Pallets	Very High	0.90
Battery Initiates	B6	Safety Clips	Very High	0.90

Table 5.20 Listing of Probability of Intent (β) Against the Safeguards

High Risk Threats	High Risk Assets	Safeguard	Probability of Intent	Factored Probability of Intent
Truck Fire	A2	Regular Truck Maintenance	Moderate	0.10
Truck Fire	A2	Train Drivers	Marginal	0.05
Truck Fire	A2	Cushions for Pallets	Low	0.01
Storage	A4	Temp & Humidity Maintenance	Low	0.01
Storage	A4	Periodic Inspection	Low	0.01
Autoignition	A4	Temp & Humidity Maintenance	No	0.00
Autoignition	A4	Cushions for Pallets	No	0.00
Autoignition	A4	Proper Packaging	No	0.00
Autoignition	A4	Periodic Inspection	Low	0.01
Battery Initiates	A4	Safety Clips	m	0.10
Rail Fire	B2	Cushions for Pallets	Low	0.01
Rail Fire	B2	Temp & Humidity Maintenance	No	0.00
Rail Fire	B2	Periodic Inspection	Low	0.01
Truck Fire	B4	Regular Truck Maintenance	No	0.00
Truck Fire	B4	Train Drivers	Marginal	0.05
Truck Fire	B4	Cushions for Pallets	Low	0.01
Storage	B6	Temp & Humidity Maintenance	Low	0.01
Autoignition	B6	Electrical Inspection	Low	0.01
Autoignition	B6	Proper Packaging	Low	0.01
Autoignition	B6	Cushions for Pallets	Low	0.01
Battery Initiates	B6	Safety Clips	Low	0.01

The stage is now set to generate payoffs and form the game to evaluate the safeguards against each other. Player 1 in the game would be the safeguards, whose objective is to secure the assets and player 2 is the threats with an objective to disrupt the assets. The payoffs $S_{j,k}$ and $A_{j,k}$ are computed using equation 3.4 and 3.5 respectively. Figure 4.4 shows the payoffs to the two players. The payoff matrix is now generated with the safeguards as the row field and assets as the column field. The Payoff Matrix for stage 1 is shown in Figure 5.5.

The payoff matrix in Figure 4.5 highlights two factors, the most vulnerable asset (shown in red) and the most effective safeguard (shown in green). In stage 1 of the case

study, the payoff matrix suggests that the most vulnerable asset/activity is A2 and the safeguards which can secure A2 are “train drivers”, “regular truck maintenance” and “cushions for pallets”. Hence, it is imperative that A2 needs to be secured, but the choice of safeguards to secure A2 must be made based on highest payoff function. Among these safeguards, the safeguard with the highest total payoff is “train drivers”.

High Risk Threats	High Risk Assets	Safeguard	Value of Asset	Level of Protection	Utility	Increase In value of asset	Net Utility
Truck Fire	A2	Regular Truck Maintenance	0.5	0.5	0.25	0	0.25
Truck Fire	A2	Train Drivers	0.5	0.75	0.375	0.001	0.374
Truck Fire	A2	Cushions for Pallets	0.5	0.75	0.375	0.0001	0.3749
Storage	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Storage	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Autoignition	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Autoignition	A4	Cushions for Pallets	0.25	0.5	0.125	0.0001	0.1249
Autoignition	A4	Proper Packaging	0.25	0.25	0.0625	0	0.0625
Autoignition	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Battery Initiates	A4	Safety Clips	0.25	0.75	0.1875	0.001	0.1865
Rail Fire	B2	Cushions for Pallets	0.75	0.5	0.375	0.0001	0.3749
Rail Fire	B2	Temp & Humidity Maintenance	0.75	0.25	0.1875	0	0.1875
Rail Fire	B2	Periodic Inspection	0.75	0.5	0.375	0	0.375
Truck Fire	B4	Regular Truck Maintenance	0.5	0.75	0.375	0	0.375
Truck Fire	B4	Train Drivers	0.5	0.75	0.375	0.001	0.374
Truck Fire	B4	Cushions for Pallets	0.5	0.5	0.25	0.0001	0.2499
Storage	B6	Temp & Humidity Maintenance	0.5	0.25	0.125	0	0.125
Autoignition	B6	Electrical Inspection	0.5	0.75	0.375	0	0.375
Autoignition	B6	Proper Packaging	0.5	0.25	0.125	0	0.125
Autoignition	B6	Cushions for Pallets	0.5	0.5	0.25	0.001	0.249
Battery Initiates	B6	Safety Clips	0.5	0.75	0.375	0.001	0.374


 Indicates Threat Asset Pairs with risk value Not Acceptable

Figure 5.3 Screenshot of the Utility Calculation Table.

High Risk Threats	Assets/ Activity	Safeguard	α - Reliability	β - Probability of Intent	Factored Consequence	Factored Cost	Factored Utility	Payoff to Safeguard S_{ij}	Payoff to Threat/ Asset A_{ij}
Truck Fire	A2	Regular Truck Maintenance	0.75	0.100	1.11	1.78	1.04	0.7736	0.1103
Truck Fire	A2	Train Drivers	0.90	0.050	0.50	0.60	1.56	1.7803	0.0250
Truck Fire	A2	Cushions for Pallets	0.50	0.005	0.50	0.50	1.61	0.9933	0.0025
Storage	A4	Temp & Humidity Maintenance	0.25	0.005	0.25	0.30	0.55	0.3535	0.0013
Storage	A4	Periodic Inspection	0.50	0.010	0.25	0.80	0.54	0.3100	0.0025
Autoignition	A4	Temp & Humidity Maintenance	0.50	0.001	0.25	0.30	0.53	0.5525	0.0003
Autoignition	A4	Cushions for Pallets	0.50	0.001	0.25	0.40	0.51	0.4942	0.0003
Autoignition	A4	Proper Packaging	0.10	0.001	0.25	0.15	0.25	0.3295	0.0003
Autoignition	A4	Periodic Inspection	0.75	0.010	0.25	0.70	0.46	0.6135	0.0025
Battery Initiates	A4	Safety Clips	0.90	0.100	0.25	0.80	0.66	0.9574	0.0250
Rail Fire	B2	Cushions for Pallets	0.10	0.005	0.75	0.60	1.30	0.0294	0.0038
Rail Fire	B2	Temp & Humidity Maintenance	0.25	0.001	0.75	0.40	0.67	0.3068	0.0008
Rail Fire	B2	Periodic Inspection	0.75	0.010	0.75	0.60	1.29	1.2553	0.0075
Truck Fire	B4	Regular Truck Maintenance	0.90	0.001	0.50	1.00	1.34	1.5416	0.0005
Truck Fire	B4	Train Drivers	0.90	0.050	0.50	0.90	1.40	1.6086	0.0250
Truck Fire	B4	Cushions for Pallets	0.10	0.010	0.50	0.60	1.00	0.0000	0.0050
Storage	B6	Temp & Humidity Maintenance	0.50	0.005	0.50	0.40	0.50	0.1353	0.0025
Autoignition	B6	Electrical Inspection	0.75	0.010	0.50	0.70	1.34	0.9116	0.0050
Autoignition	B6	Proper Packaging	0.10	0.010	0.50	0.15	0.50	0.0000	0.0050
Autoignition	B6	Cushions for Pallets	0.90	0.005	0.50	0.10	0.80	0.0000	0.0025
Battery Initiates	B6	Safety Clips	0.90	0.010	0.50	0.80	1.00	0.0000	0.0050

 Indicates Threat Asset Pairs with risk value Not Acceptable

Figure 5.4 Screenshot of the table listing the payoffs $S_{i,k}$ and $A_{j,k}$.

		Assets ▾					
Safeguard ▾	Data ▾	A2	A4	B2	B4	B6	Grand Total
Cushions for Pallets	Sum of Sij	0.68	0.15	0.24	0.00	0.00	1.07
	Sum of Aij	0.01	0.00	0.01	0.01	0.01	0.03
Electrical Inspection	Sum of Sij					0.40	0.40
	Sum of Aij					0.01	0.01
Periodic Inspection	Sum of Sij		0.17	0.62			0.80
	Sum of Aij		0.01	0.01			0.02
Proper Packaging	Sum of Sij		0.17			0.00	0.17
	Sum of Aij		0.00			0.01	0.01
Regular Truck Maintenance	Sum of Sij	0.15			0.69		0.84
	Sum of Aij	0.11			0.00		0.11
Safety Clips	Sum of Sij		0.33			0.00	0.33
	Sum of Aij		0.05			0.01	0.06
Temp & Humidity Maintenance	Sum of Sij		0.38	0.11		0.00	0.50
	Sum of Aij		0.00	0.00		0.01	0.01
Train Drivers	Sum of Sij	0.85			0.72		1.58
	Sum of Aij	0.06			0.05		0.11
Total Sum of Sij		1.69	1.21	0.97	1.41	0.40	5.68
Total Sum of Aij		0.17	0.06	0.02	0.06	0.04	0.36

↖
↘

Most Vulnerable Asset
Most effective Safeguard

Figure 5.5 Payoff matrix for stage 1.

5.4 Case Study - Stage 2

This stage simulates the implementation of the most effective safeguard and displays reevaluated risk levels. The previous stage identified the most effective safeguard to secure asset A2 from the threat of “truck fire” as “train drivers”. This demonstrates that training the truck drivers to handle trucks in a more controlled manner reduces the frequency of abrupt braking, thereby reducing the probability of truck fire. The implementation of the safeguard is now simulated and the risk values reassessed. The safeguard “train drivers” provides a “high” level of protection and hence reduces the frequency of occurrence of truck fires from “High” to “Occasional”. The updated risk values are displayed with the threat/activity listing in Figure 5.6.

	Threats	Assets	Risk Values	Risk Status
Factory to Factory Storage	Forklift tines puncture container	A1	1.00E-08	Acceptable
	Pallet Falls	A1	1.00E-08	Acceptable
	Truck Fire	A2	1.00E-08	Acceptable
	Detonation of Cartridge	A2	1.00E-08	Acceptable
	Truck Accident	A2	1.00E-09	Acceptable
	Bullet Punctures container	A2	1.00E-08	Acceptable
	Forklift tines puncture container	A3	1.00E-08	Acceptable
	Pallet Falls	A3	1.00E-08	Acceptable
	Storage	A4	1.00E-06	Hot Acceptable
	Autoignition	A4	1.00E-06	Hot Acceptable
Battery Initiates	A4	1.00E-06	Hot Acceptable	
Fire	A4	1.00E-08	Acceptable	
Reaction with other items	A4	1.00E-08	Acceptable	
Factory to COHUS Storage (Rail)	Forklift tines puncture container	B1	1.00E-08	Acceptable
	Pallet Falls	B1	1.00E-08	Acceptable
	Rail Fire	B2	1.00E-05	Hot Acceptable
	Detonation	B2	1.00E-08	Acceptable
	Bullet Punctures container	B2	1.00E-08	Acceptable
	Rail Accident	B2	1.00E-09	Acceptable
	Forklift tines puncture container	B3	1.00E-08	Acceptable
	Pallet Falls	B3	1.00E-08	Acceptable
	Truck Fire	B4	1.00E-08	Acceptable
	Detonation	B4	1.00E-08	Acceptable
	Bullet Punctures container	B4	1.00E-08	Acceptable
	Truck Accident	B4	1.00E-09	Acceptable
	Forklift tines puncture container	B5	1.00E-08	Acceptable
	Pallet Falls	B5	1.00E-08	Acceptable
	Storage	B6	1.00E-06	Hot Acceptable
	Autoignition	B6	1.00E-06	Hot Acceptable
	Battery Initiates	B6	1.00E-06	Hot Acceptable
	Fire	B6	1.00E-08	Acceptable
Reaction with other items	B6	1.00E-08	Acceptable	

Indicates Acceptable Level of Risk
 Indicates Risk Level Hot Acceptable
Acceptable Risk Level **1.13E-07**

Figure 5.6 Screen shot of the threat/activity table with updated threat levels.

The new risk status for the threat asset pairs from stage 1 is shown above. The updated utility formulation table is shown in Figure 5.7 and the updated payoff matrix is displayed in Figure 5.8. Note that, as the threats become acceptable, the utility and payoffs of the safeguards are reset to zero.

Threats	Assets/ Activity	Safeguard	Value of Asset	Level of Protection	Utility	Increase in value of asset	Net Utility
Truck Fire	A2	Regular Truck Maintenance	0.5	0.5	0.25	0	0
Truck Fire	A2	Train Drivers	0.5	0.75	0.375	0.001	0
Truck Fire	A2	Cushions for Pallets	0.5	0.75	0.375	0.0001	0
Storage	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Storage	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Autoignition	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Autoignition	A4	Cushions for Pallets	0.25	0.5	0.125	0.0001	0.1249
Autoignition	A4	Proper Packaging	0.25	0.25	0.0625	0	0.0625
Autoignition	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Battery Initiates	A4	Safety Clips	0.25	0.75	0.1875	0.001	0.1865
Rail Fire	B2	Cushions for Pallets	0.75	0.5	0.375	0.0001	0.3749
Rail Fire	B2	Temp & Humidity Maintenance	0.75	0.25	0.1875	0	0.1875
Rail Fire	B2	Periodic Inspection	0.75	0.5	0.375	0	0.375
Truck Fire	B4	Regular Truck Maintenance	0.5	0.75	0.375	0	0
Truck Fire	B4	Train Drivers	0.5	0.75	0.375	0.001	0
Truck Fire	B4	Cushions for Pallets	0.5	0.5	0.25	0.0001	0
Storage	B6	Temp & Humidity Maintenance	0.5	0.25	0.125	0	0.125
Autoignition	B6	Electrical Inspection	0.5	0.75	0.375	0	0.375
Autoignition	B6	Proper Packaging	0.5	0.25	0.125	0	0.125
Autoignition	B6	Cushions for Pallets	0.5	0.5	0.25	0.001	0.249
Battery Initiates	B6	Safety Clips	0.5	0.75	0.375	0.001	0.374



 Indicates Threat Asset Pairs with risk value Not Acceptable
 Indicates Threat Asset Pairs with risk value Acceptable

Figure 5.7 Screenshot of the updated utility formulation table.

		Assets ▼					
Safeguard ▼	Data ▼	A2	A4	B2	B4	B6	Grand Total
Cushions for Pallets	Sum of Sij	0.00	0.43	0.71	0.00	0.00	1.13
	Sum of Aij	0.00	0.00	0.01	0.00	0.01	0.01
Electrical Inspection	Sum of Sij					0.40	0.40
	Sum of Aij					0.01	0.01
Periodic Inspection	Sum of Sij		0.68	1.17			1.85
	Sum of Aij		0.01	0.01			0.02
Proper Packaging	Sum of Sij		0.43			0.00	0.43
	Sum of Aij		0.00			0.01	0.01
Regular Truck Maintenance	Sum of Sij	0.00			0.00		0.00
	Sum of Aij	0.00			0.00		0.00
Safety Clips	Sum of Sij		0.64			0.00	0.64
	Sum of Aij		0.05			0.01	0.06
Temp & Humidity Maintenance	Sum of Sij		0.89	0.43		0.00	1.32
	Sum of Aij		0.00	0.00		0.01	0.01
Train Drivers	Sum of Sij	0.00			0.00		0.00
	Sum of Aij	0.00			0.00		0.00
Total Sum of Sij		0.00	3.05	2.31	0.00	0.40	5.76
Total Sum of Aij		0.00	0.06	0.02	0.00	0.04	0.12

↙
↘

Most Vulnerable Asset
Most effective Safeguard

Figure 5.8 Updated pay off matrix after implementation of safeguard.

The updated payoff matrix reveals that the most vulnerable asset has now shifted from A2 to A4 and the most effective safeguard is now 'Periodic Inspection'. Hence, the frequency of occurrence for threat associated with asset A4 and B2 will be updated next. In this manner, the safeguards can be implemented one after the other till all the risk levels are below acceptable limits.

5.5 Case Study - Stage 3

This stage aims at determining the response of the methodology to change in degree of consequence of a threat on an asset. To achieve this, it is assumed that the severity of consequence of fork tines puncturing the container housing the explosive material has increased by one level, thereby increasing the risk to unacceptable levels.

Notice that the treat level for asset A1 has become unacceptable due to the increase in consequences of the threat "fork tines puncture container". The safeguard proposed for securing the containers against fork tines is by providing "proper packaging" for explosives inside the container. This would reduce the frequency of occurrence and thereby the risk associated with it. The utility table is displayed in Figure 4.10 and the payoff formulation for stage 3 is as shown in Figure 4.11.

The payoff matrix displayed in figure 4.11 indicates that the most attractive asset is now A4 and the most effective safeguard is 'proper packaging'. The safeguard implemented thus reduces the frequency of occurrence thereby reducing the risk associated with each threat/asset pairs.

	Threats	Assets	Risk Values	Risk Status
Factory to Factory Storage	Forklift tines puncture container	A1	1.00E-06	Not Acceptable
	Pallet Falls	A1	1.00E-08	Acceptable
	Truck Fire	A2	1.00E-08	Acceptable
	Detonation of Cartridge	A2	1.00E-08	Acceptable
	Truck Accident	A2	1.00E-09	Acceptable
	Bullet Punctures container	A2	1.00E-08	Acceptable
	Forklift tines puncture container	A3	1.00E-08	Acceptable
	Pallet Falls	A3	1.00E-08	Acceptable
	Storage	A4	1.00E-06	Not Acceptable
	Autoignition	A4	1.00E-06	Not Acceptable
Battery Initiates	A4	1.00E-06	Not Acceptable	
Fire	A4	1.00E-08	Acceptable	
Reaction with other items	A4	1.00E-08	Acceptable	
Factory to COIUS Storage (Rail)	Forklift tines puncture container	B1	1.00E-08	Acceptable
	Pallet Falls	B1	1.00E-08	Acceptable
	Rail Fire	B2	1.00E-05	Not Acceptable
	Detonation	B2	1.00E-08	Acceptable
	Bullet Punctures container	B2	1.00E-08	Acceptable
	Rail Accident	B2	1.00E-09	Acceptable
	Forklift tines puncture container	B3	1.00E-08	Acceptable
	Pallet Falls	B3	1.00E-08	Acceptable
	Truck Fire	B4	1.00E-08	Acceptable
	Detonation	B4	1.00E-08	Acceptable
	Bullet Punctures container	B4	1.00E-08	Acceptable
	Truck Accident	B4	1.00E-09	Acceptable
	Forklift tines puncture container	B5	1.00E-08	Acceptable
	Pallet Falls	B5	1.00E-08	Acceptable
	Storage	B6	1.00E-06	Not Acceptable
	Autoignition	B6	1.00E-06	Not Acceptable
	Battery Initiates	B6	1.00E-06	Not Acceptable
	Fire	B6	1.00E-08	Acceptable
Reaction with other items	B6	1.00E-08	Acceptable	

Indicates Acceptable Level of Risk
 Indicates Risk Level Not Acceptable
Acceptable Risk Level 1.13E-07

Figure 4.9 Screenshot of table listing risk status of the threat/activity pairs with new threat activity.

Threats	Asset/Activity	Safeguard	Value of Asset	Level of Protection	Utility	Increase In value of asset	Net Utility
Forklift tires puncture container	A1	Proper Packaging	0.75	0.75	0.5625	0	0.5625
Truck Fire	A2	Train Drivers	0.5	0.75	0.375	0.001	0
Truck Fire	A2	Cushions for Pallets	0.5	0.75	0.375	0.0001	0
Storage	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Storage	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Autoignition	A4	Temp & Humidity Maintenance	0.25	0.5	0.125	0	0.125
Autoignition	A4	Cushions for Pallets	0.25	0.5	0.125	0.0001	0.1249
Autoignition	A4	Proper Packaging	0.25	0.25	0.0625	0	0.0625
Autoignition	A4	Periodic Inspection	0.25	0.5	0.125	0	0.125
Battery Initiates	A4	Safety Clips	0.25	0.75	0.1875	0.001	0.1865
Rail Fire	B2	Cushions for Pallets	0.75	0.5	0.375	0.0001	0.3749
Rail Fire	B2	Temp & Humidity Maintenance	0.75	0.25	0.1875	0	0.1875
Rail Fire	B2	Periodic Inspection	0.75	0.5	0.375	0	0.375
Truck Fire	B4	Regular Truck Maintenance	0.5	0.75	0.375	0	0
Truck Fire	B4	Train Drivers	0.5	0.75	0.375	0.001	0
Truck Fire	B4	Cushions for Pallets	0.5	0.5	0.25	0.0001	0
Storage	B6	Temp & Humidity Maintenance	0.5	0.25	0.125	0	0.125
Autoignition	B6	Electrical Inspection	0.5	0.75	0.375	0	0.375
Autoignition	B6	Proper Packaging	0.5	0.25	0.125	0	0.125
Autoignition	B6	Cushions for Pallets	0.5	0.5	0.25	0.001	0.249
Battery Initiates	B6	Safety Clips	0.5	0.75	0.375	0.001	0.374

Indicates Threat Asset Pairs with risk value Not Acceptable
 Indicates Threat Asset Pairs with risk value Acceptable

Figure 4.10 Utility Table for stage 3.

		Assets						
Safeguard	Data	A2	A4	B2	B4	B6	A1	Grand Total
Cushions for Pallets	Sum of Sij	0.00	0.43	0.71	0.00	0.00		1.13
	Sum of Aij	0.00	0.00	0.01	0.00	0.01		0.01
Electrical Inspection	Sum of Sij					0.40		0.40
	Sum of Aij					0.01		0.01
Periodic Inspection	Sum of Sij		0.68	1.17				1.85
	Sum of Aij		0.01	0.01				0.02
Proper Packaging	Sum of Sij		0.43			0.00	1.93	2.36
	Sum of Aij		0.03			0.05	0.00	0.08
Regular Truck Maintenance	Sum of Sij				0.00			0.00
	Sum of Aij				0.00			0.00
Safety Clips	Sum of Sij		0.64			0.00		0.64
	Sum of Aij		0.05			0.01		0.06
Temp & Humidity Maintenance	Sum of Sij		0.89	0.43		0.00		1.32
	Sum of Aij		0.00	0.00		0.01		0.01
Train Drivers	Sum of Sij	0.00			0.00			0.00
	Sum of Aij	0.00			0.00			0.00
Total Sum of Sij		0.00	3.05	2.31	0.00	0.40	1.93	7.69
Total Sum of Aij		0.00	0.09	0.02	0.00	0.08	0.00	0.19

Figure 4.11 Payoff Matrix for Stage 3.

CHAPTER 6

DISCUSSION AND SCOPE OF FUTURE RESEARCH

Clearly, the risks that exist in today's complex supply chain networks are significant and on the rise. To mitigate these risks, it is important to understand system vulnerabilities and what the potential consequences are. The challenges are not only in assessing risk for an individual asset or activity, but also relate those up to causal events at all levels from the supplier to customer. Companies who opt to brush aside supply chain risk open themselves to significant vulnerabilities that can dramatically impact business continuity.

The future of supply management is reliant on the abilities of the risk manager to balance return and risk to achieve a desired outcome in the financial and sustainability perspectives. The timely identification and mitigation of supply chain risk on a global basis will enable a strong and reliable business model with capabilities to lower the long term costs and drive supply chain management results that secure businesses. But creating and implementing a supply risk mitigation and management strategy is not simple. Successful enterprises must understand both the internal and external factors that drive supply risks, as well as develop scenario and risk mitigation strategies that take into account the market condition extremes and reduce business risk through proactively managing the global supply network.

To create supply chain strategies that weigh supply chain risk against the cost of mitigating the risk, firms should employ a systematic, but comprehensive analytical risk mitigation framework. The methodology should have the ability to identify centralized risk elements, filter out high-contingency risks by analyzing risk influences and estimate

the impact associated with each risk. Safeguards must then be identified to mitigate the effects of the threats that pose risk. Threats can be prevented, reduced or averted based on the extent or frequency of consequences of threat elements on the business assets and their related vulnerabilities. To ensure stability, these vulnerabilities and weaknesses should be resolved before the threats exploit them.

Risk mitigation has a wider ambit than just identifying the cause of risk and implementing any protective measure that can mitigate the risks. The causes of risks have to be effectively measured, appropriate safeguard alternatives identified and the best safeguard implemented. Safeguards should be assessed based on the utility they provide toward securing the assets against the threats, their reliability, cost of implementation and the overall effectiveness of the safeguard. A good safeguard should provide a good utility for its cost, secure assets effectively and should not be vulnerable to disruptive factors.

The Supply Chain Risk Assessment and Management methodology discussed in this thesis provides the risk manager with a highly elaborate and robust tool to analyze and manage supply chain risks more effectively with ease. The risk mitigation methodology proposed imparts a certain degree of intelligence making strategic risk mitigation decisions undemanding. The use of game theoretic model provides a two-sided perspective to the risk environment – the attractiveness of the assets (for threat elements) and the vulnerabilities of the asset (for risk manager). This clearly identifies the assets, which are most vulnerable, and enables prioritizing the assets to be secured.

The mathematical approach proposed for the generation of payoffs is comprehensive taking into consideration the factors which would contribute to rational decision making – the reliability of the safeguard, the number of assets the safeguard

secures, its utility, cost of implementation and any disruptive threat influences on the safeguard. This detailed safeguard evaluation enables the risk manager to evaluate the safeguards from various points of view and choose the safeguard that not only provides good utility but also is reliable and justifies its cost.

Risk assessment for any risk environment is futile unless backed up by a good risk mitigation approach and vice versa. Hence an integrated approach toward risk management is entailed with reliable risk identification and mitigation resources to confer organizations the competitive edge during uncertain times.

Scope of Future Work

The Supply Chain Risk Assessment and Management System (SCRAMS), being developed as a web based application at Multi-Lifecycle Engineering Research Center (MERC), envisions being the next generation risk management tool that can enable better visibility of the risk elements and their degrees of impact within the supply chain and thereby enabling more sophisticated approach to risk management. The risk assessment module capable of identifying and analyzing risk influences has been developed by Venkata Kallepalli and has been seamlessly integrated into the web based architecture. However, data extraction has not been embedded into the SCRAM system. Data pertaining to the supply chain assets and activities could be extracted from legacy databases or from the ERP systems like SAP.

The supply chain risk mitigation methodology proposed in this thesis needs to be embedded into the web-based architecture of the SCRAMS. The integration of Bayesian networks or fuzzy logic with game theoretic decision making, needs to be explored further.

APPENDIX A

RISK ASSESSMENT AND MITIGATION METHODOLOGY

Figure 7.1 illustrated the systematic approach that has been designed to generate the Supply Chain Risk Analysis and Management (SCRAM) tool. The first section of the diagram demonstrates the risk assessment approach and the latter section of the flow diagram illustrates the risk mitigation approach.

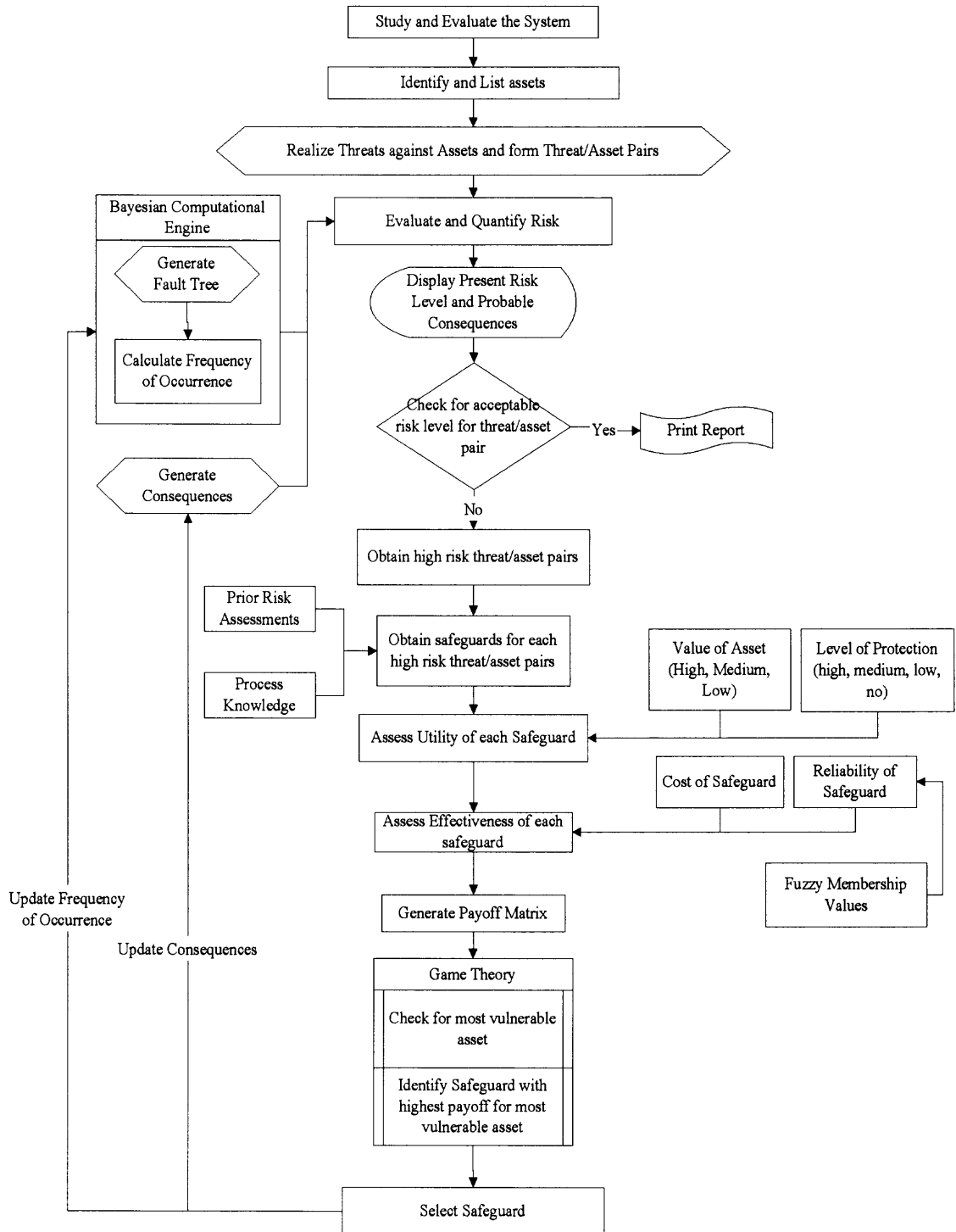


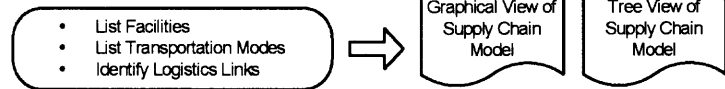
Figure 7.1 Illustrates the risk management approach adopted in the SCRAM System.

APPENDIX B

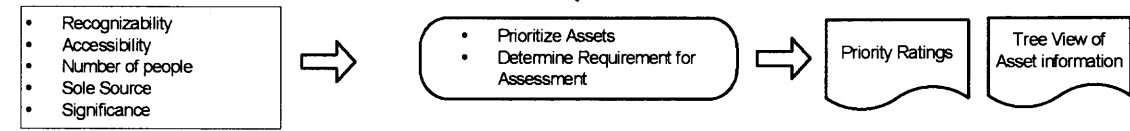
SCRAM SYSTEM APPROACH

The SCRAM system is a web-enabled risk assessment and management system developed to address the issue of securing the business supply chains against vulnerabilities. Figure 7.2 illustrates the sequential approach of the decision tool.

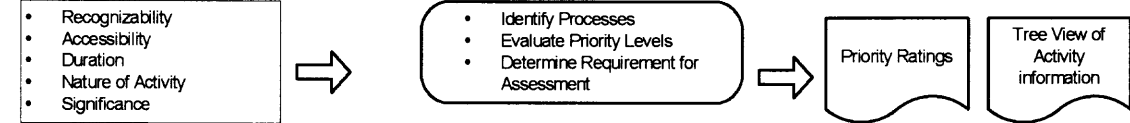
1. Input Model



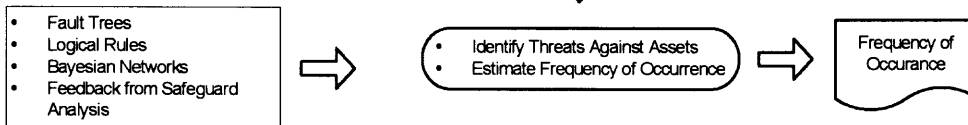
2. Screening



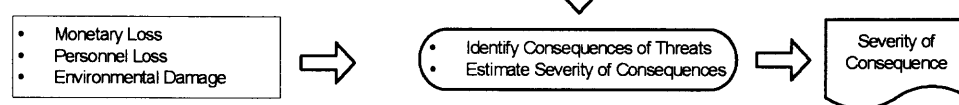
3. Activity Identification



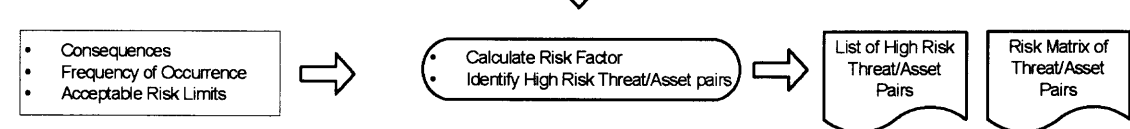
4. Threat Identification



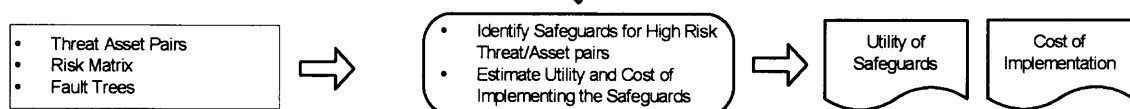
5. Consequence Analysis



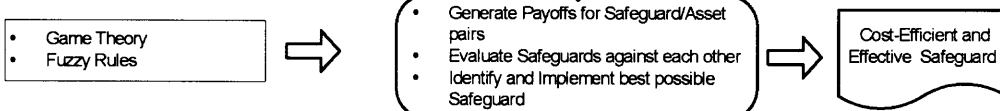
6. Risk Quantification



7. Safeguard Identification



8. Safeguard Analysis



9. Report Generation

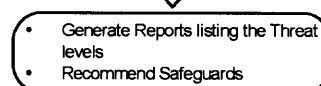


Figure 7.2 Sequential approach adopted by SCRAM system.

REFERENCES

1. Donovan Michael R., "Supply Chain Management: A Plan to Succeed", Performance Improvement Journal, 2002.
2. Jenkins B. D., "Security Risk Analysis and Management, Safeguards Inc", 1998.
3. Sesel Jonathan, "The History of Professional Risk Management", Article, 2002
4. Armstrong Mary S., "Risk Management Plan for EMD Project", ECS Maintenance and Development Project Proposal, December 2003.
5. "Vulnerability Assessment and Survey Program – Overview of Assessment Methodology", US Department of Energy, Office of Energy Assurance, September 2001.
6. "Vulnerability Assessment Worksheet", Municipal Police Officers Education and Training Commission. Retrieved April 4, 2004 from World Wide Web: <http://www.mpoetc.state.pa.us>.
7. "Executive Report on behalf of Department of Transport, Local Government and the Regions", Cranfield University, January 2002.
8. Sandia National Laboratories. Retrieved April 4, 2004 from World Wide Web: <http://www.sandia.gov/capabilities/mod-sim/index.html>
9. Hudson Linwood D., Ware Bryan S., Laskey Kathryn B., Mahoney Suzanne M., "An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners", submitted to UAI, 2002.
10. Ware Bryan S., Hudson Linwood D., Kerr Robert S., "A Knowledge-Based Simulation Architecture for Assessing and Managing Risk", Digital Sandbox, Inc., 2001.
11. Digital Sandbox. Retrieved April 4, 2004 from World Wide Web: http://dsbox.com/products/sandbox_technology.html
12. Kickert Walter J. M., "Fuzzy Theories on Decision Making", 1978.
13. The Buddy System. Retrieved April 4, 2004 from World Wide Web: <http://www.buddysystem.net>
14. The Cobre Group. Retrieved April 4, 2004 from World Wide Web: <http://www.cobre.com/helpmate.html>

15. The E Team. Retrieved April 4, 2004 from World Wide Web:
<http://www.eteam.com/resources/index.html>
16. Los Alamos National Laboratories. Retrieved April 4, 2004 from World Wide Web:
http://www.lanl.gov/quarterly/sim_science.html.
17. Palisade Group. Retrieved April 4, 2004 from World Wide Web:
<http://www.palisade.com/>
18. Kilgore Michael J., "Mitigating Supply Chain Risks", 89th Annual Supply Chain Conference, April, 2004.
19. Leslie Helm, "Improbable Inspiration", Article, Los Angeles Times, October 1996.
20. Wray Buntine, "A Guide to the Literature on Learning Probabilistic Networks From Data", IEEE Transactions on Knowledge and Data Engineering, 1996.
21. Leonhardt David, "Adding Art to the Rigor of Statistical Science", Article, New York Times, April, 2001.
22. Heckerman. David, Mamdani Abe, Wellman Michael P., "Real World Applications of Bayesian Networks", Communications of ACM, 1995.
23. Korb B. Kelvin, Nicholson E. Ann, "Bayesian AI Tutorial", Lecture Notes, 2001.
24. Phadnis. Aparna, Nasser. Sara, "Fuzzy Belief Networks", Powerpoint Presentation, September 2002.
25. Lerner N. Uri, "Hybrid Bayesian Networks for Reasoning about Complex Systems", PhD Dissertation, Stanford University, October 2002.
26. Pan Heping, Okello Nickens, McMichael Daniel, Roughan. Mathew, "Fuzzy Causal Probabilistic Networks and Multisensor Data Fusion", SIPE International Symposium on Multispectral Image Processing, October 1998.
27. Said Ahmed, Stevens K. David, Sehlke Gerald, "Exploration of Conservation Schemes and TDML Using Bayesian Networks", March 2002.
28. Martin Neil, Tranham Ed, "Using Bayesian Networks to Predict Operational Risk", Operational Risk, August 2002.
29. Pan Heping, McMichael Daniel, "Fuzzy Causal Probabilistic Networks – A New Ideal And Practical Inference Engine", May 1998.
30. Myllymaki Petri, "Advantages of Bayesian Networks in Data Mining and Knowledge Discovery", Helsinki Institute of Information Technology, 2001.

31. Heckerman David, "Bayesian Networks for Data Mining", *Data Mining Knowledge Discovery* 1, 79-119, 1997.
32. Haddawy Peter, "An Overview of Some Recent Developments in Bayesian Problem Solving Techniques", *AI Magazine Special Issue on Uncertainty in AI*, Summer 1999.
33. Chickering David M., Geiger Dan, Heckerman. David, "Learning Bayesian Networks is NP-Hard", *Technical Report MSR-TR-94-17*, November 1994.
34. Marshall Dave, "Lecture Notes on AI, Bayes Theorem", September 2002.
35. Blair Andrew N., Ayyub M. Bilal, "Fuzzy Stochastic Cost and Schedule Risk Analysis: MOB Case Study", 1999.
36. Bezdek James C., "Comments On Fuzzy Sets – What are they and Why ?", *IEEE transaction on Fuzzy systems* , Vol 2 , No 1, February 1994.
37. G´erard P. Cachon and Serguei Netessine, "Game Theory in Supply Chain Analysis", invited chapter for the book *Supply Chain Analysis in the eBusiness Era*.
38. Von Neumann J., and Morgenstern O., "The Theory of Games and Economic Behavior", Princeton University Press, 2nd edition, 1947.
39. Pauly Marc, "Coalitional Ability in Multi-Agent Systems: A Logical Approach", *AAAI Spring Symposium*, 2001.
40. Zhu Qiumin, Junping Sun, "Building a Bayesian-Game-Theoretic Decision Support Agent", *IEEE SMC*, 2002.
41. Zhang Yan-Qing, Kandel A, Friedman M, "Hybrid Decision-Making System for Fuzzy Moves", *IEEE*, 1995.
42. Stanford Encyclopedia of Philosophy, "Game Theory", Retrieved April 4, 2004 from World Wide Web: <http://plato.stanford.edu/cgi-bin/encyclopedia/>