ABSTRACT

SUPPLY CHAIN RISK ANALYSIS

by
Venkata R. Kallepalli

A new decision support system is proposed and developed that will help sustaining business in a high-risk business environment. The system is developed as a web application to better integrate the supply chain entities and to provide a common platform for performing risk analysis in a supply chain. The system performs a risk analysis and calculates risk factor with each activity in the supply considering its interrelationship with other activities. Bayesian networks along with fault tree structures are embedded in the system and logical rules are used to perform a qualitative fault tree analysis, as the data required to calculate the frequency of occurrence is rarely available.

The developed system guides the risk assessment process: from asset identification to consequence analysis before estimating the risk factor associated with each activity in the supply chain. The system is tested with a sample case study on a highly explosive product. Results show that the system is capable of identifying high-risk threats.

The system further needs to be developed to add a safeguard analysis module and to enable automatic data extraction from the enterprise resource planning and legacy databases. It is expected that the system on complete development and induction will help supply chain managers to manage business risks and operations more efficiently and effectively by providing a complete picture of the risk environment and safeguards required to reduce the risk level.

SUPPLY CHAIN RISK ANALYSIS

by
Venkata R. Kallepalli

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 ANALYSIS

Venkata R. Kallepalli

Dr. Reggie Caudill, Thesis Advisor — Date
Executive Director of 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, Laboratory for Discrete Event Systems and
Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Venkata R. Kallepalli

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 Engineering in Manufacturing Engineering,
  Bangalore University, Bangalore, India, 2001

Publications and Presentations

V. Kallepalli, R. Pai, 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

ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude to Dr. Reggie J. Caudill, who with his research experience and knowledge steered this research work. Also, Dr. Caudill has been a constant source of inspiration and without his support the research work would have never been finished.

I thank Dr. Paul Ranky and Dr. Mengchu Zhou for serving on the thesis committee. Mr. Najeeb Alli, former Systems Manager, MERC, deserves a special note of appreciation for his assistance while implementing the risk assessment framework.

Special thanks to Mr. Donald Yee and Mr. Bob Goldberg of Picatinny Arsenal, the United States Army Armament Research, Development and Engineering Center, for providing the case study and crucial information regarding Picatinny Arsenal's requirements that initiated the research effort.

I am grateful to Multi-Lifecycle Engineering Research Center for providing the necessary infrastructure and support to carry out the research work. I also thank Mr. David Dickinson for the valuable suggestions he provided during the initial phase of the research work. I will always be obliged to Mr. Roshan Pai, who always motivated and inspired me as friend and research-partner.

Finally, I would always be indebted to my family members and friends for their encouragement and support at each step of this work.

Whenever I hear, "It can't be done," I know, I'm close to success.
- **Michael Flatley**

Dedicated to my mom and dad, who taught me to believe in myself.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

Chapter **Page**

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

LIST OF TABLES

LIST OF TABLES
(Continued)

LIST OF TABLES
(Continued)

LIST OF TABLES
(Continued)

LIST OF FIGURES

LIST OF FIGURES
(Continued)

Figure **Page**

CHAPTER 1

INTRODUCTION

1.1 Background

A supply chain is a complex network of business relationships extending from raw material suppliers, component manufacturers, and logistics operators to manufacturers, retailers and consumers. The supply chain starts with customer's requirements and ends with multiple tiers of suppliers and service providers. These chains involve a constant flow of cash, material and information and aim at generating revenues by selling products/services to customers. Continuity of the supply chain operations is of utmost importance and any disruption can severely impact business operations and product flows. Managing disruptions efficiently and effectively has become the key factor in deciding the success of a business.

Supply chains are as old as trade and the roots could be traced back to the barter system. Even though supply chains always existed, their importance was not realized until early 1960's [1]. After 1960, rapid strides were taken to improve efficiency and effectiveness. Prior to 1960's, each business entity worked independently. And, resources were planned and optimized for each unit without considering other entities in the chain. As a result, each company used to maintain a safety stock to account for the uncertainties associated with other business partners. After 1960, the importance of the supply chains was realized and management principles were extended beyond an individual business to consider the supply chain as a single system. Due to the improved collaboration and

coordination, inventory levels were drastically reduced resulting in significant cost savings.

The Japanese formulated the just-in-time (JIT) philosophy that emphasizes near zero inventory levels to enhance the cost effectiveness of the chain. The fierce competition in the market, with ever increasing customer expectations for better quality products at lower cost, resulted in adoption of the just-in-time philosophy.

Today, many companies operate with inventories less than for a couple of hours. Also, companies reduced their supplier base drastically to reduce overhead and order processing costs and to get quantity discounts. Xerox, for example, reduced its supplier base from 5000 to 400 between 1981 and 1985 and reduced costs by 10% and lead-time by 34 weeks [2].

The just-in-time philosophy is an ideal production practice if the flow variability is low. However, the terrorist events of 9-11, labor strike at 19 West Coast Ports and the black out in the Northeast coast have led companies to reassess of the robustness of their supply chains and the impact of disruptions on production flow. Due to the terrorist attacks, borders were sealed and security was tightened. Many companies had to suspend operations, as they were unable to procure components from overseas suppliers or experienced prolonged delays in arrival of the shipment. Toyota suspended operations, as one of its suppliers did not receive the steering sensors from a German supplier due to closure of the borders [3]. Even though companies were not directly targeted, heavy economic losses resulted due to precautionary measures taken by the government to protect people from further attacks.

Questions like what would be the response of the supply chain if one of the ports or a production plant were compromised are becoming increasingly relevant. These kinds of extraordinary events are extremely difficult to predict when and where they will occur, but understanding these events has become extremely important to business survivability in a highly competitive market. However, these types of extraordinary events are not the only threats to the supply chain. But, minor events like delay in arrival of goods or an accident at a facility have the potential to disrupt the entire chain, as inventory levels are almost zero.

Supply chain vulnerabilities always existed but were mostly ignored in the past due to economic considerations. For example prior to September 11, Ericsson reported a loss of 1.8 billion US dollars and lost market share by 4% due to complete dependence on Philips for a computer chip. Due to a fire accident in one of their plants, Philips was not able to supply computer chips to Ericsson. The disadvantage of having single source suppliers became apparent to Ericsson [4].

Apart from maintaining continuity of the business chain, ensuring the safety and security of employees and products is equally important. Events like the Bhopal gas tragedy or the Chernobyl nuclear accident in the former Soviet Union are totally unacceptable [4]. Employees, assets and operations need to be protected.

Today, managers are confronted with many operational and business questions. For example, if sole sourcing is a high-risk proposition then how many alliances should be made? Should production facilities be centralized to reduce costs or should they be dispersed to improve security. If near zero inventory level poses a significant threat then what should be the ideal inventory level. In the past, managers relied on their experience

to answer these questions. But today, with constantly changing business environment and new threats emerging every day, it may not be possible to continue relying on experience.

Building inventories or constructing safeguards along the entire chain may ensure safety and continuity of operations, however, the economic advantage of JIT may be lost. Industry has come a long way in implementing innovative techniques to improve productivity and cost effectiveness. Abandoning all of those techniques at this point of time may not be advisable since billions of dollars have been invested.

Instead of building inventories to offset disruptions, new decision tools need to be developed that allow flexible supply chain management in a rapidly changing environment. For example, if a storm is expected to hit one of the logistics links then the inventory levels can be temporarily increased or the shipment can be rerouted to reduce risk and maintain business continuity. The capability to make real time decisions and to operate flexibly will allow companies to reap the benefits of being just-in-time while managing disruptions efficiently. The key factor to develop such a system lies in understanding the core vulnerabilities and how assets and operations should be protected to avoid disruptions in the operations.

Risk analysis is a classical subject that could help answer some of the questions that industry is facing today. Risk analysis is a very powerful tool for decision-making under uncertainty and has been successfully applied to many industries, especially the nuclear and aerospace industries. Risk analysis aims at identifying and quantifying the threats and their consequences. It follows a system analysis approach to identify the threats and associated causal events in the system that could disrupt the system. Such an analysis not only identifies system threats but also enables a better understanding of the

vulnerabilities of the system. Knowledge of system threats, vulnerabilities and consequences will allow risk-aware and more rational decision-making.

1.2 Research Needs

Risk analysis techniques in the past have been mainly focused toward stand-alone systems like a nuclear facility or product failures in aerospace industry. Even though the underlying concepts of risk analysis are system independent, the direct application of existing techniques developed is restricted by the very nature of the supply chain.

In a supply chain, the business units are interdependent and performance of one unit depends on the other. These interdependencies are very complex and often difficult to understand and model. For example, consider two supplier's A and B, who supply two different components to manufacturer C. If there is a work halt at A's facility then B's business will also get affected even though they are not directly related. This is a simple and straightforward example of interdependence. Consider the business of B getting affected due to a work halt at the nth tier supplier of A. These kinds of interrelationships need to be considered while analyzing risks. These interrelationships make supply chain risk analysis much more challenging. A recent report by the National Research Council recognizes the gaps in existing systems analysis, risk modeling and network techniques to handle the complexity associated with assessing infrastructure security issues. Basic research is required to better understand and to model this type of complex interrelationships, supply chain vulnerabilities and chain dynamics.

The global nature of the supply chain also posses a significant challenge in the risk analysis of the supply chain. Supply chains often extend across corporate and

national boundaries. Even though the businesses are interdependent, they work independently and exchange a limited amount of data with one another. For example, the manufacturer might have information on the status of the shipment from the supplier but rarely has information on the problems/ threats that the supplier is facing. Without much supplier information, the manufacturer may not be able to perform a complete and effective risk analysis, as his operations are dependent on the supplier. Data availability is a key factor that needs to be addressed. The supply chain units need to be better integrated horizontally as well as vertically to improve information flow.

Risk analysis is a very data intensive subject and often this hinders the motivation to perform the analysis. However, the data required to perform the analysis may be residing in one of the databases and could be extracted without much effort. For example, the probability of work stoppage due to inventory shortages is directly dependent on the inventory level in a plant. This data (inventory level) resides in an Enterprise Resource Planning (ERP) database and could be extracted automatically to estimate the probability of a work stoppage. New tools are required that would identify the data source and automate data extraction.

The inherent dynamic nature of the supply chain and continuously changing business environment also make risk analysis of a supply chain more challenging and distinctively different from traditional risk analysis. Risk analysis of the supply chain should be performed on a continuous real time basis as opposed to one time risk assessment. Risk levels need to be constantly updated based on the new information as and when it flows into the system. It may not be possible to monitor manually, requiring the process to be automated.

Logical inference techniques like Bayesian networks have the capability to calculate new threat levels based on new available information. These inference techniques combine new and prior information to deduce an inference. However, which inference technique is ideal for risk analysis of supply chains has still not been resolved. Research is needed to identify the best technique for analyzing risks in a supply chain.

Computer based risk analysis systems are highly sought due to their immense computational capability. Presently, none of the risk assessment software available in the market has the capability to assess risks in a supply chain. Software's like Site Profiler and Buddy System from Digital Sandbox and Counter Measures, Inc, respectively, assess risks in a stand-alone facility. Neither software, however, has the capability to account for the complex interrelationships that exist among business partners while analyzing risks. Thereby, rendering them ineffective for risk analysis of a supply chain.

Clearly, basic research is required to better understand the supply chain vulnerabilities, formalize the risk assessment procedure for a supply chain and to bridge the research gaps to build a robust streamlined next-generation risk analysis and management system. The system has to be extremely reliable and flexible to incorporate any changes in the supply chain configuration. Also, it should enhance operational efficiency and effectiveness while analyzing and mitigating risks.

1.3 Envisioned System

A new decision tool, Supply Chain Risk Analysis and Management System (SCRAMS), is envisioned that will help reduce the risk level in a supply chain. By providing a complete picture of the risk environment, the supply chain manager will be better able to make risk aware decisions. The architecture of the tool is given in Figure 1.1.

The primary objective of supply chain risk analysis and management system is to assess and estimate business risks in a supply chain. The tool will be built upon the existing standards MIL-STD-882D guidelines from the United Stated Department of Defense and driven by a rule-based structure to better understand vulnerabilities and assess risks. The analysis framework will be developed using a Bayesian/Fuzzy Logic structure with rules derived from previous risk assessment reports. The web-enabled architecture will be knowledge based with modules for extracting computer-aided design data, simulating consequences and customizing standard report generators. Supply Chain Risk Analysis and Management System may also interface with SAP enterprise resource planning and management system and potentially with other legacy databases to extract supplier, production and material data relevant for the threat hazard assessment.

Given the product design data in Pro-Engineer format, the system will automatically generate the bill of materials and product structure by extracting the data directly from the Pro-Engineer model. The system will then identify the suppliers and construct the supply chain model by extracting data from the corporate, legacy and ERP databases. From the supply chain model, the system will identify assets and processes, and screen and evaluate them to identify high-priority assets and processes. Then, the system will identify and present to the analyst a list of plausible threats against each asset

using the system knowledge. Once the analyst selects the threats then the system will run a simulation module to determine the consequences. The risk factor with each asset will be estimated to identify high-risk assets. For the identified high-risk assets, an interactive safeguard simulation module will be run to identify the most cost-effective and efficient safeguards. Risk factor will be again estimated with the safeguards in place to check if the new risk level is acceptable or not. If the risk level is acceptable then the system will keep monitoring the supply chain for new threats and vulnerabilities.

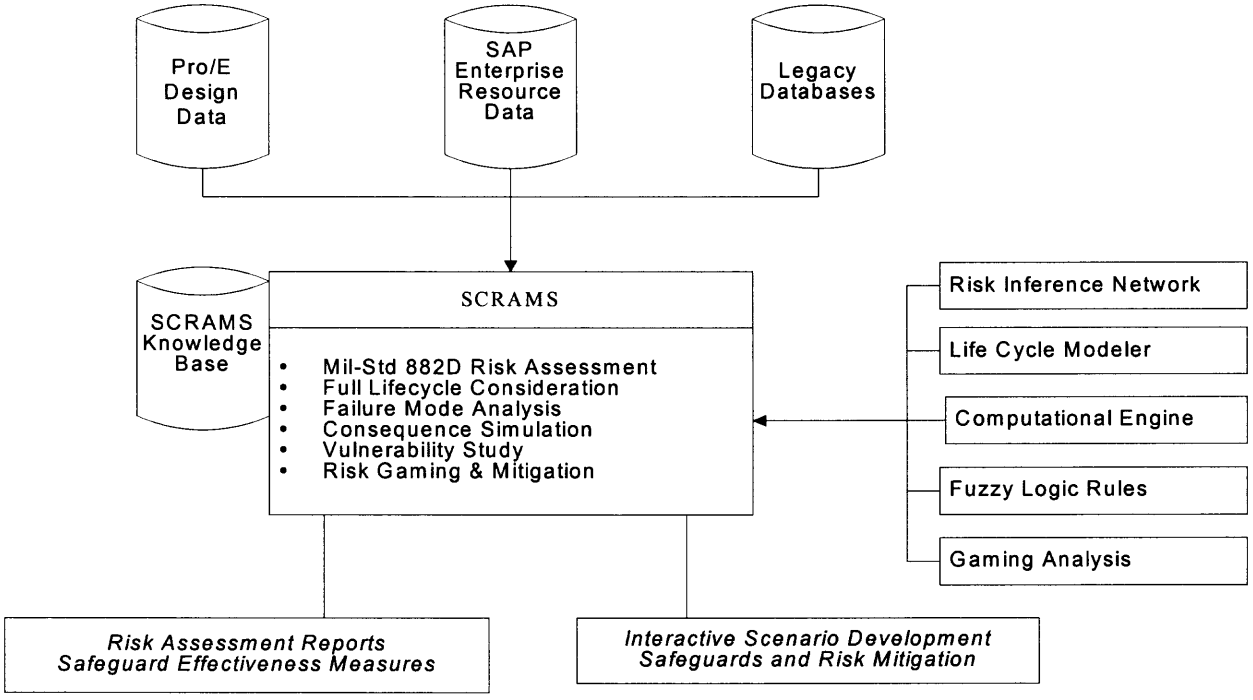

Figure 1.1 Overview of SCRAMS Architecture.

1.4 Thesis Objectives

Development of such a system can be broadly divided into three different phases. They are risk assessment, safeguard analysis and system integration. The first phase estimates the risk factor, second phase identifies safeguards to reduce risk level and finally the system integration phase integrates the modules developed in the first two phases with the ERP system and other legacy databases. This thesis focuses on the first phase and aims at developing and implementing a framework to assess risks in a supply chain.

First, an effort will be made to understand the supply chain elements and their vulnerabilities to develop a risk assessment procedure. The supply chain elements will be identified and modeled to construct a supply chain network model. Each of the network elements will be further studied to understand their core vulnerabilities and to develop a risk assessment procedure. Also, an effort will be made to keep the procedure consistent with the existing risk assessment techniques in related fields. Second, fault trees and Bayesian networks will be explored to model the causal interrelationships that exist among business units. Finally, the framework developed will be implemented as a web-based system that would be able to perform risk analysis of a supply chain. The system will be developed with in the context of a supply chain manager who may not be well versed with the concepts of risk analysis but is adept in supply chain management. The system will guide the entire risk analysis procedure and will be highly interactive. At the end of the risk assessment procedure, the system will identify high-risk assets and alert the supply chain manager to identify and implement safeguards.

1.5 Thesis Format

Chapter 2 of this thesis explores the current state of the technology in risk analysis and disruption management. Bayesian Networks, Fault trees and Fuzzy Logic have been extensively studied to evaluate their usefulness for risk analysis of supply chains. A methodology to assess and evaluate the threats in the supply chain is proposed in Chapter 3. Chapter 4 describes the implementation of this technique as a web application and Chapter 5 presents a case study to evaluate the effectiveness of the system developed. Chapter 6 concludes the thesis and summarizes the results obtained. This final chapter also identifies the opportunities for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Supply chain risk analysis is a relatively new field and the literature directly relating to this subject is limited. However, risk analysis and supply chain management have been researched extensively and significant accomplishments have been achieved. The relevant literature supporting the subject, Supply Chain Risk Analysis, can be broadly divided into four different areas: risk analysis, business continuity planning, logical inference techniques and supply chain management. The literature review indicates that even though supply chain vulnerability has always been the key issue of interest to the industry, little has been done to understand the risks or to mitigate them. This is now changing as the awareness, as well as concern for supply chain security has grown exponentially.

2.2 Risk Analysis and Vulnerability Assessment Process

Risk analysis is the process of identifying threats and system vulnerabilities to analyze consequences and estimate the expected loss. Risk management, on the other hand, is defined as the process of reducing or averting risk associated with the system to an acceptable level by implementing safeguards or by eliminating/avoiding the threat. Risk analysis and management can be broadly classified into three categories – risk assessment, consequence analysis and safeguard implementation [5].

Development of risk analysis techniques primarily began with the fatal flash fire accident while testing the launch test pad of the Apollo AS 240 mission, resulting in the death of three astronauts. This event resulted in a total loss of $410 million and set back the mission by 18 months [6]. Since then, NASA rigorously developed risk assessment techniques to identify plausible causes for mission failure and potential consequences. Even though, development of risk analysis techniques started with the aerospace industry, much of the work has been done by the nuclear industry. Nuclear Regulatory Commission released the Probabilistic Risk Assessment Guide in 1983 and The Fault Tree handbook in 1981 that standardized the risk assessment procedure for the nuclear industry [6]. Risk analysis and safety assessment is of special interest to the United States Department of Defense (DoD). The DoD has to ensure the safety of personnel and munitions. Also, it has to ensure that a safe working environment is provided to employees. This resulted in the development of a series of guidelines for the program managers to assess the risk associated with various processes and operations. These guidelines are also known as Military Standard 882 series, with 882D being the most recent guideline. Several risk assessment techniques have been developed as a result of the extensive research work carried out in a variety of fields.

Some of the techniques are [7]:

- Cause-Consequence Analysis
- Event Tree Analysis
- Failure Modes and Effects Analysis
- Failure Modes, Effects and Criticality Analysis
- Fault Tree Analysis

- Hazard and Operability Analysis
- Preliminary Hazard Analysis
- What-If / Checklist Analysis
- What-If Analysis

Selection of a technique depends on the application or system under consideration. It may not be possible to judge a technique to be better than others, as each serve a specific problem area. However, among all of the techniques, fault tree analysis is of special interest as it starts relating threats to associated causal events and tries to model interrelationships.

2.2.1 Terminology

Risk analysis techniques have been simultaneously in many fields. As a result, the terminology has also been defined uniquely for each field. The following terminology is the most common set of definitions used and will be used in this thesis [9].

Risk - Negative outcome of an activity due to an unwanted or unplanned activity.

Asset – Anything with monetary or operational value that needs to be protected.

Threat – An unwanted event with the potential to cause damage.

Vulnerability –A system weakness that could be exploited.

Expected loss – Anticipated negative impact to assets due to a threat.

Safeguard – Precautionary measures taken to mitigate the risks.

Consequence – The resulting effect of an action or change

Target - Combination of a threat asset pair

2.2.2 Risk Analysis Process

The main objective of risk analysis and management is to reduce the overall loss from a threat by implementing safeguards. Therefore, the cost of implementing and maintaining safeguards should be less than the loss from a threat. In risk analysis, the cost of implementing and maintaining a security measure and the indicated loss from the threat are traded off to retain the cost benefits. However, in some cases the implementation of the countermeasures may be guided by the significance of the asset under consideration rather than costs alone.

Risk management is an ongoing process for maintaining an acceptable security level. Once the level has been established, the system has to be updated on a day-to-day basis and system has to be assessed regularly to check for new vulnerabilities and the status of the security level. Hence, the risk management includes assigning and tracking corrective actions and security levels.

Sandia National Laboratories developed a risk assessment technique that estimates the risk factor using a risk matrix for a given asset/threat pair. The rows and columns in the matrix represent consequences and frequency of occurrence values, respectively and each cell in the matrix gives the corresponding risk value [10, 11].

Sandia's technique has been used by the National Department of Justice in developing a methodology for vulnerability assessment of chemical facilities [10]. The technique begins with the identification and evaluation of the facilities in an organization to select high priority facilities. Activities in the high priority facilities are then identified and evaluated to select 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.

The utility of the risk matrix was evident in the recent symposium organized by Multi-Lifecycle Engineering Research Center on Economic and Business Security held at New Jersey Institute of Technology in July 2003. Howard Forbes, Director of the global security group at Merck, presented a risk assessment technique used by Merck, which is based on Sandia's technique [11]. With the risk assessment technique in place Merck is able to identify some of the high-risk threats and safeguard operations. The risk matrix developed by Sandia provides a good methodology to combine the frequency of occurrence and consequences value to estimate the risk factor. This technique, however, does not consider causal events and interrelationship between entities.

A recent report from the National Academy of Engineering clearly suggests that most of the risk analysis techniques developed date back to NASA's space exploration or Strategic Submarine programs. And, none of these techniques has the capability to fulfill the requirements of a counter terrorism problem. In a counter terrorism problem, threats are dynamic, and adversaries change tactics and targets based on the circumstances. Also, the report advocates that a national strategy is required to protect critical infrastructure elements from terrorist attacks. To protect critical infrastructure elements in various industries like power and aerospace industries, constituting elements of the industry need to be better understood and modeled to understand core vulnerabilities. The report has also called for dedicated research in systems analysis, systems engineering, risk modeling and assessment, and related model development to protect critical infrastructure and better understand system vulnerabilities [12].

Digital Sandbox group has developed a framework for assessing terrorism threats to a military installation. This approach uses Bayesian inference engine to which data is fed dynamically at run time to identify most plausible threats to an installation. The application has been developed for a stand-alone military establishment and does not account for complex interrelationships among installations. The software is discussed in detail in the subsequent sections.

2.2.3 Vulnerability Assessment

Vulnerability assessment is an integral part of analyzing the risk. Vulnerability assessment consists of three stages – threat assessment, target analysis, and prioritizing mitigation recommendations and countermeasures [13]. The threat assessment stage aims at identifying the potential threats, possible threat responses and consequences. Target analysis determines the susceptibility of the asset to the threats based on certain factors like the functionality, value, and importance to society. The last step in vulnerability assessment is to rank the countermeasures based on a cost-benefit analysis. Until recently, vulnerability assessment did not include terrorism risk. However, terrorism is now being considered as an important potential to disruption. Hence, performing a vulnerability assessment would identify more of such reasons.

2.2.3.1 Supply Chain Vulnerability. Supply chain vulnerability has also been defined as an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain [14]. Supply chain vulnerability arises due to a variety of reasons.

Some of the reasons are: [14-16]

1. Global nature of the chain leading to greater vulnerability to risks
2. Complexity of the chain or network of chains leading to lack of visibility and coordination
3. Lean inventories making the system susceptible to minor disruptions
4. Dependence on a single supplier for a particular type of material or service
5. Non standardized products and practices
6. Fraud and abuse
7. Centralization of resources making the system more vulnerable
8. Outsourcing leading to high dependency on the supplier
9. Lack of visibility and control procedures leading to bullwhip effect
10. Volatility in demand leading to unreliable forecasts
11. Highly customized services or products thereby reducing the chances of outsourcing in cases of emergency
12. Friction in supply chain leading to conflicting responsibilities and delegation power
13. Accidents, sabotage and natural disasters
14. Recognition or the attractiveness of assets to adversaries

2.2.3.2 Vulnerability Assessment Process. According to B.D. Jenkins of the Countermeasures, Inc, vulnerability assessment is carried out based on the following axioms [9]:

1. The same population of threats exist for all systems and networks
2. The threats posed to a system are infinite in number and variety.
3. 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.

4. The level of the vulnerability decreases as the safeguards increase. Implementation of safeguards reduce risk in a system, the extent of reduction in risk depends on the safeguard implemented.

5. All safeguards have inherent vulnerabilities.

6. An acceptable level of vulnerability can be achieved through the implementation of countermeasures.

The vulnerability of the target is assessed based on the following factors [17]:

1. Level of visibility - awareness of target presence and visibility of the target

2. Level of criticality -usefulness to population, economy

3. Value of target -value associated with the asset

4. Access to target -ease with which the target can be entered

5. Level of hazard -based on presence and concentration of hazardous material

6. Population density -max no of individuals at given time

7. Potential for collateral damage - based on the number of people residing

Once the vulnerability of a system has been clearly identified, the next step is to weigh various safeguards to mitigate risks. Some of the safeguards are standardization of business processes, having multiple and reliable supplier base, decentralization of resources, and cross training of employees. However, due to businesses constraints, mainly the cost involved, the implementation of safeguards is restricted.

2.2.4 Risk Management Software

The vulnerability to a terrorist attack is of special interest to military and techniques like DSHARP and THREATCON have been developed to evaluate the vulnerability associated with the assets. These methods, however, are not very effective [18]. Department of Defense (DoD) in collaboration with Digital Sandbox developed a new

tool Site Profiler to assess vulnerability of its establishments. However, the Site profiler mainly deals with terrorist threats and other security issues associated with an asset. The Combating Terrorism Technology Support Office is using the Site Profiler for the Joint Vulnerability Assessment Tool Program, which will be 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 Site Profiler to track passenger and cargo to detect possible threats [18-19].

The Buddy System, which is developed by Counter-Measures Incorporation, Hollywood also works on similar lines. The software is designed to evaluate vulnerability of assets to threat not only from terrorism, but also those from other accidents like fire as well. Raytheon Corporation is using the Buddy System in support of work related to Presidential Decision Directive 63 for the National Communications System and the Joint Program Office-Special Technologies Countermeasures. Major organizations like Novartis, NASA and Dryden also use this software [20]. Both the Site Profiler and the Buddy System can evaluate the threats to physical assets only. The industry on the other hand is seeking a tool that will address the risk issues associated with physical and operational security.

The Cobre Group has developed software, Helpmate, to develop knowledge bases by identifying and characterizing operations in an organization. The developed knowledge bases then aid in decision-making by providing the required process information. But, it cannot neither predict the risk factor nor recommend safeguards for

risk mitigation. E Team, Inc. 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. E-Team provides a common enterprise level platform which helps coordinate and communicate between managers to help recover from a disaster. This software like Helpmate does not estimate risk.

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 countermeasures and show the relative effect of their implementation. The system by itself does not seem to suggest any countermeasure but the simulations represented graphically can be interpreted better [21].

Palisade's @RISK is a financial risk analysis and Monte Carlo simulation add-in for Microsoft Excel. @RISK seamlessly integrates with the excel spreadsheet, adding risk analysis to the existing models. @RISK uses probability distribution functions to define uncertainties and calculates all possible outcomes in a situation and their probabilities of occurrence. The output of @Risk is a probability distribution function. @Risk requires probability distributions to define the behavior of uncertain parameters in a system like demand fluctuations, seasonal variations. For rare events, the data required to estimate the frequency of occurrence value or to assign an uncertainty distribution

might not be available. Even though, @Risk is powerful tool for financial risk analysis, the application of this tool is restricted for a supply chain.

Risk analysis software currently available in the market serve specific problem areas and do not have the capability to assess risks in a supply chain. For example, Site Profiler and @ Risk specifically address the issue of physical security and financial risk respectively and cannot assess risks interchangeably. But, in a supply all aspects of risk are important and they have to be assessed simultaneously. Apart from security and financial risk, operational risk is also important in a supply chain. None of the risk analysis software identify operations carried out in an organization to assess the risk of a disruption. Also, the software do not identity causal events and model interrelationships. Fault tree analysis is a well-known technique to model causal interrelationships. Fault tree capability is required for a supply chain risk analysis tool as the interrelations among the business need to be strongly accounted. The flowing two sections describe two of the most relevant software to assess risks in a supply chain.

2.2.4 .1 Buddy System [9]. The Buddy System, a product from "Counter-measures, incorporation", was launched way back in 1987. The software was developed based on the experiences of US Department of Defense. Later on, the product was extended to meet the requirements of industry. The product identifies and deals with the risk associated in a system. The package uses quantitative and qualitative analysis methodologies to assess the system vulnerability. The system after determining the current level of vulnerability suggests countermeasures to mitigate the risks associated in the system. The software works on the assumption that implementing countermeasures will reduce vulnerability.

The package uses visual fox-pro as a relational database and employs an intelligent data collection module. The software presents the vulnerability of the system graphically, to give a clear picture of the vulnerability associated with the system. At the end of the analysis, the software generates a detailed report of system vulnerabilities and the safeguards to be implemented to mitigate the risks. Finally, a report is generated using Microsoft word.

The software collects data through survey questionnaires and has the capability to store unlimited number of datasets and surveys. The software has three modules: configuration module, survey module and analysis module. Configuration module customizes the dataset. Data collection module collects the data required to do the analysis. The data can be collected through web-based surveys, local area networks, personal interviews etc. Analysis module evaluates the vulnerability of the system against each of the threat considered in the system. After the evaluation of vulnerability of each asset, the module recommends safeguards to mitigate the risk. The software can be linked to MS project and uses Excel graphics to present the output. The software has been extensively used in all kinds of industry, from health services to consulting firms.

The website, however does not mention the threats considered in the package. Most probably the software can be applied only to stationary units, like buildings. The software does not consider the interrelationship between different units in a supply chain, which means that it does not analyze the vulnerability of a unit in relation to another.

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

1. Comprehensive survey to generate or update a 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. Recommends safeguards
10. Generates formal Project level risk analysis report

The utility of buddy system in analyzing supply chain risks is very limited. As, the software does not neither consider interrelationships among business units nor supply chain questions while analyzing risks. Moreover, since the technique derives most of the information from a questionnaire, it may not be the most appropriate approach to analyze risks in a supply chain.

2.2.4.2 Site Profiler [18]. The Site profiler is developed based on a generic application development environment that dynamically feds Bayesian inference engine with data at the run time. This model combines evidence from analytic models, simulations, historical data and user judgments to estimate the risk factor.

The Joint Vulnerability Assessment Tool program uses the Site profiler for anti-terrorism risk assessment and planning. Site profiler uses an architecture that can feed

network nodes with data from disparate sources. The disparate sources include the planner's own subjective and objective assessments, historical database information, analytical model results and simulation results that are integrated into various nodes on the Bayesian Network. The fragments in the risk influence Bayesian Network are designed to match the user's knowledge of domain concept, ensuring a scalable modular and maintainable model.

The specific aims for designing the model are listed as follows

- Modeling the capabilities and intent of terrorist organizations
- Determine the plausibility of various types of weapon systems and tactics that could be employed against the installation
- Assess the target value of the installation and its assets in the eyes of the terrorists
- Calculate the susceptibility of each of those assets to attack by a given weapon system
- Model the consequences of an attack in lives, property damage and mission effect, should it occur

The model requires a characterization of assets of an installation and threats to be considered as an input to generate the Risk influence Network (RIN) for each asset/threat pair. Relational information is also required for the generation of the threat/asset pairs and the manual entry of the relational aspects of this being infeasible, the relational aspects are calculated using Bayesian Networks based on complete characterization of the assets and threats. The Site Profiler uses seven objects to create the RIN [19] –

1. Installation
2. Asset
3. Threat
4. Weapon system

5. Terrorist organization
6. Target
7. Attack

The system constructs a RIN for each threat/asset pair and runs software simulation and database queries, applies evidence and computes risks, which are presented back to the user. The RIN contains the information regarding the installation, the asset, the threat, the asset threat target pairing and the attack event. Nodes in the Bayesian network define the risk elements, which in turn combine to contribute towards the definition of risk associated with a target – likelihood of event, susceptibility of an asset to the event, consequences of the event and the risk of the event.

The system model is constructed in a 3D environment. User interface screens are created dynamically by inspecting the asset and entering the user set attributes. The building is algorithmically constructed by reading its height material type etc. Blast models then calculate the risk and structural response.

The assessments allow the prioritization and the assessment of an installation's vulnerabilities. To model the RIN (Risk Influence Network), two factors – recognizability and accessibility are defined. Recognizability is queried from the user, but accessibility is obtained from various factors such as weapon delivery systems, terrain, road networks, physical security and many other factors. Just like the previous application, threat vectors are used to define accessibility for each threat/asset pair.

Risk management requires the testing of safeguards for effectiveness and efficiency. Site Profiler uses AT (Anti-terrorism) functions are used for this purpose. AT functions are composed of safeguards, procedures, and organizations. These AT

functions are applied to risks by characterizing procedures and safeguard effectiveness against potential attacks. The effectiveness model considers a set of parameters for each AT function – delay, denial, deterrence, detection, mitigation, interdiction, response and cost. The model has the ability to create AT functions that addresses the risk that are critical and select the best AT function based on their effectiveness, availability and cost [19].

The core components of the software architecture are listed below:

- User interface that can customize itself to the particulars of each installation
- Database of historical and current data regarding terrorists and weapons
- Modeling environment to describe the assets, installation and infrastructure under consideration
- Simulation engine to interpret models and simulate threats against it
- Plug-in interface to incorporate external models
- Automatic document generator to prepare DoD standardized reports

All the consequence models of the software are implemented as plug-ins. This allows the model to be to be registered with the system as they are developed, ensuring availability of current and highest quality data without requiring a code change. Every piece of data in the RIN is stored as a node, which is then used to calculate Belief through probabilistic inference. This belief is interpreted as the probability of a certain event occurring, based on all the data.

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 to 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

Site Profiler is the most advanced risk analysis software to date. However, the software has been developed for military sites. The threats against a military facility and supply chain entities are totally different. Site Profiler, even though brings in strong engineering and system analysis concepts, does not have the capability to analyze risks considering independencies.

2.5 Business Continuity Management

Recent events exposed the vulnerability of supply chains and demonstrated that the business continuity and disaster recovery plans in place were inadequate. Business continuity management, also known as business continuity planning and contingency planning, was never given due importance due to economic reasons and firms belief that government is fully responsible for disaster response and recovery.

Business continuity management has become vital to the survival of a business, as firms operate with JIT production and maintain lean inventories. Furthermore, globalization of supply chains has made the chain susceptible to cross border disruptions.

As the chains are becoming increasingly complex and interdependent, any minor disruption in any part of the chain can have crippling effect along the entire supply chain. Moreover, with the advancement in technology, the lead-time has been reduced significantly. Due to the reduced lead-time, the time available to recover from the disruption without affecting business is significantly less than before [22].

Based on the survey conducted by the Council of Logistics Management, the following figures were presented [23-24]:

- 58% of the organizations were affected by the events of September 11th.
- 12 % were severely affected.
- Firms with large inventory turnovers were more affected.
- Only about 61% of US firms have disaster recovery plans.
- Most of the plans cover data centers and the estimate is that only 12% cover total organization recovery.
- Specific plans to sustain supply chain operations are given limited coverage in most business continuity plans.
- Approximately 72% of executives do not have crisis management or equivalent teams; even fewer have supply chain representation.
- Crisis response training is only active in approximately 27% of firms.
- Approximately 57% of managers are not satisfied with their company's crisis response capabilities.
- Estimates indicate that 43% of businesses that suffer a major fire (or other major damage) never reopen for business after the event.

Apart from the reasons listed above, having a good business continuity plan in place would improve confidence among business partners and improve the firm's credibility in the market. To continue business and flourish in an uncertain and global environment, it is necessary to have an effective and tested business continuity management plan in

place. Business continuity management anticipates a disaster and recommends mitigation plan to recover from the disaster while trying to reduce recovery time and loss. This plan is sketched out based on what-if scenarios. Historically, firms were dependent on the insurance to safeguard their interests against unwarranted incidents. Using historical data, assessments were made regarding the occurrence of an incident. This data is used to evaluate the insurance premium. This process safeguarded the firm against financial and capital loss. However, this did not cover intangibles losses, including lost customer base or lost reputation.

Moreover, disaster recovery and emergency planning was initiated after the occurrence of an unwanted event. Often, managers avoided processes/practices that added risk to their business. Procuring a component, for example, from an offshore supplier may be more risky than procuring it from a local supplier as the possibility of a disruption or delay in shipment arrival is extremely high. If the manager decides against the offshore supplier without analyzing the full implications then he is jeopardizing significant amount of business.

As the markets and business environment has changed and markets have become uncertain, policies which worked fine in the past no longer hold. The events of September 11 resulted in the removal of all forms of terrorist acts from the regular insurance coverage and a separate terrorism insurance coverage has to be bought at an exorbitant price [25]. Also, in the event of a disaster, the firm has to stand up to the requirements and expectations of different groups.

They are

- Customers and shareholder's expect the management to be fully operational.

- Employees expect their livelihoods to be protected
- Suppliers expect revenues to continue.
- Law enforcement bodies expect the firm to adhere to the law irrespective of the consequences
- Insurance companies expect due care to be exercised.

With effectiveness being the most crucial factor in implementing a recovery plan it may not always be possible to develop an optimal recovery plan with so many constrains after the disaster occurs. Though the firms have effective disaster recovery plans if something goes wrong within their firm like a fire in the factory, but they don't have a plan to recover from an event that happens in their supply chain. With the recent extraordinary events- i.e. events with low probability and high consequences, it is imperative that firms should have an effective business continuity plan in place. Business continuity planning should be driven by both the probability of occurrence and the consequences of an event. Usually risk mitigation plans consider events with high occurrence and events with low probability were left out. But with threats emerging up which have a low probability and high consequences both factors have to considered to design an effective business continuity plan.

Business continuity management can be divided into two distinct areas. They are disaster recovery and emergency planning. A disaster is defined as an unexpected occurrence causing a widespread and long-term damage to the firm's business. An emergency is defined as a situation, which develops in a short period of time and calls for immediate action. Most the time, business continuity and disaster recovery plans are inclined towards information security and data retrieval. This is due to the fact any loss in data may be fatal to the company.

Business Continuity and Supply Chain Management firms conducted a survey to find the most significant threats perceived by the industry. Loss in IT capital tops the list, followed by loss in skill and damage in corporate image. The survey indicates that even though, loss in it capacity in the most significant risk but at the same the industry is facing risks from other threats too, which cannot be neglected [26].

Business continuity management is based on business impact analysis. Business impact analysis is a systematic approach to assess the business damage due to a threat [27]. Planners identify various possible worst-case scenarios and conduct impact analysis. Business impact analysis is analogues to risk analysis. While business impact analysis is based on the worst-case scenario, risk analysis is based on the various threats identified against the system. In business impact analysis, critical assets and processes are identified and evaluated for possible responses due of a threat. Based on the impact analysis, risk mitigation and recover plans are designed. Nicole Ross argues that the worst-case scenario should be acceptable for the firms business. For example, Virtual Corporation, a New Jersey based business continuity planning firm, while analyzing the business continuity plans of a large brokerage firm in New York assumed that its worst-case scenario would single building in Wall Street. In such an event they planned to shift their business temporarily to the other building in Wall Street [28]. In wake of the terrorist attacks, the whole of lower Manhattan was closed, disrupting their business and rendering their plan to be useless. However, planning for extraordinary incidents may not be possible for all firms especially mid-sized and small firms. McCarthy argues that, if a firm plans and puts the Enterprise Risk Management model in place, a framework can be created to handle any scenario [27, 29]. The Committee of Sponsoring Organizations of

the Treadway defines, Enterprise risk management as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives [30].

A business continuity plan should be incorporated into the firms business like the way in which total quality management has been incorporated. Firms strive to provide high quality products and services, and quality improvement and management is an important corporate goal. Quality management is a basic necessity rather than a requirement. Likewise, business continuity management should also become a part of corporate policy and should not be performed as requirement. Management involvement and their interest to implement a business continuity plan are key factors that decide the success of a plan. Also, the success of a plan depends on the effectiveness with which it can be implemented and its ability to recover from a disaster. Effective implementation requires exercise of the plan, requiring the involvement of all employees in the firm. The employees in the firm should be aware of the plan and know their part of duty and responsibility. Business continuity planning is a continuum, where the plan is revised periodically. In the past, business continuity plans were event driven and were evaluated and revised after the occurrence of an incident. However, with the emergence of new threats it has been realized to evaluate the plan periodically irrespective of the occurrence of the incidents. A business continuity plan varies from industry to industry depending on its type and infrastructure. A generic continuity plan can be divided to five basic steps.

They are business impact and risk analysis, strategy development, response scenarios, awareness and training, and exercise and maintenance.

John Sharp, former Chief Executive Officer of The Business Continuity Institute, proposed a model for business continuity planning or business continuity management, which is based on ten certification standards of the Business Continuity institute [26]. The model performs a business impact analysis, through which the most vulnerable areas are identified. In this method, loss in customer base or confidence is the highest weighed risk. First, the critical vulnerabilities and threats in the firm are identified and then a risk analysis is done to quantify the risk. The result of the risk analysis is used to prioritize the business functions. Once the key risks are identified, mitigation strategies are recommended which can successfully recover the business from a disaster. The drafted plan is then disseminated among the employees.

The next stage is to exercise and test the plan. The plan is rigorously practiced and tested so that the firm and its employees are ready for any eventuality. With proper training chaos can be avoided, thereby enabling the firm to maintain customer and shareholder's confidence, which are of utmost importance. Moreover, employees are the key assets to any firm; protecting employees and retaining their emotional stability are important for a quick recovery from the disaster. Proper training and exercise of the plan could reduce workforce loss and help the firm to continue business in an uncertain environment.

Often, business continuity planning is done at organizational level and does not include scenarios wherein business would be affected due to problems with partnering firms. For example, business continuity planning does consider that data loss is a major

threat. But, continuity planning does consider the scenario where the sole source supplier is out of business or decides not to supply. Business continuity planning like supply chain management should be a collaborative effort by all firms in a supply chain. Also, it may not be possible for a firm to design continuity plans for a partnering firm. Cooperation and information sharing among the supply partners is a critical issue, which will decide the implementation of the business continuity plan along the supply chain.

Until recently, there were no standards or metrics to measure the effectiveness of a continuity plan. But, it is extremely important to measure the effectiveness of a business continuity plan and compare it the plans of competing organizations to have an upper hand in the market. Also, a methodology to measure the effectiveness of a plan will enable firm's to judge their responsiveness to an emergency.

In January 2002, Scott Ream, President of Virtual Corporation, introduced the concept of Business Continuity Maturity Model [31]. The model, based on certain parameters like management leadership and business continuity awareness, evaluates the effectiveness of a business continuity plan and assigns an efficiency level.

For each parameter, a numeric value is assigned to determine the overall effectiveness of the plan [32]. The model estimates the effectiveness of a business continuity planning at organizational level of the enterprise. The model is still in the development being developed in collaboration with the industry. At this stage, the model does not evidently address supply chain security issues. Hopefully, the model on completion will have the capability to address business continuity issues from supply chain perspective.

Business continuity management has been concerned with post-disaster recovery. The evolving philosophy, however, is to avoid or avert the disruptive event to eliminate or minimize consequences. Studying the causal events contributing to the disruptive event is necessary to avoid the threat, in addition to studying the possible consequences of the threat. Business continuity management should not be remediation effort but should try to eliminate the risk source.

2.4 Logical Inference Techniques to Solve Uncertainty Problems

To analyze any risk environment, it is vital to know the paths of threat propagation and the probability associated with each. Damage can be caused by various events and often an event of disruption triggers a set of events as in a chain reaction. Therefore, a complete causal tree structure and an inference engine are required to determine the most probable path and the relative probabilities of occurrence for any chain of events. Bayesian networks and fuzzy logic are most popular and frequently used inference tools.

2.4.1 Bayesian Networks

These are also called Belief Networks or Probabilistic Inference Networks. The idea of Bayesian networks was initially developed by Pearl in 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. The theorem gives a methodology to combine subjective beliefs and the evidence available. 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 can be done automatically. This gave a new dimension to development and understanding of Bayesian networks [33-34].

Initially a brute force algorithm was used to solve an inference problem. As this technique was not adequate, rule-based methods were developed in the late 70's and 80's. This method was based on if-then propositions but the method took a long time to put the information together as the system needs all the questions to be answered clearly to give correct results.

To increase the efficiency of the systems, neural networks were developed. These networks were able to handle a huge amount of data and figure out patterns in the data. Though neural nets seemed promising they had a shortcoming, the system was not capable of handling uncertain information. Neural networks infer based on the previous experiences and the set of possible events and their corresponding outcomes has to be assigned. With neural networks it is not possible to train a system, as enough historical data would not be available to make a decision. This shortcoming leads to the search for a tool, which could decide when enough data is not available. Due to the shortcoming in AI techniques, firms in this field were almost on the verge of bankruptcy.

In the late 80's, AI researchers discovered that Bayesian networks could be used to handle uncertain information. Horvitz and his two colleagues in Microsoft started developing a network, which could diagnose the condition of patients without turning to surgery. According to Horvitz, this method was effective and efficient as it was capable of combining historical data and imprecise subjective beliefs of the experts in the field.

Horvitz with his two colleagues helped Microsoft develop and apply Bayesian networks to real world cases. With their help, Microsoft developed the system the help system in word. The help system pops up the help menu based on the movement of mouse. If the movement of the mouse is wayward, then network infers that the user is looking for something and based on the mouse movement the network pops up the help menu with possible alternatives, which the user might be looking for.

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.

Microsoft is working on techniques that will enable the Bayesian networks to "learn" or update themselves automatically based on new knowledge, a task that is currently cumbersome. Microsoft is unquestionably the most aggressive firm in exploiting the new approach. The company offers a free Web service that helps customers diagnose printing problems with their computers and recommends the quickest way to resolve them. Another Web service helps parents diagnose their children's health problems.

Bayesian Networks or Bayesian Nets work on the principle of Bayes' Theorem.

Bayes' Theorem states that:

$$P(H_I \mid E) = \frac{P(E \mid H_I)P(H_I)}{\sum_{k=1}^{n} P(E \mid H_K)P(H_K)}$$

The above equation gives the probability that the "*hypothesis is true given evidence E is equal to the ratio of the probability that E will be true given times the a*

priori evidence on the probability of and the sum of the probability of E over the set of all hypotheses times the probability of these hypotheses" [35]. The throerm requires that the set of all hypotheses must be mutually exclusive and exhaustive.

Intailly, Bayes' Rule was not used in Artificial Intellgence because it requires full joint probability distribution and the networks are extremely complex to solve. But in recent years, due to exponentail increse in computational power, Bayesian techniques have been of tremendous interest because of its capability of handling uncertain information.

Heckerman, a researcher at Microsoft, defines a Bayesian network as an annotated directed acyclic graph that encodes probabilistic relationships amoung distictions of interest in an uncertain reasoning problem. According to him, the representation rigourousy models these interrelationships and is intuitive [36]. Also, Bayesian updating provides a means of propagating beliefs along the network. Bayesian networks are a rich and powerful way of building probabilistic models. Bayesian networks are represented as a graph where the links indicate dependencies that exist between nodes. The nodes represent probabilities about events or events themselves and the Conditional probabilities quantify the strength of dependencies.

According to Peter Haddawy, " The success of Bayesian networks lies largely in the fact that the formalism introduces structure into probabilistic modeling and cleanly separates the qualitative structure of a model from the quantitative aspect." [37]. Bayesain Networks have been successfully applied in a variety of subjects like medical diagnosis, intelligent user interfaces , and threat assessment of a site.

2.4.1.1 Advantages of Bayesian Networks[38-44] :

1. Forward and backward reasoning
2. Conditional interdependance allows efficient updating and the probabilities can be changed in wake of new evidence
3. Matches the real world where probability of one event is Conditional on the probability of previous one
4. Data can be dynamicaly combined with the network at the run time thereby enabling continious monitoring
5. Elaborate research has been Conducted in this field to tap the full potential of Bayesian networks
6. Can be used on real large scale problems
7. Can combine diverse data including subjective beliefs and empirical data

2.4.1.2 Disadvantages of Bayesian Networks[43,45,38] :

1. The events represented by each node has to be mutually exhaustive
2. The number of conditional probabilities varies exponentially over the number of nodes
3. Bayesian Networks do not account for the vagueness in a system
4. Exclude the possibility of an event that is neither completely true nor completely false
5. Updating new information is difficult and time consuming
6. Exceptions like “none of the above" cannot be represented

2.4.2 Fuzzy Logic

Fuzzy logic is a superset of conventional Boolean logic with capability to account for imprecise information. Fuzzy logic permits usage of vague information, knowledge and concepts in an exact mathematical manner. Words and phrases such as fast, slow, and very fast are used to describe continuous, overlapping states. This enables qualitative and

imprecise reasoning statements to be incorporated within rule-bases to develop simple, 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. The membership values range from 0 to 1. This contrasts with conventional Boolean logic, where information can either be true or false. This graduation from zero to one smoothes out the transition 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 whereas in a crisp system, only one rule might be fired and used, 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.

A system that runs on Fuzzy control incorporates Fuzzy variables like speed, temperature and Fuzzy qualifiers like 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 like very, extremely and not very, often referred to linguistic hedges. These affect the membership function by intensifying or spreading 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.

In Fuzzy reasoning over sets, there are standard operations such as union and intersection. These operations can be defined in terms of simple mathematical operations such as maximum, minimum, and addition. The final stage of a Fuzzy evaluation is the

conversion back from Fuzzy membership values to crisp values for the output variables that is referred to as defuzzification. The two standard defuzzifiers are the centroid method, which is based on the center of gravity, and the peak method, which is based on the highest Fuzzy value.

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. Once the rules and membership functions are defined, the input variables have to compute values for output variables. This process is called the inference process, which is in turn a combination of four sub-processes – fuzzification, inference, composition and defuzzification [46].

The fuzzification sub process, the membership functions are applied to their actual values to determine the degree of truth for each rule premise. In the inference sub process, these truth-values are computed and applied to the conclusion part of each rule. In the composition sub process, all the Fuzzy subsets to output variables are combined to form a single Fuzzy subset for each output variable. The subsets are then converted to values, which are further converted to a single number, or a crisp value by the defuzzification process [46].

2.4.2.1 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. Flight aid for helicopters

5. Temperature control
6. Traffic Control

2.4.2.2 Advantages of Fuzzy Systems

1. Accounts for the ambiguity or uncertainty in describing an event [38]
2. Represents better interpolation between topologically related states for variables [38]
3. Represents uncertainty of categorization [38]
4. Provides rules for the truth value of complex statements
5. Easy system construction and implementation [47]
6. Allows formalization of vague data [48]

The other advantages of Fuzzy logic expert systems compared to non-Fuzzy expert systems are that they typically require fewer rules, need fewer variables, use a linguistic rather than a numerical description, and can relate output to input for any device without needing to understand the device's inner workings.

2.4.2.3 Disadvantages 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 [38].
2. Basic functions like min and max, which are the core components in Fuzzy logic are not supported by evidence, but are assumptions [38].
3. Backward reasoning is not possible
4. Membership values do not change in the wake of new evidence [49].

To overcome the disadvantages of the Bayesian and Fuzzy based systems, hybrid networks are now being studied. The hybrid networks can be Hybrid Probabilistic Models or Hybrid Fuzzy logic systems. These try to incorporate the advantages of both systems and minimize their disadvantages.

2.4.3 Fuzzy Belief Networks

Hybrid Fuzzy Bayesian network or Fuzzy Belief Network is a blend of Bayesian network and Fuzzy logic techniques. Heping Pan and Daniel McMichael proposed a methodology that takes advantage from both of the popular concepts to overcome the disadvantages associated with each methodology [38]. This method incorporates a non-Bayesian probability index (degree of truth rather than degree of belief) and provides a structure to propagate this index along the network. This method is also capable of combining evidence to determine the belief in a node. This method adopts three basic steps while making an inference – fuzzification, inference and defuzzification. In the first step, crisp or continuous variables are converted into Fuzzy variables using a fuzzifier function. This step maps each of the crisp variables to a set of discrete Fuzzy states.

In the second step, the variables are plugged into a Bayesian network to form a Fuzzy causal network. Each node in the network represents a Fuzzy variable and the links represent the interrelationships among the variables. To deduct an inference from the network, traditional Bayesian algorithms are used to solve the network. If required the discrete Fuzzy variables can be converted back into crisp variables using defuzzification module.

Neural networks could be integrated with Fuzzy expert systems to tune the shapes of Fuzzy membership functions of the different design variables, which will improve the reasoning and confidence performance of the entire system.

2.4.3.1 Applications

- Medical diagnostic systems
- Modeling of brain

- Data mining
- Speech recognition
- Image modelling
- Space exploration
- Intel processor fault diagnosis

2.4.3.2 Advantages

1. The number of conditional probabilities to be assigned reduces drastically
2. Account for uncertainity as well as vagueness in describing as event
3. Forward as well as backard reasoning [38]
4. Computationally simple [38]
5. Fewer constraints
6. Linear time complexity [38]

Fuzzy Belief Networks certainly look promising for solving uncertainty related models, but detailed study is yet to be done to analyze the possible drawbacks.

2.4.4 Hybrid Bayesian Networks

Hybrid Bayesian Networks provide a mode of improvement over Bayesian Networks. In the traditional Bayesian Networks, the nodes can either be discrete or continuous variables, but cannot incorporate both in the same network. However, real world scenarios can be represented only by a combination of continuous as well as discrete variables. Hybrid Bayesians incorporate this feature enabling a better representation of the real world.

The most popular class of hybrid models are known as the Conditional Linear Gaussians (CLGs). This class of hybrid Networks does not allow non-linear relations

between continuous variables and does not allow discrete nodes to have continuous parents. The main advantage of this type of network is the mathematical convenience. Given any assignment of the discrete variables, the distribution over continuous variables is a multivariate gaussian. Thus, the joint probability distribution is a mixture of gaussians, which can be handled using analytical tools.

However, CLGs have linearity restrictions and approximate inference in CLGs is NP hard. However, there are heuristics that have been developed for solving these classes of networks. The state of the art algorithm for exact inference in CLGs is Lauritzen's algorithm, which is based on the clique tree algorithm, originally developed to solve discrete Bayesian networks. Nevertheless, in many cases, Lauritzen's algorithm is intractable even for simple network structures. Moreover, the CLGs suffer the drawback of the inability to incorporate continuous parents for discrete nodes, which is more or less the case in the real world. Uri Lerner, a PhD student at Stanford University researchers has developed an algorithm for augmented CLGs, which can incorporate discrete nodes as the children of continuous parents [50]. Another class of Hybrid Bayesian Networks is the Dynamic Hybrid Bayesian Networks (DBNs), which can efficiently model stochastic processes. CLGs with linearity restrictions can be solved using Switching Linear Dynamic Systems [51].

2.4.5 Bayesian Network Vs. Fuzzy Systems

All the techniques discussed above are tools to handle uncertainty and derive a relationship between the events that can lead to uncertainty. Solving the Bayesian network has been proved to be NP hard. Probabilistic approaches make an inference based on a population of events (e.g. probability of a student getting an "A" grade given

the number the number of students and no of students getting an "A" grade), while fuzzy systems pertain to a particular event in consideration (the possibility of a student getting an "A" grade, based on his performance). Fuzzy systems are more useful are practical when conditional probabilities are not available. The Fuzzy expert system generates an inference by different combinations of Fuzzy rules. There is no method to find out the optimal combination of rules, which can give the best possible outcome. Hence, all the techniques are approximate reasoning techniques and have their relative advantages and disadvantages.

Fuzzy set theory and Fuzzy logic deal with imprecision inherent in human thinking, while probability theory is concerned with the uncertainty involved in decision-making [43]. The Bayesian theory deals with only two states for a variable – true or false. The intermediate cases are not considered. The Fuzzy systems account for the intermediate cases as well. Bayesian systems generate conditional probability tables and the number of conditional inter-relationships is exponentially related to the number of discrete variables. The use of Fuzzy systems can substantially reduce the size of this data set and may improve the stability and smoothness of system performance [43]. Fuzzy sets use "linguistic variables" like tall, medium and low instead of numerical variables. This can be of advantage while trying to make inferences from the network. Also, adjectives and adverbs like more than and less than are used to modify the membership curves mathematically.

While Fuzzy systems account for both uncertainty and vagueness, Bayesian networks account only for uncertainty. But when Fuzzy variables are involved in

complicated Fuzzy relations including functions and implications, things begin to become indeterministic. In contrast, the Baye's theory enables forward and backward inference. Fuzzy systems are better when the whole network can be represented in terms on qualitative expressions and quantitative representations are absent in the network. But, if the result has to be represented in terms of probabilities or confidence intervals then probabilistic approaches are more convenient to use. While designing a stand-alone system, a system that has to work on its own without inputs from the user or expert, fuzzy approach has an advantage over probabilistic approach [52].

According to Kathryn Laskey, in most cases Bayesian systems can out-perform Fuzzy systems when computational tractability, accuracy and usability are taken into consideration. But there may be cases when Fuzzy systems can be on the top. When one of her students made an empirical analysis to compare the two methods for a ship autopilot, the Fuzzy rules did better than the Bayesian system. Kathryn says " I am hypothesizing that the utility, averaged across exchangeable problem instances, of the Fuzzy system output is higher than the utility, averaged across exchangeable problem instances, of the Bayesian system output, if that is the case, then go with Fuzzy system."

According to Keith M. Reynolds, "Bayesian belief networks may be preferable to Fuzzy logic networks when conditional probabilities of outcomes are known. However, Bayesian belief networks, like production rule systems, are difficult to apply to large, general problems because the number of conditional probabilities that must be specified can quickly become extremely large as the conceptual scope of a problem increases. In such situations, model design not only becomes difficult to manage but many probabilities will not be well characterized and will therefore need to be supplied by

expert judgment, thus negating much of the value to be gained by a more statistically based approach to knowledge representation. [53]. According to Meyer, fuzzy logic is an appropriate tool when the way in which experts identify measure or forecast the phenomena is likely to change over time and fuzzy systems add more flexibility and robustness to the system.

To overcome the disadvantages of the Bayesian and Fuzzy based systems, hybrid networks are now being studied. The hybrid networks can be Hybrid Probabilistic Models or Hybrid Fuzzy logic systems. These try to incorporate the advantages of both systems and minimize their disadvantages.

2.5 Synopsis

Recent events had a very adverse impact on the US economy. Many industries could not sustain themselves as the economy crumpled and had to declare bankruptcy. The unexpected disruptions in the supply chain leading to heavy financial losses aroused a necessity to address the issue of vulnerability assessment and risk mitigation. American economy is not in a position to endure another serious disruption and supply chains clearly need to be secured.

The current state of the technology is not capable of addressing the issue of supply chain risk analysis, as a supply chain is a highly interdependent system. Advances in system modeling and analysis are required to model infrastructure elements for studying and analyzing core system vulnerabilities. Also, supply chains need to be further studied to understand the complex interrelationships that drive supply chain performance.

Currently, none of the logical inference techniques can be judged as the most appropriate technique for risk analysis of supply chains. Each technique has specific advantages and disadvantages. It may not be possible to select a technique unless the critical parameters influencing supply chain parameters are identified and studied.

Also, none of the software available in the market addresses the issue of supply chain risk analysis and management. Companies like the E-Team and Strohl Systems serve the area of disaster recovery and management. Moreover, business continuity planning has not yet included pre-disaster planning to avoid the risk. Software systems like the Site Profiler and the Buddy System deal with physical asset security, but does neither address inter-relationships between assets nor the operational risks within the supply chain. Researchers at the Los Alamos National Laboratories have developed simulation tools to analyze certain specific area, but the system does not incorporate more than one activity at a time nor the inter relationships between activities. Moreover, these simulations need exceptional computational power and significant resources that the commercial industry cannot afford. There are many more software's that perform a financial risk assessment like the Palisade groups @Risk, but all of them are very specific in their application.

CHAPTER 3

METHODOLOGY

3.1 Risk Analysis

Risk analysis and management is becoming an increasingly popular technique to support decision making under uncertainty. This procedure identifies and estimates the expected damage due to uncertainties in a system and recommends safeguards to mitigate or avert risk. Risk is defined as a negative outcome of an activity due to an unwanted or unplanned activity [54]. Risk analysis estimates the risk factor based on two parameters: the frequency of occurrence and severity of consequences. Frequency of occurrence is the likelihood of the threat occurring. And, severity of consequences is the loss or disutility due to the adverse outcome. Risk is calculated in many ways. In this thesis, risk will be calculated as the product of frequency of occurrence and severity of consequences.

Risk = Frequency of Occurrence * Severity of Consequences

The above equation is the most standard expression used to calculate the risk factor. Risk analysis tries to capture and quantify the uncertainties in a system. It may not be possible to determine when exactly an event will occur but the probability with which it occurs can be estimated. For example, it may not be possible to predict when a machine will fail but its failure rate can be estimated.

Even though risk in a system is calculated based on two parameters, it depends on four distinct different parameters. They are frequency of occurrence, severity of consequences, system vulnerabilities and the effectiveness of the safeguards. Figure 3.1 gives a pictorial representation of the factors contributing to risk.

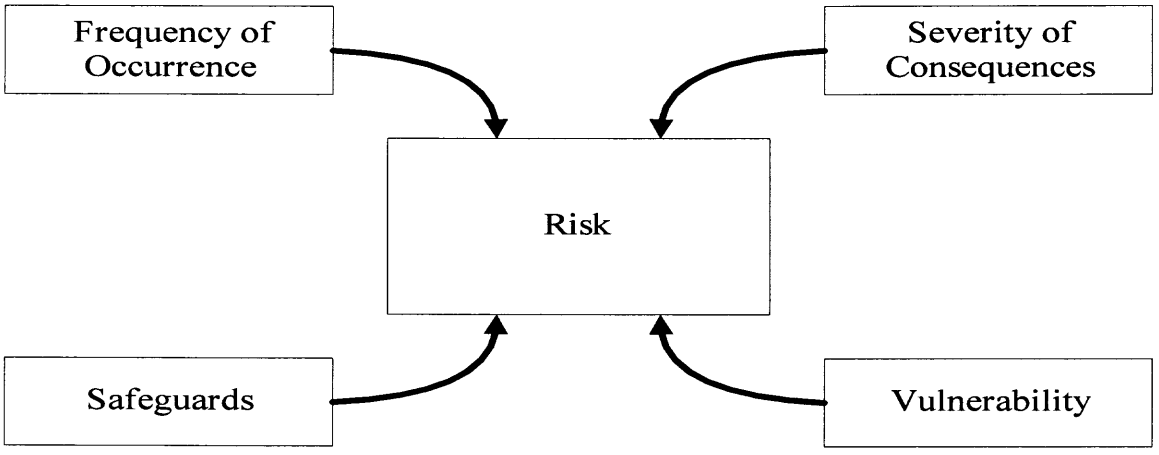

Figure 3.1 Factors Contributing to Risk.

The frequency of occurrence and severity of consequences depend on the system vulnerabilities and safeguards in place. Vulnerabilities relate to threat occurrence and consequences, while safeguards counteract threat occurrence and consequences. All of these factors play against each other to determine the risk level in the system.

3.2 Supply Chain Risk Assessment Procedure

Supply chain risk analysis is distinctively different from traditional risk analysis due the presence of complex interrelationships among business entities. The method proposed in this thesis to analyze risks in a supply chain has been derived from the methodology developed by the National Institute of Justice to assess vulnerability of chemical plants and Military Standard 882 D [13, 55]. The National Institute of Justice developed a prototype model to assess the vulnerabilities in a chemical facility. Even though the technique has been specifically developed for a chemical facility, the underlying concepts can be extended to a supply chain. Risk analysis of a supply chain is broadly divided into seven steps.

They are:

1. Asset Identification
2. Asset screening
3. Activity Identification
4. Activity Screening
5. Threat Identification
6. Threat Assessment
7. Risk Quantification

3.2.1 Asset Identification

Asset is anything that has a monetary or operational value. Assets include but not limited to people, facilities, equipment and stocks. Identification of assets is first and foremost step in risk analysis. Asset identification also enables a better understanding of the supply chain and its vulnerabilities. The asset identification can be performed at various level of detail. The extent to which the assets need to be identified should be in accordance with the objectives of the risk analysis. Identifying trivial assets can be unproductive and will waste of resources. Only priority assets should be identified.

In the context of supply chain risk analysis, two types of assets are related to facilities and logistics links. Defining an asset either as a facility or logistic link is broad enough to fit it to any supply chain configuration. While facilities either manufacture or store goods, logistics links ship them. This type of asset definition and identification also helps in construction of a network model of the chain and eases asset identification as facilities and logistics links are highly visible and can be easily identified.

Asset Modeling

A facility is considered to consist of six major elements - site, materials, people, physical structure, electric power and information. While site means the nearby adjoining areas to the facility, all other terms are self- explanatory. The major inputs to a facility are raw materials, parts/ sub assemblies, process chemicals, water and energy. Various operations are carried in the facility to process the raw materials to manufacture a product. A block diagram of a facility is shown in Figure 3.2

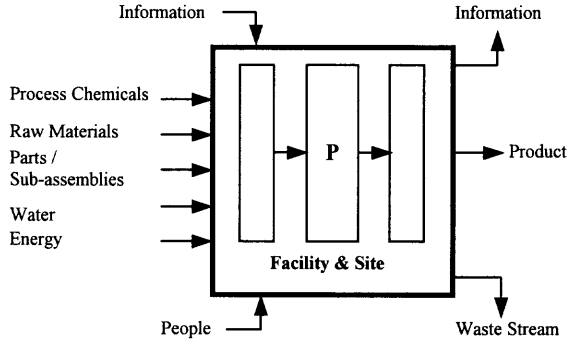

Figure 3.2 Block Diagram of a Facility.

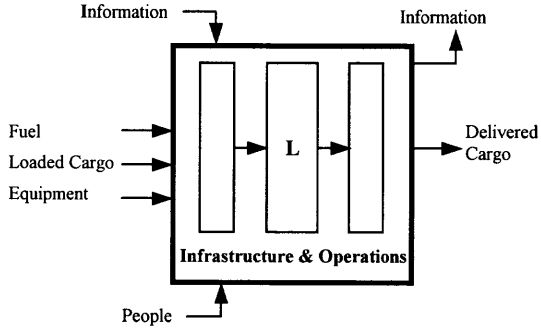

Figure 3.3 Block Diagram of a Logistics Unit.

Similarly, a logistics link consists of infrastructure, fuel, people, cargo and information. The term infrastructure includes the type of transportation and the route selected. Figure 3.3 shows the block diagram of a logistics link. The inputs to the

logistics links are fuel, cargo and equipment. And, the output of the unit is delivered cargo. When the productions units and the logistics links are linked a supply chain is created. In a chain, information and material flow along the chain to fulfill customer requirements. While, material flow is almost unidirectional, information flow is arbitrary.

Often, information flow and information security is much more important because information is crucial in operating a supply chain. Any disruption in data flow or breach in information security could be fatal to the company. With new cyber threats emerging every day, protecting data is becoming increasingly difficult. Therefore, information flow is identified and modeled as a critical element in the supply chain model.

3.2.2 Asset screening

Once the assets are identified, the next logical step is to determine whether the asset is a priority asset and if an assessment is required. Low priority assets, i.e. assets with less significance, need not be further studied and analyzed. This step eliminates insignificant assets. The idea behind eliminating assets is that a risk assessment of these assets may be much expensive than the cost benefit or utility realized from the assessment. This step determines the importance of the asset to the supply chain based on a few parameters like number of people working in the facility or its importance to the supply chain. Based on the parameters, a priority value is calculated that ranges between 1- 4, where 1 is the highest priority value and 4 is the least. If the priority value is 1 or 2 then an assessment is required. Again, if the value is greater than 2, then an assessment is not necessarily required but the supply chain manager may decide to perform an assessment. The parameters used in determining the priority value are of two types: objective and subjective parameters. For objective parameters, the quantitative value can be calculated.

But, for subjective parameters the absolute value cannot be calculated and beliefs need to be used instead. For example, the number of people working in a facility or the current inventory level can be calculated but the attractiveness of the asset to an adversary cannot be calculated and has to be approximated. Since, Facilities and Logistics links are two different entities, the parameters used to calculate the asset value also differ.

3.2.2.1 Priority value calculation for a Facility. Eight critical parameters have been identified to estimate the importance of a Facility. As discussed above, the parameter could be either objective or subjective. Again, the parameters can either have two or four possible responses.

The parameters and their possible responses are:

- Is the quantity of hazardous materials stored in the facility greater than threshold value
  - Yes
  - No
- Sole source supplier
  - Yes
  - No
- No of people that would be affected in the worst case scenario
  - More than 100,000
  - 10,000–100,000
  - 1,000–9,999
  - Less than 1,000

- Importance to the region
  - Very Important
  - Moderately Important
  - Marginally Important
  - Not Important
- Importance to the supply chain
  - Very Important
  - Moderately Important
  - Marginally Important
  - Not Important
- Importance to the nation
  - Very Important
  - Moderately Important
  - Marginally Important
  - Not Important
- Recognizability
  - Easily Recognizable
  - Recognizable
  - Somewhat Recognizable
  - Not Recognizable

The first and foremost parameter is the amount of chemicals stored in a facility. This parameter can have two responses, either "Yes" or "No". If the amount is greater than threshold value as given in Federal regulation 40 CFR 68.130, then the response will

be "Yes", other wise "No". If the response to this parameter is "Yes", then the asset has a priority value of 1 and an assessment is required. If the response is "No" then the priority value of the asset is 4. Analysis of remaining parameters is not required if the response to the first parameter is "Yes" as a risk assessment has to be carried out irrespective of other parameters. If the response is "No", then the second parameter is analyzed. The second parameter like the first one has two possible responses, either "Yes" or "No". Again, if the response is "Yes", then an assessment is required and rest of the parameters are ignored. Parameters 1 and 2 are objective and their value depends on the data collected from the facility. Parameters 3-8 are subjective and can have four possible responses as given above. No solid data is available to estimate these parameters and they have to be estimated using subjective knowledge. Each of the parameter is assigned a qualitative term, which is in turn is converted into a quantitative value. For example recognizability of an asset can be high, medium, low, and very low. Each of the terms is assigned a value of 1, 2, 3 and 4 respectively. Using qualitative values instead of quantitative is helpful as these parameters are estimated based on beliefs. Beliefs cannot be measured on an absolute scale and only a relative comparison can be done. For example, values 1-4 for recognizability may not mean anything to the supply chain manager, but qualitative values like high, medium make more sense. After a value has been assigned to parameters 3-8, the overall priority value of the asset is calculated as the value of the parameter with the highest priority rating.

3.2.2.2 Priority value calculation for a Logistic Link. Priority value for a logistics link is calculated on similar lines. The parameters used to calculate the priority value and their possible responses are:

- Does the shipment cross national borders
  - Yes
  - No
- Does the shipment contain goods that attract the adversary
  - Yes
  - No
- Are there any alternative routes
  - Yes
  - No
- Hazardous or explosive materials
  - Yes
  - No
- Shipment visibility
  - Highly visible
  - Moderately visible
  - Marginally visible
  - Not visible
- Population density associated with the route
  - High
  - Medium
  - Low
  - Very Low
- Damage in the worst case scenario

- High
- Medium
- Low
- Very Low

- Significance to supply chain operations
  - Very Important
  - Moderately Important
  - Marginally Important
  - Not Important

First four parameters can have two responses, while others have four responses. The responses to first four parameters are either "Yes" or "No". If the response to any one of the parameter is "Yes", then a risk assessment is required. Parameters 5-8 can have four possible responses and priority value is exactly as described for a facility.

3.2. 3 Activity Identification

Activity identification is the next step in risks assessment after asset screening. Activity is defined as any operation or process that is carried out in a facility or logistics link to fulfill customer requirements.

Activity identification is a very crucial step in risk analysis as the extent of activity identification dictates the reliability of risk analysis. For example, the activity of unloading the shipment from a trailer and storing it in a warehouse can be considered to be a single activity or can be divided to sub-activities. The scope of the study has to be determined by the supply chain manager based of the requirements of the assessment. A highly detailed study may waste resources, while a low level study may not be effective

in identifying all relevant threats. Once the activity has been identified, an activity type is assigned. Broadly, the activity types in a facility could be storage, material handling, manufacturing operations or waste management. These are not the only possible activity types; the manager can decide to have more activity types based on the operations being carried out in the facility. The idea behind assigning an activity type to the activities is that similar activities will have a common set of characteristics that can be exploited to simplify risk analysis process. For example, in a material handling activity threats would be almost identical and irrespective of the stations between which the activity is carried out.

After assigning an activity type, the activity is thoroughly studied and characterized to determine its significance. A priority value is calculated for each activity to check if an assessment is required. Each activity is prioritized based on its significance, recognizability, accessibility and the amount of chemicals involved in the activity.

Priority Value Calculation

The priority value is calculated based on the following parameters:

- Involvement of hazardous chemicals
  - Yes
  - No
- Quantity of chemicals used
  - 25 times greater than the threshold
  - Between 10-25 times the threshold quantity
  - Between 1-10 times the threshold quantity
  - Less than the threshold

- Frequency of the activity
    - 100 % continuous
    - 50-99% continuous
    - 25- 49% continuous
    - Less than 25 %
- Recognizability
    - Highly Recognizable
    - Moderately Recognizable
    - Marginally Recognizable
    - Not Recognizable
- Accessibility
    - Highly Accessible
    - Moderately Accessible
    - Marginally Accessible
    - Not Accessible

Each of the parameters is assigned a value ranging between 1-4, where 1 signifies highest priority and 4 the least. If a parameter has only two responses like true and false then the true value is assigned a value of 1 and 4 for false. After, all the parameters are evaluated and assigned a value, then the overall priority values is calculated as the sum of values of all parameters. If any of the parameter is critical then the activity is a high priority activity and an assessment is required. If any of parameter takes a value of 1 or 2 then an assessment is required. Otherwise, it is at the discretion of the supply chain manager.

3.2.4 Threat Identification

Threat is defined as an unwanted or unplanned activity that might have a negative impact. This stage involves identifying the threats against each of the identified activities. The number of threats against an activity could be infinite. This step should therefore focus on identifying only those threats that are relevant to the scope of the study. Threats can be broadly divided into three categories: intentional threats, accidental threats and natural hazards. The frequency with which accidental threats and natural hazards occur can be estimated by studying the past occurrence patterns. These threats are more or less static and the past is considered to be a good reflection of the future. Intentional threats on the other hand have a human motivation and are very dynamic. The adversary is intelligent and his attack is preplanned. He selects his targets with due diligence and can change his tactics any time.

It is very difficult to predict when, how and where he will attack. The number of potential adversaries like the number of threats is also infinite. Information relating to adversary's intents, capabilities and beliefs is rarely available to the commercial industry and without much of this information estimating the probability of occurrence would be difficult if not impossible. Also, these threats call for advances in system analysis, data fusion, and artificial intelligence.

An alternative way to handle this type of threats would be to identify the system vulnerabilities and study how these vulnerabilities would affect the system response. For example, the probability of a supply link being disrupted due to low inventory levels can be studied instead of studying a supply chain disruption due to a bomb explosion on the

highway. This type of analysis will be performed within the boundaries of the supply chain and does not require critical, sensitive and often confidential data.

3.2.5 Threat Assessment

Threat assessment phase examines the threats to estimate the probability of occurrence and severity of consequences. The complexity of this phase depends on the desired level of detail and scope of the analysis. The frequency of occurrence and severity of consequences can be estimated using subjective knowledge or a detailed engineering analysis can be performed. Frequency of occurrence can be estimated through fault trees analysis. Fault tree analysis often requires a very detailed study of the system and may take considerable time and effort to construct a fault tree. Likewise, severity of consequences can be estimated by developing complex simulation models like a blast analysis. Choice of the technique to assess threats depends on resource availability. Simulation models can be very expensive and also require significant amount of time and effort. However, they are much more reliable and yield better results. With simulation, events that cannot be tested in real time can be analyzed in a virtual environment. Developing highly complex simulation models may hinder the very reason for performing a risk analysis. The required level of detail also depends on the product in consideration. For example, risk analysis of an explosive/hazardous product like bombs or grenades has to be very elaborate and extensive, but for a household appliance the analysis need not be extensive.

3.2.5.1 Probability of Occurrence. Probability of occurrence illustrates the rate with which the threat is expected to occur. This can be either calculated quantitatively or qualitatively. Using qualitative terms to estimate the frequency of occurrence is more

recommendable as the data required to assign a quantitative value is rarely available and has to be estimated based on subjective beliefs. For example, it may not be possible to estimate absolute frequency value with which an earthquake in New York City or a mid air head-on collision of two jet planes will occur. Even if a quantitative value were assigned it would be very difficult to interpret and understand. For example, a probability value of 10^{-10} for an air crash is difficult to comprehend. Qualitative values on the other hand are easy to understand and are intuitive. The probability of occurrence of a mid air collision can be easily assigned as "Improbable". For frequency of occurrence, Military standard 882D recommends five levels for frequency of occurrence [55].

Military standard defines the frequency of occurrence levels as:

Frequent: Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.

Probable: Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.

Occasional: Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.

Remote: Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.

Improbable: So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.

The only problem in using qualitative terms is that there is a certain amount of overlap between the adjacent levels. For borderline cases, the supply chain manager has to decide the probability level of the threat. The probability of occurrence can be

estimated in two ways: using a simple analysis or fault tree analysis. A simple analysis is a straightforward method to estimate the frequency of occurrence of the threat. In this method the analyst uses his subjective knowledge and intuitions to assign a probability value. This technique does not consider the causal or triggering events and the enabling scenarios. This approach is very rudimentary and is not recommended. However, if the analyst feels that the threat is trivial and a detailed analysis is not required then this method may be used.

Fault tree analysis is a very sophisticated technique to estimate the frequency of occurrence of the identified threat (top event). This technique has been rigorously researched and is based on well-established systems and reliability engineering concepts.

3.2.5.2 Fault Tree Analysis. Fault trees analysis is a deductive logic analysis approach to identify the causal events and their interrelationships. In this approach, a top event is identified and it is analyzed thoroughly to identify the root events. The results of a fault tree analysis are two fold: a pictorial representation of the causal events and the probability of occurrence value of the top event. Fault tree analysis is based on Boolean logic and uses Boolean arithmetic to calculate the probability of occurrence of the top event. Fault trees basically have two types of nodes. They are gate and event nodes. Gates nodes have one or more children and event nodes are the independent events whose occurrence does not depend on other events. Events nodes are known as leaf nodes and are the triggering events. Gates nodes are of two fundamental types: "AND" and "OR" gates. In a "AND" gate all the children need to happen simultaneously to trigger the parent event. And, in an "OR" gate any one of the event can trigger the parent event. Traditionally, each of the nodes in a tree can have two states.

They are "True" and "False". However, having just two states will be very elementary and the intermediate states cannot be accounted.

Combining Bayesian networks and fault trees will provide a unique capability. With this approach, each event can have multiple states and new evidence can be combined with the existing data to recalculate new probability value. Fault tree analysis will be used to identify the causal events and to construct a network diagram. Bayesian networks will then be used to deduct an inference on the frequency of occurrence of the top event from the network structure. One of the main problems in using a Bayesian networks lies in populating the conditional probability tables. For a parent node with four children and five possible states for each node, 4^5 conditional probability values need to be entered. This is a major obstacle that has been hindering the application of Bayesian networks for years. To solve this problem, logical inference rules have been formulated. With these rules, the conditional probability tables can be easily populated.

In the proposed method, nodes can be of three types. They are: events, gates and safeguards. While events and gates can have 5 different states, safeguards have only 4 states. 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 and safeguards in place. The process is repeated until there are no further sub-causes or the analyst is satisfied with the level of detail. For the leaf events and safeguards identified, a probability of occurrence and protection level value is assigned respectively. The probability of occurrence could be "Frequent", "Probable", "Occasional", "Remote" and

"Improbable". A safeguard provides four levels of protection. They are "High", "Medium", "Low" and "Very Low".

The level of protection provided by a 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.

Logical rules, presented below, are used to populate the conditional probability tables

3.2.5.3 Logical Rules. P.L. Clemens proposed logical rules to perform a qualitative fault tree analysis [56]. These rules have been adopted and modified to suit the problem in consideration. A new set of rules has been added to incorporate safeguards into the analysis. To calculate the probability value of a gate, the safeguards associated with it are ignored in the first place and the probability of occurrence is calculated irrespective of the safeguards. Then, all events are assumed as a single node with the calculated probability of occurrence and the frequency of occurrence is recalculated with the safeguard in place.

Rules for calculating the frequency of occurrence without safeguards

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.

5. 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".

6. A safeguard providing "Medium" level of protection will reduce the frequency of occurrence by two levels.

7. A safeguard providing "Low " level of protection will reduce the frequency of occurrence by one level
8. A safeguard providing "Very Low" level of protection will affect the frequency of occurrence.

3.2.5.4 Inference Technique. After the conditional probability tables have been populated, an inference is deducted using Bayesian networks. Numerous software packages are available that would perform the Bayesian Inference. These software's use various algorithms like variable elimination algorithm, and junction tree algorithm to calculate the probability of occurrence. Notable among the software's is "Netica" from Norsys group. This software has been successfully used in "Site Profiler" and can be interfaced with most of the programming languages.

3.2.5.5 Example. Let disruption of manufacturing operations at a facility to be one of the identified threats. Disruption could be due to shortage of raw materials or due to a power failure. Power failure could be due to a transmission failure or due to the tripping of the circuit breaker. Shortage of raw materials can be related to delay in shipment arrival or to problems on the supplier side. Delay in shipment arrival can be due to a vehicle failure or delays at the port. Supplier might be facing material shortages or high

product failure rates due to which he is not able to supply on time. Two safeguards have been placed to maintain the continuity of operations. One, an electric generator is installed that could be used as a backup in case of a power failure. Two, a backup supplier is kept who could supply whenever there is a shortage of supplies from the primary supplier. The fault tree is shown graphically in Figure 3.3. In this tree, the top event is the disruption of operations. The tree contains four "OR" gates, five events and two safeguards.

Gates are:

1. Power Failure
2. Shortage of supplies
3. Delay in shipment arrival
4. Supplier problem

Events:

1. Circuit breaker trips
2. Transmission Failure
3. Material shortages
4. High product failure rates
5. Vehicle failure
6. Port delays

Safeguards:

1. Alternative supplier
2. Generator

Assume the safeguards, alternative supplier and generator, provide a high level of protection. Let the frequency of occurrence of the events be:

Circuit breaker tripping – occasional

Transmission Failure – remote

Material shortages – remote

High product failure rates – occasional

Vehicle failure- occasional

Port delay- improbable

For gates, the frequency of occurrence is calculated using the logical rules formulated. Under normal conditions Netica calculates the frequency of occurrence of the top event as occasional. The captured screen of the simulated fault free is given in Figure 3.5. If new information is obtained like Vehicle failure is frequent then threat level automatically elevates to Probable. The captured screen for inference with evidence is shown in Figure 3.6.

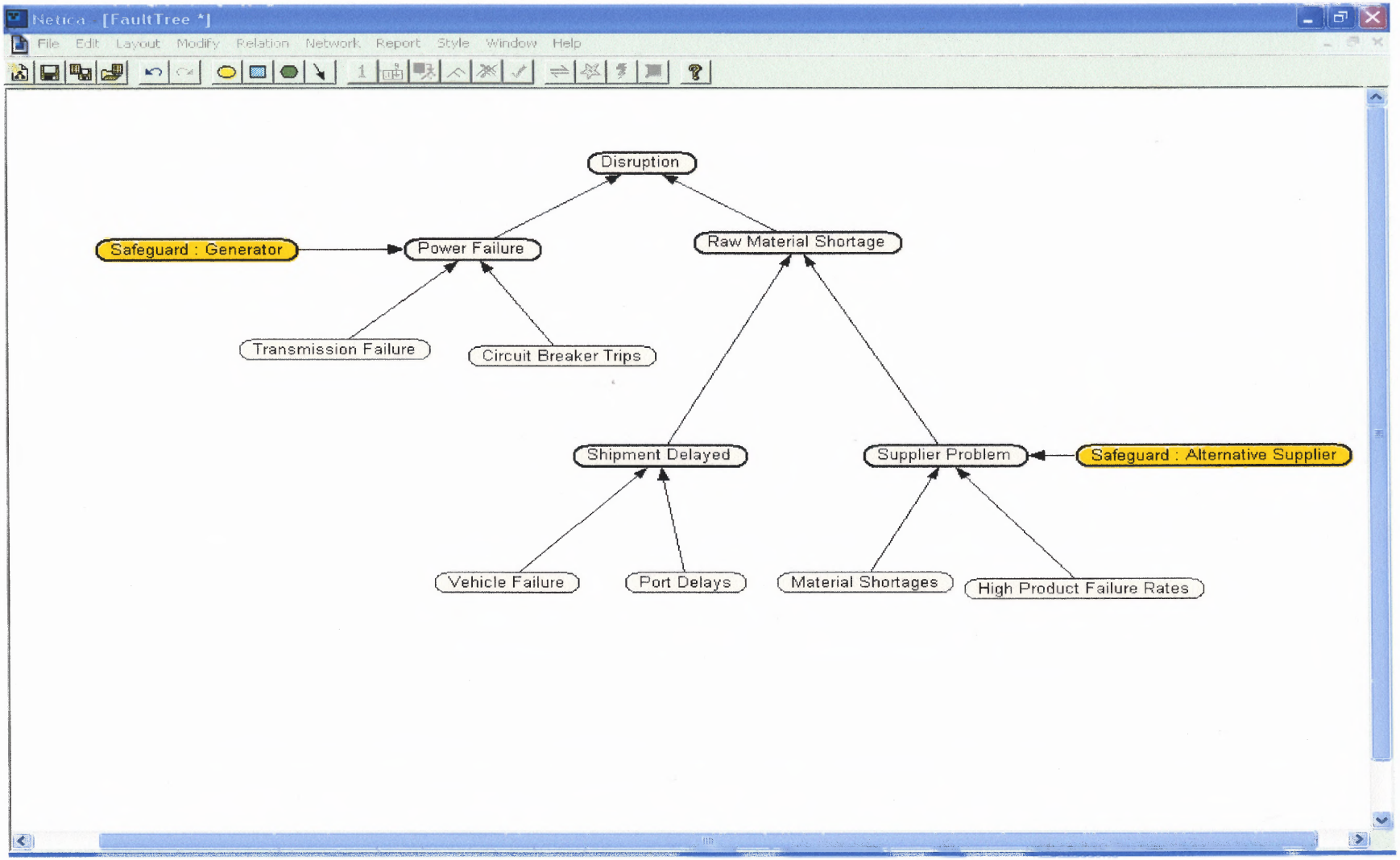

Figure 3.4 Fault Tree.

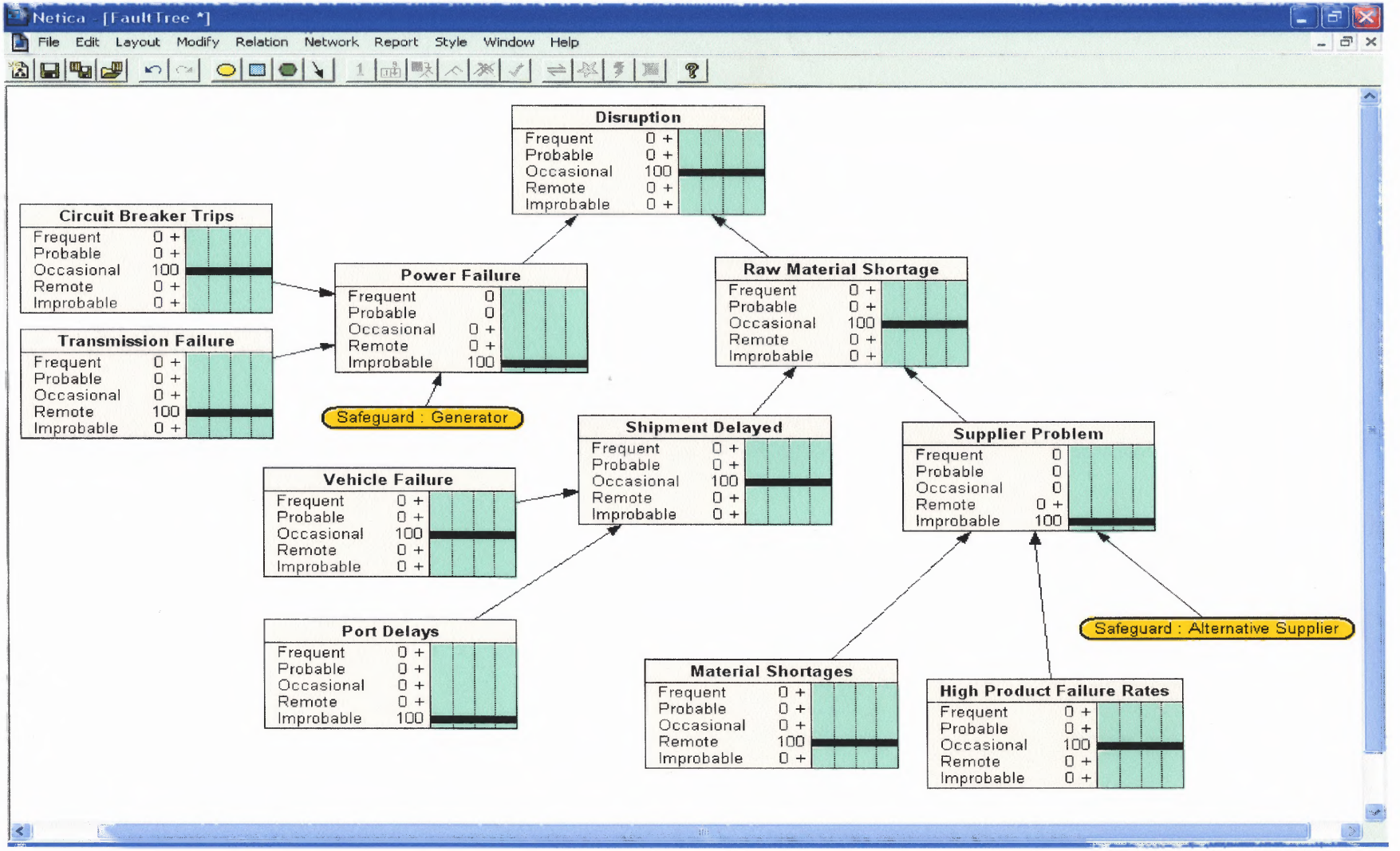

Figure 3.5 Simulated Fault Tree

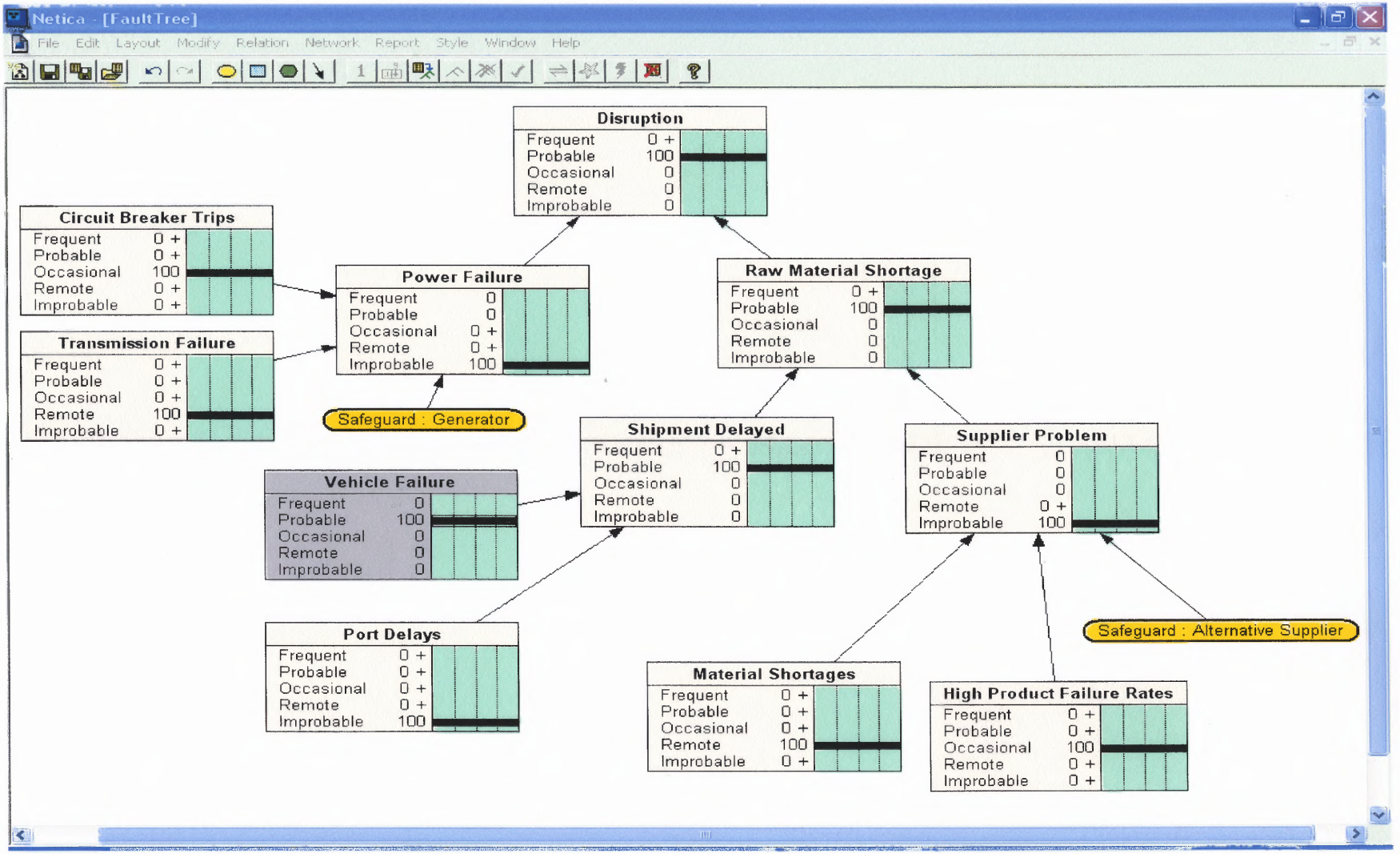

Figure 3.6 Simulated Fault Tree with Evidence

3.2.7 Consequence Analysis

Consequence analysis is the second step in threat assessment. In a supply chain, there could be a variety of consequences ranging from personnel loss to loss of customer good will. All of these consequences can be converted into a monetary value. Although monetary loss is one of the biggest concerns to companies, it is not the only concern. Personnel safety and environmental protection are equally important. Even though, both of these parameters can be converted into a monetary value, but it is not recommendable to assign values to assets such as employees and environment. For the purpose of analyzing risks in a supply chain three major types of consequences have been considered.

They are:

1. Monetary loss
2. Personnel Loss
3. Environmental Damage

Each of the above parameter can have four different levels. They are: "Catastrophic", "Moderate", "Marginal" and "Negligible". The definitions of each of these have been adopted from the Mil Standard 88 D and are as given 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 numbers in the definitions have been directly taken from the military specification and need to be changed to be in accordance with the supply chain in consideration.

3.2.8 Risk Quantification

Risk quantification is the final step in the risk assessment procedure. In this step the risk value is estimated and checked against the acceptable risk level. The threat assessment stage comes up with qualitative terms for frequency of occurrence and severity of consequences. A numerical value is assigned to each of these qualitative terms to estimate the risk value quantitatively. Tables 3.1 and 3.2 give the values assigned to frequency of occurrence and severity of consequences. These values are not absolute and do not indicate or suggest anything on their own. For example a value of 0.1 for probability of occurrence does not indicate that the event happen once in every 1000 times the operation is carried out. The values are relative to each other and indicate the relationship between the terms. For example, if a value of 0.1 and 0.001 is assigned to "Frequent" and "Probable" events then the values indicate that a "Frequent " event is 100 times more likely to occur than a "Occasional" event.

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}

3.2.9 Acceptable Risk Level

Setting the acceptable risk level is a management question and depends on the type of the supply chain in question. For example, health care and defense industry may need to have stringent risk limits while companies selling personal care goods may not have high acceptable risk levels. Acceptable risk level depends on how much risk the firm can take without hurting business. Acceptable risk level is a trade off between effectiveness and efficiency. Complete elimination of risks may not be possible and may go against the interests of the firm. Certain amount of risk has to be taken to do business profitably. Acceptable risk level has to be set with due diligence. Setting it too high will adversely

affect business due increased safeguard cost and setting it too low will not provide adequate protection.

The acceptable limit can be set a combination of frequency of occurrence and severity of consequences. These qualitative terms will then be converted into a numerical value to check against the risk factor for each threat/ activity pair. If the risk factor is greater than the acceptable limit then safeguards need to identified and implemented to reduce the risk level. Figure 3.7 summarizes the risk assessment procedure. After the safeguards have been implemented, steps through threat assessment and risk quantification need to be iterated until the risk factor is acceptable. If the risk factor is still unacceptable after implementing all possible safeguards then either the process or acceptable risk level needs to be changed.

After this stage a report is generated listing the risk factor with each activity/threat pair. The report will also identify high-risk threats. For the high-risk threats, safeguards are identified and implemented to reduce the risk level to acceptable levels.

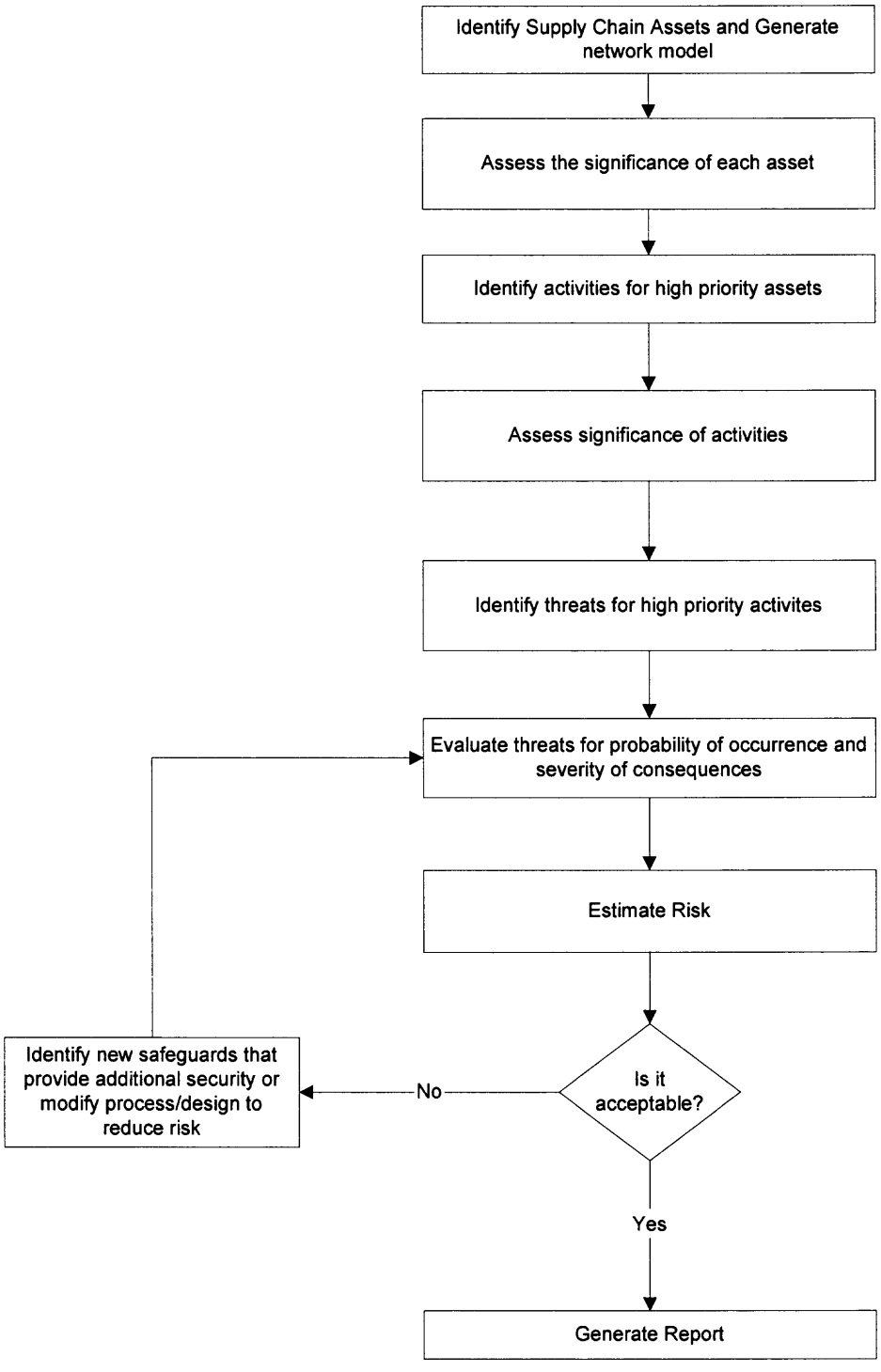

Figure 3.7 Risk Assessment Flow Chart.

CHAPTER 4

IMPLEMENTATION

4.1 Computer Based Supply Chain Risk Analysis and Management System

Risk analysis is a highly data intensive subject and a manual analysis is too arduous. A manual analysis often works against the very reason for doing the assessment. Computer based systems have the ability to handle large volumes of data and to identify the patterns in the data that are not visible to a human eye. These systems provide high computational power and can perform elaborate calculations within minutes. Computer based risk assessment systems can ease the assessment process and account for data changes without any difficulty. In a manual risk assessment, it might take a significant amount of time to incorporate minor data changes and a real time continuous risk assessment will be far from reality. Computers are highly sought for to perform data intensive applications and provide unmatched speed and accuracy.

Developing computer based systems as a web-application further enhances its capabilities. With the client – server architecture the system can be accessed from any place in the world with a computer having a web-browser like Microsoft Internet Explorer.

A web-enabled computer based system has been developed that guides the risk assessment process and calculates the risk factor with each activity. The system has been developed considering a supply chain manager who is conversant with supply management principles but may not be knowledgeable of risk assessment procedure.

4.2 System Architecture

The system architecture of the risk analysis system is given in Figure 4.1. It has been developed using Microsoft Active Server Pages with an Access database. At this stage, it is a stand – alone system but will later be integrated with ERP and legacy databases. Also, modules to extract design data from computer aided design files will be embedded into the system. The system guides and performs the risk analysis by collecting supply chain and process information.

First, the system logs in the user with a user name and password. Second, the supply chain model is entered into the system through facility and logistics link identification. After model construction, each facility is scrutinized to determine whether an assessment is required. If an assessment is required then each activity in that facility is identified and characterized to determine activity significance.

A risk assessment is not required unless and until an activity is significant to the business. If it is identified to be a significant activity, then the threats are identified and assessed. Supply chain operations, site information and process information data will be extracted from the ERP and other databases to characterize and prioritize the assets and operations.

Group technology concepts will be embedded into the system to automate threat identification process. Group technology takes advantage of similarities between entities to reduce the workload. For example, if two different products have almost the same design, then the most of the manufacturing processes will also be the same.

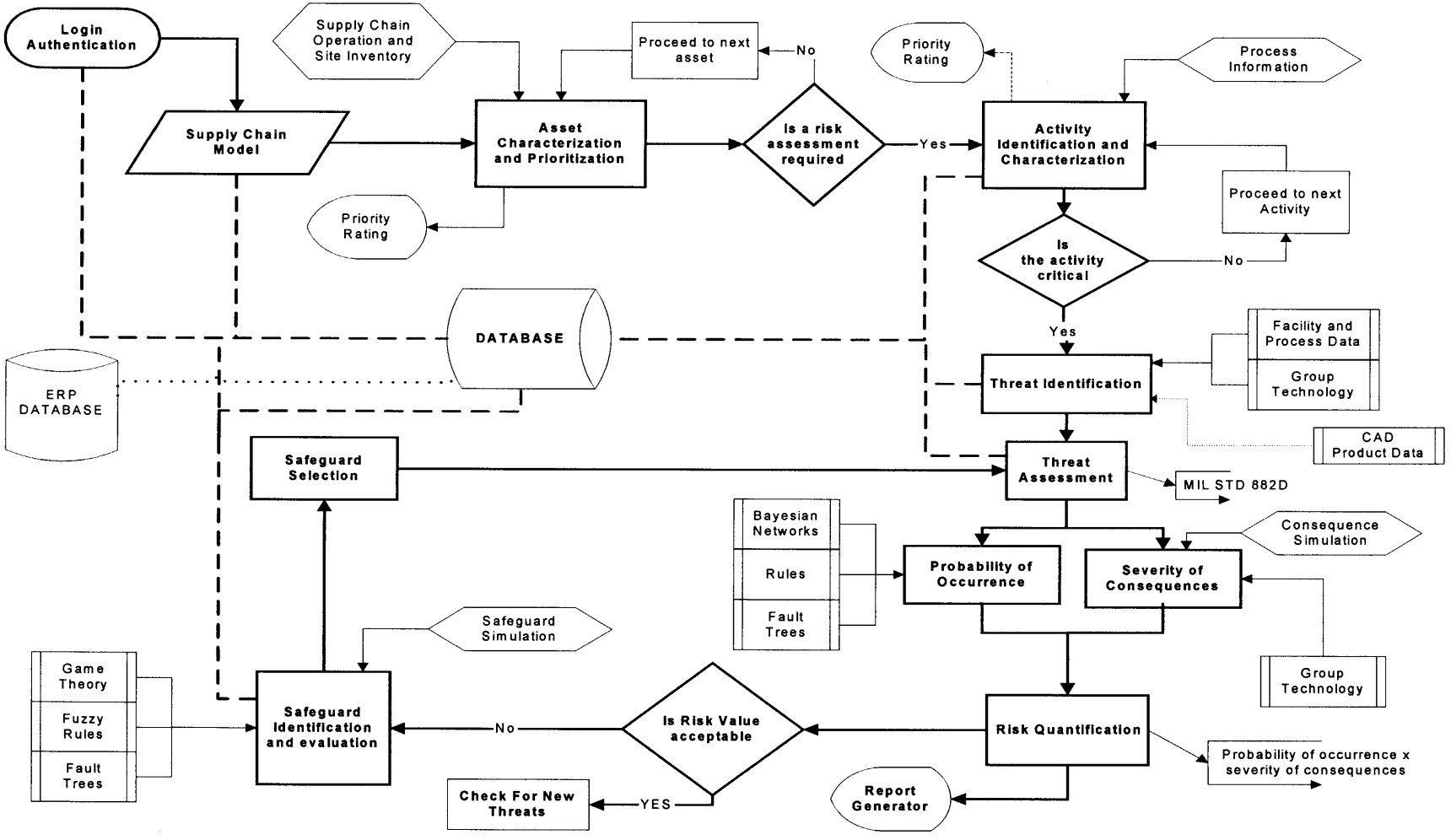

Figure 4.1 System Architecture.

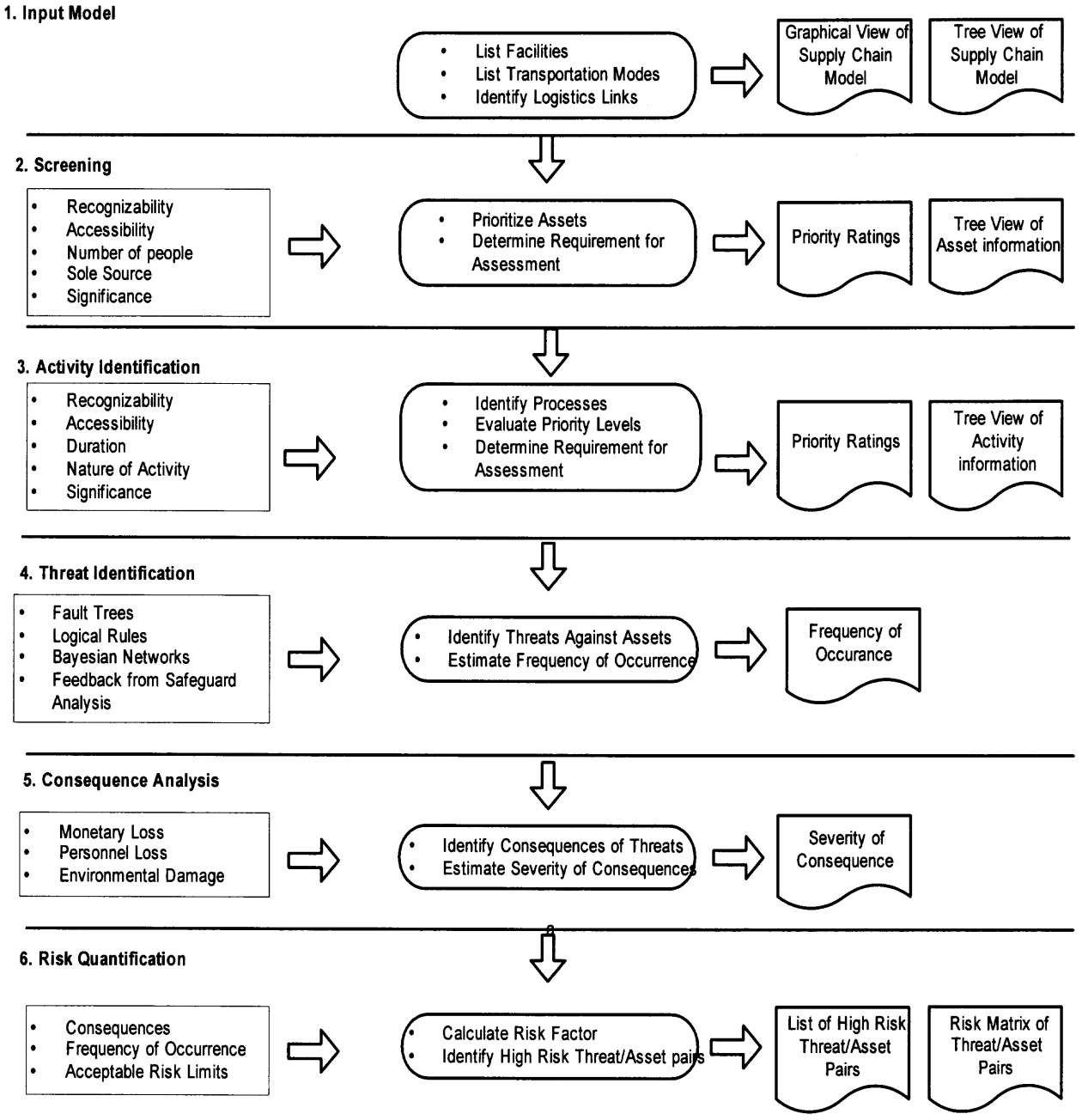

Figure 4.2 Methodology.

In the same way, if the activities are of the same type then the threats will also be identical. Again, the threats will also depend on the process being carried out and the product design. After threat identification, each threat is assessed for estimating the risk factor. After the risk factor is calculated a report is generated. If the risk level is not acceptable then the safeguards are identified and simulated to evaluate their effectives and to identify the most appropriate safeguard.

4.3 Software Description

Security is an important issue while developing a web-application. As data is online, without sufficient security measures, anybody could access and modify it. Risk analysis deals with sensitive and confidential data, which is often proprietary. Only authorized users need to be able to access the database. Each authorized user is provided with a unique user name and password, which is stored in a database. Figure 4.3 shows the captured login screen. Every time the user tries to log in, the user name and password are matched with the records in the database. Only if a match is found, the user is logged in. On successful login, the user is automatically directed to the menu page, where he is provided with two options. Either he could start a new assessment or continue with an existing assessment. Figure 4.4 shows the captured page for this step.

The risk assessment procedure is carried out in six different phases. Figure 4.2 lists all the phases in risk analysis with their inputs and outputs.

The phases are:

1. Supply chain model description
2. Asset screening
3. Activity Identification
4. Threat Identification
5. Consequence Analysis
6. Report Generation

4.3.1 Supply Chain Description

In this phase, a network model of the supply chain is constructed by identifying the facilities and logistics links in the chain. First, the facilities and transportation modes are identified and entered into the system using textboxes. Second, logistics links are identified and entered into the system using dropdown boxes. The logistics link is entered into the system by selecting the origin and destination facilities and the transportation mode from the dropdown boxes. Figure 4.5 shows the web-page implementation of this phase. After the supply chain is entered into the system, a network model of the supply chain is generated. The network model graphically depicts the facilities and the logistics links in the chain. A sample network model is shown in Figure 4.6. Also, a tree view of the supply chain is generated. The tree view displays information in a hierarchical order. In this case, the facilities are listed first, and then the corresponding linked facilities and possible transportation modes in a hierarchical order. These trees can be expanded or compacted as required. In this page clicking a facility name will list the linked facilities. The tree structure is a very powerful tool to present the data in a concise format.

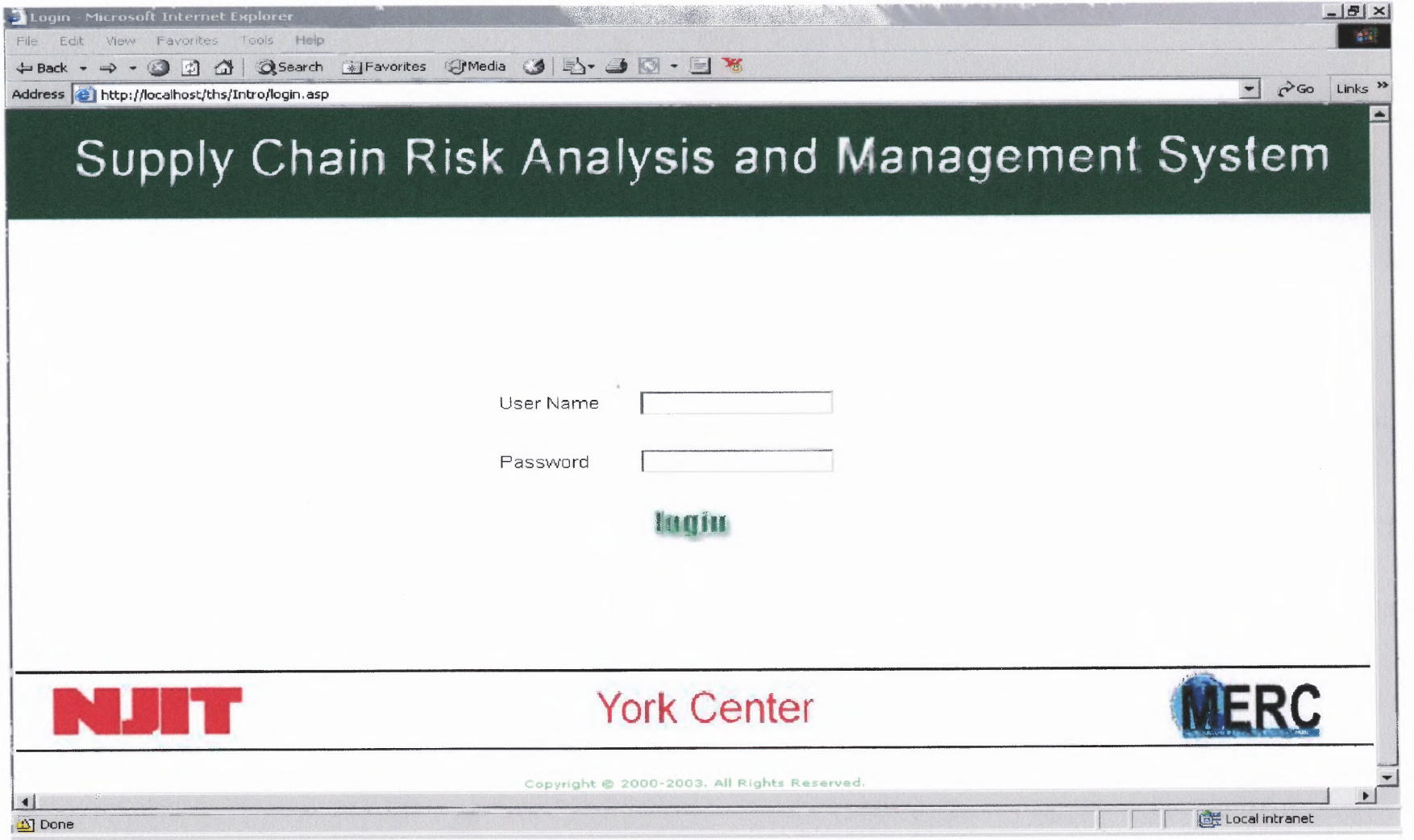

Figure 4.3 Captured Login Page.

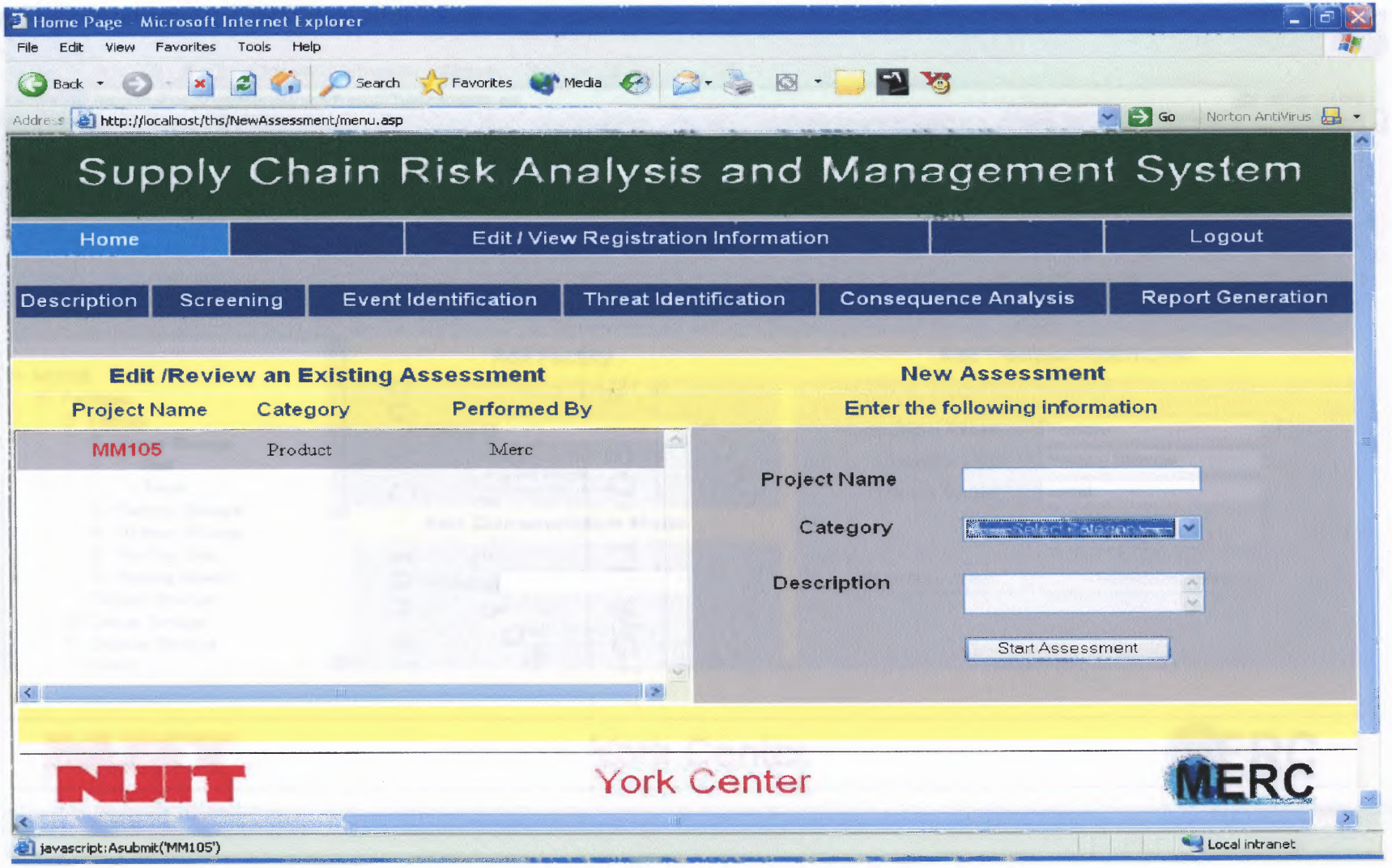

Figure 4.4 Captured Menu Page.

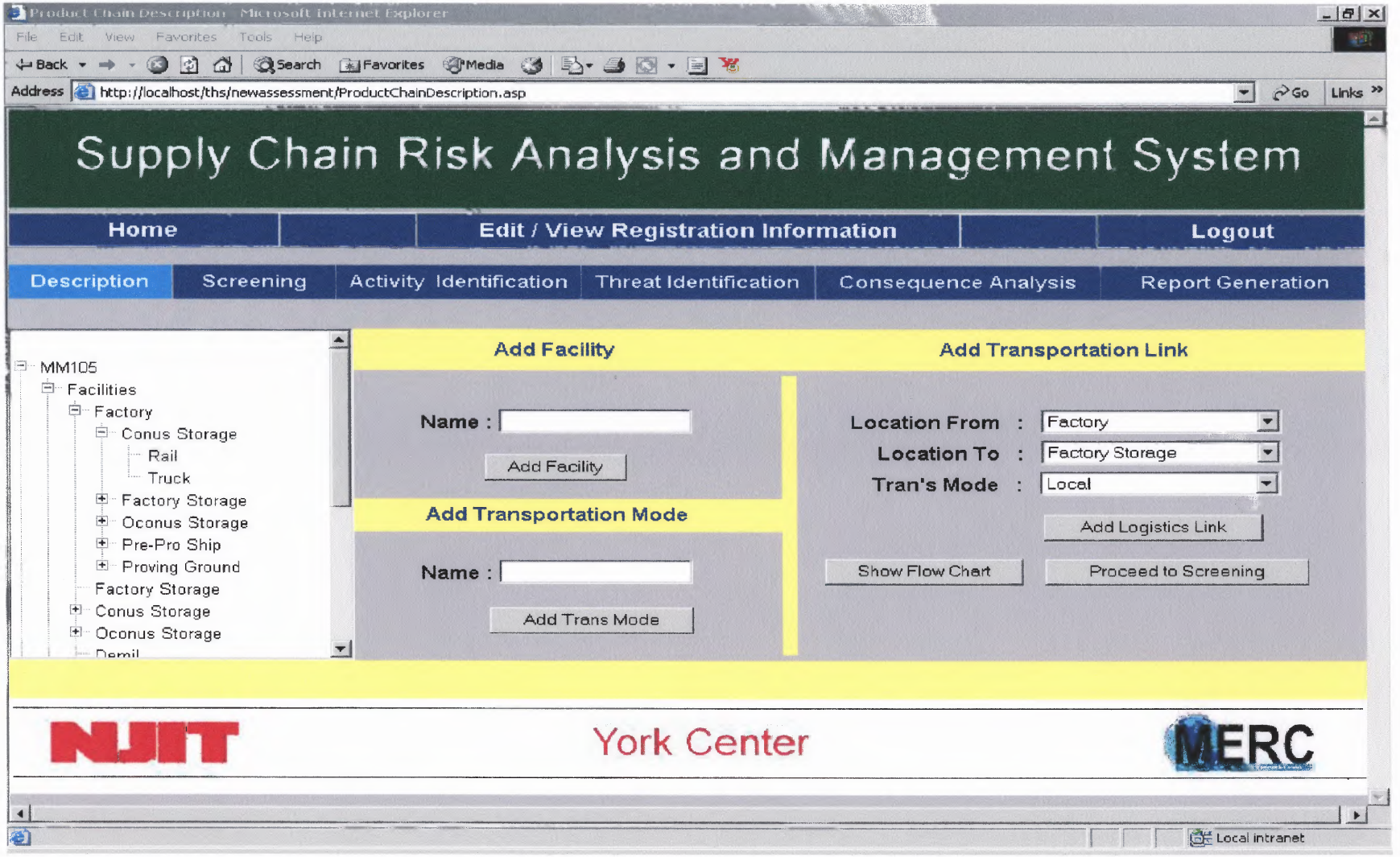

Figure 4.5 Supply Chain Description.

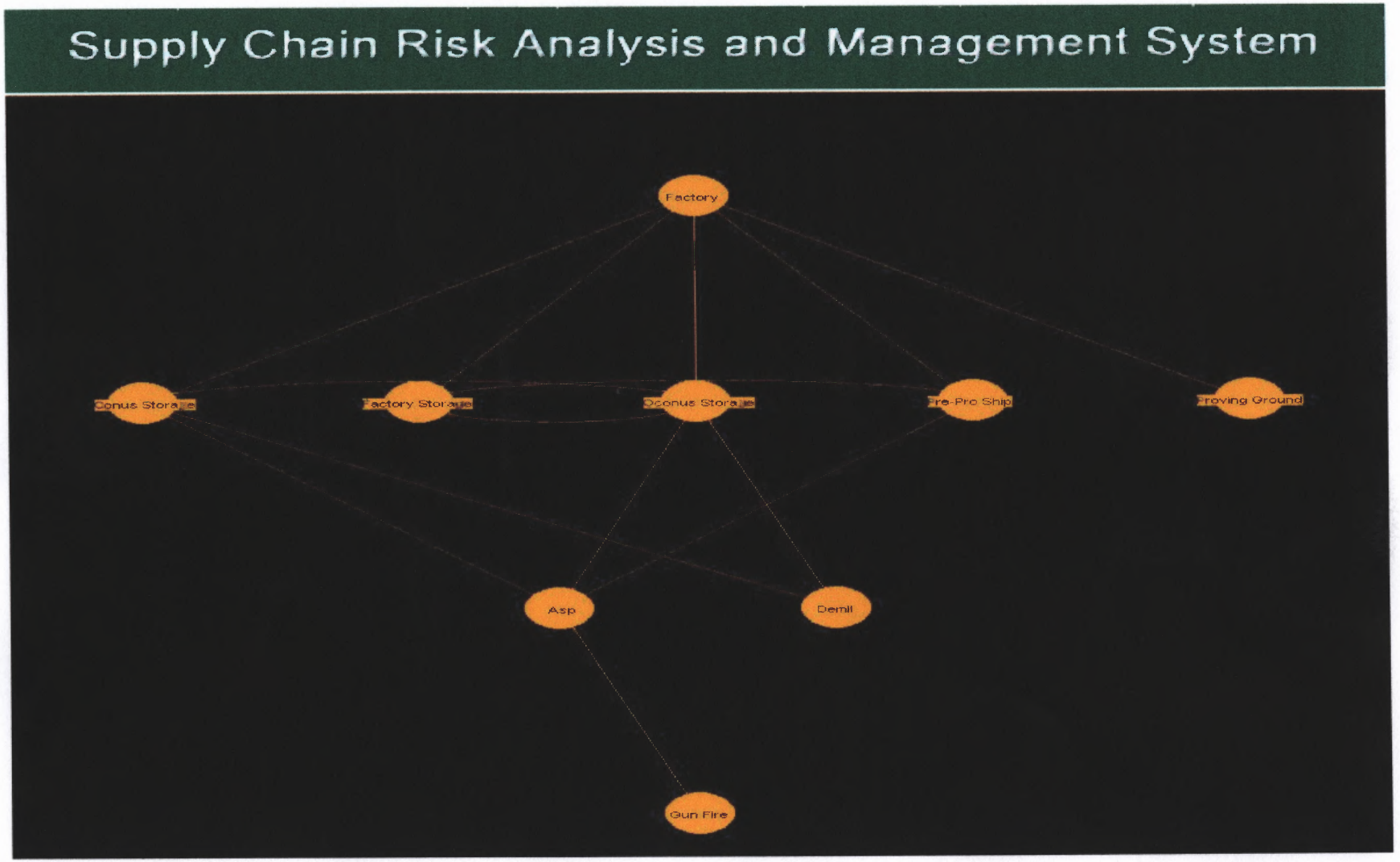

Figure 4.6 Network View of the Supply Chain.

4.3.2 Screening

This phase identifies the high priority facilities and logistics links. As discussed earlier in Chapter 3, the priority value for each facility or logistics link is calculated based on eight parameters.

To characterize a facility or logistics link, it is selected from the dropdown box. A logistics link is selected by selecting the origin and destination facility and the transportation mode. These boxes are interdependent and are analogues to the dropdown boxes used for selecting a state and city in which the entries in the city dropdown box depend on the state selected. Likewise, the entries in the destination facility box depend on the starting facility selected. Also, the list of facilities and logistics links is in the drop down boxes is dynamic. The facility or logistics link is automatically taken off from the list once it has been screened for a risk assessment. This page calculates the priority value based on the parameter values entered by the user. If an assessment is not required then the system prompts the user to make a decision. The screening information entered is stored in a database and displayed as a tree view on the left hand side. The tree view displays values of all parameters and the requirement for an assessment. Figure 4.7 and 4.8 show the web implementation of this phase for a facility and logistics link respectively.

4.3.3 Activity Identification

For the high priority facilities and logistics links that need an assessment, the various activities that are carried out are identified, characterized and entered into the system. The characterization is based on the parameters discussed in chapter 3. In this phase, a facility or logistics link is selected first and then an activity type. An activity can be

entered into the system either through a textbox or can be selected from the dropdown box. The idea behind selecting the activity type in the first place is that the system will automatically generate a list of possible activities based on the selected activity type.

The system scans through the database and selects all activities with the selected activity type. This technique has two advantages. One, it benefits from other risk assessments and two, reduces the thought process. Based on the responses to the parameters, the system calculates the priority value for the activity and determines whether an assessment is required or not. If the system determines that activity is not of high priority then the system asks the user whether he still wants to perform the assessment. The captured pages for this phase are shown in Figure 4.9 and 4.10.

4.3.4 Threat Identification

In this phase, threats are identified and entered into the system. The captured screen for this page is shown in Figure 4.11. For adding a threat, the corresponding facility or logistics link and the activity are selected from the drop-down box. A threat can be added into the system in two ways. The threat could be either selected from the dropdown box or a new threat can be entered using the text box. The system populates the drop-down threat box by identifying possible threats based on the activity type. The system runs through the database and selects threats with the same activity type as that of the selected activity.

Frequency of occurrence is also entered in this page. Frequency of occurrence can be either estimated using beliefs or a full fault tree analysis can be performed. This page also offers the capability to perform a full fault free analysis. In case of a fault tree analysis, a cause is identified and entered into the system. For the identified cause, a

cause type is assigned. As discussed in chapter 3, the cause could be a gate, event or safeguard. If it is an event or safeguard, then the frequency of occurrence or protection level is assigned respectively. For a gate, the system calculates the frequency level using logical rules. For each cause identified a parent is assigned. Possible parents for the cause are listed in the drop-down box. Once, the fault tree is constructed, the system calculates the frequency of occurrence of the top event by using the logical rules and stores it in a database. The tree view on the left side of the page lists all threats and their frequency of occurrence.

4.3.5 Consequence Analysis

Consequence analysis is the last step before generating the reports. The captured screen for this phase is shown in Figure 4.12. The identified threats are grouped by activity type. In this phase, the activity type is selected first from the dropdown box. On selecting the activity type, the box listing the threats will be automatically populated. Each threat is assessed based on three parameters: personnel loss, monetary loss and environmental damage. Based on the user responses the severity of consequences is calculated.

4.3.6 Report Generation

This the last phase in risk assessment. In this phase, reports are each generated either for facilities or logistics links. The report is in a tabular form, where the rows and columns represent the activity and threats respectively. For each activity–threat pair the risk value is calculated. Sample reports are shown in Figure 4.13 and 4.14.

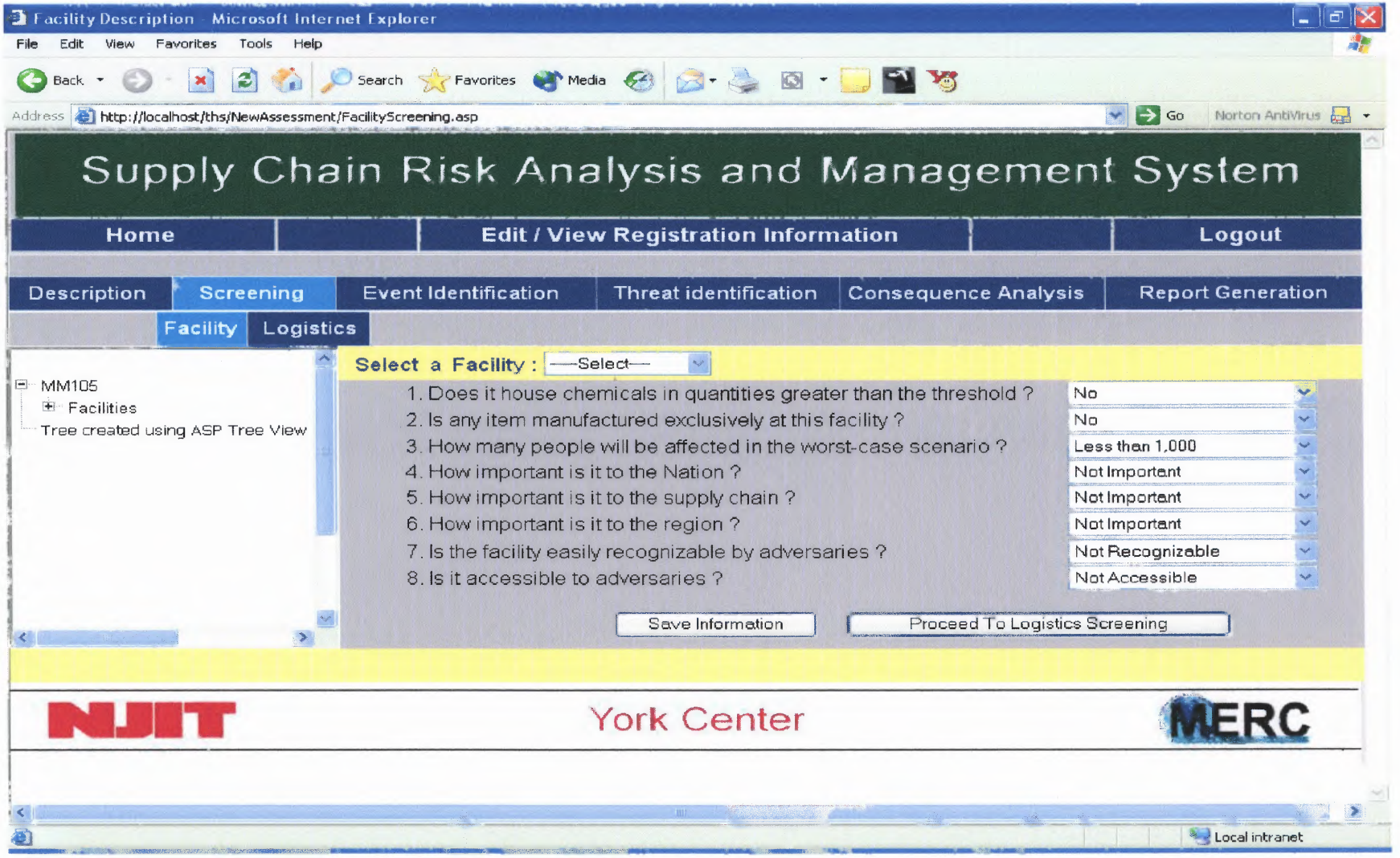

Figure 4.7 Captured Screening Page for a Facility.

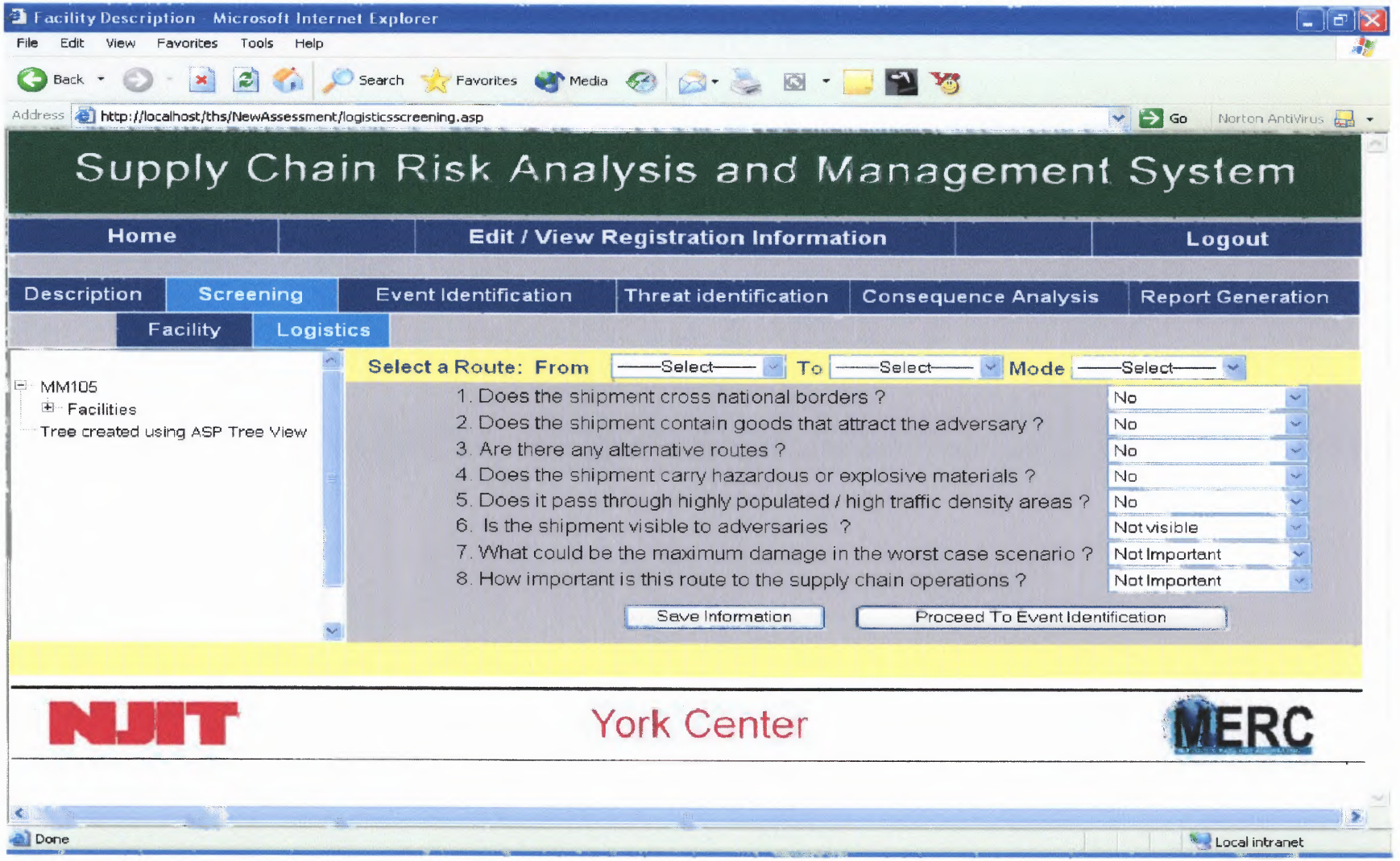

Figure 4.8 Captured Screening Page for a Logistics Link.

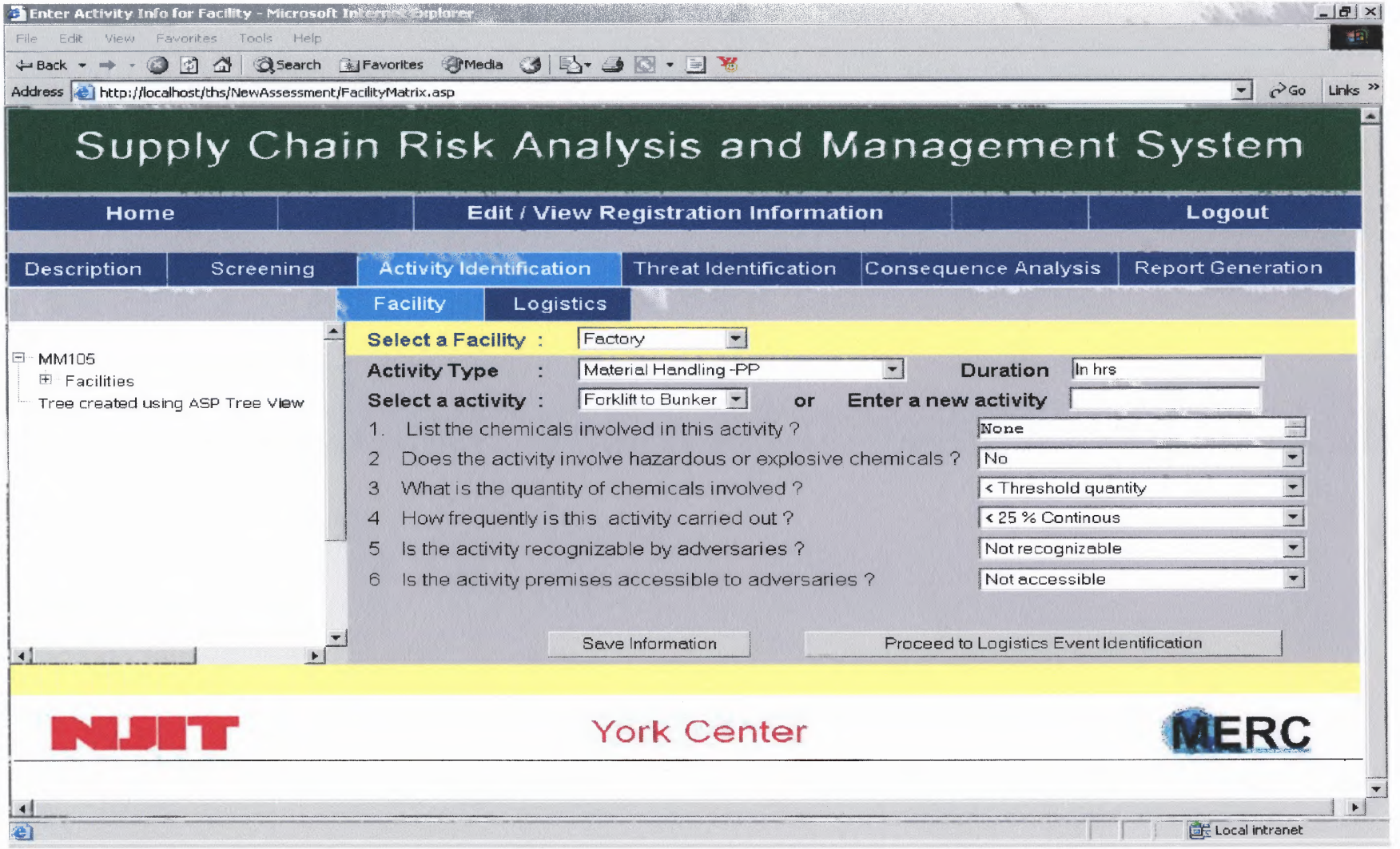

Figure 4.9 Captured Activity Identification Page for a Facility.

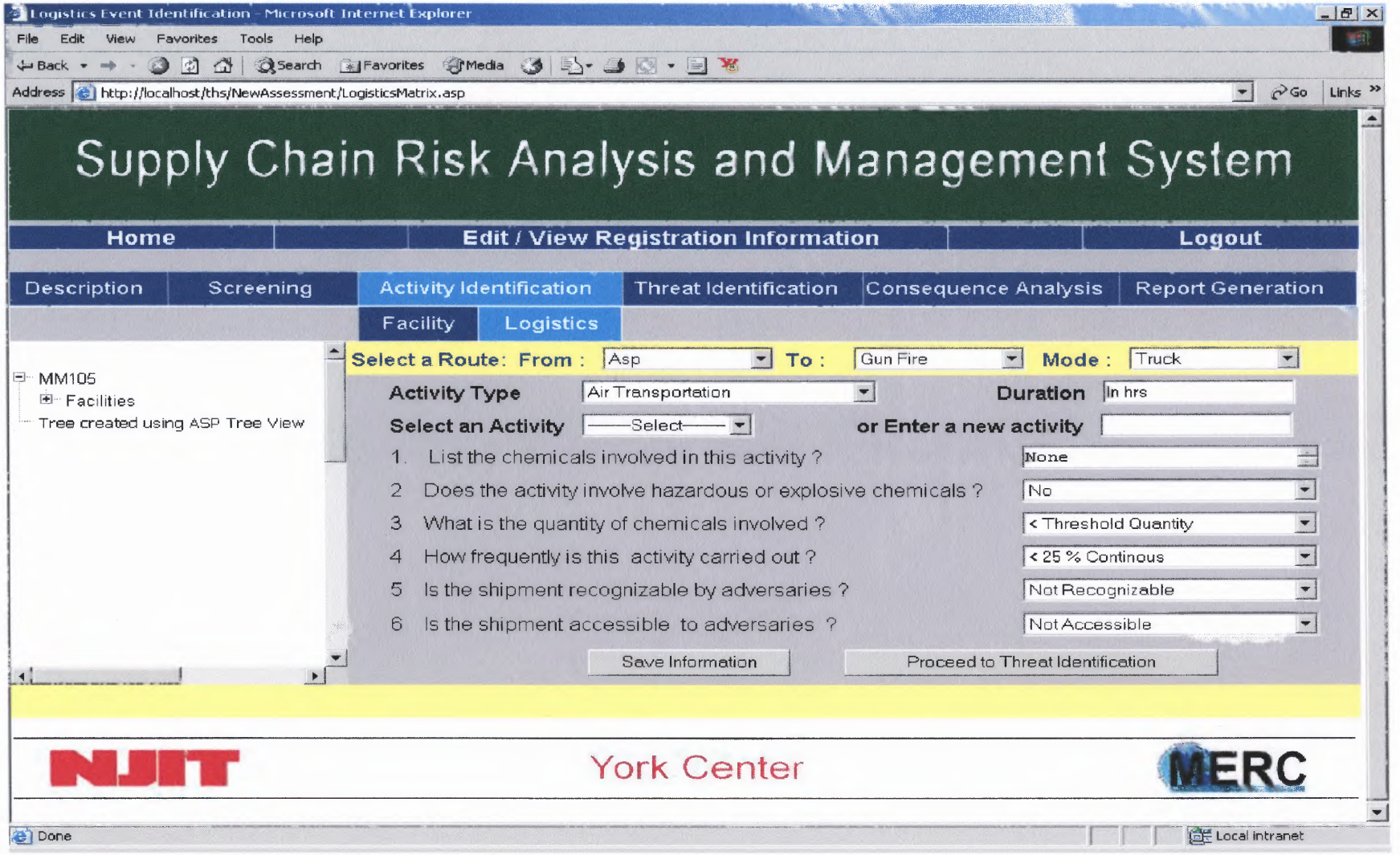

Figure 4.10 Captured Logistics Activity Identification Page.

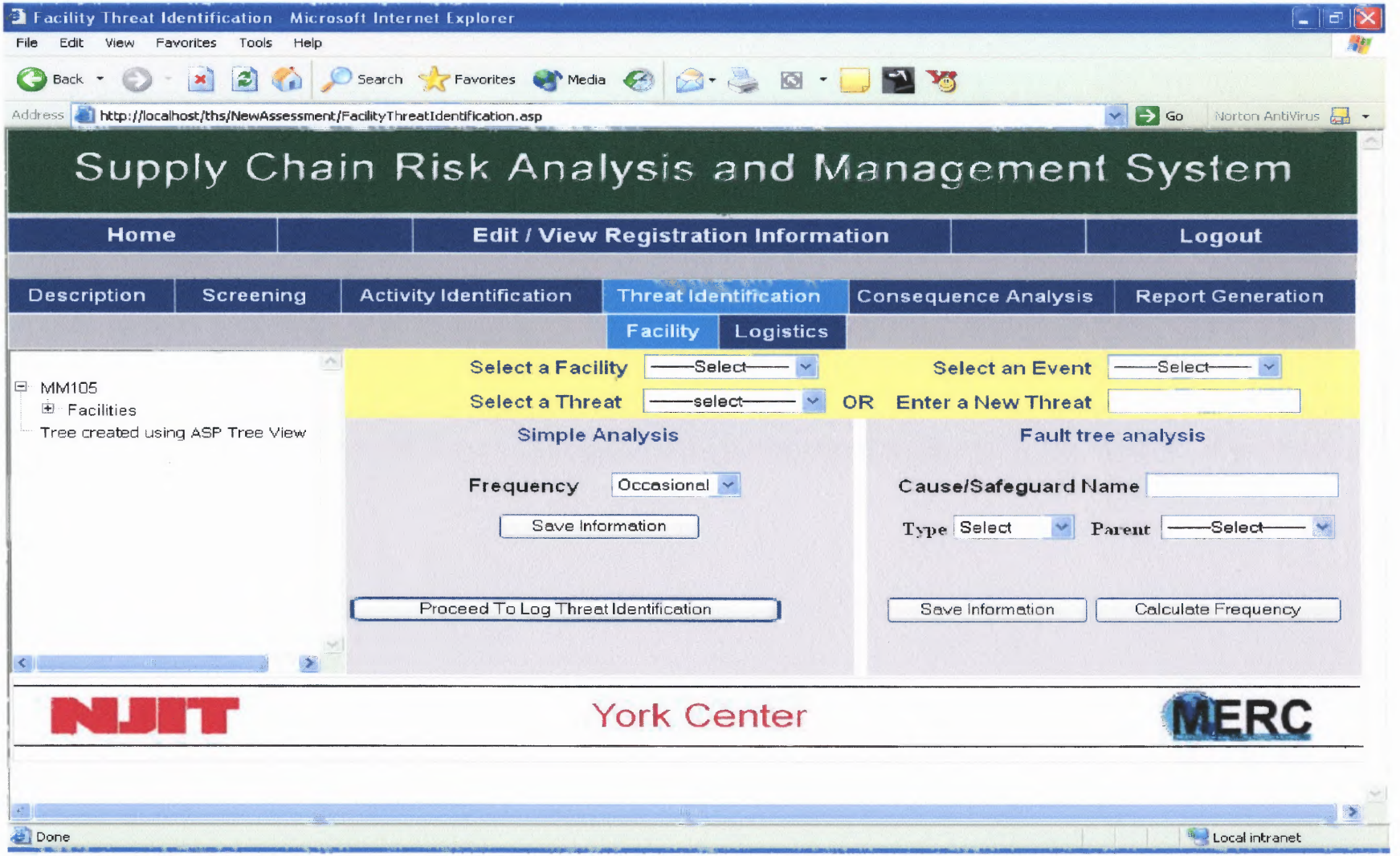

Figure 4.11 Facility Threat Identification.

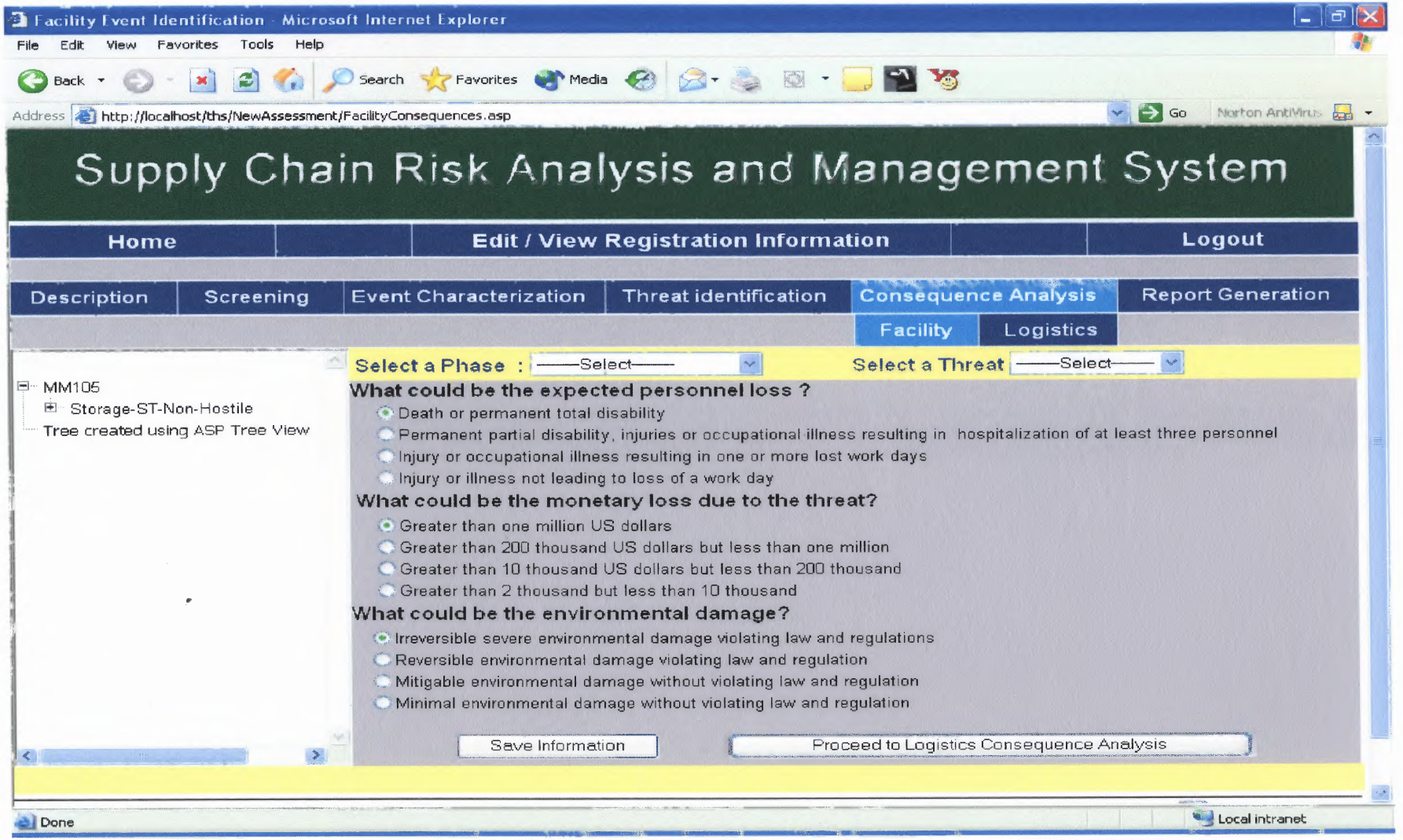

Figure 4.12 Facility Consequence Analysis.

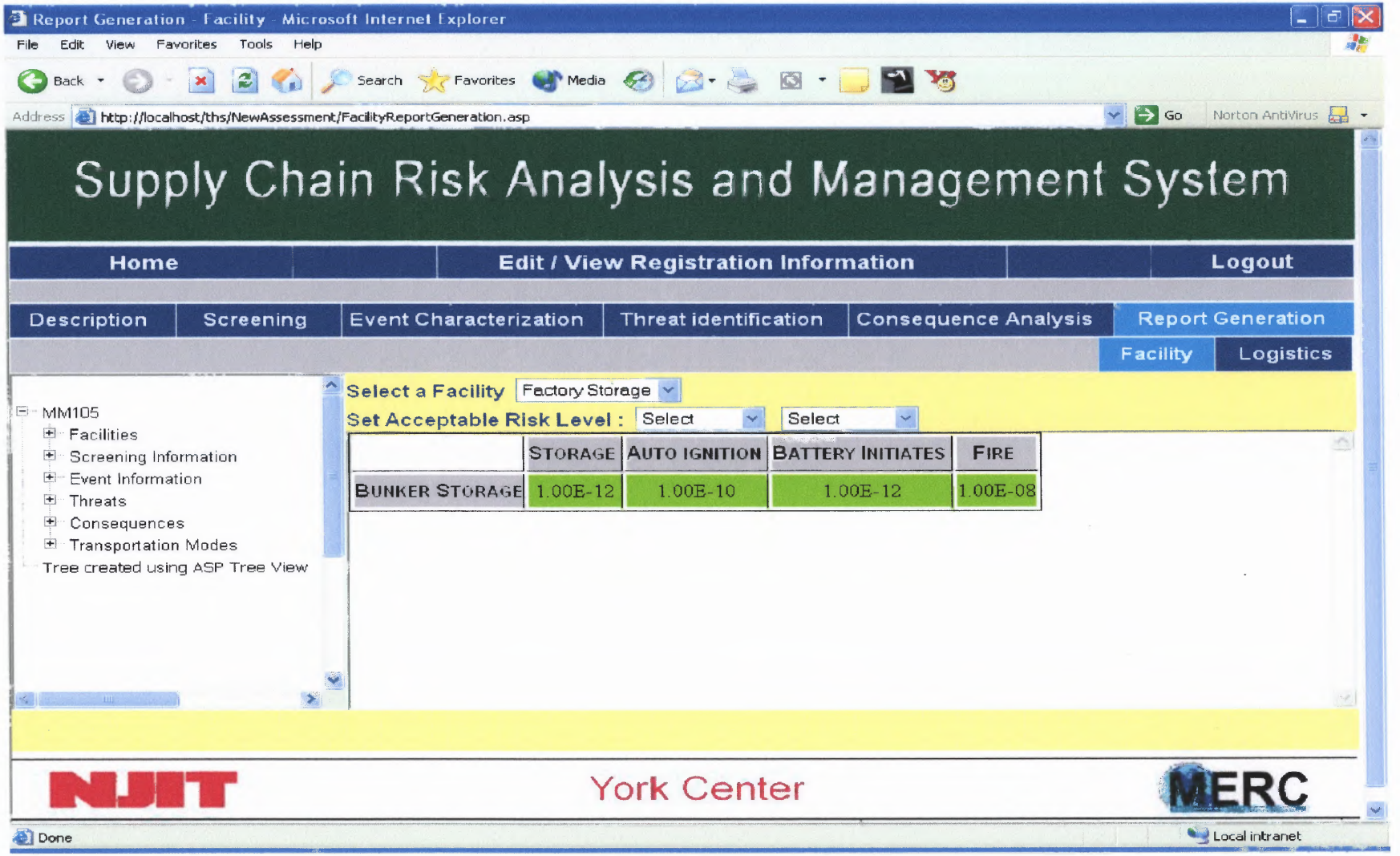

Figure 4.13 Facility Report Generation.

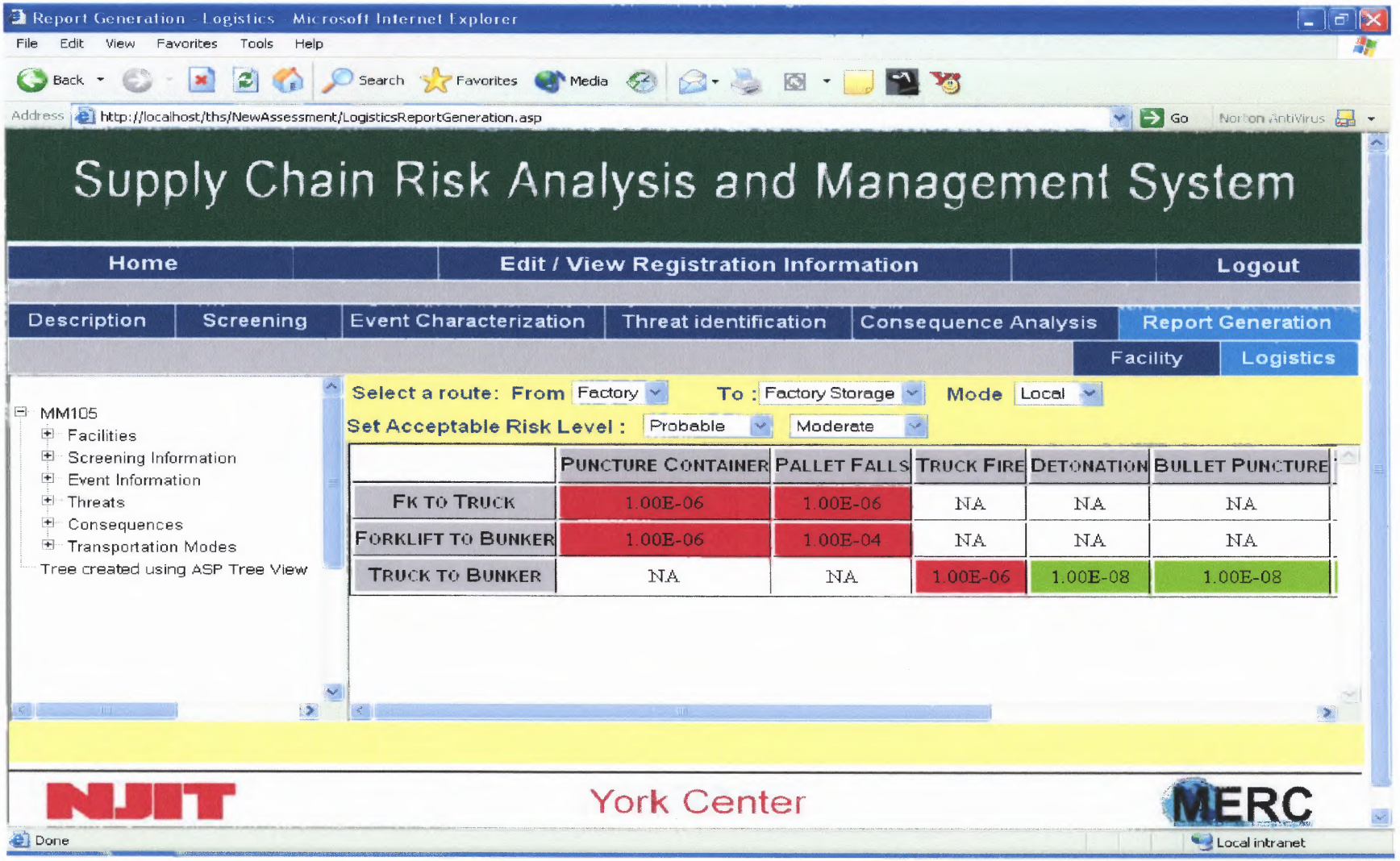

Figure 4.14 Logistics Link Report Generation.

CHAPTER 5

CASE STUDY

5.1 Case Study – Highly Explosive Product

The risk analysis methodology developed in this research work is tested with a case study provided by Picatinny Arsenal. The case study deals with the supply chain of a Dual-Purpose Improved Conventional Munition (DPICM) cartridge. The supply chain starts with a manufacturing plant and ends at a forward field point where the cartridge is used. The purpose of this study is to identify high-risk threats, which may occur during the lifecycle of the product.

5.2 Hardware Description [55]

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 submunition 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 grenade uses a new Electronic Self Destruct Fuse. This fuse will reduce the number of DPICM duds in the battlefield. Also, the fuse will be reasonably safe for friendly maneuvering or advancing troops.

5.3 Supply Chain Description

The supply chain of the DPICM cartridge consists of nine facilities and twenty-three logistics links. Facilities are of two types: production plant or storage facility.

Facilities considered in the supply chain are:

- Factory
- Factory Storage
- Proving Ground
- CONUS Storage (Continental United States)
- OCONUS Storage (Outside Continental United States)
- Pre-Pro Ship (Pre-Position Ship)
- ASP (Ammunition Supply Point)
- Demil
- Gunfire

The logistics links are listed in Table 5.1. The supply chain model is depicted graphically in Figure 5.1. In this supply chain, the explosive product is manufactured at the factory and shipped and stored at Factory storage, CONUS Storage, OCONUS Storage, Proving Ground and Pre-Pro Ship using trucks and rail. From these storage points, the product is further shipped to ASP and Demil facility. From Ammunition Supply Point, the product is shipped to a forward point where it is deployed. Supply lines are also maintained between, CONUS, OCONUS and pre-pro ship to ensure supply continuity.

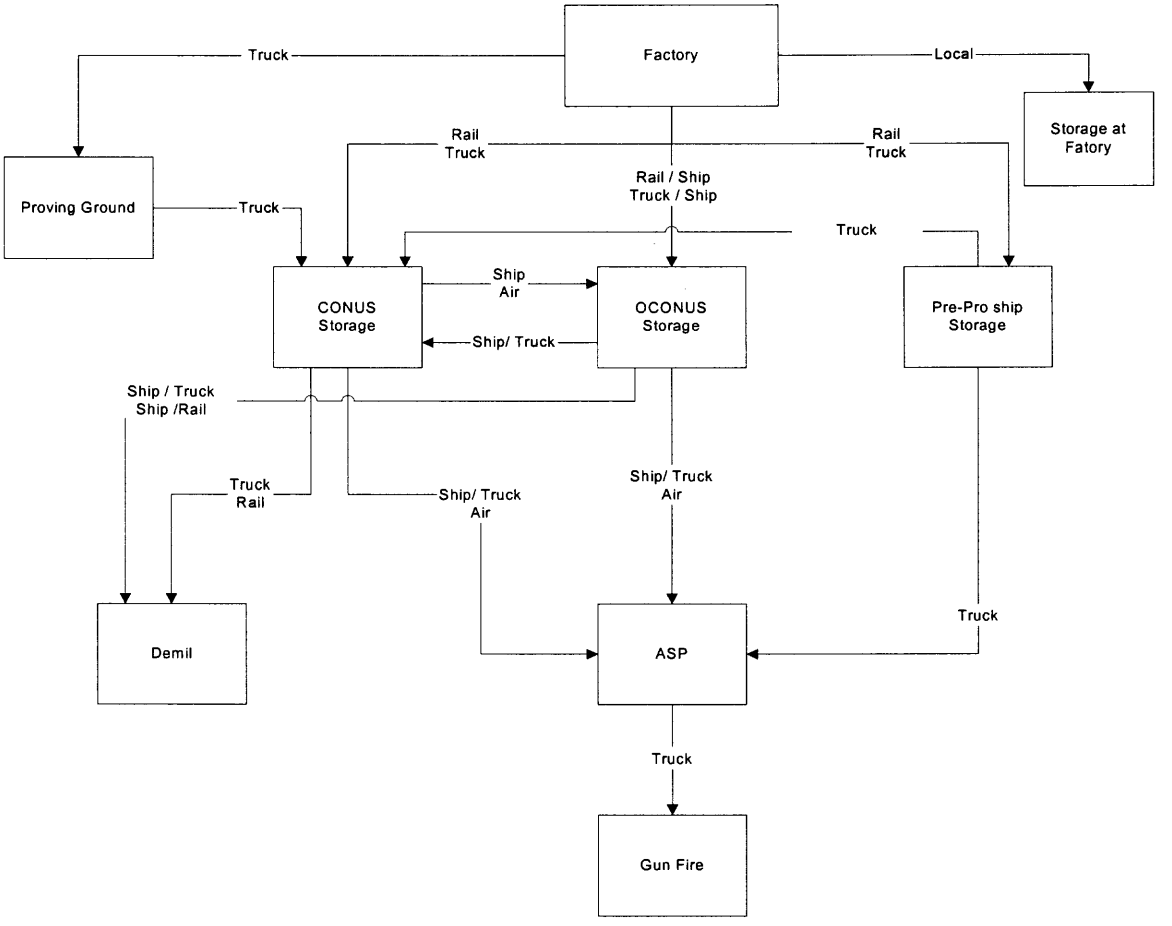

Figure 5.1 Supply Chain of DPICM Cartridge.

Table no 5.1 List of Logistics Links.

Sl No	From	To	Transportation Mode
1	Factory	Factory Storage	Local
2	Factory	CONUS Storage	Rail
3	Factory	CONUS Storage	Truck
4	Factory	OCONUS Storage	Rail/Ship
5	Factory	OCONUS Storage	Truck/Ship
6	Factory	Pre-Pro Ship	Rail
7	Factory	Pre-Pro Ship	Truck
8	Factory	Proving Ground	Truck
9	CONUS Storage	OCONUS Storage	Ship
10	CONUS Storage	OCONUS Storage	Air
11	Pre-Pro Ship	CONUS Storage	Truck
12	Pre-Pro Ship	ASP	Truck
13	CONUS Storage	ASP	Truck/Ship
14	CONUS Storage	ASP	Air
15	OCONUS Storage	ASP	Truck/Ship
16	OCONUS Storage	ASP	Air
17	OCONUS Storage	CONUS Storage	Truck/Ship
18	CONUS Storage	Demil	Truck
19	ASP	Gun Fire	Truck
20	OCONUS Storage	Demil	Rail/Ship
21	OCONUS Storage	Demil	Truck/Ship
22	CONUS Storage	Demil	Rail
23	Proving Ground	CONUS Storage	Truck

In this study, it is assumed that all the facilities as well as logistics links require a risk assessment as information characterizing each of the facility and logistics link was not provided. Also, since each of the stage involves a highly explosive product, it is imperative that each entity will require a risk assessment. Table 5.2 lists the various activities and corresponding threats in facility – Factory. Also, the duration of activity and activity type are listed in the table. The activities for the rest facilities and logistics links are added in Appendix-A as tables.

Table 5. 2 Threat List 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

5.4 Threat Assessment

Each of the identified threat is assessed to estimate the frequency of occurrence and severity of consequences. The estimated frequency of occurrence values is given along with the threats in Table 5.2. For estimating the severity of consequences, the threats are grouped by activity type and then assessed. Table 5.3 and 5.4 list the consequences for facilities and logistics links. The consequence values have been obtained either through simulations or subjective knowledge.

The acceptable risk level is set at Occasional and Moderate, which is equivalent to a value of 10^{-10}. The risk assessment reports generated for facilities Factory and Factory Storage are shown in Table 5.5 to 5.6. Reports of the rest of the facilities and logistics links are given in Appendix B. The rows and columns of the table represent the activities

and threat, respectively. If a threat does not exist against an activity then "NA" in the cell indicates it. Otherwise, the risk factor is calculated and displayed. Red color cells indicate that the risk level is not acceptable, while green suggests that risk level is acceptable.

Table 5.3 List of Facility Consequences

Activity Type	Threat	Consequence
Material Handling	Bullet Punctures Container	Critical
	Detonation	Critical
	Fire Accident	Catastrophic
	Forklift Tines Puncture	Marginal
	Gunfire from Aircraft	Critical
	Missile Attack	Critical
	Pallet Falls	Marginal
	Pierside Fire	Catastrophic
	Reaction with Items	Catastrophic
	Shaped Charge Attack	Critical
	Truck Accident	Marginal
	Truck Fire	Catastrophic
Storage	Fire	Catastrophic
	Gunfire from Aircraft	Critical
	Missile Attack	Critical
	Reaction with Items	Catastrophic
	Shaped Charge Attack	Critical
	Auto ignition	Catastrophic
	Battery Initiates	Catastrophic
	Detonation	Catastrophic
	Fire	Catastrophic
	Pallet Falls	Marginal
	Storage	Critical

Table 5.4 List of Logistics Consequences

Activity	Threat	Consequence
Air Transportation	Detonation	Catastrophic
	Pallet Falls	Marginal
	Reaction with Cargo	Catastrophic
	Takeoff or Landing Fire	Catastrophic
Land Transportation	Bullet Punctures Container	Marginal
	Detonation	Catastrophic
	Fire	Catastrophic
	Fire Accident	Catastrophic
	Forklift Tines Puncture	Marginal
	Gunfire From Aircraft	Critical
	Missile Attack	Critical
	Pallet Falls	Marginal
	Pierside Fire	Catastrophic
	Puncture Container	Marginal
	Rail Accident	Critical
	Rail Fire	Catastrophic
	Reaction with Cargo	Catastrophic
	Reaction with Items	Catastrophic
	Shaped Charge Attack	Critical
	Sniper Bullet	Critical
	Truck Accident	Marginal
	Truck Fire	Catastrophic
Ship Transportation	Fire	Catastrophic
	Forklift Tines Puncture	Marginal
	Gunfire From Aircraft	Critical
	Pallet Falls	Marginal
	Pierside Fire	Catastrophic
	Reaction with Cargo	Catastrophic
	Sniper Bullet	Critical

Table 5.5 Risk Assessment Report for Factory

	Forklift Tines Puncture	Pallet Falls	
Forklift to Rail	1.00E-12	1.00E-10	
Forklift to Truck	1.00E-12	1.00E-10	

Table 5.6 Risk Assessment Report for Factory Storage

	Auto Ignition	Battery Initiates	Fire
Bunker Storage	1.00E-08	1.00E-08	1.00E-08
Forklift to Bunker	NA	NA	NA

	Forklift Tines Puncture container	Pallet Falls	Storage
Bunker Storage	NA	NA	1.00E-10
Forklift to Bunker	1.00E-12	1.00E-10	NA

5.5 Results

Risk assessment reports indicate that any event resulting in a detonation pose a high risk. As long as the grenade does not detonate, the risk level is acceptable. Also, all activities at Ammunition Supply Point and Gunfire pose a high risk due to proximity to the adversary. Even for these sites, the acceptable risk level is set at Occasional and Moderate. However, the acceptable risk level has to be relaxed considering the possibility of a mishap is always high in a battle field.

Since any event triggering the grenade is unacceptable, a new safety trip has to be designed to be placed along with the grenade fuse. In case of an unwanted event, the safety trip will deactivate the grenade preventing an explosion.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

Supply chain security is of utmost importance to sustain business in an uncertain and high-risk business environment. Recent events highlighted the vulnerabilities of the supply chains and proved that the current business continuity plans do not provide adequate security. Since, a supply chain is a highly complex system of interdependent entities, the current risk assessment techniques are inadequate to assess risks in a supply chain. New decisions tools are required that will help development on business continuity plans based on a complete risk assessment of the supply chain. Also, none of the current risk analysis technique is capable of assessing risks in a supply chain due to interdependencies among businesses.

A supply chain risk assessment technique is proposed in this thesis that is capable of identifying high-risk threats in a supply chain. The methodology has been validated with a real case study provided by Picatinny Arsenal, the United States Army Armament Research, Development and Engineering Center.

The results show that the methodology is efficient. Also, results show that operational and strategic decisions based on the risk estimates will help in more rational decision-making and appropriate resource allocation. In the case study, for example, any event not leading to a fire is not of high significance. Resources need not be diverted to prevent the occurrence of such an event. However, any event that leads to a fire needs to be avoided and the asset / activity have to be safeguarded.

The fault tree analysis approach shows that supply chain interrelationships among businesses can be accounted while calculating the frequency of occurrence value. The use of qualitative probability values is intuitive and offers an easy method to assign the frequency of occurrence value. High data necessity has been one of the problems with Bayesian networks and other inference techniques. The logical rules formulated indicate that the data requirement and data entry can be relaxed.

Preliminary results indicate that the methodology can be applied to any supply chain as they can be divided into production and logistics units. The system guides the risk assessment process and estimates the risk factor associated with each activity – threat pair. Also, the system is one of its kinds built upon Military Standards to estimate risk in a supply chain.

6.2 Future Work

This research work is a major step toward the development of the next generation risk management tool. Roshan Pai, working collaboratively within the MERC research team, is developing a safeguard analysis module that can directly integrate with the risk assessment system developed in this thesis. Novel techniques like gaming theory and fuzzy logic are being considered to identify the most appropriate safeguard.

The utility of inference techniques for assessing risk in a supply chain is still not clear. Even though Bayesian networks have the capability to account for interrelationships, their drawbacks are not yet known. Different inference techniques need to be used and results analyzed to study their relative benefits and drawbacks. One of the major drawbacks in such an analysis is that the risk values are conservative and are not on an absolute scale. This makes the study much more complex.

The system needs to be further developed for an automated monitoring of the supply chain. Fault tree structures and inference engines need to further studied and better integrated to allow a real time risk analysis. Also, data sources need to be identified and integrated to the system so that system automatically collects new information and updates risk levels.

APPENDIX A
(Continued)

Table A.3 Threat List 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 Punctures Container Truck Accident	Remote Remote Remote Remote	Material Handling

Table A.4 Threat List for OCONUS Storage

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Forklift to Truck	1.2	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling
Forklift to Bunker	1.2	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling
Bunker Storage	61,320	Storage Auto ignition Battery Initiates Fire Reaction with Items	Remote Remote Remote Remote Remote	Storage

APPENDIX A
(Continued)

Table A.5 Threat List for Pre-Pro Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Ship Storage	0.3	Fire Reaction with Items Detonation	Remote Remote Remote	Storage

Table A.6 Threat List for Ammunition Supply Point

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Material handling to Storage	5	Gunfire from Aircraft Missile Attack Shaped Charge Attack Fire Accident Reaction with items	Probable Probable Probable Probable Probable	Material Handling
Hostile Storage	4392	Gunfire from Aircraft Missile Attack Shaped Charge Attack Fire Accident Reaction with items	Probable Probable Probable Probable Probable	Storage

Table A.7 Threat List for Demil

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Forklift to Demil	0.3	Forklift Tines Puncture Container Pallets Falls	Probable Occasional	Material Handling
Bunker Storage	8760	Storage Auto ignition Battery Initiates Fire Reaction with Items	Remote Remote Remote Remote Remote	Storage

APPENDIX A
(Continued)

Table A.8 Threat List for Factory to Factory Storage: Local Transportation

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Bunker	0.3	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

Table A.9 Threat List Factory to CONUS Storage: Rail

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Rail to CONUS	336	Rail Fire Detonation Bullet Punctures Container Rail Accident	Remote Remote Remote Remote	Land Transportation

Table A.10 Threat List for Factory to CONUS Storage: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to CONUS	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.11 Threat List for Factory to OCONUS Storage: Rail/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Rail to Port	336	Rail Fire Detonation Bullet Punctures Container Rail Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ship	1	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo	Probable Occasional Remote Remote	Land Transportation
Crane/ Forklift from Ship	1	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to OCONUS	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.12 Threat List for Factory to OCONUS Storage: Truck/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo	Probable Occasional Remote Remote	Land Transportation
Ammo ship to OCONUS Port	720	Pallet Falls Fire Reaction with Cargo	Occasional Remote Remote	Land Transportation
Crane/ Forklift from Ship	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to OCONUS	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

Table A.13 Threat List for Factory to Pre-Pro Ship: Rail

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Rail to Port	336	Rail Fire Detonation Bullet Punctures Container Rail Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ship	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.14 Threat List for Factory to Pre-Pro Ship: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/Crane to Ship	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation

Table A.15 Threat List for Factory to Proving Ground: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Proving	168	Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

Table A.16 Threat List for Proving Ground to CONUS Storage: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to CONUS	0.3	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Material Handling

APPENDIX A
(Continued)

Table A.17 Threat List for CONUS Storage to OCONUS Storage: Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ship	1	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo	Probable Occasional Remote Remote	Land Transportation
Ammo ship to OCONUS Port	720	Pallet Falls Fire Reaction with Cargo	Remote Remote Remote	Ship Transportation
Crane/ Forklift from Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to OCONUS	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.18 Threat List for CONUS Storage to OCONUS Storage: Air

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Airport	48	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift to Plane	0.3	Forklift Tines Punctures Container Bullet Punctures Container Pallet Falls	Probable Remote Occasional	Land Transportation
Plane to OCONUS	24	Takeoff/Landing Fire Reaction with Cargo Detonation	Remote Remote Remote	Air Transportation
Forklift to Truck	0.3	Forklift Tines Punctures Container Pallet Falls	Probable Occasional	Land Transportation
Truck to OCONUS	48	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

Table A.19 Threat List for Pre-Pro Ship to CONUS Storage: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Crane/ Forklift to Truck	1	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to CONUS	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.20 Threat List for Pre-Pro Ship to ASP: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Crane/ Forklift to Truck	1	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to ASP	48	Gunfire from Aircraft Pallet Falls Missile Attack Shaped Charge Attack Fire Accident Reaction with Items	Probable Probable Probable Probable Probable Probable	Land Transportation

APPENDIX A
(Continued)

Table A.21 Threat List for CONUS Storage to ASP: Truck/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Probable Probable Probable Probable	Land Transportation
Ammo ship to ASP Port	720	Pallet Falls Fire Reaction with Cargo Missile Attack Gunfire from Aircraft	Occasional Remote Remote Probable	Ship Transportation
Crane/ Forklift to Truck	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Remote Occasional Remote Remote Remote	Land Transportation
Truck to ASP	48	Gunfire from Aircraft Pallet Falls Missile Attack Shaped Charge Attack Fire Accident Reaction with Items	Probable Probable Probable Probable Probable Probable	Land Transportation
Forklift/Crane to Ammo Ship	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo	Probable Occasional Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.22 Threat List for CONUS Storage to ASP: Air

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Airport	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift to Plane	0.3	Forklift Tines Punctures Container Bullet Punctures Container Pallet Falls	Probable Remote Occasional	Land Transportation
Plane to ASP Airport	24	Takeoff/Landing Fire Reaction with Cargo Detonation	Remote Remote Remote	Air Transportation
Forklift to Truck	0.3	Forklift Tines Punctures Container Pallet Falls	Probable Occasional	Land Transportation
Truck to ASP	168	Gunfire from Aircraft Pallet Falls Missile Attack Shaped Charge Attack Fire Accident Reaction with items	Probable Probable Probable Probable Probable Probable	Land Transportation

APPENDIX A
(Continued)

Table A.23 Threat List for OCONUS Storage to ASP: Truck/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ammo Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo	Probable Occasional Remote Remote	Land Transportation
Ammo Ship to ASP Port	720	Pallet Falls Fire Reaction with Cargo Missile Attack Gunfire from Aircraft	Probable Occasional Probable Probable Probable	Ship Transportation
Crane/ Forklift to Truck	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to ASP	48	Gunfire from Aircraft Pallet Falls Missile Attack Shaped Charge Attack Fire Accident Reaction with Items	Probable Probable Probable Probable Probable Probable	Land Transportation

APPENDIX A
(Continued)

Table A.24 Threat List for OCONUS Storage to ASP: Air

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Airport	168	Truck fire Bullet Punctures Container Truck Accident	Remote Probable Remote	Land Transportation
Forklift /Truck to Plane	0.3	Forklift Tines Puncture Container Pallet Falls Bullet Punctures Container	Probable Occasional Remote	Land Transportation
Plane to ASP Airport	24	Takeoff/ Landing Fire Reaction with Cargo Detonation	Remote Remote Remote	Air Transportation
Forklift to Truck	0.3	Forklift Tines Puncture Container Pallet Falls	Probable Occasional	Land Transportation
Truck to ASP	168	Gunfire from Aircraft Pallet Falls Missile Attack Shaped Charge Attack Fire Accident Reaction with Items	Probable Probable Probable Probable Probable Probable	Land Transportation

APPENDIX A
(Continued)

Table A.25 Threat List for OCONUS Storage to CONUS Storage: Truck/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/ Crane to Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Ammo ship to OCONUS	720	Pallet Falls Fire Reaction with Cargo	Occasional Remote Remote	Ship Transportation
Crane/ Forklift from Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to CONUS	168	Truck Fire Bullet Punctures Container Truck Accident	Remote Remote Remote	Land Transportation

Table A.26 Threat List for CONUS Storage to Demil: Truck

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Demil	0.3	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

APPENDIX A
(Continued)

Table A.27 Threat List for CONUS Storage to Demil: Rail

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Rail to Demil	336	Rail Fire Detonation Bullet Punctures Container Rail Accident	Remote Remote Remote Remote	Land Transportation

Table A.28 Threat List for OCONUS Storage to Demil: Truck/Ship

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Occasional Remote Remote Occasional	Land Transportation
Forklift/ Cr to Ship	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Occasional Probable Remote Remote Remote	Land Transportation
Ammo ship to CONUS	720	Pallet Falls Fire Reaction with Cargo	Occasional Remote Remote	Ship Transportation
Crane/ Forklift to Truck	1.0	Forklift Tines Puncture Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Occasional Probable Remote Remote Remote	Land Transportation
Truck to Demil	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Probable Occasional	Land Transportation

APPENDIX A
(Continued)

Table A.29 Threat List for OCONUS Storage to Demil: Ship/Rail

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Truck to Port	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation
Forklift/Crane to Ship	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Ammo ship to CONUS Port	720	Pallet Falls Fire Reaction with Cargo	Occasional Remote Remote	Ship Transportation
Crane/ Forklift to Truck	1.0	Forklift Tines Punctures Container Pallet Falls Pierside Fire Reaction with Cargo Sniper Bullet	Probable Occasional Remote Remote Remote	Land Transportation
Truck to Demil	168	Truck Fire Detonation Bullet Punctures Container Truck Accident	Remote Remote Remote Remote	Land Transportation

Table A.30 Threat List for ASP to Gun Fire: Ammo Transport Vehicle

Activity	Duration (Hrs)	Threats	Frequency	Activity Type
Ammo Transport Vehicle to Gun	Included in **	Gunfire from Aircraft Ammo Dropped Missile Attack Shaped Charge Attack Fire Reaction with Items	Probable Probable Probable Probable Probable	Land Transportation

APPENDIX B

RISK ASSESSMENT REPORTS

Table B.1 Risk Assessment Report for Proving Ground

	Auto Ignition	Battery Initiates	Fire
Bunker Storage	1.00E-08	1.00E-08	1.00E-08
Forklift to Proving	NA	NA	NA
Forklift to Truck	NA	NA	NA

	Forklift Tines Puncture Container	Pallet Falls	Reaction with Items
Bunker Storage	NA	NA	1.00E-08
Forklift to Proving	1.00E-12	1.00E-10	NA
Forklift to Truck	1.00E-12	1.00E-10	NA

	Storage		
Bunker Storage	1.00E-10		
Forklift to Proving	NA		
Forklift to Truck	NA		

APPENDIX B
(Continued)

Table B.2 Risk Assessment Report for CONUS Storage

	Auto Ignition	Battery Initiates	Bullet Punctures Container
Bunker Storage	1.00E-08	1.00E-08	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-08	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-08	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

APPENDIX B
(Continued)

Table B.2 Risk Assessment Report for CONUS Storage (Continued)

	Reaction with Items	Storage	Truck Accident
Bunker Storage	1.00E-08	1.00E-10	NA
Forklift to Bunker	1.00E-08	NA	NA
Forklift to Rail	NA	NA	NA
Forklift to Truck	NA	NA	NA
Truck to Bunker	NA	NA	1.00E-14

	Truck Fire		
Bunker Storage	NA		
Forklift to Bunker	NA		
Forklift to Rail	NA		
Forklift to Truck	NA		
Truck to Bunker	1.00E-08		

Table B.3 Risk Assessment Report for OCONUS Storage

	Auto Ignition	Battery Initiates	Fire
Bunker Storage	1.00E-08	1.00E-08	1.00E-08
Forklift to Bunker	NA	NA	NA
Forklift to Truck	NA	NA	NA

	Forklift Tines Puncture container	Pallet Falls	Reaction with Items
Bunker Storage	NA	NA	1.00E-08
Forklift to Bunker	1.00E-12	1.00E-10	NA
Forklift to Truck	1.00E-12	1.00E-10	NA

APPENDIX B
(Continued)

Table B.3 Risk Assessment Report for OCONUS Storage (Continued)

	Storage		
Bunker Storage	1.00E-10		
Forklift to Bunker	NA		
Forklift to Truck	NA		

Table B.4 Risk Assessment Report for Pre-Pro Ship

	Detonation	Fire	Pallet Falls
Ship Storage	1.00E-08	1.00E-08	1.00E-10

	Reaction with Items		
Ship Storage	1.00E-08		

Table B.5 Risk Assessment Report for Ammunition Supply Point

	Fire	Fire Accident	Gunfire from Aircraft
Hostile Storage	1.00E-06	NA	1.00E-08
Material Handling to Hostile Storage	NA	1.00E-06	1.00E-08

	Missile Attack	Reaction with Items	Shaped Charge Attack
Hostile Storage	1.00E-08	1.00E-06	1.00E-08
Material Handling to Hostile Storage	1.00E-08	1.00E-06	1.00E-08

APPENDIX B
(Continued)

Table B.7 Risk Assessment Report for Demil

	Auto ignition	Battery Initiates	Fire
Bunker Storage	1.00E-08	1.00E-08	1.00E-08
Forklift to Demil	NA	NA	NA

	Forklift Tines Puncture Container	Pallet Falls	Reaction with Items
Bunker Storage	NA	NA	1.00E-08
Forklift to Demil	1.00E-14	1.00E-10	NA

	Storage		
Bunker Storage	1.00E-10		
Forklift to Demil	NA		

Table B.8 Risk Assessment Report for Factory to Factory Storage: Local

	Truck Fire	Detonation	Bullet Punctures Container
Truck to Bunker	1.00E-08	1.00E-08	1.00E-14

	Truck Accident		
Truck to Bunker	1.00E-12		

APPENDIX B
(Continued)

Table B.9 Risk Assessment Report for Factory to CONUS Storage: Rail

	Bullet Punctures Container	Detonation	Rail Accident
Rail to CONUS	1.00E-12	1.00E-08	1.00E-10

	Rail Fire		
Rail to CONUS	1.00E-08		

Table B.10 Risk Assessment Report for Factory to CONUS Storage: Truck

	Bullet Punctures Container	Detonation	Truck Accident
Truck to CONUS	1.00E-12	1.00E-08	1.00E-12

	Truck Fire		
Truck to CONUS	1.00E-8		

APPENDIX B
(Continued)

Table B.11 Risk Assessment Report for Factory to OCONUS Storage: Rail/Ship

	Bullet Punctures Container	Detonation	Forklift Tines Puncture Container
Ammo ship to OCONUS Port	NA	NA	NA
Crane/ Forklift from Ship	NA	NA	1.00E-08
Forklift/Crane to Ship	NA	NA	1.00E-08
Rail to Port	1.00E-12	1.00E-08	NA
Truck to OCONUS	1.00E-12	1.00E-08	NA

	Pallet Falls	Pierside Fire	Rail Accident
Ammo ship to OCONUS Port	1.00E-12	NA	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-08	NA
Forklift/Crane to Ship	1.00E-08	1.00E-08	NA
Rail to Port	NA	NA	1.00E-10
Truck to OCONUS	NA	NA	NA

	Rail Fire	Reaction with Cargo	Sniper Bullet
Ammo ship to OCONUS Port	NA	1.00E-08	NA
Crane/ Forklift from Ship	NA	1.00E-08	1.00E-10
Forklift/Crane to Ship	NA	1.00E-08	NA
Rail to Port	1.00E-08	NA	NA
Truck to OCONUS	NA	NA	NA

APPENDIX B
(Continued)

Table B.11 Risk Assessment Report for Factory to OCONUS Storage: Rail/Ship (Continued)

	Truck Accident	Truck Fire	Fire
Ammo ship to OCONUS Port	NA	NA	1.00E-08
Crane/ Forklift from Ship	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Rail to Port	NA	NA	NA
Truck to OCONUS	1.00E-12	1.00E-08	NA

Table B.12 Risk Assessment Report for Factory to OCONUS Storage: Truck/Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to OCONUS Port	NA	NA	1.00E-08
Crane/ Forklift from Ship	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to OCONUS	1.00E-12	1.00E-08	NA
Truck to Port	1.00E-12	1.00E-08	NA

	Forklift Tines Puncture Container	Pallet Falls	Pierside Fire
Ammo ship to OCONUS Port	NA	1.00E-12	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-12	1.00E-08
Forklift/Crane to Ship	1.00E-08	1.00E-12	1.00E-08
Truck to OCONUS	NA	NA	NA
Truck to Port	NA	NA	NA

APPENDIX B
(Continued)

Table B.12 Risk Assessment Report for Factory to OCONUS Storage: Truck/Ship (Continued)

	Reaction with Cargo	Sniper Bullet	Truck Accident
Ammo ship to OCONUS Port	1.00E-08	NA	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-10	NA
Forklift/Crane to Ship	1.00E-08	NA	NA
Truck to OCONUS	NA	NA	1.00E-12
Truck to Port	NA	NA	1.00E-12

	Truck Fire		
Ammo ship to OCONUS Port	NA		
Crane/ Forklift from Ship	NA		
Forklift/Crane to Ship	NA		
Truck to OCONUS	1.00E-08		
Truck to Port	1.00E-06		

APPENDIX B
(Continued)

Table B.13 Risk Assessment Report for Factory to Pre-Pro Ship: Rail

	Bullet Punctures Container	Detonation	Forklift Tines Puncture Container
Forklift/Crane to Ship	NA	NA	1.00E-08
Rail to Port	1.00E-12	1.00E-08	NA

	Pallet Falls	Pierside Fire	Reaction with Cargo
Forklift/Crane to Ship	1.00E-12	1.00E-08	1.00E-08
Rail to Port	NA	NA	NA

	Sniper Bullet	Rail Accident	Rail Fire
Forklift/Cr to Ship	1.00E-10	NA	NA
Rail to Port	NA	1.00E-12	1.00E-08

Table B.14 Risk Assessment Report for Factory to Pre-Pro Ship: Truck

	Bullet Punctures Container	Detonation	Forklift Tines Puncture Container
Forklift/Cr to Ship	NA	NA	1.00E-08
Truck to Port	1.00E-12	1.00E-08	NA

	Pallet Falls	Pierside Fire	Reaction with Cargo
Forklift/Crane to Ship	1.00E-12	1.00E-08	1.00E-08
Truck to Port	NA	NA	NA

APPENDIX B
(Continued)

Table B.14 Risk Assessment Report for Factory to Pre-Pro Ship: Truck (Continued)

	Sniper Bullet	Truck Accident	Truck Fire
Forklift/Crane to Ship	1.00E-10	NA	NA
Truck to Port	NA	1.00E-12	1.00E-08

Table B.15 Risk Assessment Report for Factory to Proving Ground: Truck

	Bullet Punctures Container	Detonation	Truck Fire
Truck to Proving	1.00E-12	1.00E-08	1.00E-08

	Truck Accident		
Truck to Proving	1.00E-12		

Table B.16 Risk Assessment Report for Proving Ground to CONUS: Truck

	Bullet Punctures Container	Detonation	Truck Fire
Truck to Proving	1.00E-12	1.00E-08	1.00E-08

	Truck Accident		
Truck to Proving	1.00E-12		

APPENDIX B
(Continued)

Table B.17 Risk Assessment Report for CONUS Storage to OCONUS Storage: Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to OCONUS Port	NA	NA	1.00E-08
Crane/ Forklift from Ship	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to OCONUS	1.00E-12	1.00E-08	NA
Truck to Port	1.00E-12	1.00E-08	NA

	Forklift Tines Puncture Container	Pallet Falls	Pierside Fire
Ammo ship to OCONUS	NA	1.00E-12	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-08	1.00E-08
Forklift/Crane to Ship	1.00E-08	1.00E-08	1.00E-08
Truck to OCONUS	NA	NA	NA
Truck to Port	NA	NA	NA

	Reaction with Cargo	Sniper Bullet	Truck Accident
Ammo ship to OCONUS	1.00E-08	NA	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-10	NA
Forklift/Crane to Ship	1.00E-08	NA	NA
Truck to OCONUS	NA	NA	1.00E-12
Truck to Port	NA	NA	1.00E-12

APPENDIX B
(Continued)

Table B.17 Risk Assessment Report for CONUS Storage to OCONUS Storage: Ship (Continued)

	Truck Fire		
Ammo ship to OCONUS	NA		
Crane/ Forklift from Ship	NA		
Forklift/Crane to Ship	NA		
Truck to OCONUS	1.00E-08		
Truck to Port	1.00E-08		

Table B.18 Risk Assessment Report for CONUS Storage to OCONUS Storage: Air

	Bullet Punctures Container	Detonation	Forklift Tines Puncture Container
Forklift to Plane	1.00E-08	NA	1.00E-10
Forklift to Truck	NA	NA	1.00E-10
Plane to OCONUS	NA	1.00E-08	NA
Truck to Airport	1.00E-12	1.00E-08	NA
Truck to OCONUS	1.00E-12	1.00E-08	NA

APPENDIX B
(Continued)

Table B.18 Risk Assessment Report for CONUS Storage to OCONUS Storage: Air (Continued)

	Pallet Falls	Reaction with Cargo	Takeoff/Landing Fire
Forklift to Plane	1.00E-12	NA	NA
Forklift to Truck	1.00E-08	NA	NA
Plane to OCONUS	NA	1.00E-08	1.00E-08
Truck to Airport	NA	NA	NA
Truck to OCONUS	NA	NA	NA

	Truck Accident	Truck Fire	
Forklift to Plane	NA	NA	
Forklift to Truck	NA	NA	
Plane to OCONUS	NA	NA	
Truck to Airport	1.00E-12	1.00E-08	
Truck to OCONUS	1.00E-12	1.00E-08	

Table B.19 Risk Assessment Report for Pre-Pro Ship to CONUS Storage: Truck

	Bullet Punctures Container	Detonation	Forklift Tines Puncture Container
Crane/ Forklift to Truck	NA	NA	1.00E-08
Truck to CONUS	1.00E-12	1.00E-08	NA

	Pallet Falls	Pierside Fire	Reaction with Cargo
Crane/ Forklift to Truck	1.00E-08	1.00E-08	1.00E-08
Truck to CONUS	NA	NA	NA

APPENDIX B
(Continued)

Table B.19 Risk Assessment Report for Pre-Pro Ship to CONUS Storage: Truck (Continued)

	Sniper Bullet	Truck Accident	Truck Fire
Crane/ Forklift to Truck	1.00E-10	NA	NA
Truck to CONUS	NA	1.00E-12	1.00E-08

Table B.20 Risk Assessment Report for Pre-Pro to Ship ASP: Truck

	Fire Accident	Forklift Tines Puncture Container	Gunfire from Aircraft
Crane/ Forklift to Truck	NA	1.00E-08	NA
Truck to ASP	1.00E-06	NA	1.00E-08

	Missile Attack	Pallet Falls	Pierside Fire
Crane/ Forklift to Truck	NA	1.00E-10	1.00E-08
Truck to ASP	1.00E-08	1.00E-10	NA

	Reaction with Cargo	Reaction with Items	Shaped Charge Attack
Crane/ Forklift to Truck	1.00E-08	NA	NA
Truck to ASP	NA	1.00E-06	1.00E-08

	Sniper Bullet		
Crane/ Forklift to Truck	1.00E-10		
Truck to ASP	NA		

APPENDIX B
(Continued)

Table B.21 Risk Assessment Report for CONUS Storage to ASP: Truck/Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to ASP	NA	NA	1.00E-08
Crane/ Forklift to Truck	NA	NA	NA
Forklift/Cr to Ship	NA	NA	NA
Truck to ASP	NA	NA	NA
Truck to Port	1.00E-12	1.00E-10	NA

	Missile Attack	Pallet Falls	Pierside Fire
Ammo ship to ASP	1.00E-08	1.00E-12	NA
Crane/ Forklift to Truck	NA	1.00E-12	1.00E-08
Forklift/Cr to Ship	NA	1.00E-08	1.00E-08
Truck to ASP	1.00E-08	1.00E-10	NA
Truck to Port	NA	NA	NA

	Reaction with Cargo	Reaction with Items	Shaped Charge Attack
Ammo ship to ASP	1.00E-08	NA	NA
Crane/ Forklift to Truck	1.00E-08	NA	NA
Forklift/Crane to Ship	1.00E-08	NA	NA
Truck to ASP	NA	1.00E-06	1.00E-08
Truck to Port	NA	NA	NA

APPENDIX B
(Continued)

Table B.21 Risk Assessment Report for CONUS Storage to ASP: Truck/Ship (Continued)

	Sniper Bullet	Truck Accident	Truck Fire
Ammo ship to ASP	NA	NA	NA
Crane/ Forklift to Truck	1.00E-10	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to ASP	NA	NA	NA
Truck to Port	NA	1.00E-12	1.00E-06

	Gunfire From Aircraft		
Ammo ship to ASP	1.00E-8		
Crane/ Forklift to Truck	NA		
Forklift/Crane to Ship	NA		
Truck to ASP	1.00E-8		
Truck to Port	NA		

Table B.22 Risk Assessment Reports for CONUS Storage to ASP: Air

	Bullet Punctures Container	Detonation	Fire Accident
Forklift to Plane	1.00E-08	NA	NA
Forklift to Truck	NA	NA	NA
Plane to ASP	NA	NA	NA
Truck to Airport	1.00E-12	1.00E-08	NA
Truck to ASP	NA	NA	1.00E-06

APPENDIX B
(Continued)

Table B.22 Risk Assessment Reports for CONUS Storage to ASP: Air (Continued)

	Forklift Tines Puncture Container	Gunfire From Aircraft	Missile Attack
Forklift to Plane	1.00E-10	NA	NA
Forklift to Truck	1.00E-10	NA	NA
Plane to ASP	NA	NA	NA
Truck to Airport	NA	NA	NA
Truck to ASP	NA	1.00E-08	1.00E-08

	Pallet Falls	Reaction with Cargo	Reaction with Items
Forklift to Plane	1.00E-12	NA	NA
Forklift to Truck	1.00E-08	NA	NA
Plane to ASP	1.00E-12	1.00E-08	NA
Truck to Airport	NA	NA	NA
Truck to ASP	1.00E-10	NA	1.00E-06

	Shaped Charge Attack	Takeoff or Landing Fire	Truck Accident
Forklift to Plane	NA	NA	NA
Forklift to Truck	NA	NA	NA
Plane to ASP	NA	1.00E-08	NA
Truck to Airport	NA	NA	1.00E-12
`Truck to ASP	1.00E-08	NA	NA

APPENDIX B
(Continued)

Table B.22 Risk Assessment Reports for CONUS Storage to ASP: Air (Continued)

	Truck Fire		
Forklift to Plane	NA		
Forklift to Truck	NA		
Plane to ASP	NA		
Truck to Airport	1.00E-08		
Truck to ASP	NA		

Table B.23 Risk Assessment Report for OCONUS Storage to ASP: Truck/Ship

	Pallet Falls	Pierside Fire	Reaction with Cargo
Ammo ship to ASP	1.00E-12	NA	1.00E-08
Crane/ Forklift to Truck	1.00E-08	1.00E-08	1.00E-08
Forklift/Crane to Ship	1.00E-08	1.00E-08	1.00E-08
Truck to ASP	1.00E-10	NA	NA
Truck to Port	NA	NA	NA

	Reaction with Items	Shaped Charge Attack	Sniper Bullet
Ammo ship to ASP	NA	NA	NA
Crane/ Forklift to Truck	NA	NA	1.00E-10
Forklift/Crane to Ship	NA	NA	NA
Truck to ASP	1.00E-08	1.00E-08	NA
Truck to Port	NA	NA	NA

APPENDIX B
(Continued)

Table B.23 Risk Assessment Report for OCONUS Storage to ASP: Truck/Ship (Continue)

	Truck Accident	Truck Fire	
Ammo ship to ASP	NA	NA	
Crane/ Forklift to Truck	NA	NA	
Forklift/Crane to Ship	NA	NA	
Truck to ASP	NA	NA	
Truck to Port	1.00E-12	1.00E-08	

Table B.24 Risk Assessment Report for OCONUS Storage to ASP: Air

	Bullet Punctures Container	Detonation	Fire Accident
Truck to Airport	1.00E-08	NA	NA
Forklift / Truck to Plane	NA	NA	NA
Plane to ASP Port	NA	NA	NA
Forklift to Truck	1.00E-12	1.00E-08	NA
Truck to ASP	NA	NA	1.00E-06

	Forklift Tines Puncture Container	Gunfire From Aircraft	Missile Attack
Truck to Airport	NA	NA	NA
Forklift / Truck to Plane	1.00E-10	NA	NA
Plane to ASP Port	NA	NA	NA
Forklift to Truck	1.00E-10	NA	NA
Truck to ASP	NA	1.00E-08	1.00E-08

APPENDIX B
(Continued)

Table B.24 Risk Assessment Report for OCONUS Storage to ASP: Air (Continue)

	Pallet Falls	Reaction with Cargo	Reaction with Items
Truck to Airport	NA	NA	NA
Forklift / Truck to Plane	1.00E-08	NA	NA
Plane to ASP Port	NA	1.00E-08	NA
Forklift to Truck	1.00E-10	NA	NA
Truck to ASP	1.00E-10	NA	1.00E-06

	Shaped Charge Attack	Takeoff or Landing Fire	Truck Accident
Truck to Airport	NA	NA	1.00E-12
Forklift / Truck to Plane	NA	NA	NA
Plane to ASP Port	NA	1.00E-08	NA
Forklift to Truck	NA	NA	NA
Truck to ASP	1.00E-08	NA	NA

	Bullet Punctures Container		
Truck to Airport	NA		
Forklift / Truck to Plane	NA		
Plane to ASP Port	NA		
Forklift to Truck	NA		
Truck to ASP	1.00E-12		

APPENDIX B
(Continued)

Table B.25 Risk Assessment Report for OCONUS Storage to CONUS Storage: Truck/Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to OCONUS	NA	NA	1.00E-08
Crane/ Forklift from Ship	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to CONUS	1.00E-12	NA	NA
Truck to Port	1.00E-12	1.00E-08	NA

	Forklift Tines Puncture Container	Pallet Falls	Pierside Fire
Ammo ship to OCONUS	NA	1.00E-08	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-12	1.00E-08
Forklift/Crane to Ship	1.00E-08	1.00E-12	1.00E-08
Truck to CONUS	NA	NA	NA
Truck to Port	NA	NA	NA

	Reaction with Cargo	Sniper Bullet	Truck Accident
Ammo ship to OCONUS	1.00E-08	NA	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-10	NA
Forklift/Crane to Ship	1.00E-08	1.00E-10	NA
Truck to CONUS	NA	NA	1.00E-12
Truck to Port	NA	NA	1.00E-12

APPENDIX B
(Continued)

Table B.25 Risk Assessment Report for OCONUS Storage to CONUS Storage: Truck/Ship (Continued)

	Truck Fire		
Ammo ship to OCONUS	NA		
Crane/ Forklift from Ship	NA		
Forklift/Crane to Ship	NA		
Truck to CONUS	1.00E-08		
Truck to Port	1.00E-08		

Table B.26 Risk Assessment Report for CONUS Storage to Demil: Truck

	Bullet Punctures Container	Detonation	Truck Accident
Truck to Demil	1.00E-12	1.00E-08	1.00E-12

	Truck Fire		
Truck to Demil	1.00E-08		

Table B.27 Risk Assessment Report for CONUS Storage to Demil: Rail

	Bullet Punctures Container	Detonation	Rail Accident
Rail to Demil	1.00E-12	1.00E-08	1.00E-10

	Rail Fire		
Rail to Demil	1.00E-08		

APPENDIX B
(Continued)

Table B.28 Risk Assessment Report for OCONUS Storage to Demil: Truck/Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to CONUS	NA	NA	1.00E-08
Crane/ Forklift to Truck	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to Demil	1.00E-12	1.00E-08	NA
Truck to Port	1.00E-12	1.00E-08	NA

	Forklift Tines Puncture Container	Pallet Falls	Pierside Fire
Ammo ship to CONUS	NA	1.00E-08	NA
Crane/ Forklift to Truck	1.00E-10	1.00E-08	1.00E-08
Forklift/Crane to Ship	1.00E-10	1.00E-08	1.00E-08
Truck to Demil	NA	NA	NA
Truck to Port	NA	NA	NA

	Reaction with Cargo	Sniper Bullet	Truck Accident
Ammo ship to CONUS	1.00E-08	NA	NA
Crane/ Forklift to Truck	1.00E-08	1.00E-10	NA
Forklift/Crane to Ship	1.00E-08	1.00E-10	NA
Truck to Demil	NA	NA	1.00E-12
Truck to Port	NA	NA	1.00E-12

APPENDIX B
(Continued)

Table B.28 Risk Assessment Report for OCONUS Storage to Demil: Truck/Ship

	Truck Fire		
Ammo ship to CONUS	NA		
Crane/ Forklift to Truck	NA		
Forklift/Crane to Ship	NA		
Truck to Demil	1.00E-08		
Truck to Port	1.00E-08		

Table B.29 Risk Assessment Report for OCONUS Storage to Demil: Rail/Ship

	Bullet Punctures Container	Detonation	Fire
Ammo ship to OCONUS	NA	NA	1.00E-08
Crane/ Forklift from Ship	NA	NA	NA
Forklift/Crane to Ship	NA	NA	NA
Truck to CONUS	1.00E-12	NA	NA
Truck to Port	1.00E-12	1.00E-08	NA

	Forklift Tines Puncture Container	Pallet Falls	Pierside Fire
Ammo ship to OCONUS	NA	1.00E-08	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-12	1.00E-08
Forklift/Crane to Ship	1.00E-08	1.00E-12	1.00E-08
Truck to CONUS	NA	NA	NA
Truck to Port	NA	NA	NA

Table B.29 Risk Assessment Report for OCONUS Storage to Demil: Rail/Ship (Continued)

	Reaction with Cargo	Sniper Bullet	Truck Accident
Ammo ship to OCONUS	1.00E-08	NA	NA
Crane/ Forklift from Ship	1.00E-08	1.00E-10	NA
Forklift/Crane to Ship	1.00E-08	1.00E-10	NA
Truck to CONUS	NA	NA	1.00E-12
Truck to Port	NA	NA	1.00E-12

	Truck Fire		
Ammo ship to OCONUS	NA		
Crane/ Forklift from Ship	NA		
Forklift/Crane to Ship	NA		
Truck to CONUS	1.00E-08		
Truck to Port	1.00E-08		

REFERENCES

1. Online Executive Development Program – IIT Delhi and Macmillan India collaboration, http://www.develop.emacmillan.com/iitd, viewed on April 24, 2004.

2. S. Pochard, "Managing Risks of Supply-Chain Disruptions: Dual Sourcing as a Real Option ", Masters Thesis, Massachusetts Institute of Technology, August 2003.

3. Y. Sheffi, "Supply Chains and Terrorism", http://web.mit.edu, viewed on April 24, 2004.

4. N. Bahr, "System Safety Engineering and Risk Assessment: A Practical Approach", Published by Taylor and Francis Ltd.

5. W. Geoffrey, S. Robert, "Risk Analysis Techniques", Disaster Recovery Journal 1997.

6. T. Bedford and R. Cooke, "Probabilistic Risk Analysis: Foundations and Methods", Published by Cambridge University Press.

7. V. DeGiorgio, "Understanding Your RISK, The RISK Assessment Process", Power Point Presentation, www.nepss.org/presentations/Risk_26June02.ppt, viewed on April 29, 2004.

8. Air Force System Safety Handbook, United States Air Force Safety Agency, July 2000.

9. B. Jenkins, "Security Risk Analysis and Management, Countermeasures Inc", 1998.

10. "A Method to Assess the Vulnerability of U.S. Chemical Facilities", National Institute of Justice, Nov 2002, http://www.ojp.usdoj.gov/nij.

11. H. Forbes, "Supply Chain Security", Presented in the Symposium of Economic and Business security held at New Jersey Institute of Technology, July 2002.

12. "Making The Nation Safer: Role of Science and Technology for Countering Terrorism", National Research Council, 2002.

13. "Vulnerability Assessment and Survey Program – Overview of Assessment Methodology", US Department of Energy, Office of Energy Assurance, September 2001.

14. Executive Report on behalf of Department of Transport, Local Government and the Regions, Cranfield University, January 2002.

REFERENCES
(Continued)

15. M. Swiatocha and J. Bentivoglio, "Conducting a Clinical Compliance Risk Assessment in Pharmaceutical Industry", Presentation to 2nd Annual Medical Research, March 2002.

16. B. Bestercy, K. Collier, and J. Davidson, S. Lee, D. Smith, "Logistics Outsourcing and the Future War Fighting Environment: Risk and Control", Advanced Management Program, June 2001.

17. "Vulnerability Assessment Worksheet", Municipal Police Officer's Education and Training Commission, http://www.mpoetc.state.pa.us.

18. L. Hudson, B. Ware, K. Laskey, S. Mahoney, "An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners", submitted to UAI, 2002

19. B. Ware, L. Hudson, R. Kerr, "A Knowledge-Based Simulation Architecture for Assessing and Managing Risk", Digital Sandbox, Inc., 2001.

20. http://www.buddysystem.net/html/news.shtmlBuddy, as viewed on May 2003.

21. Los Alamos National Laboratories, Website as on 4th April 2003, http://www.lanl.gov /quarterly/sim_science.shtml.

22. J. Martha and S. Prabhakaran, "Targeting a Just-In –Time Supply Chain for the Inevitable Next Disaster ", Supply Chain Management Review, September 2002.

23. H. Omar, C. Robert, "Securing the Supply Chain", Council of Logistics Management, 2002.

24. Business Continuity and Supply Chain Management, Survey Report, The Chartered Management Institute, London, www.thebci.org, as on March 15, 2003.

25. L. Widmer, "Terrorism Insurance: Where's the Coverage?", http://www.riskand insurance.com, as viewed on April 29, 2004

26. J. Sharp, "Origins and Current State of Art in Risk and Business Continuity Management", www.thebci.org/BCAWKA1.htm, as on February 2, 2003

27. http://www.business-continuity-world.com/bia.htm, as viewed on April 25, 2003.

28. N. Ross, "Terrorism: How Will It Impact Contingency Planning?", Contingency Planning & Management, September, 2001, pp14-17.

REFERENCES
(Continued)

29. G. Gilbert and M. Gips, "Supply –Side Contingency Planning", March 2000.

30. "Enterprise Risk Management Framework", Draft report from Committee of Sponsoring Organizations of the Treadway Commission.

31. S. Ream, "How Does Your Company Measure Up? The Business Continuity Management (BCM) Maturity Model", Planning and Management, Pages 39-41.

32. S. Ream, "Measuring Your Program: 3 Methods for Evaluating Business Continuity", Contingency Planning and Management, November-December 2003, Pages 10-15.

33. L. David, "Adding Art to the Rigor of Statistical Science", Article, New York Times, April 28, 2001.

34. L. Helm, "Improbable Inspiration", Article, Los Angeles Times, October 28, 1996.

35. A D Marshall, "Lecture Notes on Baye's Theorem", http://www.cs.cf ac.uk/Dave/AI2/, as viewed on February 2003.

36. D. Heckerman, A. Mamdani, M. Wellman, "Real World Applications of Bayesian Networks", Communications of ACM, 1995.

37. P. Haddawy, " An Overview of Some Recent Developments in Bayesian Problem Solving Techniques", AI Magazine Special Issue on Uncertainty in AI, Summer 1999.

38. A. Phadnis and S. Nasser, "Fuzzy Belief Networks", Powerpoint Presentation, September 2002.

39. H. Pan ,N. Okello, D. McMichael, M. Roughan, "Fuzzy Causal Probabilistic Networks and Multisensor Data Fusion", SIPE International Symposium on Multispectral Image Processing, October 1998.

40. K. Korb, A. Nicholson, "Bayesian AI Tutorial", Lecture Notes, 2001.

41. A. Said, D. Stevens, G. Sehlke, "Exploration of Conservation Schemes and TDML Using Bayesian Networks", March 2002.

42. Neil. Martin, Tranham. Ed, "Using Bayesian Networks to Predict Operational Risk", Operational Risk, August 2002.

REFERENCES
(Continued)

43. H. Pan, D. McMichael, "Fuzzy Causal Probabilistic Networks – A New Ideal And Practical Inference Engine", May 1998.

44. D. Heckerman, "Bayesian Networks for Data Mining", Data Mining Knowledge Discovery 1, 79-119, 1997

45. D. Marshall, "Lecture Notes on AI, Bayes Theorem", September 2002.

46. E. Horstkotte, "Fuzzy Logic", The Net's Original Fuzzy Logic Archive, 2000

47. A. Bonde, "Fuzzy Logic Basics", 2000.

48. A. Blair and B. Ayyub, "Fuzzy Stochastic Cost and Schedule Risk Analysis: MOB Case Study", 1999.

49. J. Bezdek, " Coments On Fuzzy Sets – What Are They And Why ?", IEEE transaction on Fuzzy systems , Vol 2 , no 1 , february 1994.

50. U. Lerner, E. Segal, D. Koller, "Exact Inference in Networks with Discrete Children of Continuous Parents", 2001.

51. U. Lerner, "Hybrid Bayesian Networks for Reasoning about Complex Systems", PHd Dissertation, Stanford University, October 2002.

52. M. Meyer, K. Butterfield, W. Murray, R. Smith, J. Booker, "Guidelines for Eliciting Expert Judgment as Probabilities or Fuzzy Logic" , Draft Copy , submitted to Fuzzy Logic and Probability Applications ,American Statistical Society.

53. R. Keith, "Fuzzy Logic Knowledge Bases in Integrated Landscape Assessment: Examples and Possibilities", General tchnical report PNW-GTR-521, September 2001.

54. M. Stamatelatos, "Probabilistic Risk Assessment: What is it and why is it worth performing it?", NASA Office of Safety and Mission Assurance.

55. "Standard Practice For System Safety: MIL STD 882D", United States Department of Defense.

56. P.L. Clements, "Combinatorial Failure Probability Analysis Using MIL- STD 882", 2002, http://www.sverdrup.com/safety/combine.pdf, as viewed on November 2003.

57. Threat Hazard Assessment, SGI Group.