The design of a decision support system for supply chain risk management

by

Vinay Deshmukh

Bachelor of Engineering (Electronics and Communication)
Diploma in business management
Master of Technology (Computer Science and technology),IIT, Roorkee, India.

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2007

Signature of Author_____

Vinay Deshmukh
System Design and Management Program
April 2007

Certified by____

David Simchi-Levi (Thesis Supervisor)
Professor of Civil Engineering, Engineering systems division and Co-director, MIT LFM-SDM program
Massachusetts Institute of Technology

Accepted by_____

Patrick Hale
Director
System Design & Management Program, Massachusetts Institute of Technology

This page is intentionally left blank

This thesis has been a truly exhilarating experience. What appeared to be an insurmountable task was made easy by the able guidance and deep insights provided by Dr.David Simchi-Levi, the rock solid support and encouragement given by Prof.Pat Hale and the unwavering commitment of my family members including my wife, Swati and children Ashlesha and Soham. The three fortune 200 companies who provided valuable inputs, data and the precious time of their senior executives deserve a special mention although their names could not be published in order to protect their confidentiality. SDM seniors and colleagues deserve a big thank you and so do my other family members including my parents, my sister and her family, and my in-laws.

The design of a decision support system for supply chain risk management

The design of a decision support system for supply chain risk management

By
Vinay Deshmukh

Submitted to the System Design and Management Program on Jan 31, 2007 in partial fulfillment of the requirements for the degree of

Master of Science in engineering and management

Abstract

Where can things go wrong? This deceptively simple question has fascinated mankind since time immemorial. The question in fact forms the basis of risk management. The focus of this thesis is the risk management of supply chains. Any factor that is likely to disrupt the procurement, production, or delivery of a good or a service constitutes a supply chain risk. As several case studies from around the world indicate [4], disruptions to an enterprise's supply chain could be catastrophic to business, human safety, market competitiveness, and even national and international economies. It is therefore imperative that an a priori assessment of the factors that pose a risk to the supply chain be conducted and contingency plans developed at strategic, tactical, and operational levels to monitor and mitigate those risks.

This thesis will identify all major risks that are likely to disrupt a supply chain; identify the data needed to continuously monitor each risk; suggest a synthesized framework for managing supply chain risks; propose different models to quantify risks and asses their consequences; and suggest guidelines for model use. Further, it will present a case study based on the models developed and propose a decision support system based on these models and necessary data.

This work will help enterprises develop risk management plans at the strategic, tactical and operational levels, along various time horizons, and be able to execute them when supply chain risks are encountered. The target audience for this thesis includes a broad spectrum of supply chain professionals, consultants, supervisors, top executives, risk professionals, managers, software entrepreneurs, academicians, and students.

Contents

List of Figures

List of Tables

Section 1

1.1 Introduction

"If something can go wrong, it definitely will" - Murphy

1.1.1 Overview

With increasing globalization, intensified competition, demanding customers, and the commoditization of products and services, supply chains can no longer afford disruptions. The following case studies excerpted from various sources amply demonstrate the importance of supply chain risk management.

- Hurricane Katrina submerged P&G's Folger coffee plant, affecting 40% of coffee consumption in North America in August 2005. P&G's first priority was attending to their workers. P&G set up a temporary housing facility for its workers. By Sep 23, just 3 weeks after the hurricane, P&G managed to resume 85% of its production. This was possible due to a detailed contingency plan .The contingency plan included flexible staffing, secondary suppliers, and digital images of every part of the company's operation.[1]
- Simulation of supply chain disruption is a part of Wal-Mart management's fire drills. Distribution flexibility is a vital part of Wal-Mart's operations. A given distribution network supports many types of items.
- In 1999, a fire occurred at a plant manufacturing beryllium oxide that reduced global production capacity of this chemical by 40%.
- The fire that destroyed Toyota's brake supplier plant in 1997 stopped Toyota's production lines and cost Toyota an estimated $40 million per day. However Toyota was back in business in a week due to the close relationship with their suppliers.[2]

Although efficiency and responsiveness continue to be key performance indicators of supply chains, *resilience* has been added to the lexicon for supply chain performance indicators. Prof.Yossi Shafi describes resilience as the ability to withstand and recover from disruptions. Being resilient requires a deep understanding of factors that could disrupt the supply chains and contingency plans to mitigate them.

Key research issues of interest include identifying a generic framework for supply chain risk management; determining a way to identify the soft spots in the supply chain; learning how to strengthen these soft spots against risks; and research how other industries (e.g. the defense and financial industries) deal with risks.

1

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage&articleId=9000810&taxonomyId=19

2

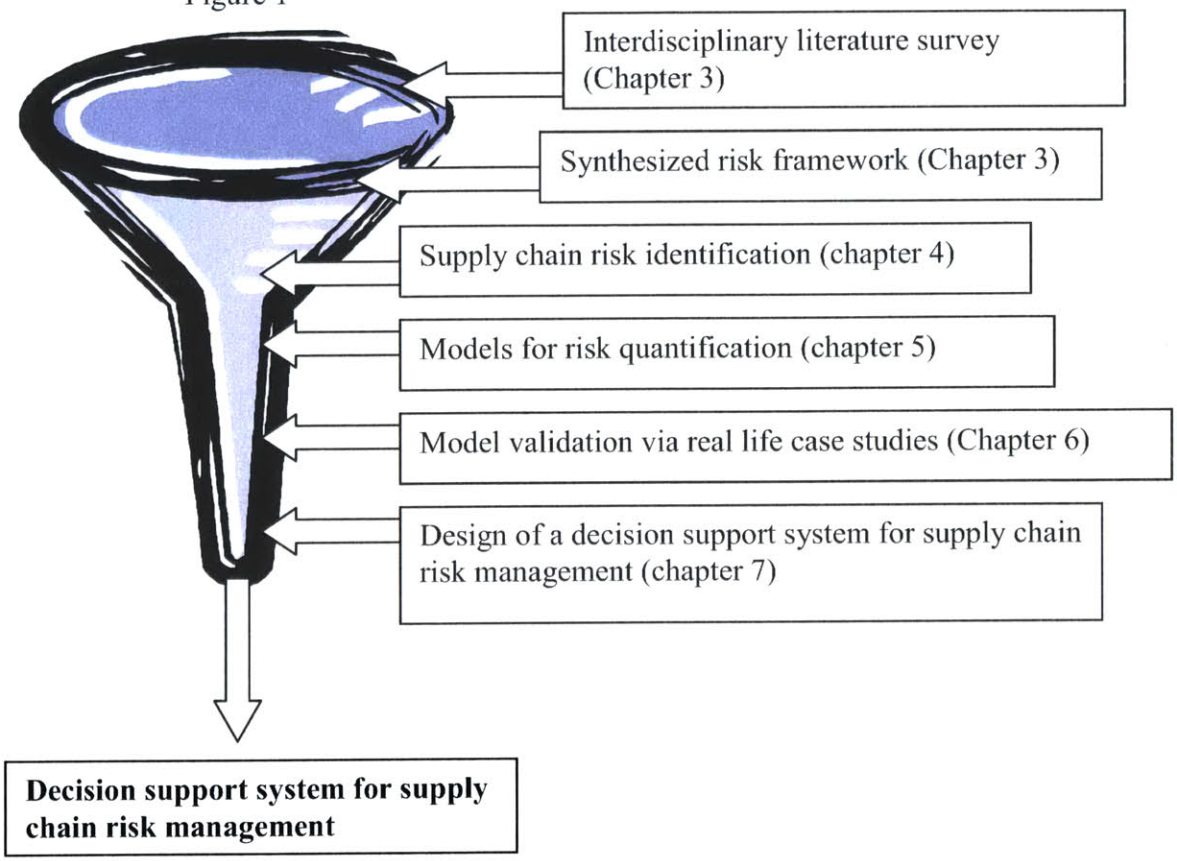
http://209.85.165.104/search?q=cache:bnobBAYSlLAJ:www.business.uiuc.edu/Working_Papers/papers/05-0116.pdf+toyota+supplier+fire,+Nelson+1998&hl=en&ct=clnk&cd=1&gl=us

1.1.2 Objective

The objective of the thesis is to provide a generic framework and more specifically a decision support system to help enterprises identify, assess and mitigate supply chain risks. The ultimate objective is to help enterprises become resilient.

1.1.3 Approach

Figure 1



This thesis takes a funnel approach to the problem (similar to Pugh's methods of controlled convergence) by starting broad and then gradually zeroing in on the solution. This was done by researching risk management techniques in the financial industry, the military, the six sigma literature and finally INCOSE – the International Council of Systems Engineering. The patent database[3] and prior SDM/LFM theses on the topic were also consulted. Synthesizing the techniques from all these industries and disciplines, a generic framework evolved to manage risks. The factors that constitute supply chain risk were identified and categorized. Then, several models were developed to quantify these risks and data needed to monitor them on an ongoing basis was identified. Real life case studies were used to validate the models. Finally a decision support system was designed to partially or fully automate the task of supply chain risk management. The integration of the decision support system with conventional supply chain management software was also examined.

[3] www.uspto.gov

1.1.4 Structure of the thesis

Section two provides a background of supply chain risk management in the context of enterprise risk management. Section two also examines the role of a decision support system for supply chain risk management.

Section three conducts an extensive literature survey of risk management techniques across different industries such as the financial services industry and the military. Different professional organizations such as INCOSE and quality systems such as six sigma are also examined. Further, work done by well known authorities in this field including David Simchi-Levi, Yossi Shafi, Zsidisin, and others was examined.

Section four provides a list of risks that impact the supply chain and an approach to identifying them. Section four also identifies the key performance indicator associated with each risk along with the data needed to identify it.

Section five proposes various models to quantify and mitigate risks.

Section six presents a case study that illustrates the application of the above framework and models.

Section seven is dedicated to the design of the decision support system.

Section eight summarizes the results and conclusions.

Section nine provides recommendations for future work.

Section ten includes the appendices.

Section eleven is a brief introduction to the author and the thesis advisor.

Section twelve acknowledges the contributions of all those who made this thesis possible.

Section thirteen concludes the thesis with the bibliography.

1.1.5 Chapter summary

This section presents an overview of the supply chain risk management and its importance to an enterprise. Specific research topics were posed that serve as the goals of this thesis. While the ultimate objective is to help enterprises become resilient, the objective of this thesis is the development of a framework for supply chain risk management and, more specifically, the design of a decision support system based on this framework.

Section 2

2.1 Background

"Running an enterprise is like playing the game of snakes and ladders. You need to know where the snakes are and where the ladders are" – Anonymous.

2.1.1 Enterprise risk management

Figure 2

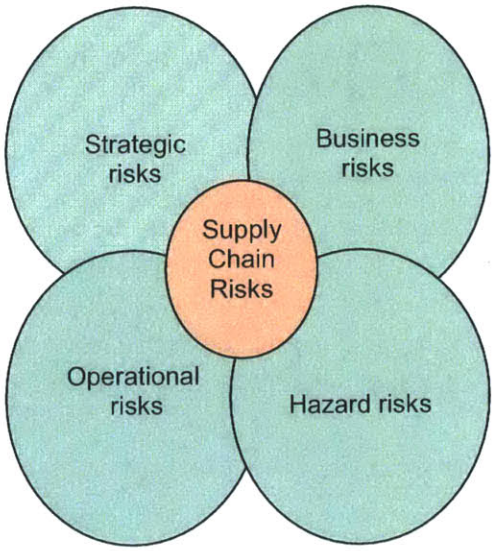


Figure one depicts the scope of enterprise risk management. Enterprise risk management can be categorized as strategic risk management, operational risk management, business risk management and hazard risk management. As can be seen , supply chain risk management cuts through each of these circles implying that supply chain risks affect the enterprise's strategy, business, operations and disaster mitigation planning.

Strategic risks

Strategic risks are those that affect the enterprise's strategy. For example new and emerging global competitors, geo political risks such as change of governments, change of domestic and international policies, mergers and acquisitions, and rationalization of plants and distribution centers are strategic risks.

Huawei, a Chinese manufacturer of internet routers and switches, is a main competitor to Cisco. Amidst allegations of copyright violations by Huawei (which Cisco later dropped [4] and a former Huawei employee claiming that his former employer copied Cisco down to every software bug , Huawei has grown steadily to 25% of Cisco's size.[5] Regardless of the truth behind the allegations, the strategic risk of reverse engineering of products and services by low cost manufacturers is conspicuous.

Operational risks

Operational risks include, for example, logistic route disruptions, stockouts, talent shortage, IT failures, power failures, and so on.

A perceptible trend in the last few years has been lean manufacturing. There has been an increase in the number of companies trying to emulate the Japanese operations management techniques such as JIT, Kanban and lean manufacturing. A side effect of

[4] http://www.expressindia.com/fullstory.php?newsid=34373
[5] http://www.businessweek.com/magazine/content/05_06/b3919079.htm

these techniques has been the increased vulnerability to risks. For example, companies that have successfully reduced inventories without increasing forecast accuracy have faced increased stockouts. The dependence on a single supplier has reduced overheads and ensured the consistency of quality (multiple suppliers supplying the same part are bound to have variance in their manufacturing and distribution processes thus causing variance in the quality of their products or services) at the expense of their ability to withstand disruptions to their supplier's production.

A large American fast food chain has traditionally relied on one major meat supplier. While this has ensured consistent quality, the operational risks include a single point of failure and reduced leverage when negotiating purchasing agreements. [6]

Business risks

Events such as recession, currency fluctuations, and credit ratings pose a threat to business. Recession can convert consumers of goods into suppliers of the same goods as explained below.[7]

The global steel industry underwent a period of massive recession from 1997 to 2001. With a weak Yen, a meltdown in the South East Asian economy, maturing Western markets for steel and excess capacity around the world, the prices of steel began to plummet. Many countries all over the world became net exporters of steel after they had been net importers. It was not until 2002 that the industry staged a recovery with increased demand for steel from China and a global agreement organized by the OECD.

Hazard risks

Events such as earthquakes, fires, and acts of terrorism constitute hazard risks. Perhaps the most significant impact of hazard risks was caused by 9/11.

As Prof Anant Raman of Harvard Business School notes in an article by David Stauffer[8]*, "In the days after 9/11, the retailing executives with whom he's in regular contact discovered that their initial concerns that they would have too few dresses were misplaced. In fact, the terrorist attacks led to a severe shortage of customers and thus a problem of too many dresses on the market."*

Hazard risks, especially the ones due to terrorist attacks, have the additional dimensions of public outrage and political ramifications besides the loss of life, limb, property and business. In fact, this thesis asserts that enterprises should assume the probability of hazard risks to be 1. This implies that they should start with the baseline assumption that such hazards are bound to occur and then analyze the consequences of such an event.

2.1.2 The role of supply chain risk management in enterprise risk management

The global market size of supply chain and logistics is estimated at 3 trillion USD.

---

[6] Excerpts from a Harvard business case study on Operations Strategy , a course taught by Prof.Pisano.
[7] http://www.indiansteelalliance.com/globalsteel.asp
[8] http://hbswk.hbs.edu/item/3442.html

While the US spends about 11% of its GDP on supply chain related costs, India spends about 13-15% of its GDP.[21] With such a huge investment at stake, supply chain risk management is critical to any enterprise. The impact of supply chain risks is not limited to finance. Supply chain risks could pose a threat to the enterprise's reputation, brand name, and political and social status.

2.1.3 The role of a decision support system in managing supply chain risks

While numerous studies have been conducted in the field of supply chain risk management and several models have been proposed, risk assessments are typically done without the help of a decision support system. The drawbacks of such an approach, called the manual approach are:–

- *Scalability* – As supply chains become more complex, it is almost impossible to perform risk assessments manually while ensuring completeness and accuracy.

- *Visibility* – The risk factors and mitigation plans must be visible to every stakeholder in the supply chain. Web based decision support systems are capable of providing such visibility.

- *Auditability* – Supply chain risk assessment is a continuous process. All changes need to be documented and approved.

- *Person independence* – Risk management systems must be person independent. Key person dependency is itself a risk.

- *Multi level and multiple horizons* – Risk management needs to be done at all levels – strategic, tactical and operational and across all time periods from weeks, months to years.

- *Role based* – While C-level executives are concerned with strategic risk management, mid-level management deals with tactical issues and lower-level personnel deal with operational issues. Supply chain risk management is therefore a role based function.

Risk management is becoming an integral part of sales and operations planning. Supply chain management vendors such as SAP and Oracle have sales and operations planning solutions. The current trend is to augment S&OP solutions with risk management decision support systems.

2.1.4 Chapter summary

This chapter provides an overview of enterprise risk management and categorizes it into strategic, operational, business and hazard risk management. Supply chain risk management overlaps with each of these risk areas and is performed at all strategic, tactical, and operational levels and across all time horizons. The role of a decision support system in risk management was also examined.

Section 3

3.1 Literature Survey

"Let knowledge come to us from all universe" - Vedas

Historical perspective

Risk management has been known to mankind since time immemorial.[14] According to Vincent Covelo and Jeryl Mumpower, the earliest risk assessments known to mankind were performed by a group called the Asipu in the Tigris-Euphretis valley in 3200 BC. The Asipu would help assess the risks on issues such as building a site, starting a business or entering a matrimonial alliance. The Asipu would analyze the risk factors underlying the problem at hand, suggest alternatives, and come up with the best alternative in a fairly quantitative manner. In 792 BC, "bottomry contracts" were used to mitigate risks. Bottomry contracts consisted of three elements – loan , interest rates, and risk premiums. The concept of a *general avertage* was developed around the same period. This evolved into the concept of insurance. Insurance, therefore, is one of the oldest risk mitigation strategies. With the tremendous advances in probability theory during the seventeen and the eighteenth century, probability theory became an important risk assessment tool. By the 19^{th} century, probability theory was used in a wide range of disciplines from finance to engineering. Each domain however had specific tools and methods.

3.1.1 Risk management techniques from the financial world

Some of the well known techniques in the financial world are –

1. Value at risk calculations

Top management: What is the financial risk of this decision ?
Risk manager: We are 90% confident that we will not lose more than 500K.

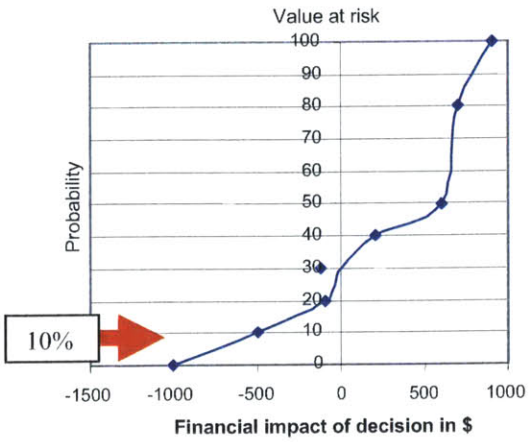
Thus, 90% VAR = 500K USD.

Also, 90%VAR = 10% probability on the cumulative probability distribution curve.

This implies that the probability of losing more than 500K is 10% and that of losing less than 500K is 90%.

This is depicted in the following cumulative distribution function:

Figure 3



2. The efficient frontier

Modern portfolio theory states that there is a direct relationship between risk and return implying that higher returns can only be obtained through higher risk. The efficient frontier is the upper part of the risk-return curve. Each point on the efficient frontier indicates the maximum return for a given risk. Risk is expressed as a standard deviation of the portfolio on the X-axis and return on the Y-axis.

3. Probability-Impact-Detectability

An important concept used in the financial world is that of risk volume. Risk volume is the product of the probability of an event, the magnitude of its impact, and the detectability of the risk. While traditional risk management literature has focused on the two dimensional model of probability and impact, detectability is a useful third dimension. Consider the following scenarios:

1. The probability of a supplier resorting to litigation could be low but its impact could be high if the case is lost. However such an event is detectable because as the litigation progresses, it will becomes gradually evident if the supplier is going to win. The risk of litigation therefore is manageable although its impact is high.

2. Consider terrorist attacks; the risk is low and the impact high. Moreover the detectability is extremely low. Prof.Yossi Shafi terms the threats of attacks to be adaptive which means if one part of the system is plugged the other becomes vulnerable. [4] The adaptive nature of the threat implies low detectability.

Yet another risk management technique used in the financial world is real options. Risk diversification is a common technique to mitigate risks. This technique evaluates the impact of future options using decision tree analysis.

3.1.2 Risk management techniques from six sigma literature [7]

Design for six sigma (DFSS) is a popular technique that deals with product and process design. Design activities have several latent risks. DFSS defines risk as follows:

> *Risk is the degree of exposure to an event that might happen to detriment the intended result.*

DFSS risk management is mainly concerned with project failures due to time and cost overruns or scope creeps. Figure 3 below depicts the 4 steps involved in risk management according to six sigma.

Figure 4 Risk Identification

Risk identification

Risks are identified using the following qualitative tools .

- Multi Generation Planning
- Technology Assessment
- Failure Modes Effect Analysis
- Quality Function Deployment
- TRIZ
- Best Judgment
    - team experience
    - subject matter experts
- Lessons Learned

Risks could also be identified using the following quantitative tools.

- Simulation
- Decision Tree
- Fault Tree
- Designed Experiments
- Prototypes, Pilots,
- Capability studies
- Design Scorecards
- Design Review
- Project Plan

Risk Analysis

Risk analysis comprises of assessing the probability of occurrence and assessing the severity of impact. Since each risk assessor may have his/her own subjective ratings of probability and severity, a common constructed scale has been suggested to minimize subjectivity (see table 1).

Table 1

Occurrence	Scale	Description of Criteria
Very Unlikely	1	Less than 10% probability of occurrence.
Unlikely	3	Between 10%-30% probability of occurrence.
Likely	5	Between 30%-70% probability of occurrence.
Very Likely	7	Between 70%-90% probability of occurrence.
Almost Certain	9	Greater than 90% probability of occurrence

Table 2 below depicts a constructed scale for the severity of impact due to risk.

Impact Of Severity	Scale	Technical	Cost	Schedule
Negligible	1	Minimal or no impact on meeting requirements	Minimal impact on budget	Minimal impact on schedule
Marginal	3	Minor modification and redesigns required to meet requirements. No major impact on scope	Budget or unit cost impact < 5%	Critical path unaffected. Non critical path tasks late, additional tasks added.
Significant	5	Requirements not being met. Solutions available. Project scope change.	Budget or unit cost impact 5-10%	Critical path in jeopardy. Minor delay in key milestones.
Critical	7	Requirements not being met. Significant changes required. Significant scope change.	Budget or unit cost impact 10%-25%. High cost escalation.	Critical path affected. Milestones significantly delayed.
Crisis	9	Cannot meet requirements. No alternatives evident.	Budget or Unit cost impact >25% Program affordability in question.	Critical path significantly affected. Milestones significantly delayed. <80% schedule adherence.

Risk response

Table 3 summarizes the risk response strategies recommended by the six sigma body of knowledge. Response to risks can be avoidance, mitigation, transfer or acceptance.

Table 3

Risk Avoidance:	Risk Mitigation
• Completely eliminates the risk • Employs redesign, change of scope etc. to attack risk opportunities • It is ideal if no side effects • Triz can be used to resolve conflicts • Residual Risk is zero • Impacts project metrics and scope	• Reduces high Occ and Sev values • Uses known methods and controls • e.g. action part of FMEA • Risks are reduced but not eliminated • New lower levels of Occ and/or Sev • Cost and budget implications exist • Minimal impact on scope
Risk Transfer:	**Risk Acceptance**
• Transfer risk to another project, vendor, or generation for more effective and efficient risk reduction • The residual risk is zero – for now • Non trivial future and transfer risks • Low impact on project and scope.	• Used when Risk Level is low • Basically a "no action" strategy • Residual risk is same as before • Contingency plans can be developed to handle this risk • No impact on project and scope

3.1.3 Risk management techniques from the US army

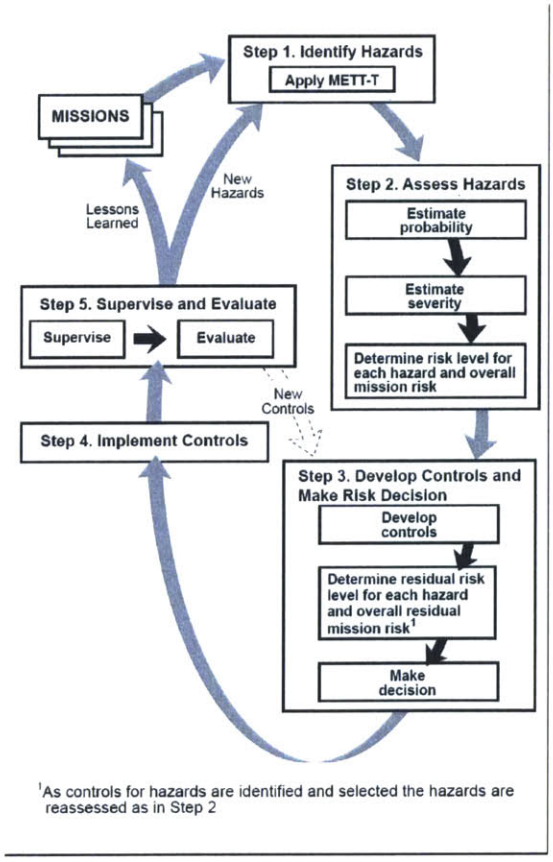
> *"Sizing up opponents to determine victory, assessing dangers and distances is the proper course of action for military leaders"*
> Sun Tzu, The Art of War, "Terrain"

Risk management is an integral part of every aspect of the army's operations. Failure to manage risks could have negative political, economic, and environmental impacts besides resulting in total or partial loss of combat power. Risk management must be second nature as far as planning and executing operations are concerned. The overarching goal of the US army is to defeat the enemy with minimum loss of life and limb. Wars are characterized by uncertainty, ambiguity and friction. Uncertainty comes from the lack of precise information; ambiguity results from the thin line of distinction between fact and impression; and friction emanates from fatigue and operational hazards. [10] Risk management strategies must therefore consider these three key risk elements into account. The following five stepos summarize the risk management strategies of the US army:

- Step 1. Identify hazards
- Step 2. Assess hazards to determine risks.
- Step 3. Develop controls and make risk decisions.
- Step 4. Implement controls.
- Step 5. Supervise and evaluate.

Figure 4 below reproduced from [10], pp 2-20 is a pictorial view of the risk management practices in the US army.

Figure 5



The above steps are integrated into each task undertaken by the army as applicable. Course of Action development (COA) is one such task. The appropriate risk management actions for COA development are steps 1, 2, and 3 above.

Table 4 below depicts the integration of risk management activities into each task undertaken by the army. As can be seen, not every risk management activity applies to every task but there is at least one risk management related activity that is applicable to every task.

Table 4 (reproduced from [10] pp – 2-1)

Military Decision-Making Process	Risk Management Steps				
	Step 1 Identify Hazards	Step 2 Assess Hazards	Step 3 Develop Controls and Make Risk Decision	Step 4 Implement Controls	Step 5 Supervise and Evaluate
Mission Receipt	X				
Mission Analysis	X	X			
COA Development	X	X	X		
COA Analysis	X	X	X		
COA Comparison			X		
COA Approval			X		
Orders Production				X	
Rehearsal[1]	X	X	X	X	X
Execution and Assessment[1]	X	X	X	X	X

[1]All boxes are marked to emphasize the continued use of the risk management process throughout the mission

- Lessons learned from previous missions are incorporated to present risk management scenarios.
- Competency building is considered to be a prerequisite to risk taking.
- Risk management is done at the appropriate level of command. Operational and tactical issues are handled at the lower and middle levels in the organization, strategic risks are dealt with the upper levels.
- Risk management is incorporated into the training of military personnel.
- Statistics indicate that loss of life and limb has occurred due to accidents, such as friendly fire incidents. Internal sources of risk are therefore equally important.
- Risk management is a closed loop and continuous process that takes place on and off duty.
- Risk assessment is similar to six sigma methodology except that the constructed scales for probability and severity are different.
- The effectiveness of a unit's risk management program is assessed periodically.

Table 5

Risk Assessment Matrix						
		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L

E – Extremely High Risk
H – High Risk
M – Moderate Risk
L – Low Risk

3.1.4 INCOSE – Risk management processes

The International Council of Systems Engineering (INCOSE) is the leading group in the field of systems engineering. The INCOSE handbook mentions risk management as a function that lies at the intersection of systems engineering and project management. While INCOSE mainly deals with project risks, specifically the risks of cost overruns, schedule slippages, and project scope risks, their principles are fairly generic. INCOSE refers the reader to the Project Management Institute (PMI) and the institute of risk management for additional details, but their general recommendations are very straightforward. INCOSE states that key steps to risk management include risk identification, risk assessment, risk handling, risk tracking and control, and risk mitigation. Expert interviews have been suggested as the key source of identifying risks. However, it is important that the right expert be chosen, the risk analyst be competent enough to ask pertinent questions and to translate the expert's qualitative inputs into quantitative terms, and that the expert be willing to share information. Furthermore, getting the right data has been suggested as critical to the success of risk management.

3.1.5 Prior work on supply chain risk management

- Prof.Yossi Shafi , The resilient enterprise

  Professor Shafi provides excellent insights into enterprise risk management in general and, more specifically, supply chain risk management in his book *The Resilient Enterprise.*[4] He based his work on several real life cases and a thorough qualitative analysis. Of particular interest is the concentric vulnerability map [4,pp 25] where he has mapped several risks on a constructed scale of probability and consequence.

- SDM04 – Atul Sharma

  Atul Sharma, SDM 04, in his thesis titled *A Systems Approach to Enterprise Risk Management in the High Tech Industry* proposes a 3-T, 4-R model as the basis of risk management. He demonstrates the use of value-at-risk and basic reliability theory for supply chain risk management. This thesis attempts to take his work further by developing additional models and identifying the circumstances in which they are applicable. Moreover an attempt is made to automate the whole process by suggestion a decision support system.

- SDM05 – David Michaud

  In his thesis titled *Screening Vulnerabilities in Water Supply Networks* David Michaud applies probabilistic risk assessments and multi attribute utility theory to the problems of water infrastructure risk management.

- Prof.Nancy Levinson

  Dr.Nancy Levinson's work focuses on system safety. The summary of her work as presented at the SDM alumni conference, October 2006 is given below –

  - Her work is based on a system dynamics based model
  - Her work models human beings as well
  - Her work has been applied to a wide range of industries
  - Focuses on safety as the essential objective of risk management

3.1.6 A synthesized framework for supply chain risk management

The following table summarizes the risk management techniques used in various disciplines and risk management techniques used in software development.

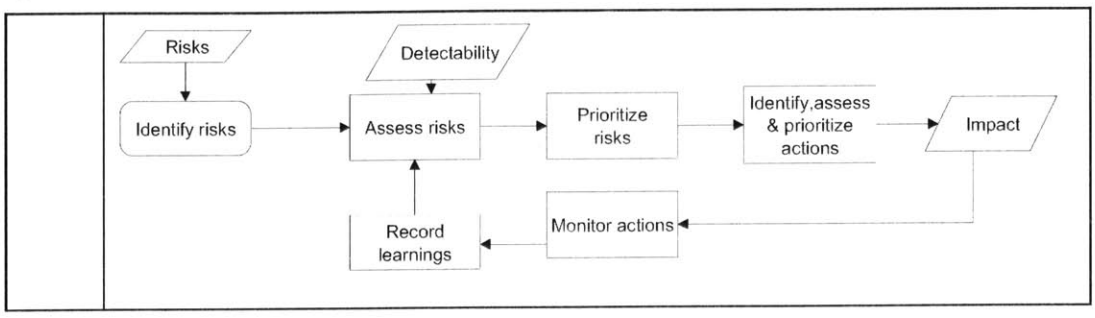
Table 6

Parameter	INCOSE	Commercial Software development	Financial	US Army	Six sigma
Overall concept	Viewed as a function that lies on the intersection of System Engineering and Project Management	No formal risk management. Risk management done implicitly by following best practices.	Categorized hazard risk, risk and financial risk. Focus on quantifying risks vs returns.	Integrated risk planning into mission planning and execution.	Focuses on design risks
Risk Assessment	Risk assessment categorized into Technical risk, architectural risk, ambient risk cost risk schedule risk Talks about Probability vs. consequence	Competitive risk is foremost. Business and Technological risks are also considered.	Formal model Involving Probability, severity and detectability. Risk volume = probability * severity* detectability		Risk assessment is based on probability and Constructed scales provide guidance and standardization across the enterprise. The model does not suggest detectability or predictability.
Opportunity Assessment	Balanced view of opportunity vs. risk	Opportunity often emphasized over risk. (e.g The case of Thorac-25 case outlined in INCOSE, Oracle e-business 11 quality issues upon release. 8000 patches sent after product launch)	Value-at-risk and Efficient Frontiers used to assess opportunities. Assessment done at all levels up to transaction level.	Little consideration of opportunity due to a highly conservative approach. Primary objective is to minimize losses.	The framework does not suggest opportunities.
Risk strategies	Transference, Avoidance, Acceptance	Mostly focused on acceptance. "Risk denial syndrome"	Transference, avoidance, acceptance, elimination, mitigation	Avoidance, elimination	Avoidance, transference, mitigation, acceptance.
Risk tools	Risk Matrix, FMEA, cost benefit analysis, fault trees	Mental maps	FMEA, value-at-risk, efficient frontier	Risk matrix	FMEA Risk matrix
Key person dependence	Person independent processes. Well documented	Person dependent. Past experience a crucial factor in decision making. Lack of documentation.	Person dependent due to the lack of a decision support system.	Mission specific and hence to some degree person dependent	Person independent to some extent. Lack of a decision support system makes it person dependent.

Based on all the above disciplines, a synthesized approach to risk management is given below.

A synthesized approach to supply chain risk management

Figure 6



Identify risks (and opportunities)
Supply chain risks are dependent at least on.

1. **Geography**
   Certain risks are more applicable to developing countries. For example transportation risks due to poor infrastructure or loss of production due to power outages. Even within a country , risks could vary by geography. The risks of hurricanes in New Orleans and those of earthquakes in California are some examples.

2. **The industry in question**
   The risks and opportunities in maturing industries are different from those in high growth industries. An example is the downturn faced by the steel service industry in Greater Boston in 2001-2004 leading to acquisitions, shutdown of distribution centers and layoffs. On the other hand a sudden spurt in demand for ipods around 2002-2003 necessitated a higher supplier capacity.

3. **The company in question**
   Even within an industry , different companies might face different risks due to differences in the supply chain architecture, processes and technology.

4. **Time**
   Certain risks are seasonal and the others are valid only for a short duration.An example of the former is the spurt in the demand for winter clothing in December while an example of the later is the threat of supplier's non compliance with respect to environmental laws such as the reduction of hazardous substances - RoHS. However the threat is eliminated at least for a duration once compliance certification is obtained.

Expert interviews are the recommended way to evaluate risks although we suggest using the framework presented in chapter 4 as a guiding principle. Risk studies are sensitive subjects and hence familiarity with the experts is important.

Assess risks .
One of the models for assessing risks is risk volume which is the product of probability, severity, and detectability although other models will be presented later in chapter 5.

Probability of occurrence : (frequent, likely, occasional, seldom, unlikely)
Severity of occurrence: (catastrophic, critical, moderate, marginal, Negligible)
Detect ability of occurrence: (scale of 1-5 , 5 being most difficult to detect)

Prioritize risks
Risks should be prioritized based on risk volume or other performance indicators such as lead time, loss of profit, etc.

Identify actions
Specific actions need to be identified in order to deal with the risk in question and assigned to specific individuals with a timeline for implementation.

Assess actions
Actions need to be assessed by estimating the risk volume again or by using simulation techniques.

Prioritize actions
Actions need to be prioritized based on key performance indicators such as reduction of risk volume, profits etc.

Monitor actions
It is important to monitor the impact of actions on a regular basis. For example, if a suggested action is to develop an alternate supplier, the order to delivery time needs to be monitored for the alternate supplier along with the health of the relationship with the original supplier.

Record learnings
Risk management should be person independent. It is therefore important to record learnings and share them with all those who have the prerequisite authority and responsibility.

Reassess risks
Risk assessment is a continuous process because most risks are time and environment dependent. Also, they depend on the risk actions undertaken in previous periods. They should therefore be reassessed periodically. Operational and tactical risks would need more frequent assessment compared to strategic risks.

Figure 6 illustrates the synthesized approach. The identification, assessment and prioritization of risks and actions comprise of the feed forward loop in the system. The

feedback loop comprises of monitoring the actions by measuring the impact and recording the learnings. Risks may have to be reassessed periodically. The system therefore is a closed loop negative feedback control system and is also adaptive.

3.1.7 Chapter summary

This chapter presents the risk management techniques from various disciplines. The synthesized approach based on these disciplines is also presented. The synthesized approach represents a negative feedback closed loop control system. The conventional risk management model is two dimensional with the probability of event occurrence on one axis and the magnitude of impact on the other. This model was improved upon by introducing the concept of detectability which is an indicator of how soon a risk can be detected. A risk can then be assessed by multiplying the probability of its occurrence with the magnitude of its impact and its detectability.

Section 4

"In God we trust. Everybody else brings data"
– Attributed to Prof. Demming.

4.1 Approach to the identification of supply chain risks

To begin, prior work in this field by Prof.Yossi Shafi and Prof.Zsidisin was examined. A leading vendor of supply chain management software also provided valuable inputs. Supply chain managers of various industries were also interviewed. Using master logic diagrams, risks were structured hierarchically. As indicated in Section Three, each risk is at least dependent on the geography, time, industry, and company dimensions. Therefore, the following hierarchical list can at best serve as a broad guideline. Exact risk assessments need expert interviews, company case studies, and industry data.

4.1.1 List of risks that impact the supply chain

The following figure is descriptive and not prescriptive in nature. Each company should add or delete risks as appropriate. Also there could be causal loops within and across risk categories. For the sake of simplicity such causal loops have been ignored.

Figure 7-1 Master logic diagram

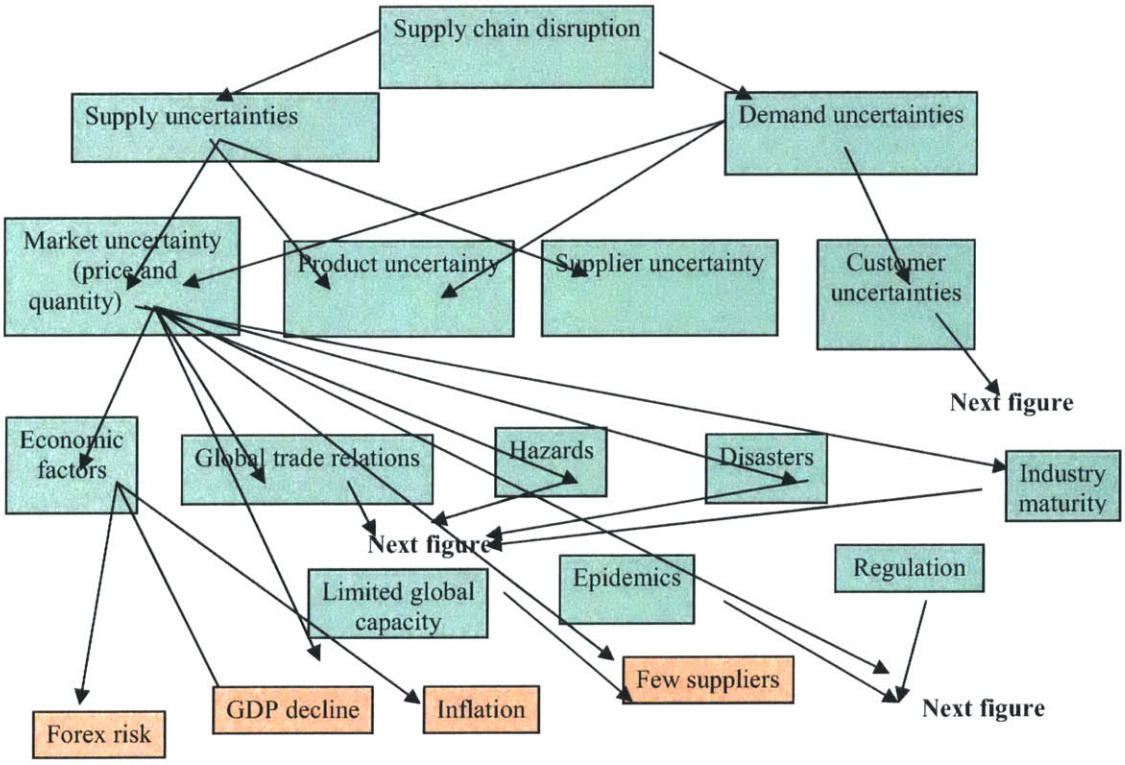


Figure 7-2

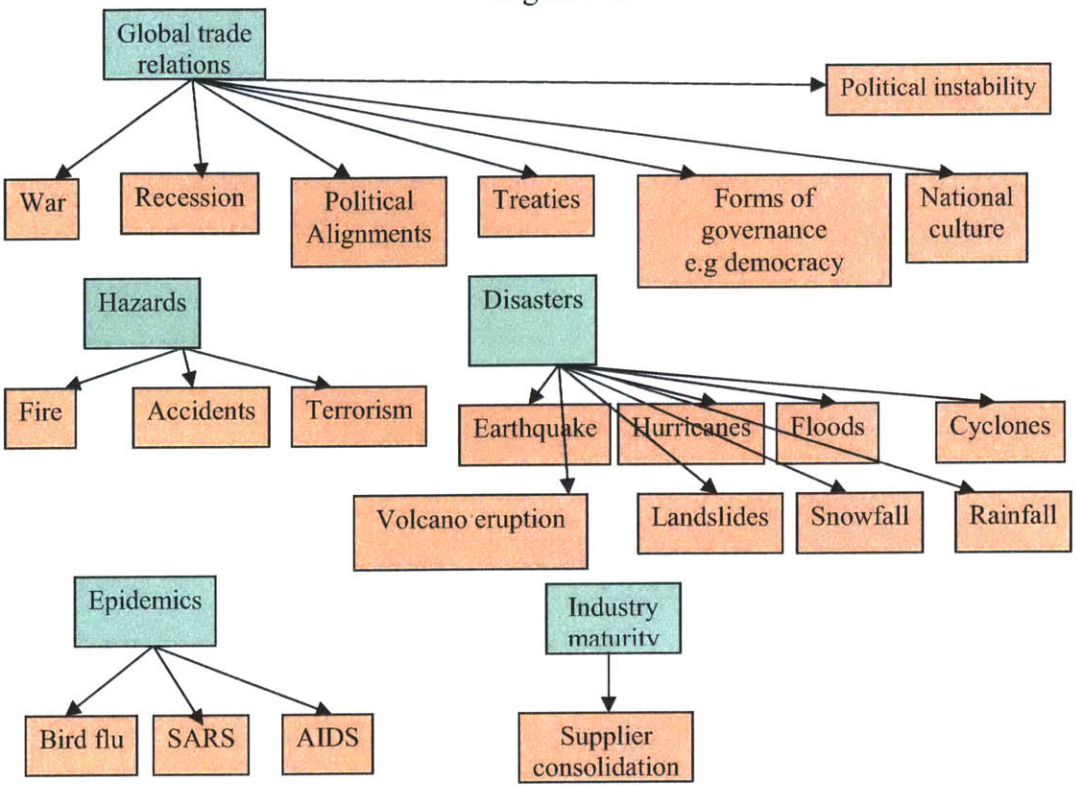


Figure 7-3

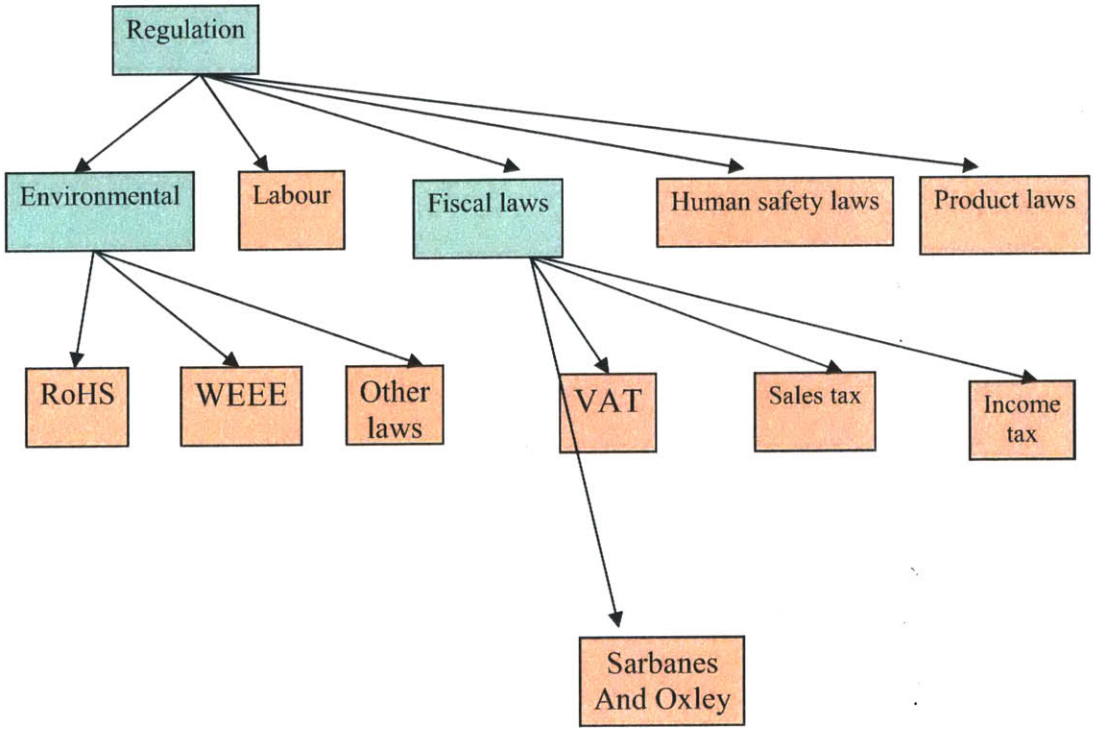


Figure 7-4

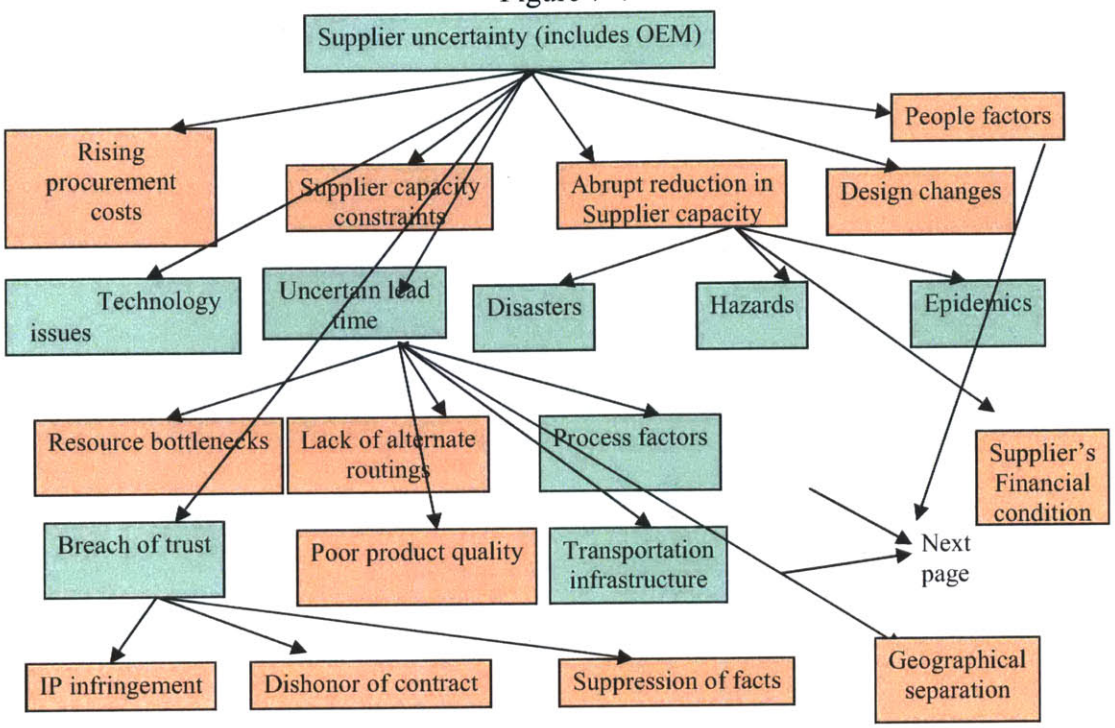


Figure 7-5

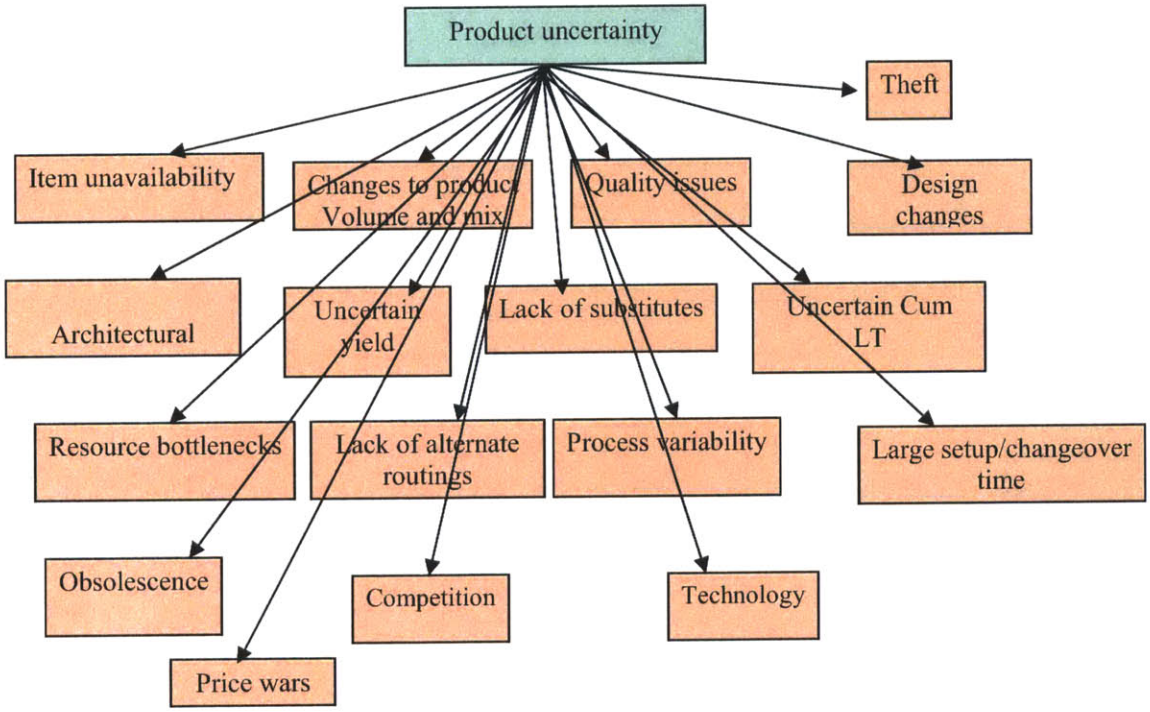


Figure 7-6

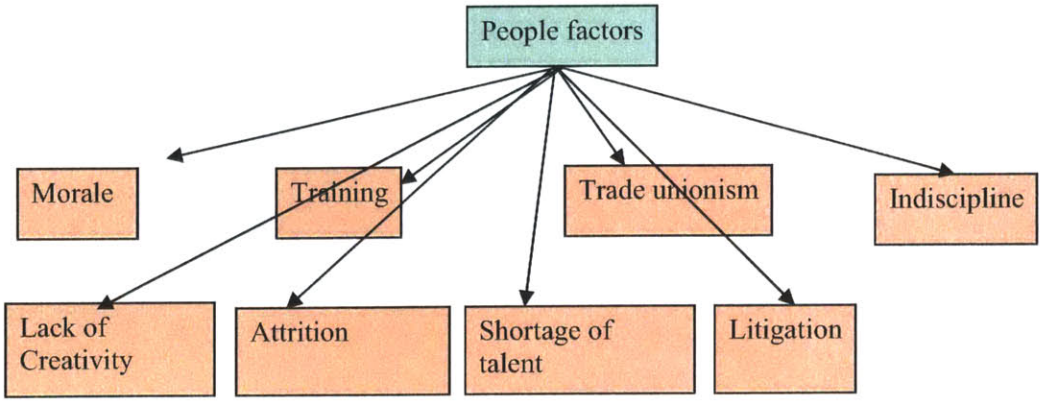


Figure 7-7

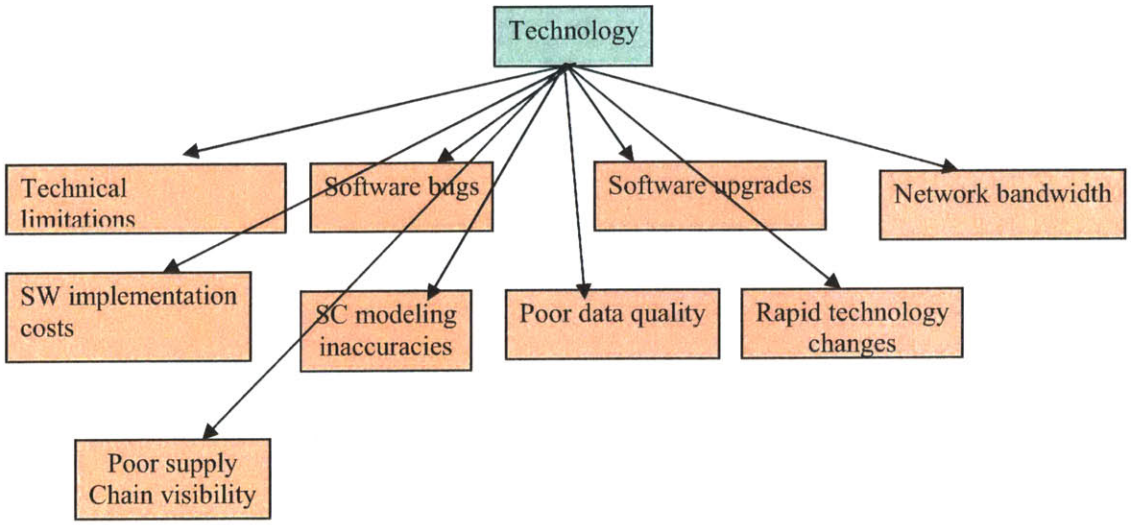


Figure 7-8

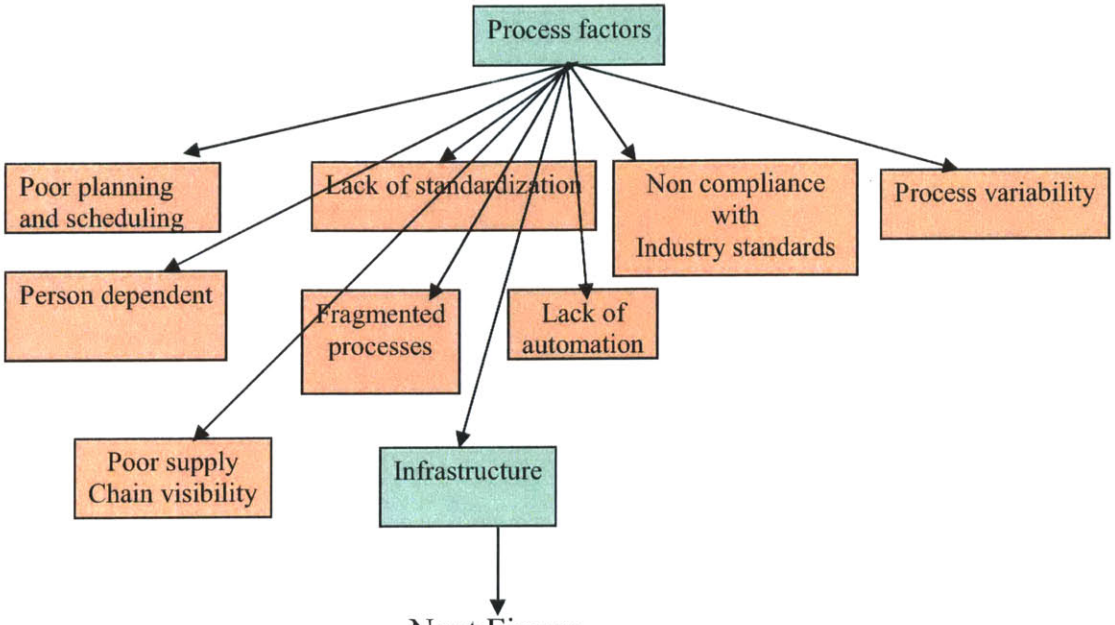


Figure 7-9

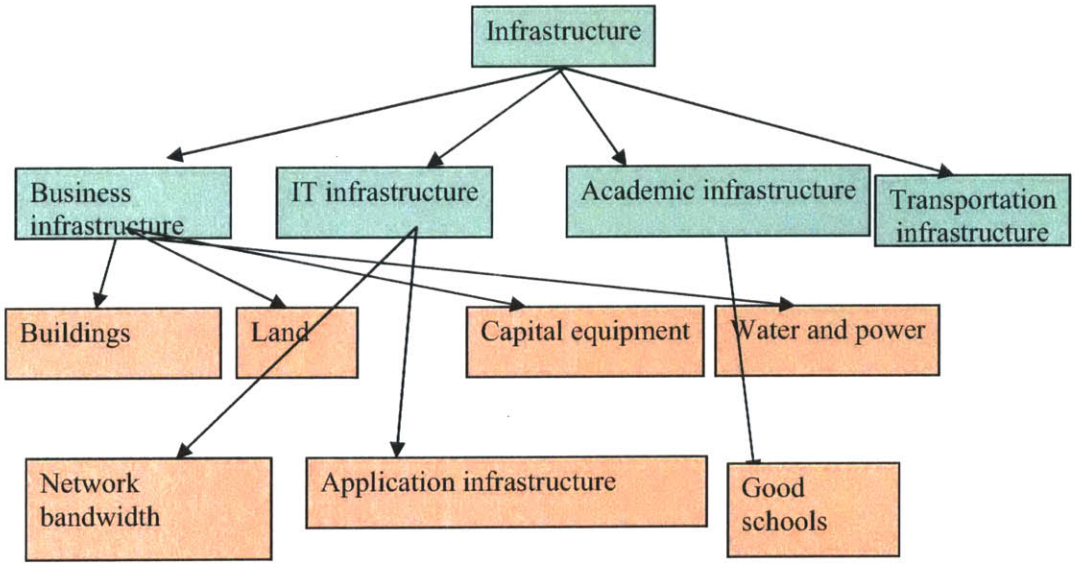


Figure 7-10

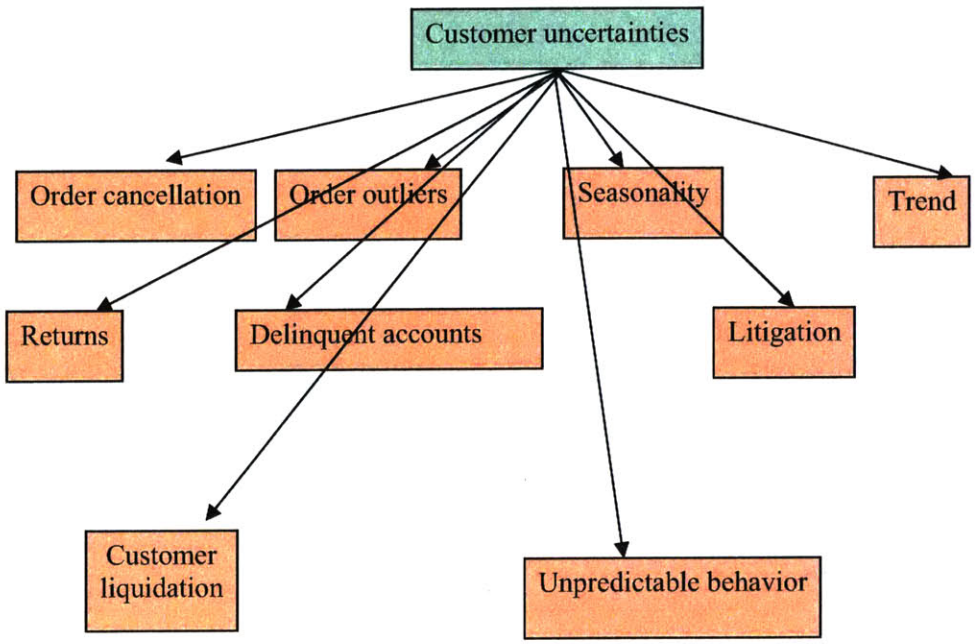
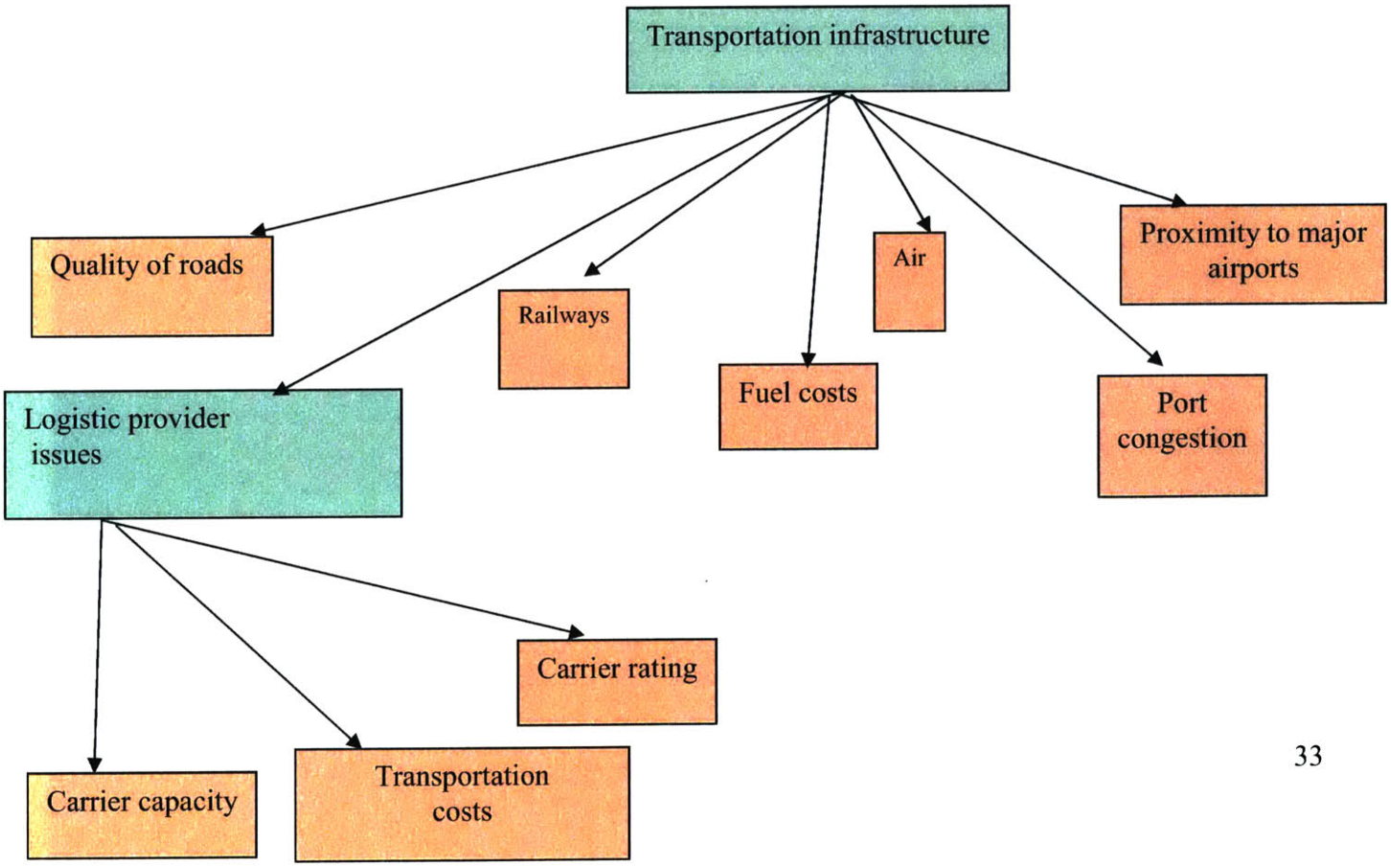


Figure 7-11



4.1.2 An approach to the identification supply chain risks

Beginning with supply chain disruption, ask the question 'why' at each stage till one cannot decompose any further. The boxes in red indicate root cause factors (ignoring the cases where there are causal loops making it difficult to distinguish the cause from the effect).

4.1.3 Key performance indicators for each risk

The table below shows the key performance indicators and the data required to quantify each risk.

Table 7

Risk	Key performance indicator	Data required
Forex risk	Currency rate trends	Daily spot rate
GDP decline	GDP trends	GDP figures countrywise
Inflation	Inflation trends	Inflation figures countrywise
Few suppliers	Number of suppliers (trend)	
	M&A activity	
	Total global capacity	Total global capacity for critical items
War		
Recession		
Political alignments		Demand
Treaties		Capacity
Political instability		Resource availability
Fire		Manufacturing cost
Accidents	Profit curves obtained via simulation	Transportation cost
Terrorism	Cost curves obtained via simulation	Inventory on hand
Earthquakes		
Hurricanes		
Floods		
Cyclones		
Volcanoes		
Landslides		
Snowfalls		
Draught		
Excess rainfall		
Bird flu		
SARS		
AIDS		
Supplier consolidation	M&A activity	Industry trends
RoHS	Percentage of hazardous elements	Bill of distribution,material composition
		of each part
Other environment laws	Compliance data	Compliance data
Sarbanes and oxley	Compliance data	Compliance data

Tax laws	Compliance data	Compliance data
Item unavilability	On hand balance	On hand for various periods
	Stockout history	Datewise stockout occurrences
	Historical inventory positions	
Excess inventory	Historical inventory positions	Historical inventory positions
Theft	Variance between physical and	Cycle counting and physical inventory
	recorded inventory	Results
Changes to product volume and mix	Planning percentages - timewise	Planning percentage
	Planned and actual production -timewise	Production data
	Number of models - timewise	Number of models
	Number of product families - timewise	Number of product families
Quality issues	Defect rates per million parts	Defect data - partwise,periodwise
Design changes	Number of ECO's (engineering change	ECO listing periodwise
	orders)	
Architectural issues	Number of ECO's	Number of ECO's
Uncertain yield	Yield % over time	Yield % over time
	Yield variance	Yield variance
Threat of substitutes		
Lack of substitutes	Number of critical items with no	Number of critical items with no
	substitutes	Substitutes
Uncertain cumulative lead time	Lead time variance	Lead time variance
Resource bottlenecks	% resource overload	% resource overload
Lack of alternate routings	Number of critical items with no	Number of critical items with no
	alternate routing	alternate routing
Process variability	Yield variance	Yield variance
	Lead time variance	Lead time variance
Changeover time	Changeover time/run time for critical parts	Changeover time,run time
Obsolesence	product life cycle time	product life cycle time
Competition	Market share trend	Market share trend
	Competitor's revenues	Competitor's revenues
Technology	Capital investment trends	**Capital investment trends**
Morale	Absenteeism , employee turnover	% employees absent (on Mondays,Fridays)
		Employee turnover
Training (lack of)	Average training days per annum	Average training days per annum
Trade unionism	Number of strikes	Number of strikes

Indiscipline	Number of incidents	Number of incidents
Lack of creativity		
Attrition	Employee turnover	Employee turnover
Shortage of talent	Days position open	Days position open
	Average days to hire	Average days to hire
Litigation	Litigation costs,number of cases	Litigation costs,number of cases
Rising procurement costs	Procurement costs vs time	Procurement costs vs time
Supplier capacity constraints	Supplier capacity	Supplier capacity
Design changes	Number of Engineering change orders w.r.t time	
	Design rework	Rework rate
Poor product quality	Defects per million parts	Defects per million parts
Supplier's financial condition	Supplier revenues and other financial metrics	Supplier revenues
IP infringement	Number of patents challenged	IP database (uspto.gov)
Dishonor of contract		
Suppression of facts		
Geographical separation		
Technical limitations		
Software bugs	Defect trends	
Software upgrades	Production downtime	
Network bandwidth	Latency, bandwidth MBPS	Latency,bandwidth MBPS
Software implementation costs	Earned value	Earned value
Supply chain modelling inaccuracies		
Poor data quality		
Poor planning and scheduling	Slack,on time completion,cost overruns	
Lack of standardization		
Blind imitation of industry standards		
Key person dependence		
Fargmented processes		
Lack of automation		
Poor supply chain visibility	Measurement of the bullwhip effect	Order sizes along the supply chain
Quality of roads		
Railways		
Airways		
Fuel costs	Cost vs time	Cost vs time
Port congestion		
Transportation costs	Cost vs time	Cost vs time
Carrier capacity	% overload	% overload
Carrier rating	Carrier rating	Carrier rating
Shortage of water and power	Hours lost in power outages/ total hrs	Hours lost in power outages/ total hrs
Buildings	Building cost, depreciation, market value	Building cost, depreciation, market value

Land	Land appreciation vs time	Land appreciation vs time
Capital equipment	Capital investment vs time	
Order cancellation	# of cancelled orders/ # of booked orders	# of cancelled orders/ # of booked orders
Returns	# of RMA/ # of orders shipped	RMA, Shipped orders
Customer delinquency	Accounts receivable	Accounts receivable
	Past due > 90 days	Past due > 90 days
Customer litigation		
Order outliers	Order size histogram	Order sizes
Irrational customer behavior	Incident tracking	Incident tracking

4.1.4 Data needed to measure the key performance indicators

The table also shows the data required to measure each risk.
The above data forms the basis for designing a dashboard to display supply chain risks.

4.1.5 Chapter summary

This chapter presents an approach to the identification of risks. Various supply chain risks are outlined and categorized in a top-down hierarchical manner to arrive at the root causes. The key performance indicators to measure various risks are identified along with the data needed to quantify these risks.

Section 5

"And there are the known unknowns and the unknown unknowns"
– Dr.David Simchi-Levi

5.1 Models for the evaluation of supply chain risks

This chapter identifies the various models used to evaluate supply chain risks. The use of different models is demonstrated with examples. The level at which risk is being managed (strategic, tactical or operational) and the company's maturity in terms of the risk management process which in turn determines the level of sophistication desired are important factors in deciding which models are applicable.

5.1.1 Bayesian risk model

The Bayesian model is good for tactical and operational risks. Bayesian theorem helps combine historical data and expert opinion. Consider the following pattern of material received from a supplier.

Table 8

Transaction	Delay
Received on day 1	2
Received on day 2	3
Received on day 3	4
Received on day 4	5
Received on day 5	2
Received on day 6	0

The probability of delay of receipts getting delayed by 2 days based on historical data is

P(delay=2) = 2/6 = 1/3
P(delay=3) = 1/6
P(delay=0) = 1/6 (This is the probability that the supplier will deliver on time)

Now, consider the expert opinion from the company's sales and operations meeting.

"Based on the discussions with the suppliers there is a 50% chance that the supplier will be delayed by 2 days and a 50% chance that the supplier will deliver on time".

Revaluate the probability that the supplier will deliver on time.

Let E= evidence based on the sales and operations meeting.
= 50% chance that the supplier will deliver on time
and a 50% chance of delay=2 days

Let $P(D_i)$ denote the probability of the material getting delayed by i days.

$P(E/D_0) = 0.5$
$P(E/D_2) = 0.5$
$P(E/D_3)=0$
$P(E/D_4) = 0$
$P(E/D_5) = 0$

$P(delay = 0 / E) = P(E/D_0) * P(D_0) / (SUM(P(E/D_i) * P(D_i))$
$= 0.5 * (1/6) / [0.5 * 1/6 + 0.5 * 1/3]$
$= 1/3$

- The risk of not delivering the material on time based on statistical forecast was $1 - 1/6 = 5/6 = 0.83$
- The risk of not delivering on time based on expert opinion was $\frac{1}{2} = 0.5$
- The risk of not delivering on time based on Bayesian theorem was $= 1 - 1/3 = 0.66$
- Therefore the inference based on historical data was pessimistic while the expert opinion was optimistic. Bayesian theorem arrived at a conclusion which "balanced" expert opinion with historical data.

5.1.2 Risk model based on strategic network optimization

Strategic network optimization is a powerful technique to assess and evaluate risks. It helps one perform a scenario based analysis of various sourcing strategies. Consider the following real example (names and data have been masked) .

> A large manufacturer of automobiles procures fuel injection pumps, a key component from two suppliers. The automotive manufacturer has three plants P1,P2 and P3. The total demand for vehicles is 150000 per annum. The unit cost of procuring pumps from supplier 1 is 1000 while from supplier 2 is 1500. Unit transportation costs are given below.

Table 9

	P1	P2	P3
Supplier (S1)	10	15	20
Supplier (S2)	12	17	22

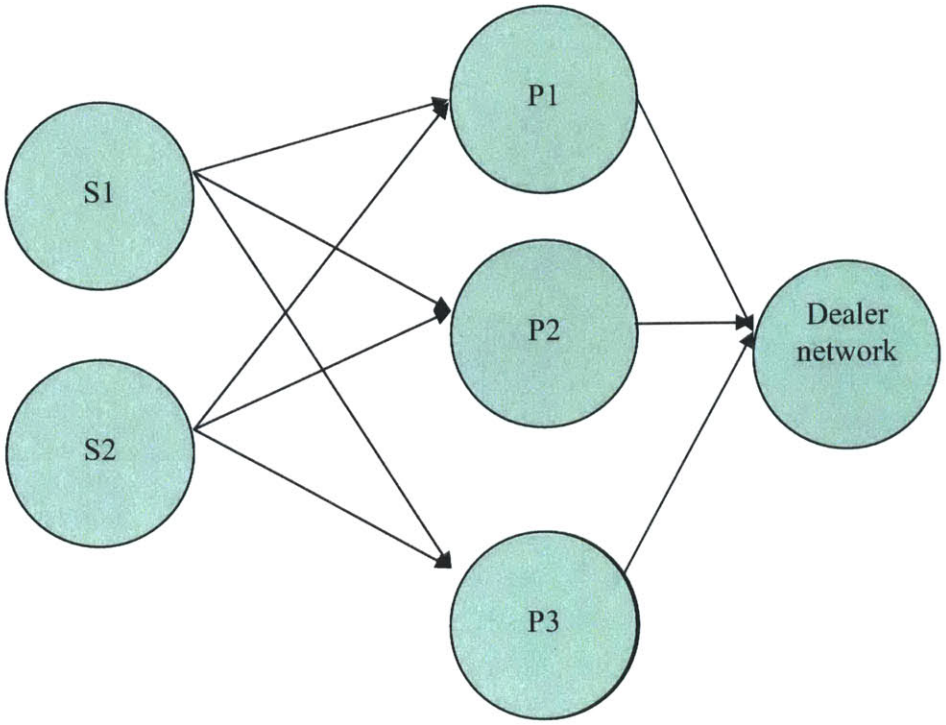
S1 has a capacity of 150000 while S2 has a capacity of 60000 per annum.
Each plant has a capacity of 50000 vehicles per annum.
Each vehicle sells for 10000USD.

Under these circumstances evaluate –

1. The maximum profit.
2. Analyze the scenario where S1's factor catches fire reducing its capacity .

The network is depicted below. (the dealer aspect of the network has been excluded from this analysis)

Figure 8 – Supply chain network of an automotive manufacturer for a certain part



Let $x_{ij}=0$ be the quantity procured by plant i from supplier j.
i=1,2 and j=1,2,3
Objective function
Maximize profit $\text{sum}(X_{ij} * P_{ij})$
Subject to the following constraints

Supplier capacity constraints

The total number of fuel injection pumps ordered from each supplier should not exceed their respective capacity.

$X_{11} + X_{21} + X_{31} <= 150000$
$X_{12} + X_{22} + X_{32} <= 60000$

Demand constraints
Assuming one fuel injection pump per vehicle and ignoring independent demand for fuel injection pumps, the total demand for fuel injection pumps cannot exceed the total market demand for the vehicles.

$X_{11} + X_{21} + X_{31} + X_{12} + X_{22} + X_{32} <= 150{,}000$

Plant capacity constraints
The total number of pumps ordered by each plant cannot exceed its capacity.

For plant P1 ,

$X_{11} + X_{12} <= 50000$

For plant P2 ,

$X_{21} + x_{22} <= 50000$

For plant P3 ,

$X_{31} + X_{32} <= 50000$

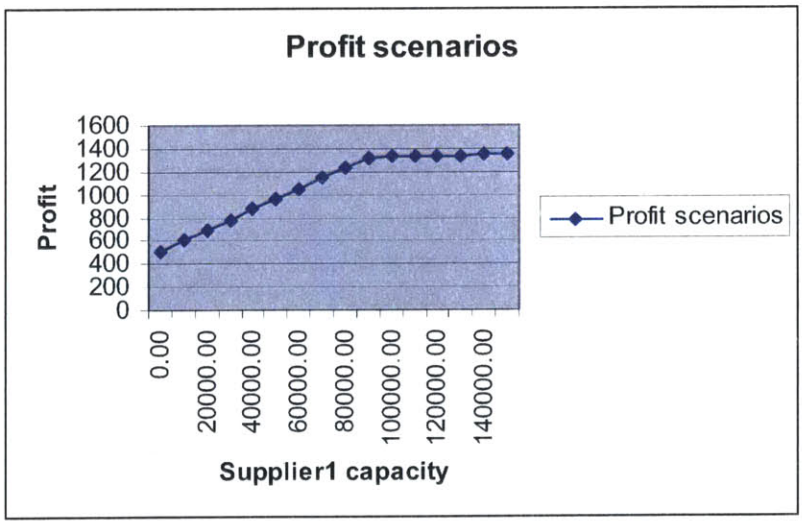
Integrality constraints

X_{ij} must be an integer.

Non negativity constraints

$X_{ij} >= 0$

Figure 9



As illustrated in Appendix 1, the optimal solution to the above integer linear programming problem is a profit of $1348M USD. Also, the recommended sourcing is 50000 from supplier 1 and 100,000 from supplier 2. Now, investigate various scenarios to model the situation where the supplier's factory catches fire thereby reducing their capacity to produce fuel injection pumps. The solution below has been computed using solver tables by varying the capacity of the supplier from 0 to 150000.

It is obvious from the above graph, that profit starts to decline if the supplier's capacity drops below 90000 which is 60% of their full capacity.

The model can be enhanced to include multiple periods and handle stochasticity.

5.1.3 Risk model based on failure mode and effect analysis

Failure mode and effect analysis is a valuable tool to quantify and prioritize tactical risks.

Simply stated, FMEA attempts to answer the question "Where can things go wrong ?" It is based on the concept of risk volume which is the product of the likelihood of occurrence, the severity of impact and the detectability of the risk. Risks that have a high risk volume receive high priority. Failure mode and effect analysis also tracks the actions taken in response to the risk and the risk volume after the action was taken.

The following table depicts a typical FMEA analysis.

Table 10

#	Process Function (Step)	Potential Failure Modes (process defects)	Potential Failure Effects (Y's)	SEV	Potential Causes of Failure (X's)	OCC	Current Process Controls	DET	VOL	Recommend Actions	Responsible Person & Target Date	Taken Actions	SEV	OCC
1	Sourcing a critical item	Item unavailable	Loss of business	5	Fire in the supplier factory	2	None	5	50	1.Alternate source	John	1	2	2
2										2.Block supplier's remaining capacity				
3										3.Maintain buffer stock				
4		item does not match specifications	Loss of business	5	Design change	4	None	1	20	Provide visibility to engineering change orders to suppliers	John		5	1
5			Loss of quality	4	Communication issue	3	None	3	36	Implement collaborative design tool	IT		4	1
6														
7									106	STARTING TOTAL RISK VOLUME		TOTAL RISK VOUME AFTER ACTION		

FMEA is carried out for each supply chain activity. For example, consider the activity procuring (sourcing) a critical item from a supplier. Continuing the example, the process can fail in several ways, for example, the supplier may simply fail to deliver the item or the delivered item may not match the specifications.

The effect of the first failure mode is a loss of business. The effect of the second failure is a loss of quality. The effect should be assigned a weight from 1 to 5, 5 being the most severe and 1 being the least severe. FMEA should be conducted with all the stakeholders present and the severity should be arrived at after thorough discussions. In my experience, FMEA for one process might require three to four hours of discussions with stakeholders. The role of a moderator is vital to a successful FMEA. Having assigned a weight to the severity of the occurrence, the next step is to identify the cause of the failure. For example the cause of failure to deliver may be a fire in the supplier's facility or the cause of poor quality could be communication issues. The master logic diagram developed previously could serve as an aid to identifying the root causes.

The next step is to assign the likelihood of occurrence to each cause on a scale of 1 through 5, 5 being the most likely and 1 being the least likely. Then, document controls,

if any, that would help detect the cause in advance. Causes with no controls would generally have poor detectability and hence would receive a 5. On the other hand causes that can be detected well in advanced are highly detectable and receive a 1. For example, design changes can be detected far in advance while a fire at a supplier cannot. Risk volume is then the product of the severity, the likelihood, and the detectability. The higher the risk volume, the more prone the process is to failure. The soft spots in the supply chain are the processes that have a high risk volume. Finally, recommended actions and actions ultimately taken must be documented. It can be generally expected that risk volume will decrease after the actions have been taken unless the actions themselves introduced failure modes that increased the overall risk volume.

The advantages of FMEA are that it can be performed without requiring the users to have advanced knowledge of quantitative techniques. The other advantage is that FMEA automatically results in a risk mitigation plan.

The disadvantages are subjectivity in the assignment of weights and the lengthy nature of the process. Moreover, it does not capture the complex interaction between processes. Prof. Yossi Shafi, Prof. Steven Spear, and other academicians have argued that vulnerabilities arise as a result of the extremely complex interactions between processes, as is evident from disasters such as Union Carbide's Bhopal gas disaster. FMEA, nevertheless, is a powerful technique if an organization is just starting to implement risk management and if the risks being considered are tactical or operational in nature.

5.1.4 Simulation based risk model

Simulation based models are very useful when it is important to perform a "what if" analysis for various scenarios, graphically observe the flow of material and/or information for various scenarios, or automatically derive key performance indicators such as cycle time for various scenarios.

The following graph revisits the same example previously discussed with 2 suppliers and 3 plants, The graph drawn using igrafx software represents a cross section of the supply chain with 2 suppliers and 1 plant. The activities being performed at the manufacturer's end are.

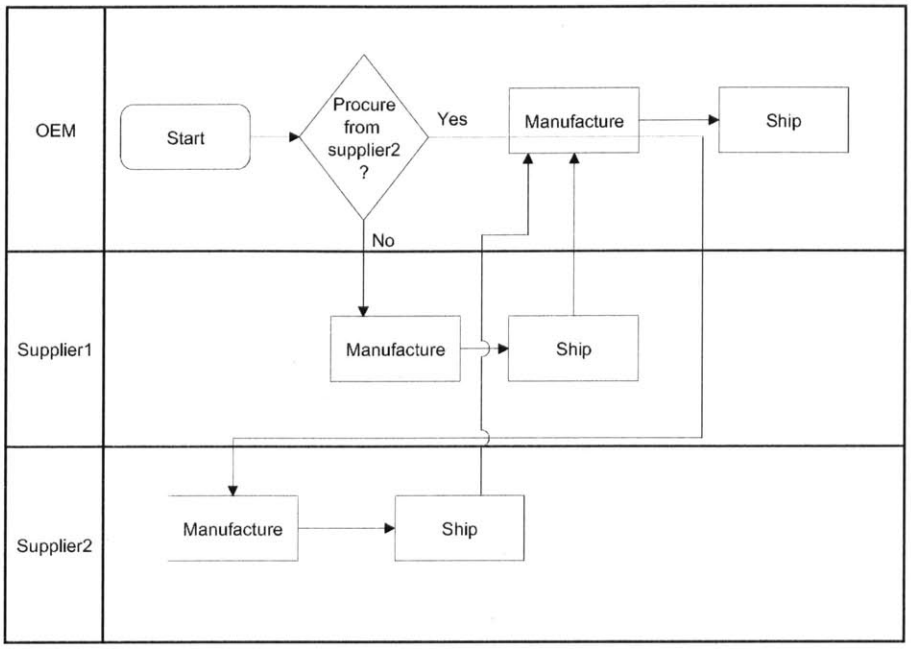
1. Procuring material from the supplier.
2. Manufacturing using the components supplied by the supplier.
3. Shipping the product to distribution centers.

The activities being performed at the supplier's end are –

1. Manufacturing the ordered part.
2. Shipping it to the OEM.

The figure below represents the cross section of the supply chain being simulated in this model.

Figure 10



The other parameters to the initial model are given below.

Table 11

Parameter	Value	Comments
End demand	Interarrivals time normally distributed between 1 and 3 days.	In other words each sales order is received between 1 and 3 days on the average by the OEM
Simulation horizon	90 days	
Size of each sales order	1 unit per sales order	
Sourcing split	50:50 between supplier 1 and supplier 2.	
Manufacturing lead time at the supplier 1	Normally distributed between 3 and 5 days	
Transportation lead time from supplier1 to OEM	Fixed time of 3 days	
Manufacturing lead time at the supplier 2.	Constant 3 days.	
Transportation lead time at the supplier2	Normally distributed between 15 and 20 days	
Manufacturing lead time at the OEM	Normally distributed between 3 and 5 days	
Capacity constraints	Represented by the lead times.	
Resource constraints	Represented by lead time. Not modeled explicitly.	
Transportation lead time from OEM to distributor	Constant 3 days	

Simulation results for the original model

The simulation was run for a period of 90 days. The results are summarized below.

Table 12

Transaction Statistics (Days)							
Count	Avg Cycle	Avg Work	Avg Wait	Avg Res Wait	Avg Block	Avg Inact	Avg Serv
45	20.6	20.6	0	0	0	0	20.6

Table 13

Transaction Statistics (Days)								
	Count	Avg Cycle	Avg Work	Avg Wait	Avg Res Wait	Avg Block	Avg Inact	Avg Serv
OEM	45	7.06	7.06	0	0	0	0	7.06
Supplier1	23	7.05	7.05	0	0	0	0	7.05
Supplier2	22	20.33	20.33	0	0	0	0	20.33

Table 14

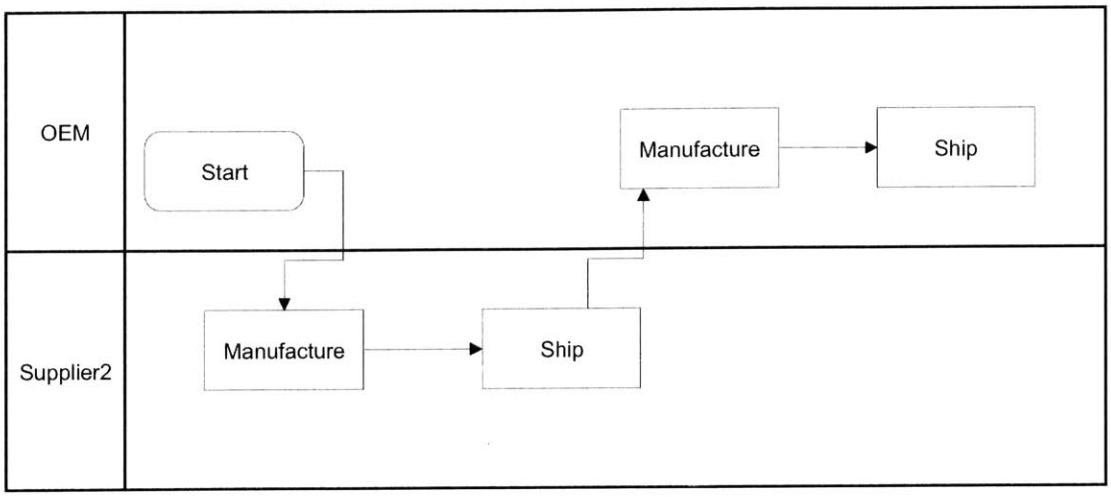
Activity Statistics (Days)								
	Count	Avg Cycle	Avg Work	Avg Wait	Avg Res Wait	Avg Block	Avg Inact	Avg Serv
OEM – Start	45	0	0	0	0	0	0	0
OEM - Manufacture	45	4.06	4.06	0	0	0	0	4.06
OEM – Ship	45	3	3	0	0	0	0	3
OEM - Procure from supplier2 ?	45	0	0	0	0	0	0	0
Supplier1 – Manufacture	23	4.05	4.05	0	0	0	0	4.05
Supplier1 – Ship	23	3	3	0	0	0	0	3
Supplier2 – Manufacture	22	3	3	0	0	0	0	3
Supplier2 – Ship	22	17.33	17.33	0	0	0	0	17.33

As indicated in the tables above, the average lead time from the placement of an order to the delivery of the item is 20.6 days. It is also obvious that the bottleneck activity is shipment from supplier 2 with an average cycle time of 17.33 days.

Now, model the scenario whereby supplier 1 has a fire in their factory thereby reducing their capacity to 0. The new supply chain graph is depicted below.

Revised model with supplier1 capacity reduced to 0

Figure 11



Simulation results

Table 15

Transaction Statistics (Days)								
Count		**Avg Cycle**	**Avg Work**	**Avg Wait**	**Avg Res Wait**	**Avg Block**	**Avg Inact**	**Avg Serv**
	45	27.5	27.5	0	0	0	0	27.5

Transaction Statistics (Days)								
	Count	**Avg Cycle**	**Avg Work**	**Avg Wait**	**Avg Res Wait**	**Avg Block**	**Avg Inact**	**Avg Serv**
OEM	45	7.06	7.06	0	0	0	0	7.06
Supplier2	45	20.45	20.45	0	0	0	0	20.45

Transaction Statistics (Days)								
	Count	Avg Cycle	Avg Work	Avg Wait	Avg Res Wait	Avg Block	Avg Inact	Avg Serv
Process1	45	27.5	27.5	0	0	0	0	27.5

Activity Statistics (Days)								
	Count	**Avg Cycle**	**Avg Work**	**Avg Wait**	**Avg Res Wait**	**Avg Block**	**Avg Inact**	**Avg Serv**
OEM - Start	45	0	0	0	0	0	0	0
OEM - Manufacture	45	4.06	4.06	0	0	0	0	4.06
OEM - Ship	45	3	3	0	0	0	0	3
Supplier2 - Manufacture	45	3	3	0	0	0	0	3
Supplier2 - Ship	45	17.45	17.45	0	0	0	0	17.45

As seen in the above table, the average order to delivery lead time increased by 33% from 20.6 to 27.5 when supplier 1 could not supply any product. This assumed that supplier 2

had the capacity to meet the excess demand. It is therefore obvious that even under ideal condition, the impact of disruptions could be severe. The impact is exacerbated by real world constraints such as finite supplier capacity, resources, shifts, calendars, and human factors such as motivation and morale.

5.1.5 Chapter summary

Four models were presented in this chaper.

1. Model based on Baye's theorem.
2. Model based on a mixed integer programming problem.
3. Model based on failure mode and effect analysis
4. Model based on simulation of what-if scenarios.

Bayesian model is suitable to employ at tactical levels over a horizon spanning a few months. While it is useful for analysis such as the risk of stock outs or for combining historical forecasts with expert opinion, it is not suitable for strategic risk modeling such as plant rationalization (an example would be an automobile company deciding which plants to shut down).Also the Bayesian model assumes the availability of historical data and the delicate processes of sales and operations planning. This implies that the organizations demonstrate a prerequisite high level of process maturity. Network optimization based on mixed integer programming models is applicable at the strategic level over a longer planning horizon. These models are suitable for events that have a low likelihood but a very high magnitude of disruption. Events such as loss of factory in a fire or terrorist attacks can be simulated using the network optimization model. The advantage of this model over those that require catastrophe modeling is that it does not require the probabilities of the occurrence of the hazard. In fact the model assumes the probability to be 1. Failure mode and effect analysis are suitable at the operational level where there could be many events of low to medium magnitude which cumulatively pose a high risk of disruption. FMEA can be performed at the strategic level in conjunction with the network optimization models. The advantages of this model include simplicity, the involvement of stakeholders, and most importantly, stakeolder prioritization of risks. The very act of stakeholder involvement creates a sense of accountability ,urgency, and ownership. The drawback though is that it tends to be a drawn out process and is, to a certain extent, a subjective model. Furthermore, it fails to capture the complex interactions between various processes. Simulation based models can be used at all levels and for all planning horizons. The advantages of modeling using simulation software are graphical display, easy tuning of parameters, and automatic computation of key performance indicators. The biggest drawback is the inaccuracy introduced in the model due to simplifying assumptions such as resource constraints or calendars. On the other hand, without such simplifying assumptions, the model would soon become unwieldy.

The following table compares and contrasts the four models.

Table 16

Factor	Baye's theorem	Network optimization	FMEA	Simulation
Level	Tactical	Strategic	Any	All
Horizon	Months	Years	Weeks, months	All
Severity of risk	Low-medium	Very high	Low-medium	Low-medium
Likelihood of risk	Any	Low	Any	Any
Organization maturity expected	High	High	Low	Low
Quantitative vs qualitative	Quantitative	Quantitative	Mix	Mix
Examples of risk modeling	Stockouts, forecasts	Hazards, terrorist attacks	Transportation delays, machine breakdowns	Lead time variability, Port strikes

Section 6

"An ounce of practice is worth a pound of theory" – English proverb.

6.1 Case study 1: Risk identification of the supply chain for a large financial institution

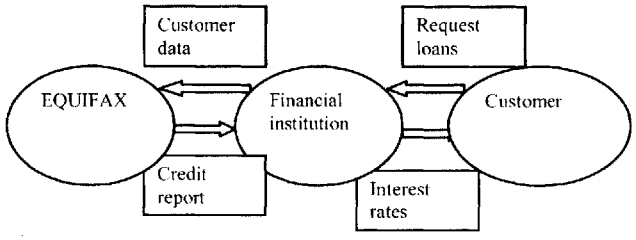
This case study deals with the risk identification of one of America's largest financial institutions. The expert interview method was employed to develop the case study. Two in depth sessions with a senior executive of the supply chain division were conducted to identify and assess risks[9].

The annual supply chain related costs of this company are several billion dollars per annum[10]. The supply chain mostly deals with indirect procurement (i.e procurement of goods and services that are indirectly related to the company's products and services.) of goods and services from their suppliers. For example, such goods are office supplies, materials for facility construction, carpets, windows, landscaping, hardware, and software. Examples of services are on-line bill payment service provided by a third party or credit checking provided by EQUIFAX. The main categories of supply chain costs are spending on technology infrastructure such as computers, network equipment and other devices; corporate real estate and facility maintenance consumer products such as mortgage appraisal, money counting and fund transfer.

6.1.1 Salient aspects of their supply chain

The company's supply chain strategy includes the risks associated with not only physical goods but also services such as credit checking or on line software.
For example consider the following service supply chain.

Figure 12



EQUIFAX provides customer credit reports to the financial institution which in turn determines the interest rates of loans based on the report.

Risk assessment is done at a frequency based on the supplier's tier ("tier" implies the criticality of the supplier, not the conventional meaning). Suppliers have been categorized into tier 1, tier 2, and non tier suppliers. There are about 500 tier 1 and tier 2 suppliers who undergo risk assessments at a greater frequency. Criticality of a supplier is determined based on the volume as well as the risk of doing business with them.

[9] Name of the executive not revealed to protect confidentiality.
[10] Exact costs masked to protect confidentiality.

Customization of goods and services makes it difficult to have more than one supplier. The risk mitigation strategies the company adopts are relationship building, monitoring through on site audits and supplier rating. However certain goods and services are commodities. The risk mitigation strategy employed for such good and services is supplier backup. The ARIBA exchange platform is extensively used for indirect procurement. About 10 to 15% of the company's suppliers are on this platform and it is estimated that they save 2-3% of the transactions costs due to this platform. Large suppliers serve more than one customer. Also, these suppliers are geographically dispersed throughout US.

Risk identification
The institution has identified critical 15 categories of risks. A questionnaire comprising of a total of 298 risks, is sent to each supplier and to the concerned departments within the company. This gives a fairly quantitative assessment of the risks involved. The process employs the FMEA model described earlier in chapter five. A key observation is that the risks are more or less the same as described earlier in chapter two, however, the classification of risks is specific to the company and industry. In fact, the executive stated that one of the important requirements from the decision support system would be to add new risk categories or modify existing ones which implies that risk perceptions are dynamic.

Risk Categories

The following are the major categories of risks encountered when making indirect purchases from the suppliers.

Market commodities
Risks associated with market commodities result from the following factors:

- Contract pricing concerns
- Lack of market data
- Geographical risk
- Market changes
- Risk of obsolescence
- An example of obsolescence would be the on line bill pay provider not coping up with the migration from html to xml.

Intellectual assets
An important consideration is the core competence of the supplier. For example, evaluating if the supplier has six sigma talent ?

Financial risks

- Solvency of the supplier
- Bankruptcy
- Errors in invoicing
- Having the right controls in place
- Alignment of goals with the supplier.

Ethics

- Compliance with international standards
- Are material facts disclosed by the supplier ?
    - For example, disclosing that their CEO is about to leave the supplier's company or is about to sell key businesses .
- Fraud
    - e.g Are we dealing with suppliers likely to commit an accounting fraud ?
- Briberies and kickbacks
    - Do they resort to briberies and kickbacks to get work done?

Contractual risks

- Subcontracting to others
- Do they understand the contract with the financial institution?
- Do they have a process to ensure that subcontractors meet the terms and conditions of the financial institution's contract ?

Information protection

- Do supplier's share data inappropriately?
- Do they have information security gaps?
- Can they remediate information security problems ?
- Do they have information security plans?

Concentration

Single source of supply – This typically happens for their customized products.

Compliance

- Do they know the laws?
- Are they aware of the regulatory environment they operate in?
- Do they have the funding to ensure regulatory compliance?
- Do they have visibility to their supplier's plans?
- Do they expose the financial institution in any way to compliance risks?

Business continuity

- Financial stability of suppliers.
- Disaster recovery.
- Geographical proximity of suppliers making them all vulnerable to a single natural disaster.
- Impasse between the financial institution and the supplier.
- Failure to recover from disaster.
- Failure to share business recovery plan.
- Failure to provide monthly feedback of financial performance.

Technology

- Risk of over customization of software.
- Failure to forecast increase in volume.

- Inadequate testing.
- Lack of software development lifecycle.
- Inability to meet industry standards.
- Inability of the IT department to communicate needs to vendors.
- Inability to advance technology.
- Aging technology (e.g COBOL)
- Risk of using open source
- Inability to sunset old technology and replace with modern one.

Program risks

- Poor program management.
- Financial institution's capabilities to execute and monitor the program.

Privacy

- Transmission and retransmission of sensitive data.
- Misuse of data by the supplier. e.g Using data for non approved purposes.
- Violation of HEPA regulations.
- Inability to handle breach of privacy complaints.

Physical security

- Physical security of locations.
- Monitor access to buildings.
    - e.g cards to get in.
- Safety of people.
- Environmental conditions.

Performance

- Quality
- On time delivery
- Price

Offshore activities

- Failure to identify off shoring by suppliers.
    - e.g Some data given to the suppliers cannot leave US soil.
- Lack of process to approve supplier off shoring.
- Enforce rights and laws internationally.
- Lack of clarity.
- Federal regulations.
- Monitoring service level agreements (SLA's).
- Risk of data residing outside US even when it is allowed.

Risk mitigation strategies

The institution currently adopts the following strategies to mitigate risks.

Supplier portfolio index

This index measures combines three scores with 1/3 weight given to each.

- Supplier certification as performed by management.
  - The certification is based on factors such as their knowledge of policies and procedures.
- Supplier's performance appraisal
  - This is based on a well defined performance matrix.
- Composite supplier risk index
  - This is based on their responses to the risk factors presented earlier.
- On site inspections
  - On site inspections are carried out frequently.
- Web based systems for data acquisition from suppliers
  - The data includes orders, invoices, payments, financial statements etc.
- A holistic view of supply chain risks combining goods and services, hardware and software.
  - They have a dedicated team for supply chain risk management.
- Tiering of suppliers and rigorous monitoring of the critical ones.

6.1.2 User's inputs on the decision support system

The executive stated that the decision support system should have at least the following features:

- Flexibility to add new categories of risks.
- Receive data from suppliers.
- Keep track of updates.
- Supplier scorecard.
- Good reporting tool breaking up the analysis by suppliers and categories.
- Keep track of updates.
- Collaborative.

6.1.3 Case study summary

The case study provided insights into the risks associated with indirect procurements, an important element of supply chains. While the risk factors are almost the same as identified earlier in chapter 4, their classification into risk categories may vary based on the company and the industry. The study confirmed the utility of the FMEA model for strategic and tactical risk assessments. The user's confirmed the utility of having a decision support system and also enlisted their key requirements from such software.

6.2 Case study 2

Strategic risk assessment for a global packaging giant

The following case study evaluates the strategic risks associated with the operations of a global Fortune 200 company's Indian subsidiary[11]. This company is a diversified global

[11] Name of the company withheld as per the request of the senior executives.

manufacturing company engaged in the design and production of an array of highly engineered fasteners and components and consumable systems and specialty production and equipment. They have 625 decentralized operations in 44 countries and employ 47500 personnel who are focused on innovating solutions and products for their customers. The Indian subsidiary offers unique solutions to diverse industry verticals spanning across the following segments.

Industrial packaging solutions
The Indian subsidiary has two manufacturing sites which provide packaging solutions such as strapping, wrapping, taping, protective packaging, contract packaging and consulting to a wide range of industries including automobiles, steel, textile, FMCG and fiber.

Speciality chemicals and equipment
This array of solutions caters to the needs of the maintenance, repair and overhaul (MRO) segment of the industry through its manufacturing facilities in India.

Engineered components and specialty fasteners
The specialty fasteners and engineered components primarily serve the needs of the automotive and appliances industries.

The Indian subsidiary employs about 700 personnel and reaches out to their customers through a network of 16 offices and 200 dealers and distributors. They export their products to various countries including SAARC, ASEAN and African and Middle Eastern countries.

Approach to risk identification
The approach to risk identification included a visit to their plant in 2004 and day long discussions with their executives and officers including the plant controller, the head of the manufacturing department, and the head of the quality department. Also, extensive telephonic conversations were recently held with their plant controller. The focus of these conversations was on the supply chain risks associated with their steel strap plant.

Supply chain for the steel straps

Figure 13

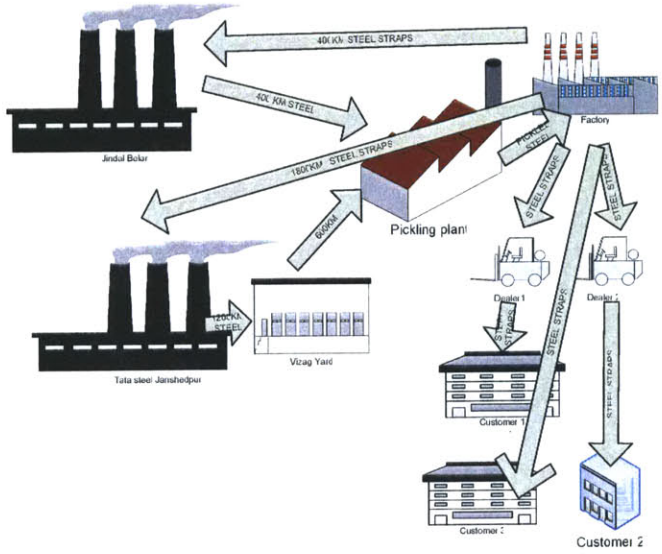


Figure 15 illustrates their steel strap's network in India.

They have a large plant located near a metropolitan city in India which manufactures steel straps. Raw material required for steel straps are steel, procured from two major steel companies in India in the form of hot rolled coils (HR coils). 'Each coil carries about 10 to 20 tons of steel. The steel procured from both suppliers

contains medium carbon which is useful in preserving the strength and other special qualities of straps. Only two suppliers provide this kind of steel required for making steel straps. One of the suppliers is located at a distance of 1800 km, but they have a yard located at about 600 km which stores about 15 to 20 days of inventory. The yard is located in the same state as the steel strap plant and hence serves to reduce local taxes and tariffs. The other supplier's plant is located in the same state and is about 400 km. The suppliers are giant companies and as such do not have capacity constraints. Their annual capacity is close to 4 million tons of steel each. However, each supplier has a memorandum of understanding with the company to provide them a certain quantity each year. This memorandum is not legally enforceable however it helps the company get volume discounts for the purchase of steel. Production yield is about 95% which means for every ton of strap produced about 1.05 ton of raw material is required. Steel is first received by a contract manufacturer who "pickles" it before sending it to the steel strap plant. Pickling is the process of removing dust and other impurities from steel.

Product variation

Steel straps vary in thickness and width. Monthly production is done for a given thickness and width.

Lead times and capacities

The order to delivery times for raw material is 1 to 2 months for both suppliers. However, demand is more or less uniform throughout the year which yields accurate forecasts. The steel strap can produce up to 2500 tons per month but is constrained by the capacity of the contract manufacturer who can only pickle up to 2000 tons per month.

Profit margins

The following table gives the breakup of costs for various sales channels and the estimated profits associated with each.

Table 17

Sales channels	Selling Price (per ton)	Raw material (per ton)	Tax	Mfg cost (per ton)	Transportation cost per ton	Pickle costs	Profit per ton
J	75000	30000	700	25000	1200	1000	17100
T	75000	30000	700	25000	3200	1000	15100
Dealers	50000	30000	700	12000	0	1000	6300
Direct sales	50000	30000	700	12000	0	1000	6300
Contracts	75000	30000	700	25000	2000	1000	16300

Overheads are not included in the manufacturing costs. The manufacturing costs do include direct labor. Also, contracts vary widely in size and scope. The one shown above represents an average contract.

Sales channels and the customer facing supply chain

The company has 2 major channels – direct and distributors. The direct channel accounts for 70% of the business. The direct channel is comprised of contract packaging which is 20% of the direct channel business and direct sales (to customers) which is about 80% of

the direct channel business. Distributors are located in major cities and industrial towns and do not carry much inventory. In addition to selling the steel straps, contract packaging involves providing packaging solutions on site such as labor and material. Contract packaging typically has higher profit margins and higher risks. Interestingly the two major suppliers are also their important customers. One of them buys 70-80 tons of steel straps per month while the others buys 150 tons per month. The steel strap plant also has an on site packaging contract which includes the management of their packaging supply chain. For example, to package the steel being produced by one of the suppliers, they need labor, about 70 special parts, and steel straps on site. The management of this supply chain is done by the steel strap company. The 70 parts are procured from several sources. A bill of material indicates the hourly labor and material quantity that goes into steel packaging. Rates are revised with these suppliers every quarter.

Problem statement formulation

This case study focuses on the following scenarios.

1. The impact of disruption to the steel strap plant on profits.
2. The impact of supplier 1 disruption on profits.
3. The impact of supplier 2 disruption on profits.
4. The impact of the disruption to both supplier 1 and 2 on profits.

A linear problem (LP) will be formulated and capacities involved in each of the four scenarios will be varied to observe the change in profits

Model assumptions

1. Formulate a simple single period, deterministic LP.
2. Ignore the variations in cost and prices and use average values.
3. Demand from all distributors is lumped.
4. Demand for contract packaging is also lumped, however, the demand from the two steel suppliers is treated separately.
5. Tax complexities and the impact of volume discounts are ignored.
6. The supply chain management of the 70 parts and labor at the supplier's site is ignored due to the lack of data.
7. The raw material required is available at the start of the period.
8. Steel strap plant and the dealers carry minimal inventory.

Linear Problem formulation

Appendix 4 illustrates the LP solution using solver and sensitivity analysis using solver tables. The LP formulation is given below. Let T and J be the two suppliers.

Variables

Let:

D_j = Demand from Supplier J in tons/month

D_t = Demand from Supplier T in tons/month

D_d = Dealer's demand in tons/month

D_{direct} = Direct Sale Demand in tons/month
$D_{contract}$ = Demand for Contract in tons/month

Objective Function:
Maximize Profit

$$17100 \times D_j + 15100 \times D_t + 6300 \times D_d + 6300 \times D_{direct} + 16300 \times D_{contract}$$

Supply Demand Constraint

∑supply x ∑demand
Plant capacity (P_c) = 2500
Plant inventory (P_i) = 0

$$D_j + D_t + D_d + D_{direct} + D_{contract} \leq 2500 + 0$$

Raw material requirement constraint

Let:
S_{sj} = Supply of raw material by supplier J
S_{st} = Supply of raw material by supplier T
I_{st} = Inventory at Supplier T's yard

Total raw material supply:
$= S_{sj} + S_{st} + I_{st}$
Product yield PY = 0.95

Total Raw Material Required
$= (D_j + D_t + D_d + D_{direct} + D_{contract})/ Y$

Total Raw material supply ≤ total raw material required + 20 tons

$$S_{sj} + S_{st} + I_{st} \leq [(D_j + D_t + D_d + D_{direct} + D_{contract})/ Y] + 20$$

As per business rule
S_{sj} = 50% of total demand for raw material
$= 0.5 \times [(D_j + D_t + D_d + D_{direct} + D_{contract})/ Y]$

Similarly
S_{st} = 50% of total demnad for raw material
$= 0.5 \times [(D_j + D_t + D_d + D_{direct} + D_{contract})/ Y]$

Demand Constraint as per Business Rule

$$D_j \leq 80$$
$$D_t \leq 150$$
$$D_d \leq 0.3 \times (D_j + D_t + D_d + D_{direct} + D_{contract})$$
$$D_{direct} \leq 0.56 \times (D_j + D_t + D_d + D_{direct} + D_{contract})$$
$$D_{contrac} \leq 0.14 \times (D_j + D_t + D_d + D_{direct} + D_{contract})$$

Pickling Capacity Constraint

Pickling Capacity = 2000

$$(D_j + D_t + D_d + D_{direct} + D_{contract}) \leq 2000$$

Nom Negativity Constraint

$$(D_j, D_t, D_d, D_{direct}, D_{contract}) \geq 0$$

Results

The tables below indicate the maximum profit per month under normal circumstances, the supply allocation for maximum profits across sales channels, and the profits for the four disruption scenarios outlined in the problem statement.

Table 18

Demand	J	T	Dealers	Direct sales	Contracts		Total demand
	80	150	600	890	280		2000

Sales channels	Selling Price per ton	Raw material Per Ton	Taxes	Mfg cost Per Ton	Transportation cost Per ton	Pickling	Profit Per Ton
J	75000	30000	700	25000	1200	1000	17100
T	75000	30000	700	25000	3200	1000	15100
Dealers	50000	30000	700	12000	0	1000	6300
Direct sales	50000	30000	700	12000	0	1000	6300
Contracts	75000	30000	700	25000	2000	1000	16300
Profit per ton	17100	15100	6300	6300	16300		

Objective function	B2*B11+C2*C11+D2*D11+E2*E11+F2*F11
Maximize profit	17584000

Table 19

Constraints			
Supply-demand constraint			
H capacity	2500		
H inventory	0		
H surplus capacity	500		
Raw material requirement constraint			
Steel from J	1052.631579	J capacity =	2000
Steel from T	526.3157895	T capacity=	2000
Inventory at Vizag	500	Pickling capacity=	2000
Total raw material supply	2078.947368		
Production yield	0.95		
Total raw material required	2105.263158		
Raw material supply-demand EQUALS	-26.3157895		
15-20 days of inventory	1000		
Total contract demand	510		
Demand constraints			
J demand >	70		
J demand <	80		
T demand =	150		
Dealer demand <=	600		
Direct sales <=	1120		
Total contract demand constraint <=	280		
Pickling capacity constraint (total demand) <= 2000			
Non negativity constraints			

Figure 14 - Profit curve for different capacities of the manufacturer's plant.

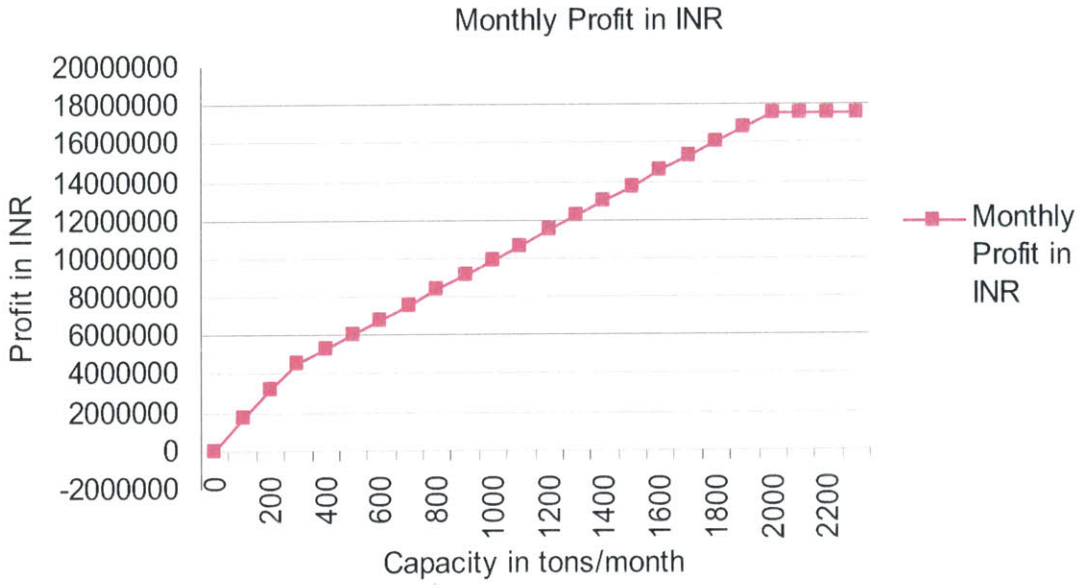


Figure 15 - Assume that T cannot meet the extra demand caused by J's capacity reduction.

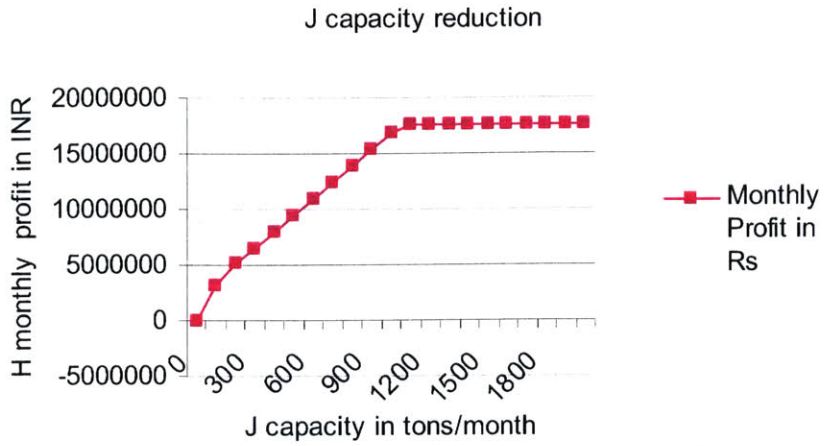
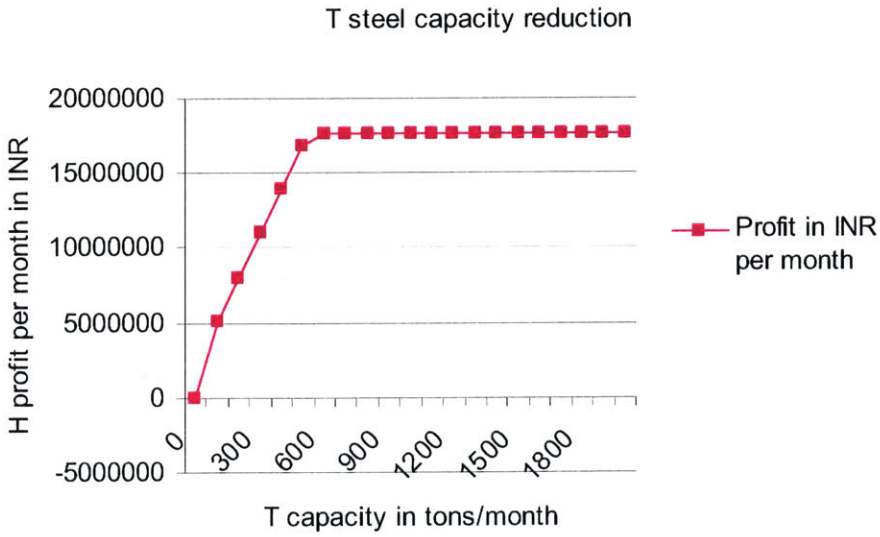


Figure 16 – T capacity reduction



Conclusions of the case study

The following risks were identified as a result of the case study.

RISK	DESCRIPTION
Monospony	J and T are major customers as well as suppliers. Monospony , monopoly and the size of their operations gives them leverage.
Monopoly	J and T might raise the price of steel and bargain hard for the buying price of steel straps.
Pickling	Pickling operation is highly capacity constrained. Single point of failure.
Contract risks	High profit margins but high risks as well due to the management of 72 items and resources for them. Mitigate them by direct or dealer sales.
Cyclicity	Steel industry is cyclical. It is a sunset industry in the west.
Disruption to H plant	This risk may have low likelihood but has high consequences. As seen from the figure, profits will decline steadily as plant capacity declines due to disruption. Plant insurance is therefore a must. The chart should be used to determine the maximum limits of liability.
J and T capacity	Minimal risk. Dual source of supply buffers risks. Impacts of J,T and both getting disrupted are shown in the results section. Negotiate with J to build a buffer at an intermediate location. T's yard at Vizag provides risk pooling. Therefore the impact of disruptions to T's capacity is not as severe as J's.

6.3 Chapter summary

Both case studies validated the FMEA and strategic network optimization approaches to risk management. While the first case study dealt with the indirect procurement of a large financial institution, the second one dealt with a fortune 200 company's operations in India. While the risks identified in both cases studied were already outlined in the master logic diagrams presented earlier, it must be emphasized that each company is pre disposed to certain kinds of risks based on the industry, geography, culture and business climate at a given time. This is similar to individuals being pre disposed to certain kinds of diseases based on factors such as genetics, lifestyle, and season. The recommendation therefore is to conduct risk assessments at the company level just as physicians examine each patient.

Section 7

We create and destroy
And again recreate
In forms of which no one knows
-Al-Waquiah Qu'ran 56:61]
Excerpted from 'Wings of Fire' by Abdul Kalam

7.1 Design of the decision support system

7.1.0 Key overview ideas

The decision support system would be split conceptually into *planning* and *monitoring*. Planning would represent the forward feed loop indicated in the synthesized framework in chapter three. Monitoring would represent the feedback loop. The decision support system would analyze strategic risks using strategic network optimization software which in turn is based on the network model illustrated earlier.[12] A key enhancement however would be to break the network systematically to represent a disruption. Losses associated with disruptions would have to be calibrated on a scale of one to five before running the optimizer. Tactical risks will be obtained from the plan runs of the supply chain planner, demand planner, inventory planner, and transportation planner.[13] Conventional supply chain and demand planners generate exceptions at each run. These exceptions are risks to be fed into the risk planner. Operational risks would be obtained from execution systems, specifically order management, transportation execution, and work in process systems. The risk planner would then present the users with all the risks obtained from the strategic network optimizer, the supply chain, demand, inventory planners, etc. Risk planners would then be able to prioritize those using FMEA analysis and take actions. The monitoring tools would provide the dashboard based on FMEA analysis. Users would be able to drill down to the root causes of the risks from the dashboard. Additional features provided by the software would be the ability to record expert interviews, auditing, seamless integration with leading SCM software, hooks to provide access to third party software or write custom code and personalization of the user interface to link sources of risk related information such as weather monitoring systems ,currency fluctuations, stock analysis and the patent database. Another interesting feature would be the ability to record learning and also store maps and pictures of all the parts of the plant.

7.1.1 Key features

Discussions with various companies revealed that supply chain risk management has traditionally been done using excel spreadsheets and macros. Data is typically imported manually into spreadsheets. The key design considerations include the following.

---

[12] Logictools, Oracle and other vendors provide this software.
[13] Vendors such as Oracle,SAP and others provide these tools.

A holistic view of risks
Despite the proliferation of tools that cater to various aspects of the supply chain, none of them provide a holistic view of risks. Moreover the exceptions generated by these tools do not give estimates of the magnitude of the impact associated with them and also fail to suggest and track actions to resolve them.

Scalability
Large geographically dispersed organizations need a web based tool that can scale to several thousand users.

Role based
Risk management is a role based function. While upper management is responsible for strategic risks, the operations managers are responsible for operational risks.

Data integrity
Spreadsheets do not necessarily guarantee the consistency and integrity of data in a multi user environment. Also collecting data from disparate sources into a spreadsheet is not an easy task.

Auditability (archival)

Any changes to risk assessments need to be documented and approved. This means that the decision support system should be workflow based. The history of changes should be archived.

Visibility
Every stakeholder in the supply chain should have visibility to the risk factors and mitigation plans. There should be a provision to grant or deny access to specific portions of the risk plan.

Person independence
Spreadsheets are person dependent. Management of risks should be role dependent, not person dependent.

7. Multiple levels and multiple horizons
There is a need to perform risk planning at strategic, tactical and operational levels. Also the horizons vary from decades to weeks.

8 Risk planning

As said earlier, risk management can be viewed as being composed of two functions – risk planning and risk monitoring. Risk planning includes the feed forward functions such as risk identification and assessment in our synthesized framework presented earlier in chapter three. Risk planning will integrate with various modules in a typical supply chain management suite of products. The primary function of a risk planner is FMEA analysis. However, the FMEA analysis will be supported by data from various modules given below. Furthermore, FMEA analysis can be done from the standpoints of a process, an

item, a plant, a resource or a network depending on what risks are to be analyzed, for what horizon and by whom. Process centric FMEA analysis was presented earlier in chapter 5. The decision support system will complement existing SCM products. The following figure indicates the integration of risk planning and risk monitoring modules with a typical supply chain management suite of products

Supply Chain Planning
Supply chain planning is typically performed for a given plan name. Risk planner will have a risk plan which will tie back to the supply chain plan. Risk plan will catch critical items and resources as flagged by the last supply chain plan. Moreover it will catch all the exception generated by the supply chain plan.

Demand Planning
Demand distribution will be fed by demand planning. Demand distribution is arrived at for a given scenario. Risk plan will therefore tie a supply chain plan and a demand plan. Risk plan will catch all the exception from the demand plan.

Inventory optimization
Safety stock information will be provided by inventory optimization. Inventory optimizers also generate exceptions which relate to risks such as stockouts and excess inventory. All these exceptions will be integrated into the risk planner.

Transportation planning
Transportation planning software will also generate a rich set of exceptions which will be integrated into the risk planner.

Order management
Data about cancelled orders, delayed orders, returned material will be included from order management.

HRMS system
Absenteeism records will be included from the HRMS system.

Financial system
Each action associated with risk mitigation entails an additional cost. These costs would be fed back to the financial system.

Product lifecycle management module
Engineering change orders will be fetched from the PLM module. The number of ECO's over time would be an indicator of technical risks.

Risk monitoring
Risk monitoring will provide the dashboard. Risk monitoring includes the feedback functions of monitoring and learning in the synthesized framework provided in chapter three.

Record learning

Actions taken in response to threat perceptions may or may not succeed in mitigating risks. Therefore recording learning is very critical. For example, an action to mitigate disruption due to fire would be to conduct regular fire drills. However fire drills may not be successful due to various reasons. The learning from fire drills should therefore be documented to ensure that the next fire drills are successful.

Store maps and pictures
Companies that store detailed maps and pictures of their plants, machinery and personnel were able to recover quickly from disruptions.

Record expert interviews
As indicated earlier risks depend on at least four dimensions – geography, industry, company and time. Therefore expert interviews are very effective in identifying the specific risks associated with a company. The ability to record these interviews is an important feature.

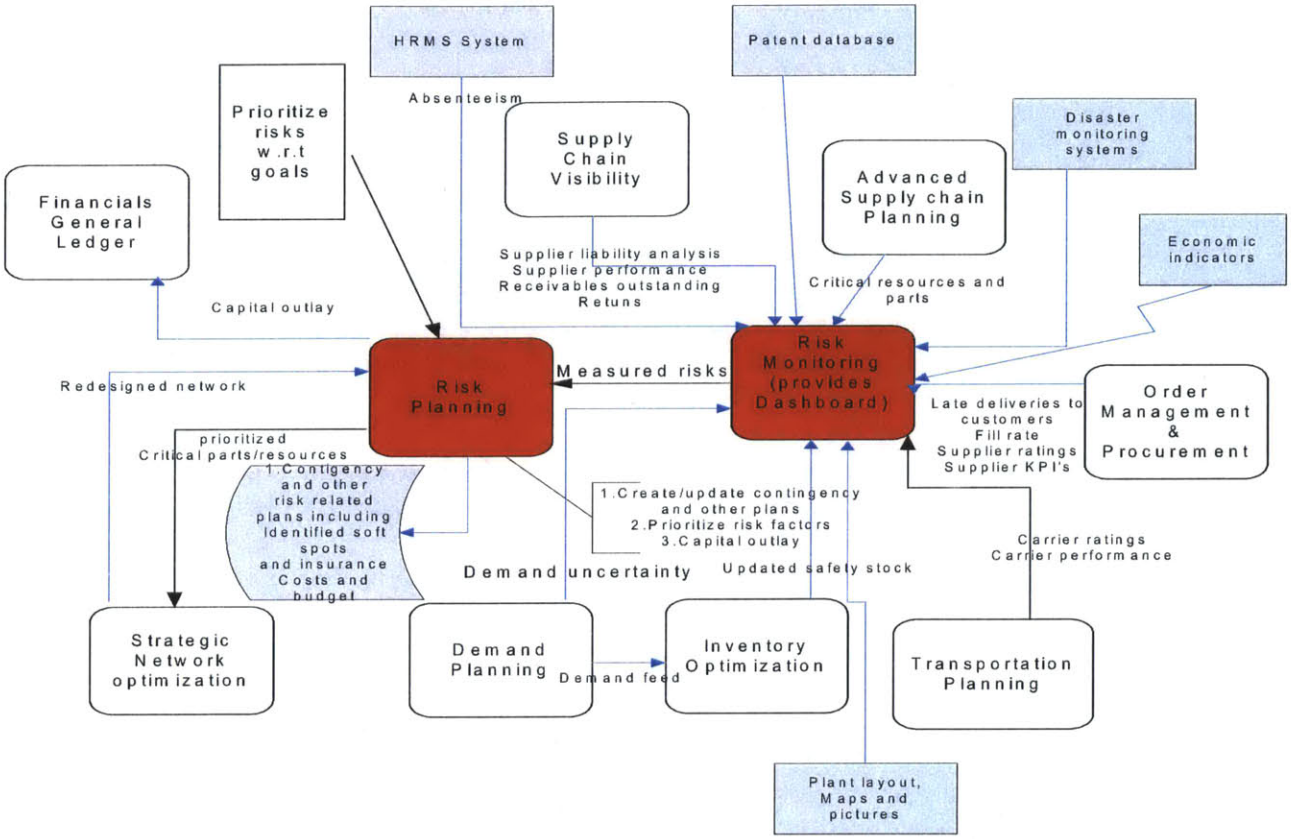
Integration with third party exchanges like Ariba and Commerceone
This requirement comes from large companies who use exchange platforms like Ariba for indirect procurement.

Incident tracking
Incident tracking would facilitate the recording of near miss incidents. An example of a near miss incident would be a case where a worked narrowly escaped a major accident.

Integration with process simulation software
Process simulation software packages like igrafx provide the simulation and live visual display of process runs. Integrating with a process simulation software vendor would be a key value addition. The lead times, sourcing splits, and supply chain network would be fed to the process simulation software.

Tying supplier risk assessments to the supplier's scorecard
Risk assessments performed for a supplier should be fed to the supply chain intelligence software in order to tie them to the supplier's scorecard.

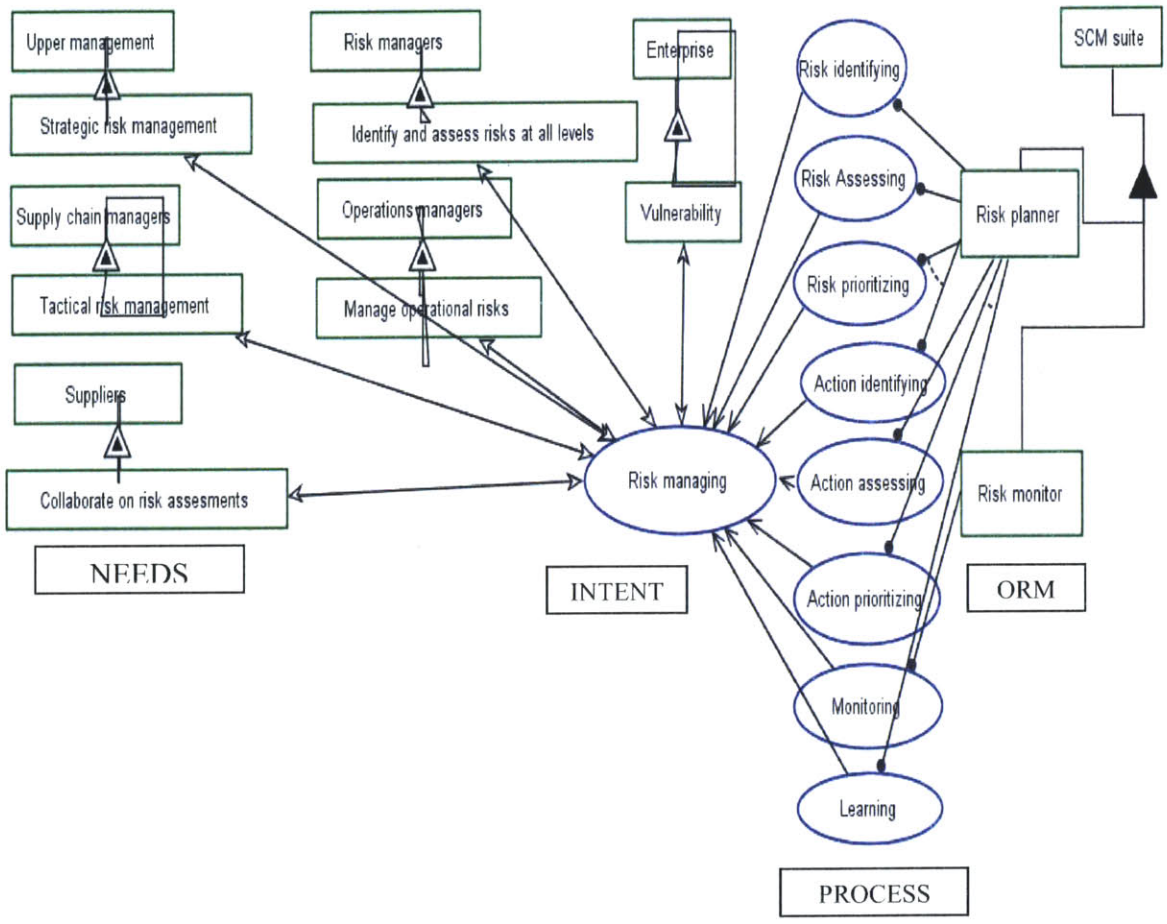
Figure 17 - Integration of risk management software with supply chain management software



7.1.3 Architecture of the decision support system

The following OPM diagram illustrates the level1 architecture of the system.

Figure 18

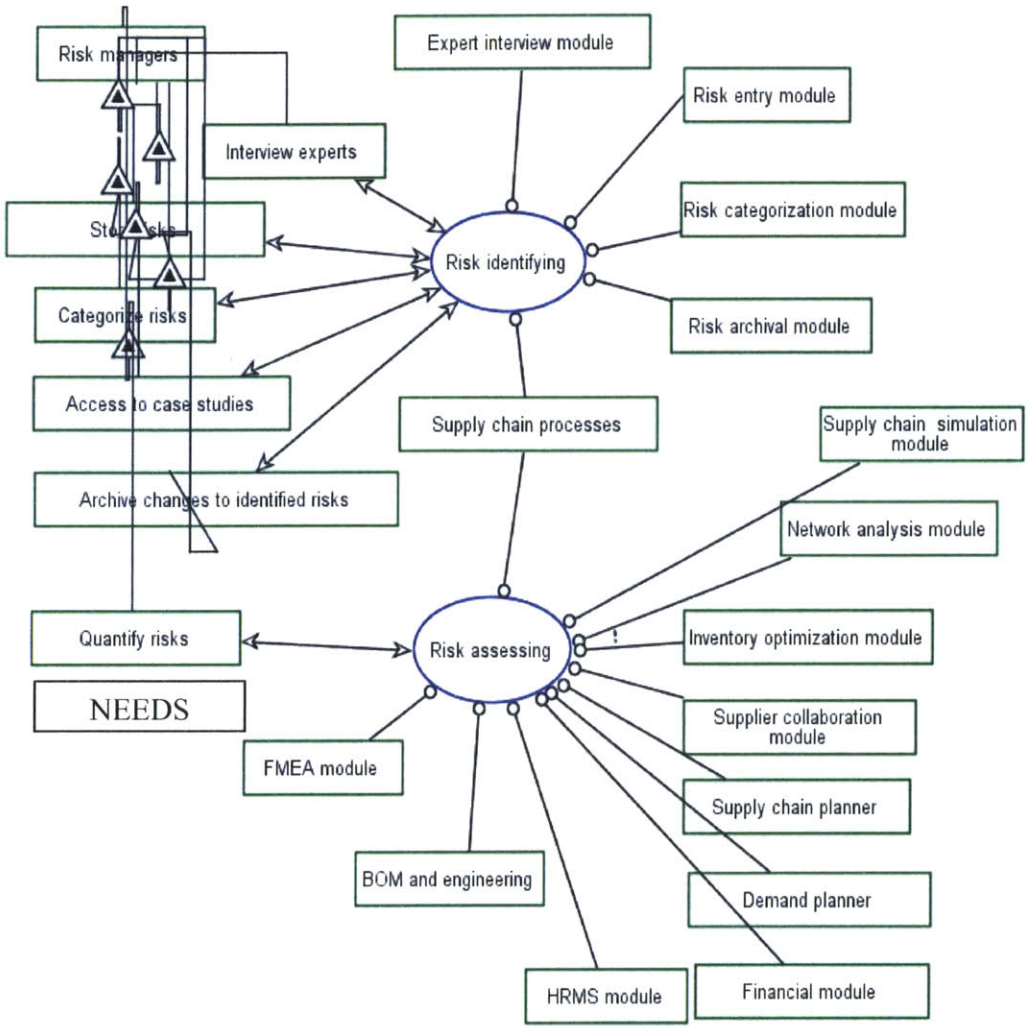


Stakeholders

The key stakeholders are C level executives, supply chain personnel, risk managers, operations managers, IT departments and manufacturing, production planning, logistics departments, customers, and suppliers. The high level needs of each stakeholders are depicted in the above diagram.

The figure below indicates the level 2 architecture of the system.

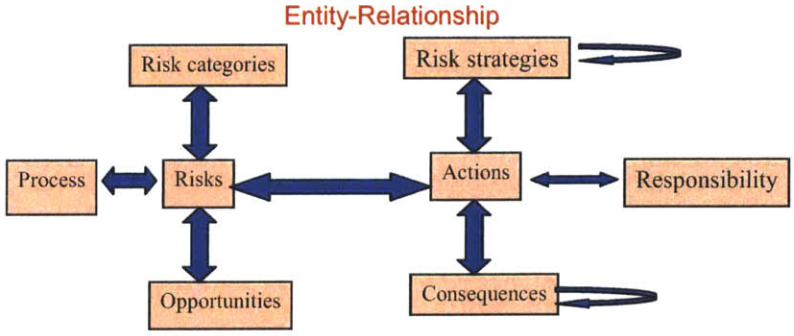
Figure 19



7.1.4 Entity relationship diagram

Having identified the major modules in level 2 of the software, we now focus on the major entities and the relationships between them. The following picture gives the E-R diagram.

Figure 20



Risks – All the risks identified in chapter four will be pre seeded in the system. However users would have the opportunity to add, delete or modify risks.

Risk categories – Risks will have pre seeded categories. Each category will by itself be a risk. Users will be free to change the

classification of risks based on their business requirements.

Opportunities – Every risk is associated with an opportunity.

Actions – Each risk could have multiple actions associated with it. Each action belongs to one or more risk strategies such as risk avoidance, risk acceptance, risk elimination, risk mitigation, and risk transference. Each action is associated with a specific responsibility. For example the action 'conduct a fire drill' is the responsibility of the security personnel. Actions have consequences which need to be recorded.

7.1.5 Major modules and sub-modules

Risk planner
The risk planner would comprise of the following sub modules

Risk entry
Risk entry module would facilitate entering and updating risks.

Risk categorization
Risk categorization module would facilitate the classification of risks. A given risk could belong to multiple categories and a given category could have multiple risks.

Risk archival
Risk archiver will record all changes to risks and risk plans.

Expert interview module
Expert interviews will be stored in text, video and audio formats in this module. The module would provide the ability to cross reference these interviews when modifying risks.

Role based security
Security will be provided at the row level. Access will be governed by user defined rules and roles.

Data acquisition module
Data acquisition module will acquire data from SC/PLM/ERP/Exchange systems in various formats such as XML, flat file or a direct SQL connection.

FMEA module
FMEA will display the data acquired from various systems and allow the users to perform an FMEA analysis. The users would be able to add their own scenarios and modify the ones collected from various systems. Learning would be recorded in this module.

Risk engine

Risk engine will provide a wrapper around typical network optimization software. The purpose of the risk engine will be to break a network systematically into scenarios and feed those scenarios to the network optimization software. Each run of the engine will be done against a risk plan number. The other task performed by the risk engine will be Monte Cel;arlo simulation of probability and severity data received from supply chain management software.

Risk monitor

Dashboard module

The dashboard would provide radar charts for each risk. The risks could be viewed by item, resource, plant, organization or supplier.

Personalization module

Personalization would facilitate changes to the look and feel of the user interface and adding links to risk related information sources.

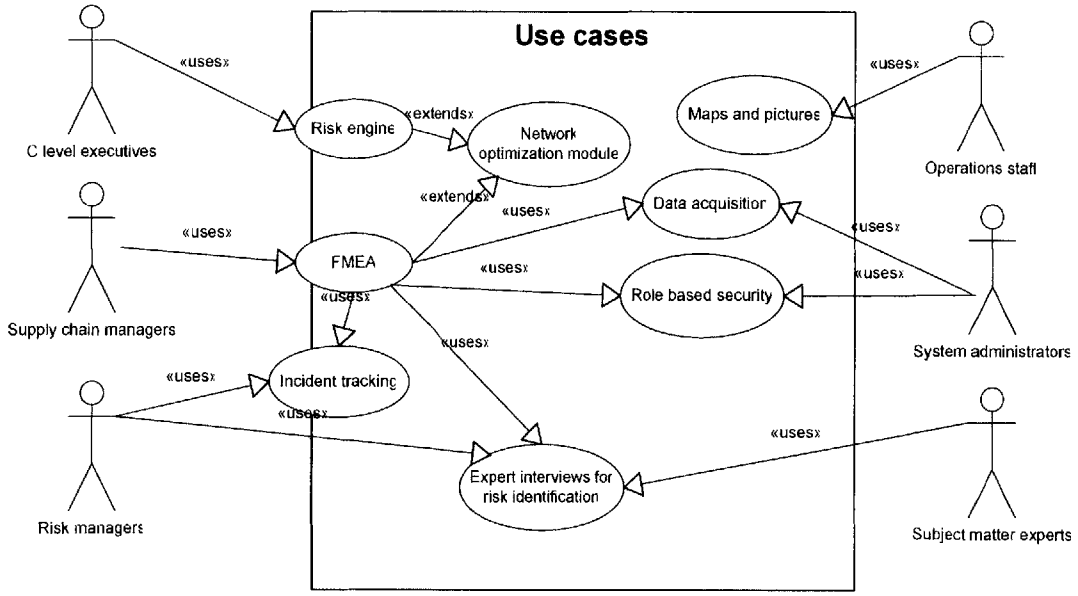
Image storage module

Image storage would facilitate storage of maps, photographs of plants, personnel, machinery and emergency exit routes. The ability to link various pictures , navigate from one to the other ,classify them and retrieve them easily are critical features.

7.1.6 Use cases

The following figure exhibits the various use cases for the decision support system. Of particular importance is the FMEA module which is at the center of risk identification and assessment and gets its inputs from all the other modules.

Figure 21



7.1.7 Graphical User interfaces

Figure 22 shows the overall UI navigation. As soon as the user logs in, the dashboard is shown. What the user can see depends on his/her role. For example a C level executive would be able to see all risks while a junior person would have limited access. Users would classify the risks using the risk identification and classification screen. This screen would allow simple drag and drop of risks and would display them in a tree structured manner. FMEA analysis can be accessed from the dashboard as well as from the risk classification screen. Expert interview interface helps record interviews while role based security screen governs access to risk data. The data acquisition screen helps collect data from supply chain management software systems. Maps and pictures would help store and retrieve pictures. Risk engine parameters would be defined and the engine launched from the risk engine user interface.

Figure 22 – UI Navigation

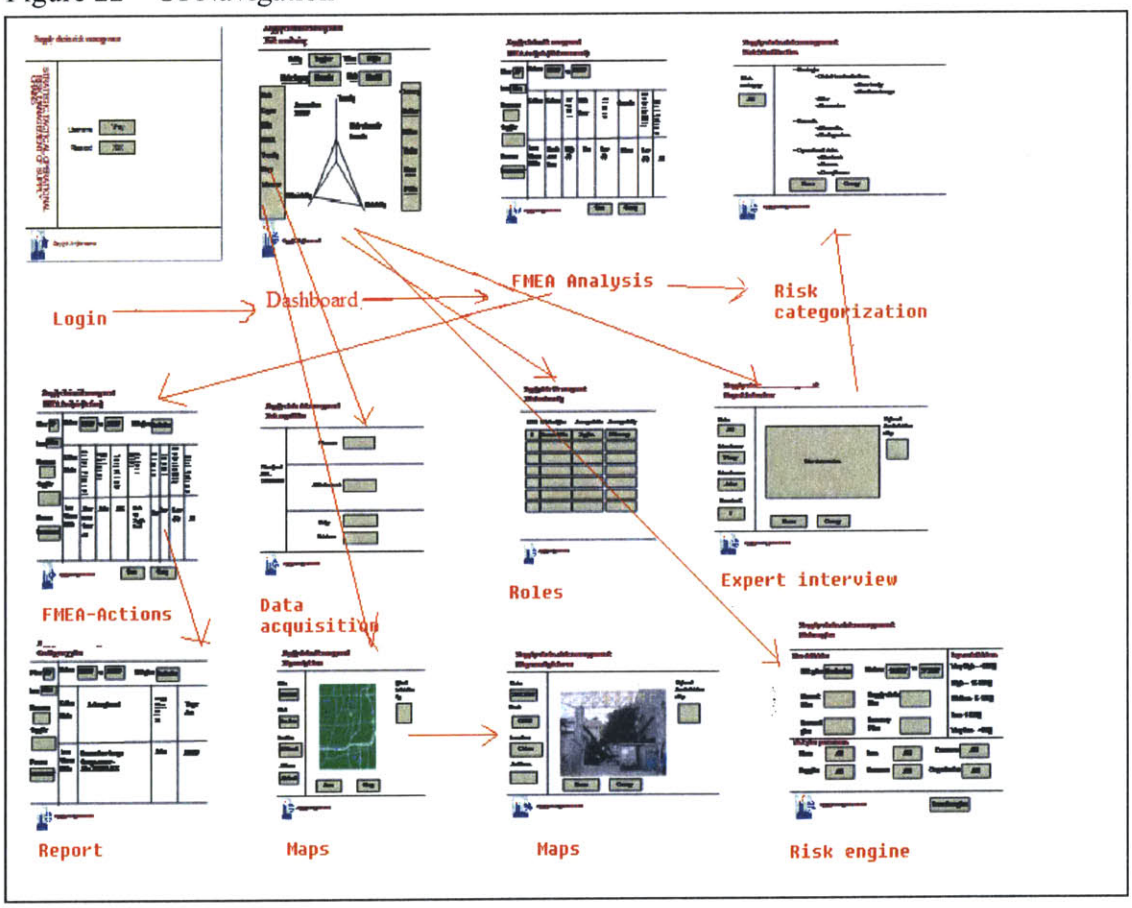


Figure 23 - Login Screen

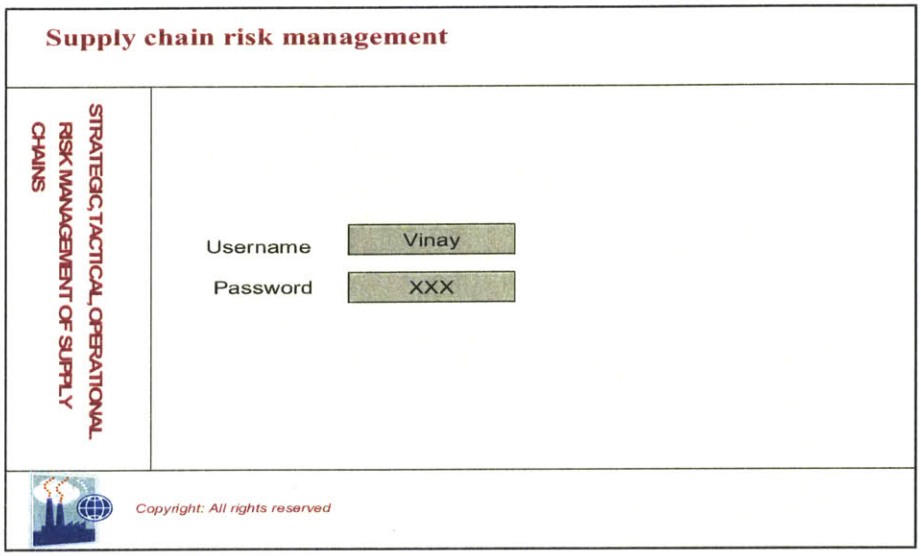


Figure 24 - Risk Monitoring Screen

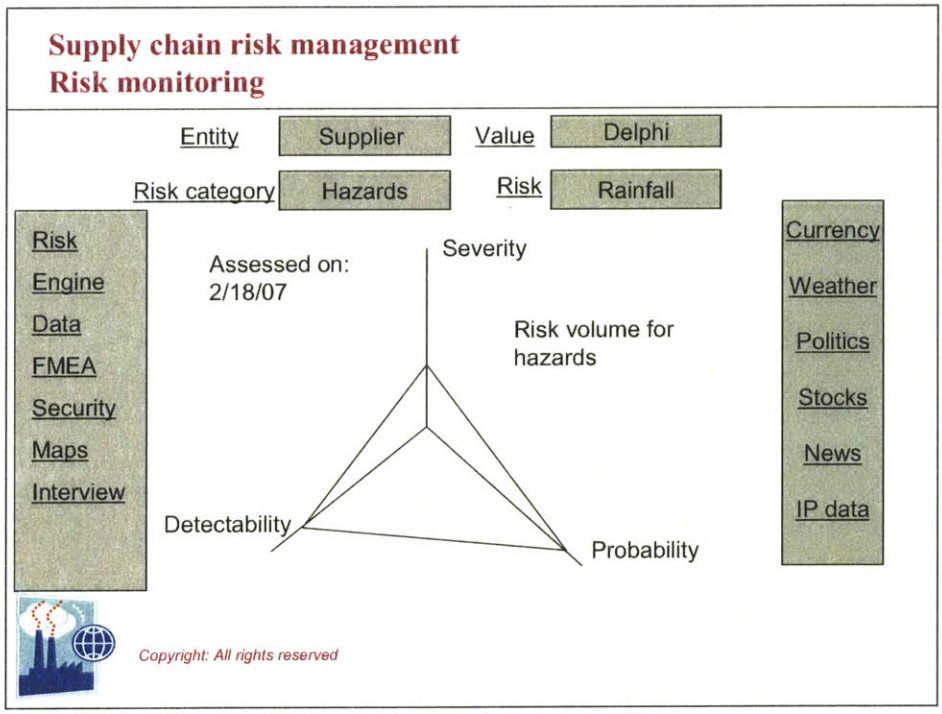


Figure 25 – Data Acqusition

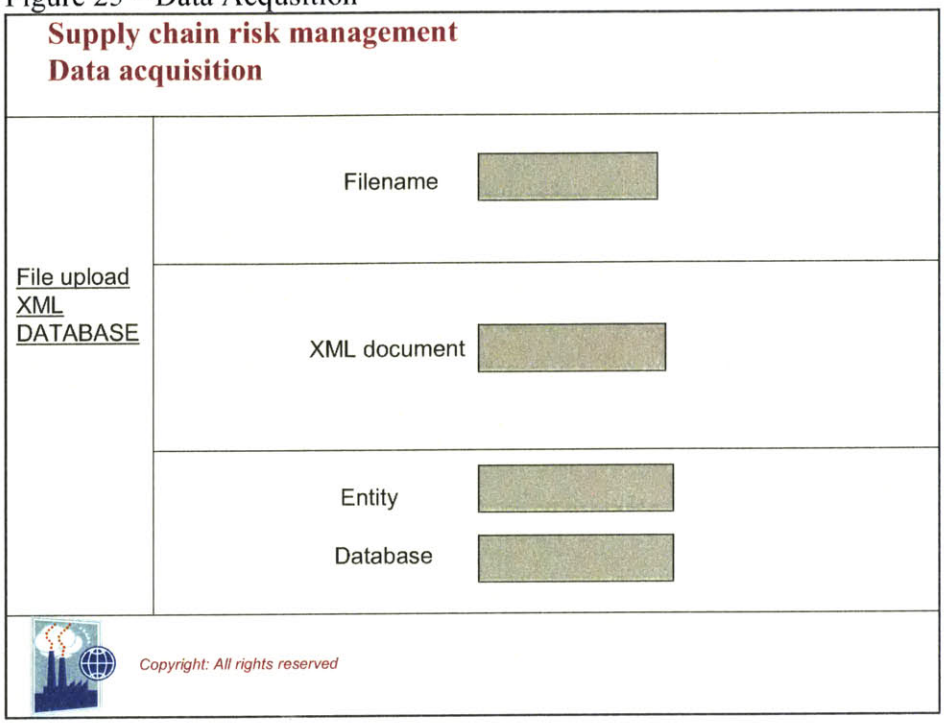


Figure 26 - FMEA Analysis

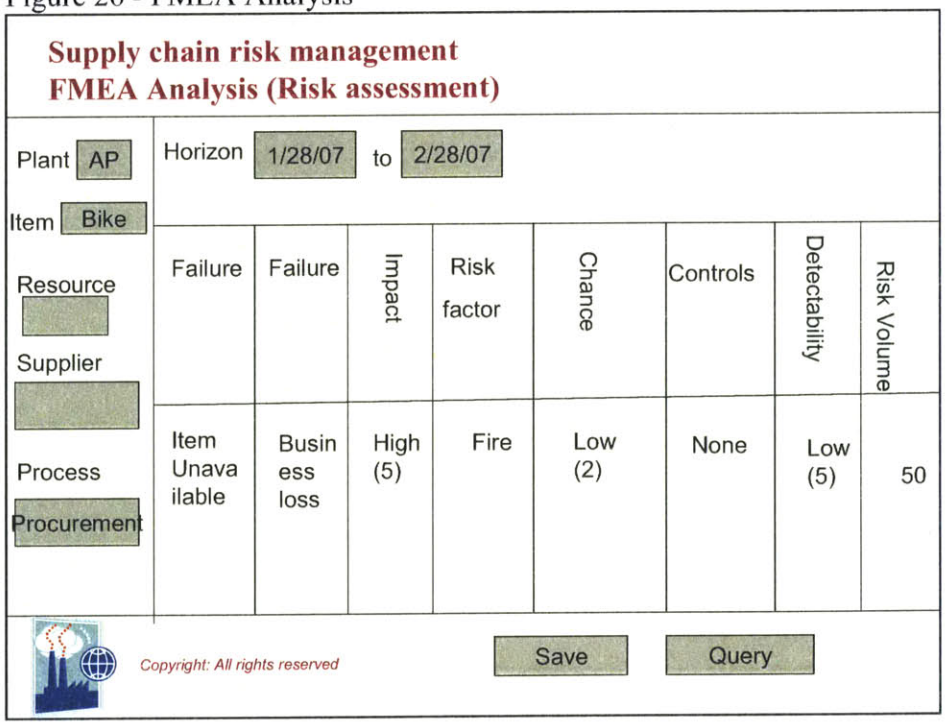


Figure 27 – FEMA Analysis (actions)

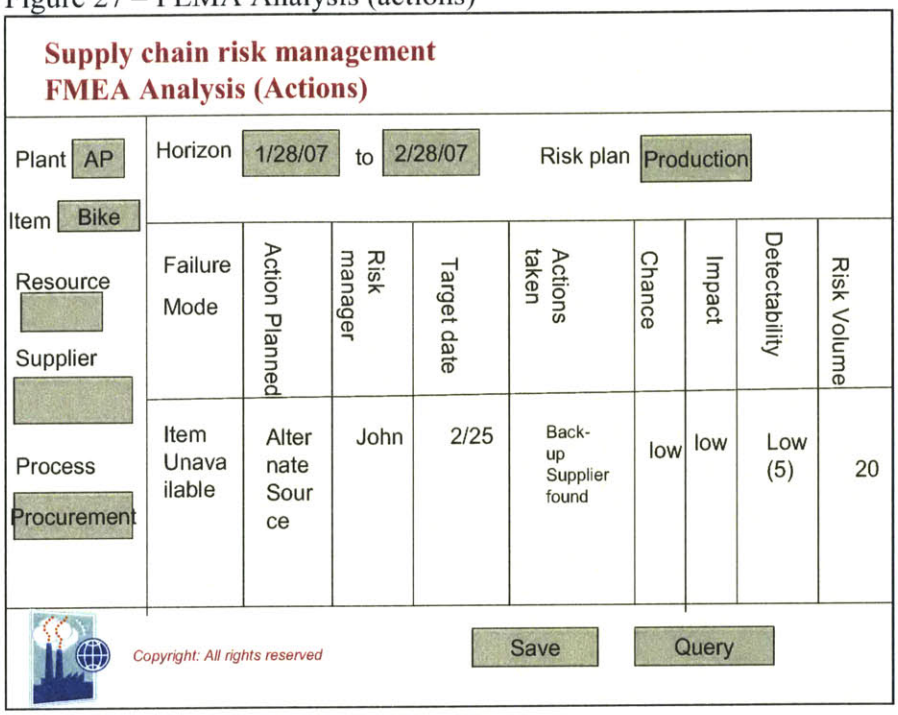


Figure 28 – Role Based Security

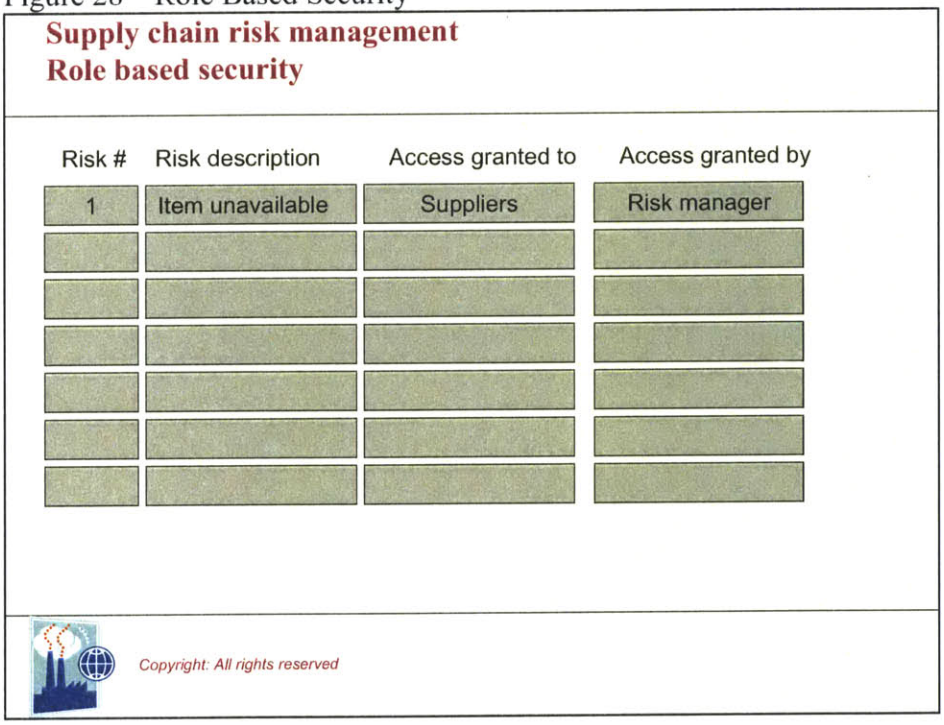


Figure 29 – Risk Identification

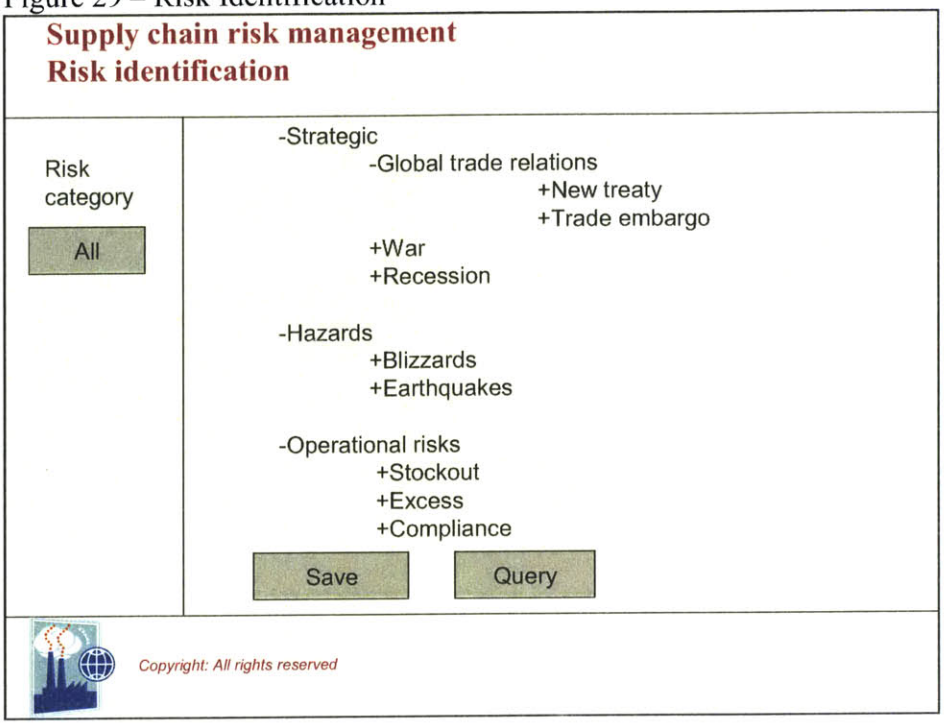


Figure31 - Expert Interview

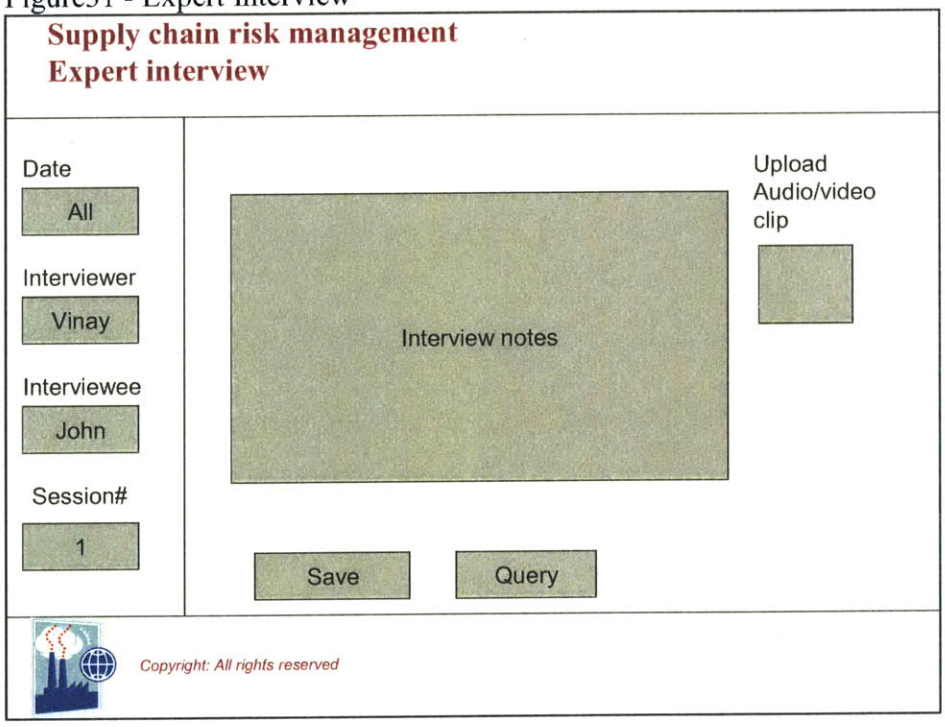


Figure 32 - Risk engine

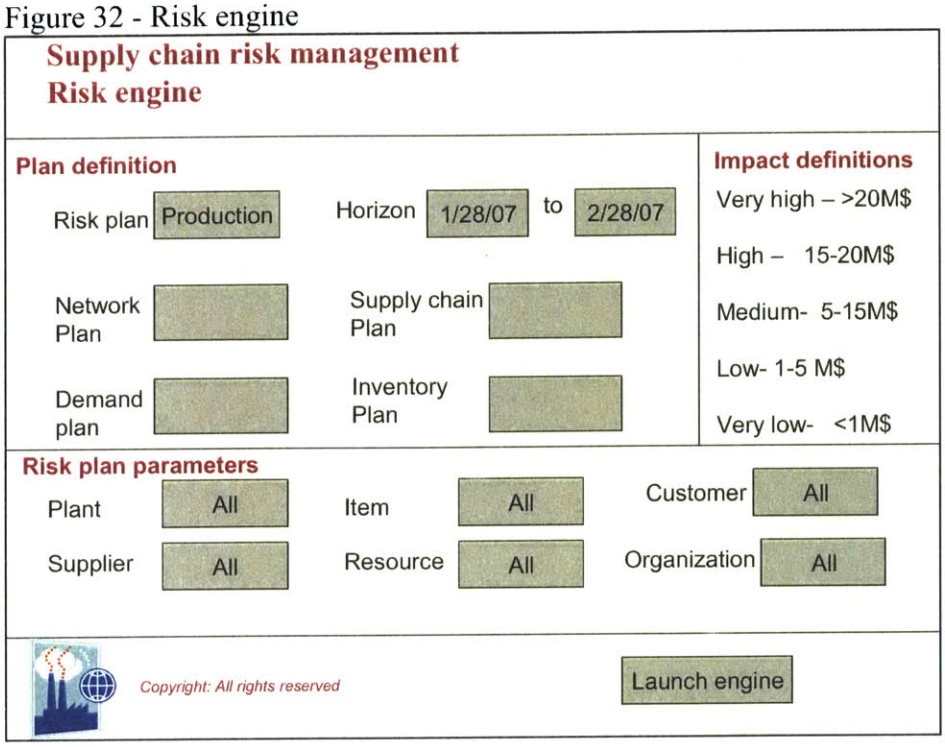


Figure 33 - Contingency plan

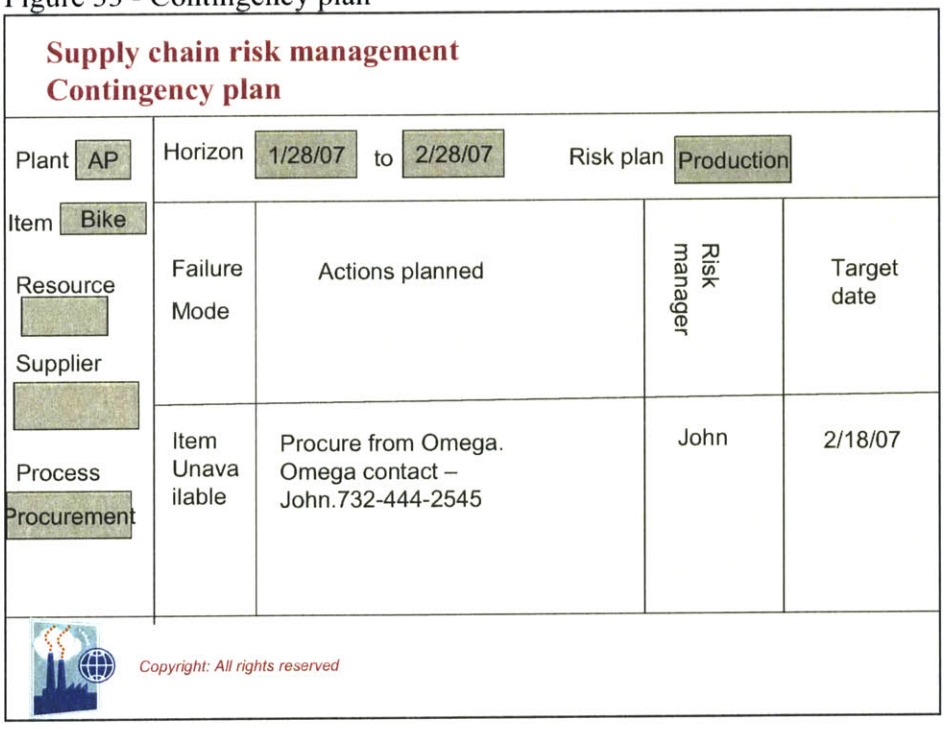


Figure 34-1 – Maps and Pictures

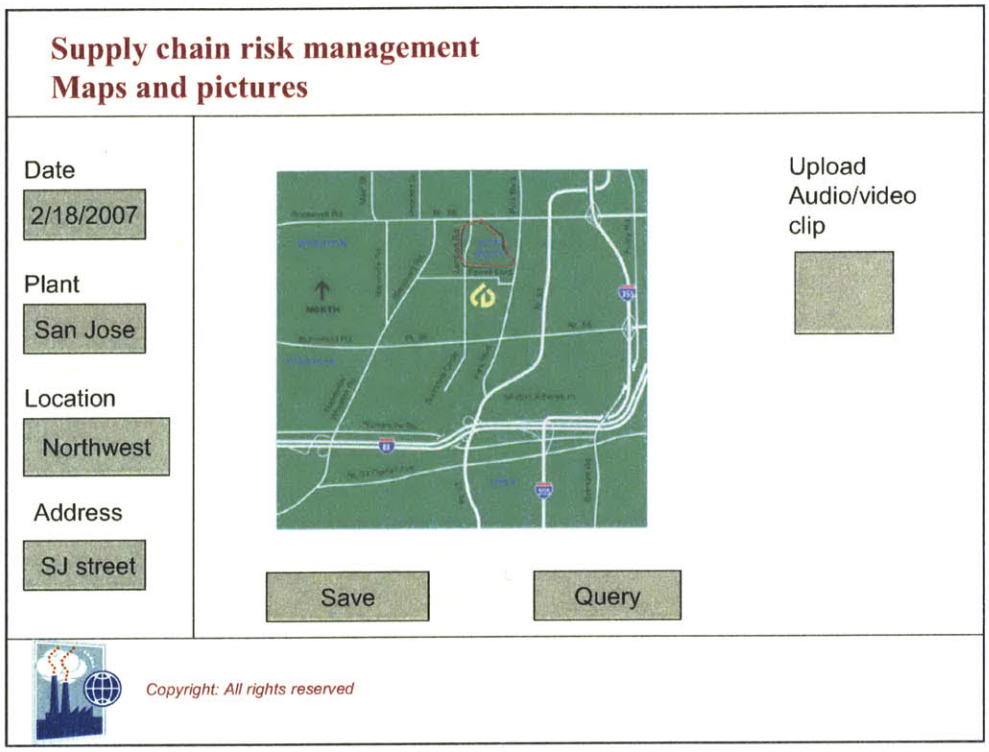
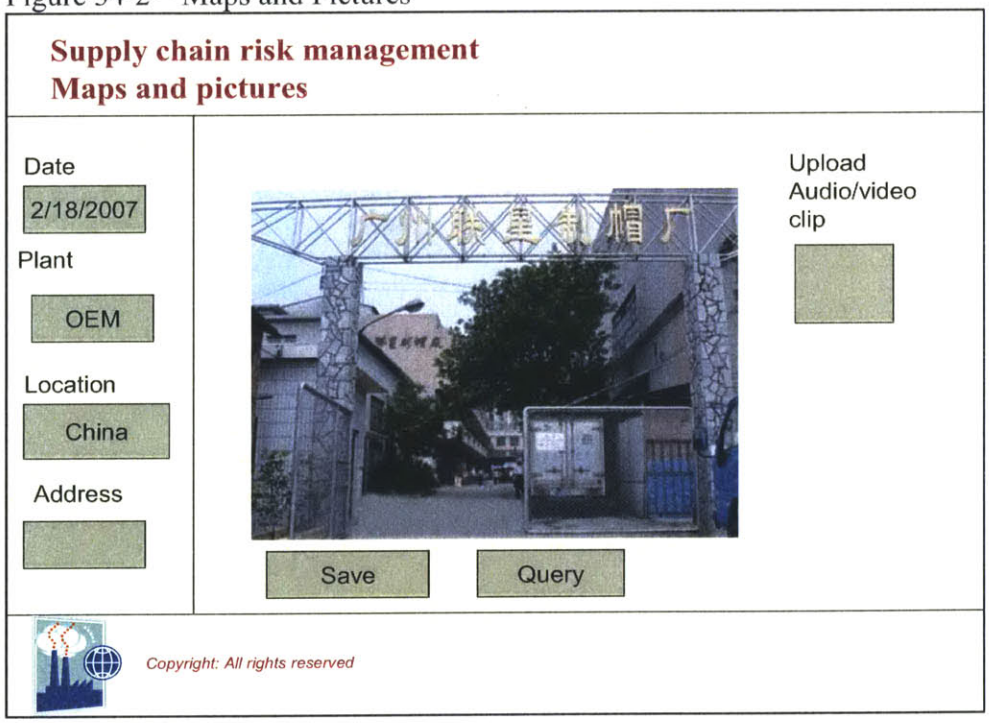


Figure 34-2 – Maps and Pictures



7.1.8 Risk management engine

The risk management engine will run risk plans. Each plan will have parameters such as the names of the network, supply chain, demand, and inventory plans tied to it as well as the horizon, the plants for which risk planning is being done, the definition of severity of impact etc.

Based on the parameters, the risk management engine will feed network information to the strategic network optimization software. It will also trigger the runs of supply chain, demand and inventory plans. Once these plans are run successfully it will automatically acquire the output of these plans into the data model for the decision support system. The data acquired from strategic network optimization would be the cost and profits for various network scenarios and the important data from supply/demand plans would be exceptions. Risk engine will store the exceptions from the previous plans and will not overwrite them. The risk engine will plot the probabilistic distribution for each exception based on historical data and data collected from the current run and run Monte Carlo simulation against the distribution of the severity of impact.

FMEA analysis will be based on the output of the risk engine.

Another design approach could be to incorporate a simpler version of network optimization in the risk engine itself in order to componentize it.

7.1.10 Chapter summary

This chapter presents a high level design and architecture of the decision support system. Needs are outlined and verified with a potential user, the concept is generated, the major modules are identified and user interface navigation is presented. User needs are described using simple English as well as case studies. Key overview ideas are presented about how the support system would function. Although the key overview ideas were presented in the beginning of the chapter for readability, they evolved gradually as needs began to crystallize. The issue of integration with supply chain management software is discussed at a high level. Detailed implementation is likely to uncover unforeseen issues.

Section 8

"Doubt is not a pleasant condition, but certainty is absurd"
– Voltaire (1694-1778)

8.1 Results, discussions and conclusions

This thesis began with the following questions.

1. What is a generic framework for supply chain risk management?
2. How can the soft spots in the supply chain be identified?
3. How can the soft spots be insured against risks?
4. How do other industries deal with risks (e.g the military and the financial industry)
5. Is risk management performed at strategic, tactical or operational levels? If it is performed at all levels, who does what at each level?
6. Can risk management be partially or fully automated using a decision support system? If yes, what are the inputs to and the outputs of the software?
7. Who would be the primary and secondary users of such a software?
8. Where does the software fit in the broader context of a supply chain suite of products?

The following section describes the answers to these questions. Our answers were arrived at after the application of the principles, methods and tools learnt in the system design management program. (see Appendix 3)

8.1.1 Results and discussion

A generic framework was developed based on risk management techniques drawn from the financial industry, the US army, design for six sigma and INCOSE – the international council of system engineering. The framework is essentially a closed loop negative feedback control system with risk identification and assessment and action identification and prioritization in the feed forward loop and monitoring in the feedback loop. The framework incorporates learning.

The identification of soft spots in the supply chain is done by identifying and quantifying risks. Supply chain risks were identified and later quantified using four different models. Two case studies, one based on supply chain risk management in the financial industry and the other based on the operations of a global packaging giant validated these models and the risks identified.

The models developed provide a quantitative estimate of risk volumes and hence help in devising the right risk management strategy. The pros and cons of each model have been identified along with specific recommendations on when to use each one of them.

Both the case studies throw light on how other industries deal with risks. The financial institution we studied has a supply chain worth several billion dollars in costs.

Risk management is performed at all the three levels – strategic, tactical and operational.

Risk management can be automated to a large extent by using a decision support system. The decision support system would integrate seamlessly with supply chain management and exchange software. Strategic risk planning would be based on network optimization while tactical and operational risk management will take as input the supply chain exceptions generated by planning engines. FMEA analysis would provide the users the opportunity to apply subjective treatment to the output of the risk engine.

The primary users would be the C level executives , the risk managers, supply chain managers, production managers and transportation and logistic personnel. Secondary users include the suppliers and the regulators.

Decision support systems for risk management can be a componentized offering but should be capable of integrating with supply chain management and exchange software. It complements SCM offerings.

8.1.2 Conclusions

The key contributions of this work can be summarized along two dimensions – scientific and commercial.

Scientific-

- A key enhancement to the traditional risk management model is the addition of the third dimension called 'detectability'[14]. The concept of risk volume which is the product of the probability of occurrence, the magnitude of impact and the detectability of the event has been introduced.
- Another key contribution is the synthesized risk management framework which includes learning and action prioritization.
- Strategic risks such as terrorist attacks and hazards need to be approached with the assumption that they will occur. (implying that their probability=1). Supply chain simulation would then indicate the magnitude of loss associated with each scenario.
- Supply chain risks were classified based on discussions with practicing managers and the works of Prof.Yossi Shafi and Prof.Zsidisin. However the perceptions of supply chain risks depend on at least 4 factors – geography, industry, company and time. Each company needs to identify risks while using the risks presented in this thesis as a reference or a check list. Moreover risk identification and assessment is a continuous process.
- The use of Bayes theorem was demonstrated to combine historical data with expert opinion.
- The use of a mixed integer programming formulation to quantify supply chain risks was also demonstrated.
- FMEA analysis was used to apply subjective judgments on top of quantified risks.

[14] The financial industry already uses detectability. Our contribution has been to apply it to supply chain risk management.

- Finally this work demonstrated the use of simulation software for quantifying operational risks.

Commercial –

- This thesis will encourage the industry to start thinking about supply chain risk management using the risk management framework, models and mitigation techniques outlined in this thesis.
- Some of the risk mitigation strategies identified were relationship building, on site visits, and supplier scorecards for single source of supply; multiple sourcing where variation in quality is not a key concern, building buffer inventory at an intermediate location and importing from the open market in case of disruptions.
- Working with a large software company, a large financial institution and a large packaging company, the need for the risk management software was identified.
- The features expected from this risk management software were identified.
- A high level design was presented which included the use cases, the architecture, the major modules, the user interface navigation and finally the user interface.
- Integration issues with supply chain and exchange software were identified along with the data needed to measure every risk.

Chapter summary

This chapter presents the results and conclusions of the work behind this thesis. Achievements along the scientific and commercial dimensions are also presented.

Section 9

"The path to our destination is not always a straight one. We go down the wrong road, we get lost, we turn back. Maybe it doesn't matter which road we embark on. Maybe what matters is that we embark"

– Barbara Hall, Northern Exposure ,Rosebud, 1993.

9.1 Recommendations and future work

While this work dealt with the models and the design of a decision support system for supply chain risk management, it did not address the following issues.

- The role of the government in ensuring a resilient supply chain. (Please refer appendix 2).
- The role of leadership in building a culture of risk awareness.
- The modeling of human beings as sources of risk.

(Prof.Nancy Levinson's work addresses this issue from a system safety perspective).

It would be worthwhile to explore these issues from the point of view of supply chain risk management.

The implementation of the decision support system is another important work that can be undertaken by entrepreneurs and by the IT departments of large corporations. While an attempt has been made to provide as much detail as possible in the software design, the integration with supply chain management software is likely to uncover unforeseen issues. Yet another topic recommended for future work is the impact of culture on the perception of risks given that certain cultures are risk averse while the others are not.[15] The opportunity side of risk could be explored further as well.

[15] http://www.geert-hofstede.com/

Section 10

10.1 Appendices

Appendix 1

Solver solution to strategic network optimization model

Scenario1 - Mixed sourcing

	s11	s21	s31	s12	s22	s32
1348	50000	100000	0	0	0	0
selling price	10,000	10,000	10,000	10,000	10,000	10,000
cost of pump	-1000	-1000	-1000	-1500	-1500	-1500
Transportation costs	-10	-15	-20	-12	-17	-22
Unit profit	8,990	8,985	8,980	8,488	8,483	8,478
capacity of s1	150000	150000				
capacity of s2	0	60000				
total demand	150000	150,000				
plant1 capacity	50000	50000				
plant2 capacity	0	50,000				
plant3 capacity	0	50,000				

869	profit made
480	profit lost
1348	max profit

Scenario 2 - Block capacity (no alternate)

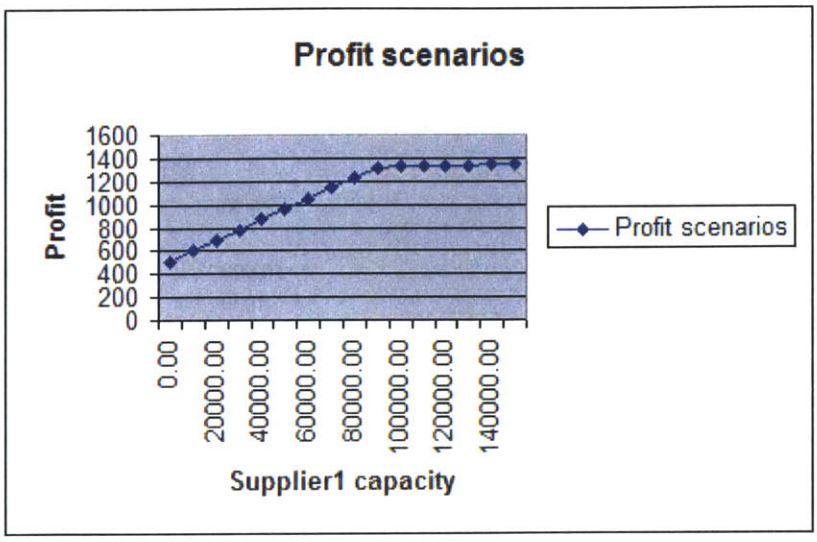
359.45	profit
988.55	profit lost
1348	max profit

Scenario 3 - Maintain buffer for 1 year

-195	Opportunity cost

	A4
0	509.205
10000	599.08
20000	688.93
30000	778.78
40000	868.63
50000	958.48
60000	1048.33
70000	1138.18
80000	1228.03
90000	1317.85501

100000	1322.9
110000	1327.92
120000	1332.94
130000	1337.96
140000	1342.98
150000	1348



Appendix 2

Notes from SIP workshop "Ready in a crisis: Business and executive preparedness"

Introduction to the resource persons

Mike Armstrong , Board of trustees , John Hopkins group of hospitals
Retired Chairman of Comcast and the retired Chairman &
CEO of AT&T and Hughes Electronics

John Deutch is an Institute Professor at MIT and has served as Chairman of the Department of Chemistry, Dean of Science and Provost.
In May 1995, he was sworn in as Director of Central Intelligence following a unanimous vote in the Senate, and served as DCI until December 1996.

Richard Falkenrath was appointed Deputy Commissioner of Counter Terrorism for the New York Police Department in June 2006. From September 1993 until December 2000, Richard worked at Harvard University's John F. Kennedy School of Government, first as a postdoctoral research fellow, then as Executive Director of the Center, and finally as Assistant Professor of Public Policy.

Notes

- Private companies operate 85% of America's infrastructure.

Key questions

- Where is the threat?
- What does the local public sector think about it?
- What kind of business leadership is required to deal with the threat?

Threats

- Health
- Environment
- Safety

Examples

- Union Carbide,Bhopal disaster
- 3 mile island nuclear plant
- Johnson and Johnson Tylenol case

Threat assessment and warning

- Warning – Tendency is to err on the side of caution.
    - Creates 'crying wolf' syndrome.
- Classified sources- Reluctance on the part of agencies to share source of information.

Type of disruptive threats

- Cyber terrorism – Information control
- Terrorist attack – Facility control
- Weapons of mass destruction - Wider control

Hypothetical scenarios

- Port closed due to a computer system problem. Export/import have come to a halt.
  - Does not harm people directly but huge economic impacts.
- 300 million $ of bank's deposits transferred.
- Virus brings down bank.
- Foreign subsidiary – CEO is held hostage.
- WMD – Biological attack, chemical attack.

CEO perspective

- How much will the government help ?
- Can I defend against such events ?
- How much insurance to buy ?

Government's perspective-

- Government's help dependent on externalities of the system.
  - e.g company distributing chlorine has trucks passing through the heart of the city. Government involvement will be high. On the other hand , if a company's operations are isolated then government intervention is not required.
- Companies must internalize external costs.
  - In other words spend on their own security
- Natural disasters are statistically patterned ,terrorist attacks are not.
  - *Assume probability = 1 as far as terrorist attacks are concerned.*
  - *Focus only on magnitude of consequences.*
- Very few insurance companies provide terrorist coverage after 9/11.
- For the board, investment in risk is perceived to be a cost. Hence poor preparedness.
- Indirect costs of attacks are usually more than the direct costs.

Characteristics of companies that have good risk management plans

- High margins
- Highly professional management
- Identifiable sources of risks
- Risk remediation through a plan of action.

Roundtable discussion points –

- Self regulation on the part of the scientific and academic community. Milk botoxin research paper withheld from publication in the interest of the public at large.

Good reports

- Think report by the National academy of sciences

Pandemic influenza

- Can strike anytime
- H5N1 - Highly mutating virus
- Simple modifications to existing pathogens can be deadly.

Case studies

- HCA hospital's enterprise risk management helped them evacuate 1200 patients, doctors etc. in 48 hours.
  - No loss of life or limb.
- Gunmen entered Hughes premises.
- Bomb hoax turned real .

Key takeaways

- Fixing accountability and responsibility for risk management
- Communication systems in place
- Command and control in place
- Resources planned
- Practice-practice-practice

Appendix 3

Principles, methods and tools used in this thesis and SDM courses from where they were learnt are shown below.

Principles and methods

Principle	Thesis chapter	SDM course
Thesis approach used the Pugh's method	Chapter 1	System engineering
Interdisciplinary approach	Chapter 3	Creativity techniques-System architecture, system engineering
Framework development	Chapter 3	Control theory
Strategic risk using network optimization	Chapter 5	System optimization
FMEA	Chapter 5	Lean six sigma, system engineering
Bayes theorem	Chapter 5	Engineering risk benefit analysis
Supply chain Simulation	Chapter 5	Supply chain and operations management
Expert interviews	Chapter 6	Product design and development
Master logic diagram	Chapter 4	Engineering risk benefit analysis.

Tool	Thesis chapter	SDM course
igrafx	Chapter 5	Lean six sigma, internship
Solver	Chapter 5	System optimization
Solver table	Chapter 5	System optimization
FMEA	Chapter 5	System engineering, internship
OPCAT (OPM)	Chapter 7	System architecture
E-R diagramming using VISIO	Chapter 7	Product design and development
Use cases using VISIO	Chapter 7	Product design and development

Appendix 4

Linear problem formulation for case study 2

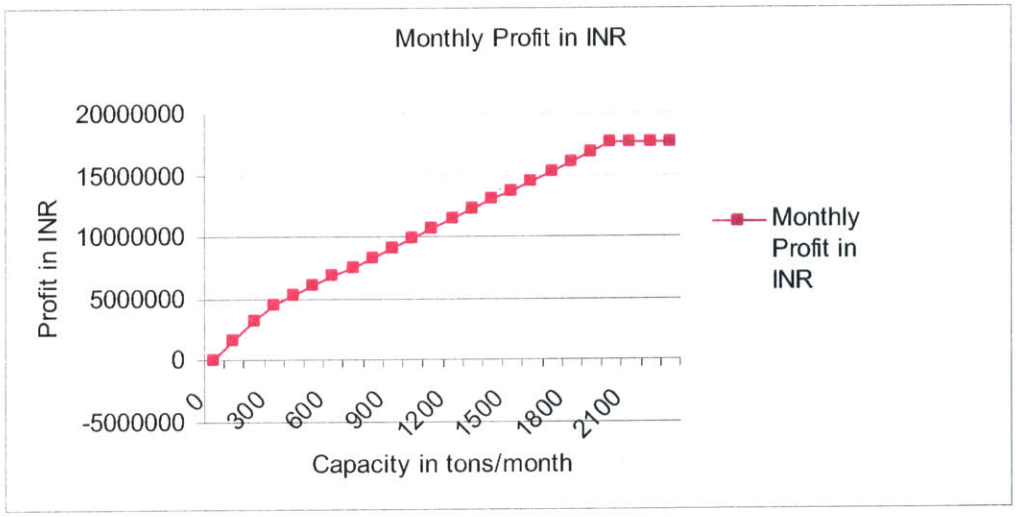
Demand	J	T	Dealers	Direct sales	Contracts
	80	150	600	890	280

Sales channels	Selling Price per ton	Raw material per ton	Taxes	Mfg cost per ton	Transportat per ton
J	75000	30000	700	25000	1200
T	75000	30000	700	25000	3200
Dealers	50000	30000	700	12000	0
Direct sales	50000	30000	700	12000	0
Contracts	75000	30000	700	25000	2000
Profit per ton	17100	15100	6300	6300	16300

Objective function	B2*B11+C2*C11+D2*D11+E2*E11+F2*F11		
Maximize profit	17584000		
Constraints			
Supply-demand constraint			
Hyderbad capacity	2500		
Hyderbad inventory	0		
H surplus capacity	500		
Raw material requirement constraint			
Steel from J	1052.631579	J capacity =	2000
Steel from T	526.3157895	T capacity=	2000
Inventory at Vizag	500	Pickling capacity=	2000
Total raw material supply	2078.947368		
Production yield	0.95		
Total raw material required	2105.263158		
Raw material supply-demand EQUALS	-26.31578947		
15-20 days of inventory	1000		
Total contract demand	510		
Demand constraints			
J demand >	70		
J demand <	80		
T demand =	150		
Dealer demand <=	600		
Direct sales <=	1120		
Total contract demand constraint <=	280		
Pickling capacity constraint (total demand) <=	2000		
Non negativity constraints			

Scenario 1
Profit curve for H

	B13
0	-6.3
100	1686800
200	3213600
300	4494000
400	5263999.998
500	6033999.997
600	6803999.995
700	7573999.994
800	8343999.992
900	9113999.991
1000	9883999.989
1100	10653999.99
1200	11423999.99
1300	12193999.98
1400	12963999.98
1500	13733999.98
1600	14503999.98
1700	15273999.98
1800	16043999.98
1900	16813999.98
2000	17583999.97
2100	17583999.97
2200	17583999.97
2300	17583999.97
2400	17583999.97
2500	17583999.97

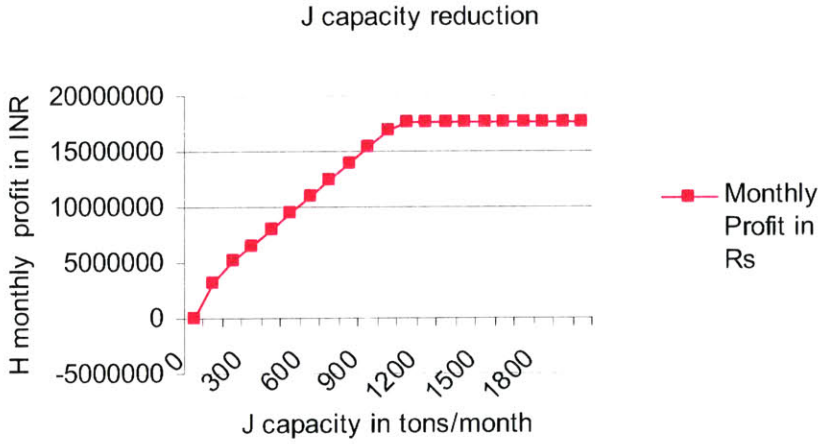


Scenario 2

J capacity reduction

Assume that T cannot meet the extra demand caused by J's capacity reduction.

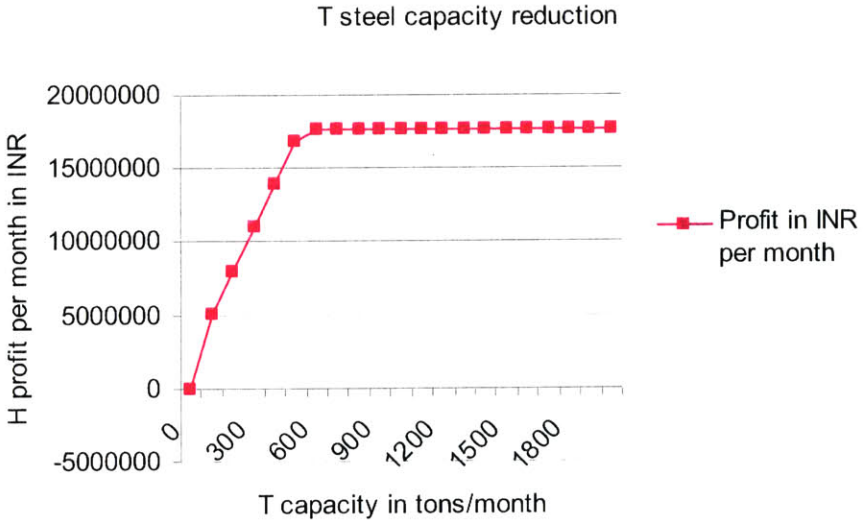
	B13
0	-6.3
100	3060920
200	5110000.108
300	6573000.034
400	8036000.031
500	9499000.028
600	10962000.03
700	12425000.02
800	13888000.02
900	15351000.02
1000	16814000.01
1100	17584000.01
1200	17584000.01
1300	17584000.01
1400	17584000.01
1500	17584000.01
1600	17584000.01
1700	17584000.01
1800	17584000.01
1900	17584000.01
2000	17584000.01



Scenario 3

T capacity reduction

	B13
0	-6.3
100	5109999.994
200	8036000.135
300	10962000.13
400	13888000.12
500	16814000.12
600	17584000.12
700	17584000.12
800	17584000.12
900	17584000.12
1000	17584000.12
1100	17584000.12
1200	17584000.12
1300	17584000.12
1400	17584000.12
1500	17584000.12
1600	17584000.12
1700	17584000.12
1800	17584000.12
1900	17584000.12
2000	17584000.12



Scenario 4
T + J capacity reduction

B13	T 0	100	200	300	400
0	-6.3	0	0.054678253	0.221018	-0.0127483
	0	3060920	3060920.003	3060920	3060919.99
100					
200	0	5110000.108	5110000.064	5110000	5110000
300	0	5110000.108	6573000.057	6573001	6572999.99
400	0	5110000.108	8036000.054	8036000	8036000.85
500	0	5110000.108	8036000.054	9499000	9498999.85
600	0	5110000.108	8036000.054	10962000	10961999.8
700	0	5110000.108	8036000.054	10962000	12424999.8
800	0	5110000.108	8036000.054	10962000	13887999.8
900	0	5110000.108	8036000.054	10962000	13887999.8
1000	0	5110000.108	8036000.054	10962000	13887999.8
1100	0	5110000.108	8036000.054	10962000	13887999.8
1200	0	5110000.108	8036000.054	10962000	13887999.8
1300	0	5110000.108	8036000.054	10962000	13887999.8
1400	0	5110000.108	8036000.054	10962000	13887999.8
1500	0	5110000.108	8036000.054	10962000	13887999.8
1600	0	5110000.108	8036000.054	10962000	13887999.8
1700	0	5110000.108	8036000.054	10962000	13887999.8
1800	0	5110000.108	8036000.054	10962000	13887999.8
1900	0	5110000.108	8036000.054	10962000	13887999.8
2000	0	5110000.108	8036000.054	10962000	13887999.8

Section 11

11.1 Author

Vinay Deshmukh is pursuing a joint degree in management and engineering at the Massachusetts Institute of technology's school of engineering and MIT's Sloan school of management. He worked for Oracle Corporation for close to 9 years before joining MIT. As a director of Oracle's E-business development, he was responsible for the design, development, implementation and maintenance of Oracle's Advanced planning and scheduling suite of products catering to supply chain optimization and collaboration. He has been instrumental in the filing of 5 international patents in the supply chain planning space. He holds a masters degree in computer science from the Indian Institute of Technology, Roorkee a diploma in business management and a bachelor's degree in electronics and communication engineering. His research interests are global product design and development, system optimization and supply chain and operations management. He can be reached at vinay.deshmukh@sloan.mit.edu.

11.2 Thesis Advisor

Dr.David Simchi-Levi is a professor of Civil and Environmental Engineering and Engineering Systems at the Massachusetts Institute of technology. He is a co-director of the Leaders for Manufacturing and System Design and Management programs. Dr. Simchi-Levi holds a Ph.D. from Tel Aviv University. His research currently focuses on developing and implementing robust and efficient techniques for logistics and manufacturing systems. He has published widely in professional journals on both practical and theoretical aspects of logistics and supply chain management. Dr. Simchi-Levi has been the principal investigator in charge of about $2 million in funded academic research. He is the Editor-in-Chief of *Naval Research Logistics*, an Area Editor for IIE Transactions, an Associate Editor for several scientific journals including *Management Science, Networks, Transportation Science and Telecommunication Systems*, and a former Area Editor of *Transportation for Operations Research*. His Ph.D. students have accepted positions in leading academic institutes including University of California, Berkeley; Columbia University, University of Michigan, Purdue University, Georgia Tech, and Virginia Tech. Dr. Simchi-Levi is co-author (with Julien Bramel) of *The Logic of Logisitics*, published by Springer in 1997 (1st Edition) and in 2004 (2nd Edition) (with Xin Chen and Julien Bramel). His second book, *Designing and Managing the Supply Chain* (with P. Kaminsky and E. Simchi-Levi) was published by McGraw-Hill in August 1999 (1st edition) and 2002 (2nd edition). It received the Book-of-the-Year award and the Outstanding IIE Publication award given in 2000 by the *Institute of Industrial Engineers*. The book also received the Outstanding First Edition of the Year award given in 2000 by McGraw-Hill. It was selected by Business 2.0 December 2001 issue, as the best source for slashing time and cost and increasing productivity in the supply chain. It has been translated to Chinese, Japanese and Korean. His new book (with P. Kaminsky and E. Simchi-Levi), *Managing the Supply Chain: The Definitive Guide for the Supply Chain Professional*, was published by McGraw-Hill in December 2003. The book serves as a

reference for consultants and managers involved in any one of the processes that make up the supply chain. He can be reached at dslevi@mit.edu.

Section 12

12.1 Acknowledgements

I am indebted to Dr.David Simchi-Levi for having given me this lifetime opportunity to work under his able guidance. I am grateful to Prof.Pat Hale for his constant encouragement and support. I have no words to express my gratitude towards all the faculty members of MIT's Sloan school of management and the School of engineering and the Harvard business school who have been the fountainheads of knowledge and wisdom in their respective subjects and without whose tacit inputs, this work might not have come to fruition. My classmates and seniors deserve a special mention for their help and inspiration. My family members comprising of my wife Swati, daughter Ashlesha, and son Soham, who have wholeheartedly supported me in all my endeavors at MIT, deserve a special mention. My extended family comprising of my parents, my wife's parents and my sister's family have all encouraged and inspired me to put my best foot forward and hence are worthy of the sincerest acknowledgement.

Section 13

13.1 Bibliography

1. Tim Payne (2006), "*Supply chain risk management Is an Emerging requirement for S&OP*", accessed from Gartner Online, April 2006
2. George A. Zsidisin, (2003), "*Managerial perceptions of supply risk*", Journal of Supply Chain Management, Jan 1 2003.
3. Protivity (2003), "Capitalizing on Sarbanes Oxley Compliance to build supply chain advantage", May 2003, http://www.gartner.com/DisplayDocument?id=491287&ref=g_sitelink (accessed June 2006).
4. Yossi Shafi, *The Resilient Enterprise*, The MIT Press, Cambridge, MA, Oct 2005
5. "Moses, Joel (2004), *Foundational Issues in Engineering Systems: A Framing Paper*", MIT-ESD, Mar 29-31, 2004
6. CRM Daily, "Customer Relationship Management for Industry Pros," http://www.crm-daily.com/story.xhtml?story_id=43987 (accessed June 2006)
7. Slides from *Working Manuscript of Design for Six Sigma* by Dr.Rajesh Jugulum, John Wiley and Sons (2007). Dr. Jugulum is a six sigma master black belt holder at a leading financial institution.
8. Schildhouse, Jill (2005). *An Interview with Joseph Yacura: Interview by Jill Schildhouse.* The Journal of Supply Chain Management, Winter 2005
9. Carr, V. and J.H.M. Tah (2007), *Information Modeling of a Construction Project Risk Management System*, Engineering, Construction and Architecture Management 20007/2, 107-119
10. *Risk Management Field Manual No.100-14,* Headquarters, Department of the Army
11. Cecere, Lora and Debra Hofman (2005), *The Agile Supply Chain*, Supply Chain Management Review, November 2005.
12. Charron,Kenneth (2006). *Why KPI's Belong in Supply Chain Contract*, Supply Chain Management Review, March 2006.
13. Ellram, Lisa and George A. Zsidisin (2003), *An Agency theory Investigation of Supply Chain Risk Management*, The Journal of Supply Chain Management, Summer 2003.
14. Covello, Vincent T. and Jeryl Mumpower (1985), *Risk analysis and risk management: An historical perspective,* Risk Analysis, 5: 2,1985.
15. Van der Vorst , J.G.A.J and D.J. Van der Zee (2005), *A Modeling Framework for Supply Chain Simulation: Opportunities for Improved Decision Making,* Decision Sciences , 36:1, February 2005.
16. Billington, Corey, Lisa M.Ellram,and Wendy L.Tate (2004), *Understanding and Managing the Services Supply Chain*, The Journal of Supply Chain Management, Fall 2004.
17. Smith, Michael and George A Zsidisin, *Managing Supply Risk with Early Supplier Involvement: A Case Study and Research Propositions*, The Journal of Supply Chain Management , Fall 2005.
18. Sharma, Atul (2004), *A Systems Approach to Enterprise Risk Management*", SDM Thesis, supervised by Paul Carlile, 2004.

19. Michaud, David (2005), *Risk Analysis of Infrastructure Systems*", SDM Thesis, supervised by George Apostolakis, 2005.
20. Kaminsky, Philip, David Simchi-Levi, and Edith Simchi-Levi (2002), *Designing and managing the supply chain – Concepts,strategies and case studies*, McGraw-Hill Higher Education, Oct 11, 2002
21. Patel, Meehakshi-Dhar, ed.(2002), *Supply Chain and Logistics* The ET Knowledge Series, The Economic Times Intelligence Group, India, 2002.
22. *INCOSE Systems Engineering Handbook*, Version 3, June 2006 .
23. Hicks, Donal A.(1999), *A Four step methodology for using simulation and optimization technologies in strategic supply chain planning,* Proceedings of the 1999 Winter Simulation Conference, IEEE. http://ieeexplore.ieee.org/iel5/6629/17693/00816843.pdf