Global Journal of Researches in Engineering: G
Industrial Engineering
Volume 14 Issue 1 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

FMEA based Quantification Analysis of Outbound Supplier Risk and its Resilience

By Karthick. M & Manikandan. V
Thiagarajar College of Engineering, India

Abstract- Supply chain is the linkage of series of organizations with facilities, functions, and logistic activities that are involved in producing and also delivering a product or service. In the past, when firms manufactured in-house, they sourced locally and sold directly to customer. During that period, supply chain risk was less diffused and easier to manage. In recent years global supply chain was hit by increasing globalization, because all organizations had to face vulnerable by different types of risk in their inbound and outbound supply chain network. The various supply chain (SC) vulnerabilities are reputation, unreliability, overstocking, price increases, corruption, natural disasters and financial failure. The implications of supply chain possessing vulnerability costlier and lead to significant customer delivery delays, etc. Though, different types of supply chain vulnerability management methodologies have been proposed for managing supply risk. To the above concern, reinforce outbound supply chain risk management by proposing an integrated methodology to classify, manage and assess outbound supply risks were made. The contributions of the work owing to namely (1) outbound supply risk factors are identified through both supply chain risk literature review and industrial interview; (2) Hierarchical risk factor classification structure is created; (3) reduction of outbound supplier risk by using six sigma methodologies was validated. This project is an attempt to quantify the outbound supplier risk with a suitable case study.

GJRE-G Classification : *FOR Code: 290502*

Strictly as per the compliance and regulations of:

FMEA based Quantification Analysis of Outbound Supplier Risk and its Resilience

Karthick. M [α] & Manikandan. V [σ]

Abstract- Supply chain is the linkage of series of organizations with facilities, functions, and logistic activities that are involved in producing and also delivering a product or service. In the past, when firms manufactured in-house, they sourced locally and sold directly to customer. During that period, supply chain risk was less diffused and easier to manage. In recent years global supply chain was hit by increasing globalization, because all organizations had to face vulnerable by different types of risk in their inbound and outbound supply chain network. The various supply chain (SC) vulnerabilities are reputation, unreliability, overstocking, price increases, corruption, natural disasters and financial failure. The implications of supply chain possessing vulnerability costlier and lead to significant customer delivery delays, etc. Though, different types of supply chain vulnerability management methodologies have been proposed for managing supply risk. To the above concern, reinforce outbound supply chain risk management by proposing an integrated methodology to classify, manage and assess outbound supply risks were made. The contributions of the work owing to namely (1) outbound supply risk factors are identified through both supply chain risk literature review and industrial interview; (2) Hierarchical risk factor classification structure is created; (3) reduction of outbound supplier risk by using six sigma methodologies was validated. This project is an attempt to quantify the outbound supplier risk with a suitable case study.

I. Introduction

Supply chain resilience is defined as the system ability to approach its equilibrium state, after being disturbed by external or internal factors. This consideration is following aspects: Supply Chain flexibility, agility, velocity, visibility and redundancy (Creating resilient SCs: A Practical guide, 2003). Flexibility helps companies in correctly answering to markets variability, the agility as the company capability to quickly respond to unpredictable demand/supply markets changes, the velocity must be interpreted as time required for moving goods along the supply chain. The velocity is usually measured in terms of lead times; the visibility is the capability of the company to see all the information regarding the flow of products, information and finances both downstream and upstream along the supply chain.

The redundancy is the augmentation of capacity and inventory in each node of the supply chain for facing supply chain disruption events (Christopher and Rutherford, 2004). This paper focused on outbound supplier risk in supply chain. Managing outbound supplier risk can be a challenging task due in part to the complex and dynamic nature of supply chain systems.A typical supply chain system can be large in scale, having many tiers of suppliers, where each supplier tier of the supply chain provides goods or services to the next level supplier tier in the supply chain. They are facing much risk in internal and external to the supply chain.

Supply chains expand globally; their risk of disruption also grows. Supply chain risk is a particular type of hazards or threats affect the supply chain performance. Commonly there are two types of risk in the supply chain. There are internal risk (quality, accident, fire, security, IT, marketing, building, human, etc.,) and external risk (political, economical, social, technological, environmental, terrorist attack, war, etc.). (Understanding Supply Chain Risk: A self assessment workbook, 2003).

II. Literature Review

Christopher S. Tang (2006) reviewed various quantitative models for managing supply chain risks. We found that these quantitative models are designed for managing operational risks primarily, not disruption risks. However, we argue that some of these strategies have been adopted by practitioners because these strategies can make a supply chain become more efficient in terms of handling operational risks and more resilient in terms of managing disruption risks.

David Bogataj (2007) et.al suggested that the costs of risk in a supply chain, which is exposed to internal and external risk, are measured using net present value of activities approach. their consider financial risk (where the financial flow has the opposite direction to the flow of goods) increases with the extension of the network, especially when in globalization processes even the currency exchange rate in this flow is not always stable.

David J.Closs (2011) et.al developed a framework to examine the threat of potential disruptions on supply chain processes and focuses on potential mitigation and supply chain design strategies that can be implemented to mitigate this risk. There are focused with unintentional causes such as accidents or natural disasters, Intentional disruptions may include theft, terrorist attack, and man-made. They are not focused with cost perspective in SC network. Their results

Authors α σ: PG scholar, Department of mechanical Engineering, Thiagarajar College of Engineering, Madurai-15, India.
e-mails: msv.kathiktce@gmail.com, aeromani36@gmail.com

illustrate that the depth and breadth of security initiatives depends on top management mindfulness, operational complexity, and product risk.

Hansuk Sohn (2011) et.al analyzed distributors' selection is based on the rough set theory approach in both equal and unequal weight features. Through this method, several rules are generated for distributors' evaluation and selection. The result not only shows the effectiveness of unequal weight incorporated rules identification, but also it shows the importance of the relationship intensity, marketing experience, and the management ability in selecting the distributors.

Jukkahalikas (2004) et.al says about complete understanding of risk management in supplier network. There are taken from internal and external to the company SC network risks are demand problem, problems in fulfilling customer deliveries, cost management and pricing, and weaknesses in resources, development and flexibility. Their results indicate that risk management is an important development target in the studied supplier networks.

Kevin McCormack (2009) et.al regarding a new approach to the identification and prediction of supply risk. they are consider to risk ,such as the increased use of out sourcing, globalization, reduction of supplier based; reduced buffers, increased demand for on-time deliveries. The results to prepare proper mitigation and response strategies associated with these suppliers by SCRM approach.

Mark Goh (2007) et.al presents a stochastic model of the multi-stage global supply chain network problem, incorporating a set of related risks, namely, supply, demand, exchange, and disruption. They provide a new solution; design an algorithm for treating the multi-stage global supply chain network problem with profit maximization and risk minimization objectives. Nurmaya musa (2011) et.al investigate the development in supply chain risk management (SCRM) by using Literature survey and citation/co-citation analysis. In Most literature still focuses on material flow issues in risk management, in particular with supplier selection. Some efforts have been made to integrate material and cash flows by adapting financial option theory.

Sameer Kumar (2005) et.al proposed model is flexible and scalable and can be extrapolated for analysis of different nodes and layers in the existing disaster relief supply chains. This frame work was used in the example of the March 2011 disaster in Japan which was the result of a Tsunami, after a strong earth quake, followed by flooding and nuclear reactors' meltdown causing radiation dispersal. The failure mode effects and critical analysis method was used assess the reliability of a relief supply chain system and its critical components.

Sri Krishna Kumar (2013) et.al considered the location, production–distribution and inventory system design model for supply chain for determining facility locations and their capacity. Risk pooling effect, for both safety stock and running inventory (RI), have been incorporated in the system to minimize the supply chain cost along with determining facility location and capacity.

Stephen M.Wagner (2010) et.al developed an approach based on graph theory to quantify and hence mitigate supply chain vulnerability. their consider natural disasters such as droughts, floods, windstorms, hurry-canes, earth quakes or tsunamis strike more often and have a greater economic impact. At the same time, the number of man-made disasters such as accidents, wars, terrorist attacks, strikes, that affect supply chains.

Teresa Wu (2006) et.al considers the inbound supply chain risk management by proposing an integrated methodology to classify, manage and assess inbound supply risks. The contributions of this paper are four-fold: (1) inbound supply risk factors are identified through both an extensive academic literature review on supply risk literature review as well as a series of industry interviews; (2) from these factors, a hierarchical risk factor classification structure is created; (3) an analytical hierarchy processing (AHP) method with enhanced consistency to rank risk factor for suppliers is created; and (4) a prototype computer implementation system is developed and tested on an industry.

Timothy J. Pettit (2008) consider the current thought on supply chain resilience and Develop the construct into a managerial process for implementation. Academics and industry leaders have seen the need to supplement traditional risk management techniques with the concept of resilience that is better designed to cope with extreme complexities, unpredictable events and adaptive threats.

J.Vander Vorst (2002) et.al considers the factors are Changes in markets, products, technology, competitors and Governmental regulations.

Walter Zinn (2009) et.al proposed process builds upon an existing risk analysis framework by incorporating an innovative methodology used by the insurance industry to quantify the risk of multiple types of catastrophic events on key supply chain locations. Supply chains are increasingly vulnerable to catastrophic events such as hurricanes or terrorist attacks

III. Resilience Framework

Supply chain resilience is defined as the system ability to approach its equilibrium state, after being disturbed by external or internal factors. The main objective of the supply chain management is minimizing the cost and maximizing the customer satisfaction. However, improving supply chain resilience requires an appreciation that supply chain vulnerabilities may come in many guises, and the drivers of risk operate at several different levels.

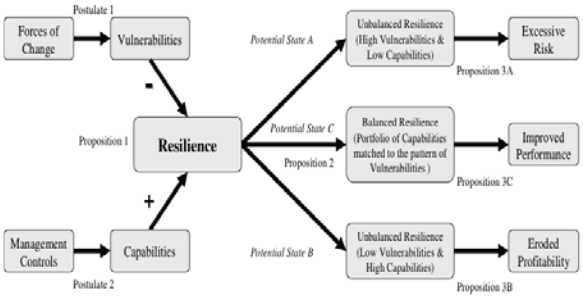

Figure 3.1

Flexibility helps companies in correctly answering to markets variability, the agility as the company capability to quickly respond to unpredictable demand/supply markets changes, the velocity must be interpreted as time required for moving goods along the supply chain.

The velocity is usually measured in terms of lead times; the visibility is the capability of the company to see all the information regarding the flow of products, information and finances both downstream and upstream along the supply chain. The redundancy is the augmentation of capacity and inventory in each node of the supply chain for facing supply chain disruption events (Christopher and Rutherford, 2004).

Supply chains expand globally; their risk of disruption also grows. Supply chain risk is a particular type of hazards or threats affect the supply chain performance. Supply chain vulnerability can be defined as an exposure to serious disturbance, arising from risks within the supply chain as well as risk external to the supply chain (Timothy Pettit, 2010).

IV. Levels of Analysis of Resilience

The main objective of the supply chain management is minimizing the cost and maximizing the customer satisfaction. However, improving supply chain resilience requires an appreciation that supply chain vulnerabilities may come in many guises, and the drivers of risk operate at several different levels.

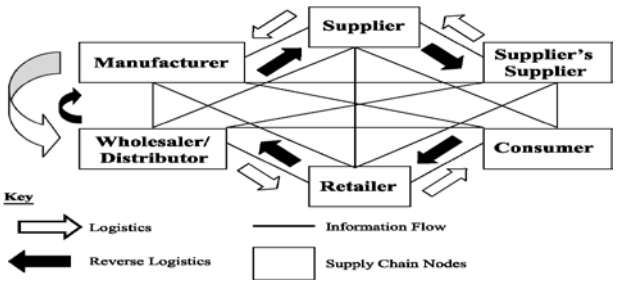

Figure 3.2

a) Events and Network Interaction

The multi-level framework outlined above breaks-down the problem of supply chain vulnerability into its constituent parts, nevertheless it should be born in mind that when an event occurs it may impact at several levels, as the celebrated example of Nokia and Ericsson illustrates (see below).

The Nokia/Ericsson example highlights the vulnerability of industries with capacity constrained production and also raises other important themes, such as the issue of common components and the consequential nature of supply chain risks. The latter is in turn linked to the fact that supply chains are linear processes within complex systems of interacting networks

b) NOKIA and ERICSSON

In March 2000 worldwide demand for mobile telephones was booming. Two of the international market leaders were Finnish electronics company Nokia and its Swedish rival Ericsson. This is the tale of how an 'Act of God' half a world away would set off a train of events that would eventually precipitate a major competitive re-alignment.

The story starts on the evening of March 17th 2000, with a thunderstorm over central New Mexico. A lightning bolt hit a power line, which caused a fluctuation in the power supply, which resulted in a fire in a local semiconductor plant owned by Dutch firm Phillips Electronics NV. The fire was brought under control in minutes, but a batch of trays containing enough silicon wafers for thousands of mobile phones were destroyed in the furnace. The damage to the factory from smoke and water was much more extensive than the fire itself, contaminating the entire stock of millions of chips. The suppliers immediately prioritized customers, according to the value of their business. Between them, Nokia and Ericsson accounted for 40% of the plant's output of the vital radio frequency chips, so these companies were put at the top of the supplier's list.

On 20th March, in Finland Nokia's event management systems indicated that something was amiss. Orders were not coming through as expected, so a components purchasing manager phoned the supplier who informed him that there had been a fire in the plant, which would disrupt production for around a week. Nokia was not unduly alarmed, but dispatched engineers to New Mexico to investigate the situation. Philips were not encouraging visitors, so having been unable to investigate the problem further, Nokia increased monitoring of in-coming supplies from weekly to daily checks. It became clear soon afterwards that the problem was so serious that supplies would be disrupted for months.

Pressure was brought to bear at the highest levels between Nokia and its supplier to ensure that all other Philips plants were commissioned to use any additional capacity to meet Nokia's requirement. In addition, Nokia immediately sent representatives out to its other suppliers in the US and Japan to secure priority

status for all available supplies of chips, and persuaded them to ramp up production as quickly as possible. Because Nokia was such an important customer, they obliged with a lead-time of less than one week.

Nokia also set about reconfiguring its products to take slightly different chips from other sources. Ericsson had also found out about the fire soon after it occurred, but having been assured by the suppliers that the fire was unlikely to cause a major problem, had not acted further until early April.

By then Nokia had already moved to secure its supplies, and unlike the quick acting Finns, Ericsson had no alternative sources of supply. Ericsson lost an estimated $400m in new product sales as a result of the fire. An insurance claim would later offset some of Ericsson's direct losses; nevertheless it was forced to cease manufacturing mobile phones.

V. Details of the Six Sigma DMAIC Tool

The DMAIC toolkit is without question the most effective process improvement framework known in industry today, and teams that learn and apply this methodology will achieve unprecedented success.

The five stages of DMAIC cycle,

Table 5.1

DEFINE	Identify the problem and Collect data from various sources
MEASURE	Measure the capability of the problem by using FMEA
ANALYSE	Classify the problem, use cause and effect analysis and prioritize for action
IMPROVE	Mitigate the problem by using FMEA
CONTROL	Improve visibility of the process. Use statistical process control.

a) Data Collections from small scale industries and literature surveys

Table 5.2

FROM LITERATURE SURVEY	FROM SMALL SCALE INDUSTRIES
Outbound supplier risks	Outbound supplier risks
Demand Security External legal issues Market characteristics Political stability Natural/man-made disaster II tier supplier	Labor strikes Loss of contracts Economical down Delay delivery Uncertainty in power supply Labor absenteeism

b) Failure Mode Effect Analysis

Failure Mode and Effect Analysis (FMEA) is a tool that makes it possible to determine a system's possible modes of risk, and then to establish the effects of those risks on the Overall performance of the system.

FMEA is widely used as a quality improvement tool that can be applied equally to physical systems (vehicles, aircraft, electronic devices and so forth) and non-physical systems such as supply chain processes. The purpose of FMEA is to prevent process and product problems during the design phase. However, conducting an FMEA on existing processes is also hugely beneficial; unlike products, processes can be re-engineered more easily.

c) Using FMEA (or FMECA), businesses can

- Exhaustively identify and catalogue the various ways in which links and nodes in the supply chain may fail.
- Determine the effects of those risks.
- Rank risks according to their likelihood of occurrence, their disruptive effect and the likelihood that imminent risk can be detected in time to put in place remedial action. Combined, this then gives an estimate of criticality, in order to guide preventative action.

d) Steps to creating a FMEA

- Identify the risks.
- List the potential risk mode for each process step.
- List the effects of this risk mode. If the risk mode occurs what does this mean to us and our customer… in short what is the effect?
- Rate how severe this effect is with 1 being not severe at all and 10 being extremely severe. Ensure the team understands and agrees to the scale before you start. Also, make this ranking system "your own" and don't bother trying to copy it out of a book.
- Identify the causes of the failure mode/effect and rank it as you did the effects in the occurrence column. This time, as the name implies, we are scoring how likely this cause will occur. So, 1 means it is highly unlikely to ever occur and 10 means we expect it to happen all the time.
- Identify the controls in place to detect the issue and rank its effectiveness in the detection column. Here a score of 1 would mean we have excellent controls and 10 would mean we have no controls or extremely weak controls.
- Multiply the severity, occurrence, and detection numbers and store this value in the RPN (risk priority number) column.
- Sort by RPN number and identify most critical issues. The team must decide where to focus first.

- Assign specific actions with responsible persons. Also, be sure to include the date for when this action is expected to be complete.
- Once actions have been completed, re-score the occurrence and detection.

i. *Seveority Rating scale*

Table 5.3

Rating	Description	Definition (Severity of Effect)
10	Dangerously high	Risk could highly affect the supplier and customers.
9	Extremely high	Risk would create noncompliance with federal regulations.
8	Very high	Risk renders the unit inoperable or unfit for use.
7	High	Risk causes a high degree of customer dissatisfaction.
6	Moderate	Risk results in partial malfunction of the supply.
5	Low	Risk creates enough of a performance loss to cause the customer to complain.
4	Very Low	Risk can be overcome with modifications to the supplier process, but there is minor performance loss.
3	Minor	Risk would create a minor nuisance to the supplier, but the supplier can overcome it without performance loss.
2	Very Minor	Risk may not be readily apparent to the supplier, but would have minor effects on the supplier process.
1	None	Risk would not be noticeable to the supplier and would not affect the supplier process.

ii. *Occurence rating scale*

Table 5.4

Rating	Description	Potential Failure Rate
10	Very High: Risk is almost inevitable.	More than one occurrence per day or a probability of more than three occurrences in 10 events.
9	High: Risk occurs almost as often as not.	One occurrence every three to four days or a probability of three occurrences in 10 events.
8	High: Repeated risk.	One occurrence per week or a probability of 5 occurrences in 100 events.
7	High: Risk occurs often.	One occurrence every month or one occurrence in 100 events.
6	Moderately High: Frequent risk.	One occurrence every three months or three occurrences in 1,000 events.
5	Moderate: Occasional risk.	One occurrence every six months to one year or five occurrences in 10,000 events.
4	Moderately Low: Infrequent risk.	One occurrence per year or six occurrences in 100,000 events.
3	Low: relatively few risks.	One occurrence every one to three years or six occurrences in ten million events.
2	Low: Risks are few and far between.	One occurrence every three to five years or 2 occurrences in one billion events.
1	Remote: Risk is unlikely.	One occurrence in greater than five years or less than two occurrences in one billion events.

iii. *Detection rating scale*

Table 5.5

Rating	Description	Definition
10	Absolute Uncertainty	Risk is not detectable and uncontrollable.
9	Very Remote	The risk can be detected only with thorough inspection and this is uncontrollable.
8	Remote	Risk is detected based on no effects in a events.
7	Very Low	The risk can be detected with manual inspection but no effects is in place so that detection is left to chance

6	Low	Risk is 100% manually detected using mistake-proofing techniques.
5	Moderate	Risk is partially detected and partially controlled.
4	Moderately High	Risk is partially detected and it is control conditions.
3	High	There is 100% detection or review of the process but it is not automated
2	Very High	All risk is 100% automatically detected.
1	Almost Certain	The risk is obvious or there is 100% automatic detection with regular calibration and easy to take a preventive action.

VI. Results and Discussions

The various inbound and outbound risks are listed

Table 6.1

Risk	Potential Failure mode	Potential Effects of failure	S	Potential Causes of failure	O	Current Process control	D	RPN (S*O*D)
Outbound Supplier risk	Demand	Forecasting Is more complex, Reduce the Performance of the Supply chain, Lack of production and delivery, Erosion of profits, Creating un balanced resilience in the supply chain	6	Sudden Changes	8	Controllable	7	336
	Security		5	Maritime pirate attack, IT/Internet Security	4	Controllable	4	80
	External legal issues		7	Labor strikes, Legal claims By customer	9	Controllable	4	252
	Market characteristics		6	Market size and growth changes, Loss of contract, low Margin	6	Uncontrollable	10	360
	Political stability		5	Economy down, new Government, Rules/ regulation Changes	7	Uncontrollable	10	350
	Natural/man-made disaster		10	Earth quake, Volcano, Flood, Hurricane, Terrorism	1	Uncontrollable	10	100
	II tier supplier		4	Poor communication	8	Controllable	2	64

VII. Prioritization of the Outbound Supplier Risk

Table 7.1

Outbound supplier risk		
Priority number	Potential failure mode	RPN
1	Market characteristics	360
2	Political stability	350
3	Demand	336
4	External legal issues	252
5	Natural/man-made disaster	100
6	Security	80
7	II tier supplier	64

The highest RPN values in outbound supplier risks are market characteristics, political stability and demand flexuation. But the demand risk is already focused in many literatures and mitigated by using suitable forecasting techniques. So first we mainly focused on political and market characteristic risks.

References Références Referencias

1. James C.Chen, Chen-Huan Cheng (2013). *Supply chain management with lean production and RFID application: A case study*. Expert systems with applications, Vol 40, PP 3389-3397.
2. Cheri speier, David J.Closs (2011). *Global supply chain design consideration: Mitigation product safety and security risks.* Journal of operation management, Vol 29, PP 721-736.
3. Kevin McCormack, Peter trkman, (2009). *Supply chain risk in turbulent environment-A Conceptual model for managing supply chain network risk.* Int.J.Production economics, Vol 119, PP 247-258.
4. Jukka hallikas, Urho pulkkinen, Iris karvonen (2004). *Risk management process in supplier network.* Int.J.Production economics, Vol 90, PP 47-58.
5. S.Nurmaya musa, Ou tang (2011). *Identifying risk issues and research advancement in supply chain risk management.* Int.J.Production economics, Vol 133, PP 25-34.
6. Samir dani, Roy kalawsky (2012). *Supply chain risk management: Present and future scope*. Int.J.logistic management, Vol 23, PP 313-339.
7. Stephan M.Wagner , Nikrouz Neshat (2010). *Assessing the vulnerability of supply chains using graph theory.* Int.J.ProductionEconomics, Vol 126, PP 121–129.
8. David Bogataja, Marija Bogataj (2007). *Measuring the supply chain risk and vulnerability in frequency space*. Int.J.Production Economics, Vol 108, PP 291–301.
9. Walter Zinn, Michael Knemeyer, Cuneyt Eroglu (2009). *Proactive planning for catastrophic events in supply chains.* Journal of Operations Management, Vol 27, PP 141-153.
10. Sameer Kumar, ThomasHavey (2005). *Before and after disaster strikes: A relief supply chain decision support framework.* Int. J. Production Economics.
11. Hansuk Sohn, Guofang Song, Rafael Gutierrez (2011). *A rough set based approach to distributor selection in supply chain management.* Expert Systems with Applications, Vol 38, PP 106-115.
12. Mark Goh, Joseph Y.S. Lim (2007). *A stochastic model for risk management in global supply chain networks.* European Journal of Operational Research, Vol 182, PP 164-173.
13. Teresa Wu, Jennifer Blackhurst (2006). *A model for inbound supply risk analysis*. Computers in Industry, Vol 57, PP 350–365.
14. Christopher S. Tang (2006). *Perspectives in supply chain risk management*. Int. J. Production Economics, Vol 103, PP 451–488.
15. Sri Krishna Kumar, M.K. Tiwari (2013). *Supply chain system design integrated with risk pooling*. Computers & Industrial Engineering, Vol 64, PP 580–588.
16. J. Van der Vorst, A. Beulens (2002), *Identifying sources of uncertainty to generate Supply chain redesign strategies.* International Journal of Physical Distribution and Logistics Management, Vol 33, PP 409–430.

This page is intentionally left blank