Industrial Engineering
& Management Systems
Vol 12, No 2, June 2013, pp.103-111
ISSN 1598-7248 | EISSN 2234-6473 |

http://dx.doi.org/10.7232/iems.2013.12.2.103

A Framework of Managing Supply Chain Disruption Risks Using Network Reliability

Shunichi Ohmori, Kazuho Yoshimoto*
Department of Industrial and Management System Engineering, School of Creative Science and Engineering,
Waseda University, Tokyo, Japan

(Received: January 31, 2013 / Revised: April 8/May 31, 2013 / Accepted: May 31, 2013)

ABSTRACT

This paper discusses how to manage supply chain disruption risks from natural disasters or other low-likelihood-high-impact risk drivers. After the catastrophic earthquake in Eastern Japan and the severe flood in Thailand, most companies have been attempting to re-establish the business continuity plan to prevent their supply chain from disruption. However, the challenges for managers and individual risks are often interrelated, and thus, actions that mitigate one risk can end up being no contribution as a whole. In this paper, we describe a framework for assessing how much impact individual mitigation strategies have on the entire supply chain protection against disruption, using network reliability. We propose three categories of risk-mitigation approaches: Stabilization, Absorption, and Duplication. We analyze the situation under which each of these strategies is the best suitable. With a clear understanding of relations between these mitigation strategies and the entire supply chain risks, managers can select effective risk-reduction approaches to their supply chain.

Keywords: Supply Chain Risk Management, Business Continuity Planning

* Corresponding Author, E-mail: kazuho@waseda.jp

1. INTRODUCTION

In this paper, we describe an assessment and mitigation model of supply chain disruption risks, focusing on the network structure. It is well known that the supply chain disruption, arising from natural disasters, plant firing, terrorism, and supplier bankruptcy, have caused serious damages to the supply chain in many industries (Table 1). To prevent such serious losses, many companies have attempted to mitigate disruption risks by adding inventories, adopting standardized parts, and dup-licating suppliers. There are, however, challenges for ma-nagers in making the choice of such mitigation strategies: 1) As off-shoring and globalization of manufacturing operations continue to grow, today's supply chains are complex, huge, and geographically more diverse and, therefore, exposed to various types of disasters (Simchi-Levi, 2010); 2) Individual risks are often interconnected and actions that mitigate one risk can end up exacerbating another (Sodhi and Tang, 2012); 3) There are trade-offs between investment cost and the risk covered, and managers must be careful if actions that mitigate risks would have no significant harm for the company's profit.

Given these difficulties, the need for risk management in a rational manner, along with scientific and engineering approaches, has been emerging, and *Supply Chain Risk Management (SCRM)* has been attracting growing interest in the recent research and practice.

There are several papers dealing with supply chain risk management. See Sodhi and Tang (2012) for general concepts and literature reviews. While there are a number of papers addressing *qualitative* conceptual frameworks for disruption management in different situations, the *quantitative* models of supply chain disruption are limited. There are several probability models or stochastic programming models in the context of disruption risk management, considering dual-sourcing models, inventory models, process flexibility models, or location models. These models are, however, single-stage models, and thus, are not applicable to the disruption risk management arising in the global network where there are typically tens or even hundreds of stages. The literature dealing with the disruption of network are a research stream of stochastic programming network design model proposed by Santoso *et al.* (2005), Garg and Smith (2008), Bundschuh *et al.* (2003), each of which minimizes the cost and risks associated with disruption. However, while these stochastic programming models can help find an optimal set of locations in a network, they do not explicitly consider variations of mitigation strategies, such as adding inventory, or reinforcing facilities resistances against breakdowns.

Table 1. Various risk events that disrupt supply chain

Year	Cause	Company	Damage
2000	Plant fire	Ericson	Opportunity loss of $390 million
2004	Earthquake (Niigata, Japan)	Nippon Seiki	Total loss of $3.2 million
2007	Supplier's bankruptcy	Land Rover	Laying off of 1,400 workers
2011	Earthquake (Eastern Japan)	Toyota	Sales reduction of 170K autos
		Renesas	Shutdown of 8 plants, extraordinary loss of $780 million
2011	Thai floods	TDK	Induration of 4 plants

In this paper, we propose a risk assessment and mitigation method for the supply chain disruption, using network reliability theory. Our model centers around the assessment and mitigations of supply chain disruption risks with respect to the network connectivity, considering several special features arising in the application in SCRM. The followings are major differences of application of network reliability to SCRM in comparison with such other areas as Computer network and transportation network.

The first is the definitions of risks. We consider that, while there are some products such as foods or medicines that need extreme level of reliability at the sacrifice of mitigation costs, it is rather reasonable to consider that in many industries even after the disruption has occurred, the damages are quite low, if the recovery speed should be maintained within the target allowance. Considering these features, we define the risks of supply chain disruption as to whether they can be recovered by the specified target time, not just whether they are simply disrupted or not.

The second development is detection of the '*weakest link*' in the network. It is known that robustness to disruption risks in a supply chain is determined by the '*weakest link*' in the chain, and therefore, it is of great importance to detect the weakest link to make an investment decision properly. In this paper, we propose the index '*risk importance*' to detect the investment points in the supply chain network. We will also derive other exceptions of this property.

The third development is the comparison of mitigation strategies. Once the weakest link is detected, managers need to determine which mitigation strategies to choose. There are various mitigation strategies discussed, but we categorize these into three strategies: Stabilization, Absorption, and Duplication. The first one is the actions to reduce the impact of risk events, and the other two are actions to reduce the likelihood of risk events (Section 2 for details). We have compared these three strategies in different parameter settings to help managers choose mitigation strategies.

Our method does not require the background of sophisticated mathematical or computer programming. The only background required is knowledge of simple calculus and the usage of spreadsheet. This convenience is beneficial, especially when quickly understanding the challenges and opportunities of risk management within the organization and its supply chain.

We should also mention what this paper is not. It is not a new model of network reliability. Nor is the paper a proposal of new heuristics for computing network reliability. Instead, we have discussed how it is to be applied to get better understanding of supply chain reliability and also vulnerability. Our coverage of numerical implementation is also highly simplified, but we feel that it is adequate for the potential user to develop working implementations.

The reminder of the paper is organized as follows: In Section 2, we provide a general framework for managing supply chain disruption risks, and also present how our proposed method can be used in our framework. In Section 3, we describe how the reliability of supply chain is calculated and also which player in a chain to choose to improve the reliability of the entire chain efficiently. In Section 4, we discuss how to select mitigation actions for selected player, and in Section 5 we make a conclusion.

2. PROPOSED FRAMEWORK FOR MANAGING RISKS OF SUPPLY CHAIN DISRUPTION

In this section, we provide a general framework for managing supply chain disruption risks, and also present how our proposed method can be used in our framework. Our framework is based on the one presented in Sodhi and Tang (2012) and gives several customizations for the use of our analysis method.

2.1 Proposed Framework for Managing Risk of Supply Chain Disruption

The framework we propose to avoid risks of supply

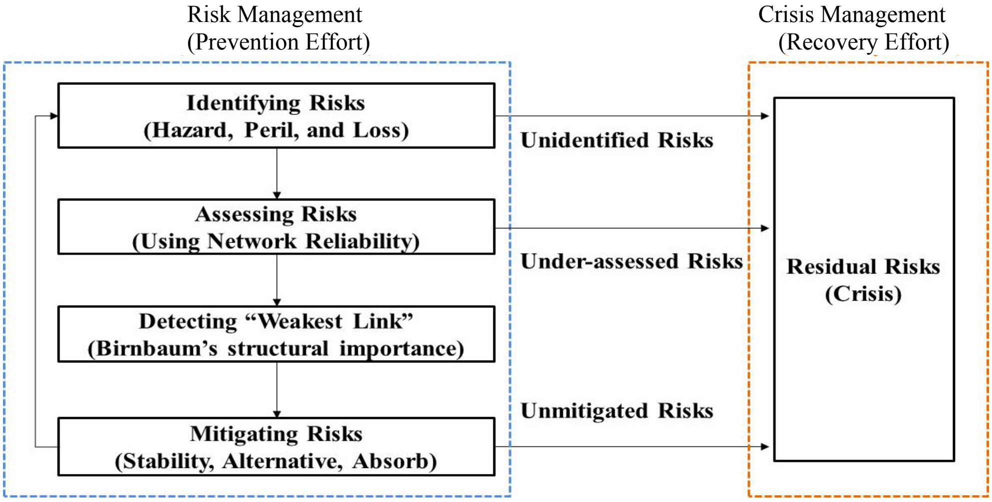

Figure 1. Proposed framework for managing risk of supply chain disruption.

chain disruption is described in the Figure 1. The detail description for each step is as follows:

1) Identifying risks: The first step of risk management is identifying risks. There are many sources of risks that drive supply disruptions. To identify such sources of risks, it is often helpful to utilize the categorization: Risks in *inbound* versus *outbound* supply chain or in *Global* versus *Local* level. It is also helpful to use the typical terminologies that distinguish the underlying *causes*, occurrence of *events*, and *consequences such* as: *Hazard*, *Peril*, and *Loss*.
2) Assessing risks: The second step is assessing risks. We use network reliability to evaluate how the local failures have an impact on the entire supply chain (Section 3).
3) Detecting 'weakest link': The third step is detecting the 'weakest link' in a chain. As previously discussed, since the strength of the supply chain is determined by the weakest link, it is important to detect which link is the weakest in the chain. We used risk importance index to detect the weakest link in the supply chain (Section 3).
4) Mitigating risks: The last step is mitigating risks. We propose the three categories of mitigation strategies: Stabilization, Absorption, and Duplication. We discuss how these strategies are applied to improve network reliability. We also analyze the situation under which each of these strategies is the best suitable.

Repeating these four steps, managers of supply chain can successively improve the reliability of weakest link so that the entire supply chain has enough robustness to the potential disruptions.

There are, to a certain extent, residual risks even with these efforts, so companies should be ready for the cases when the crisis occurs. We distinguish the terms '*risk management*', and '*crisis management*' in terms of *before* or *after* the risk events. We defined the risk management as the prevention effort that companies have to make *before* the risk events and the crisis management as the recovery effort *after* the events. Since it is impossible for the company to get rid of all possible sources of risks, the companies should work on crisis management as well, such as building business continuity plan, developing IT system, or aligning supply chain partners.

With a clear understanding of relations between these mitigation strategies and the entire supply chain risks, mangers can select effective risk-reduction approaches to their supply chain.

2.2 Definition of Risk Management

There are many ways to describe the commonly used words "*risks*" and "*risk management.*" To avoid confusions, we show the definitions of several keywords used in this paper.

As the typical definition discovered in the general purpose risk management, the term "*risk*" in this paper can be defined as:

$$\text{Risk} = \text{Impact} \times \text{Liklihood} \tag{1}$$

We defined the "*risk management*" is the process of actions that minimize the cost of investment and the associated risk, described as follows:

$$\text{min. } C + L \times P(C) \tag{2}$$

where C denotes the investment cost of mitigations, L denotes the expected loss that the supply chain would suffer from disruption, P denotes the probability of supply chain disruption.

As discussed in Section 1, we defined the risks of supply chain disruption as to whether they can be recovered by the specified target period, not just whether they are simply broken down. Considering these features, we divide the probability P into two probabilities.

$$P = p \times q \tag{3}$$

where p denotes the probability that the supply chain is down, and q denotes the probability that the supply chain cannot recover until the specified target time (Figure 2 for an illustration).

There are several advantages of this approach. First, it simplifies the calculation of network reliability. Perhaps, it seems more accurate to treat the recovery time as some degree of losses. This approach, however, requires the evaluation of 2^N combinations of binary variables used to denote the supplier up/down states. Our approach, on the other hand, requires a few combinations of binary variables at most, and thus, is convenient and also appropriate in a practical use.

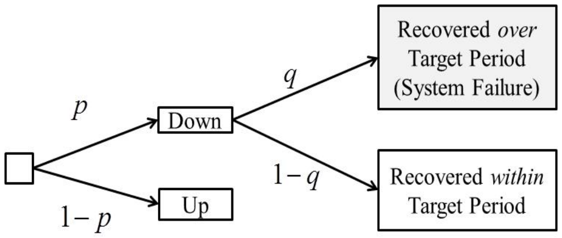

Figure 2. Illustration of system failure.

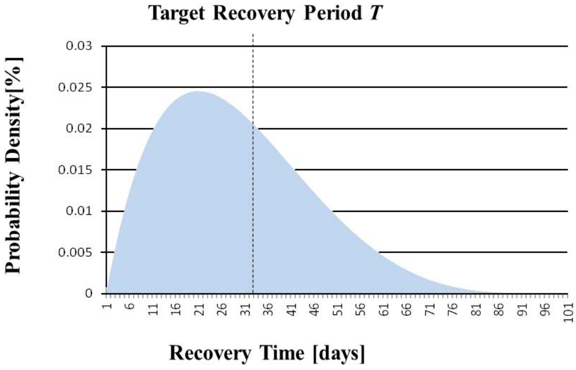

Figure 3. Recovery time estimation using beta distribution.

The benefits of this approach come also when choosing mitigation strategies (discussed in Section 4).

To make good guesses for each probability, it is helpful to use historical data, if any. Typical approach to estimate these probabilities is to assume the arrival of failure as the *Poisson Process* with mean r. Here the Poisson distribution prob ($y = k$) is distribution of the number of events over time. Using this distribution, we can estimate p or q by calculating prob ($y > 1$). We can also estimate the recovery failure probability q, using the recovery time distribution from similar disruption events. For example, assume we observed the distribution of recovery time for a particular event, say earthquake, as *beta distribution* as in Figure 3. Then, we can estimate, or at least get some hint for, the probability prob ($t < T$) with recovery time t and target recovery period T in the next similar event (next earthquake).

Of course, many disruption events are very rare, and estimating the probabilities of those failures can be difficult. The reasonable approach is, therefore, changing parameters in a certain range and conduct *what-if* analysis to ensure the supply chain has enough robustness against disruption under different situations.

3. DISRUPTION RISK ASSESMENT USING NETWORK RELIABILITY

In this section, we present the risk assessment method using network reliability. The general term '*Reliability*' is defined as "*the ability of the system to remain functional.*" This concept can be directly applied in the supply chain. There are various indices for the reliability. Among such indices, we use the '*connectivity reliability.*' Connectivity reliability is defined as 'the probability that guarantee the function of links between given pairs of points on a network.' In the context of supply chain disruption management, this can be interpreted as "the probability that guarantee the specified service level of supplies to the customers." As the specified service level, we defined suppliers are *not-broken* or *recovered within a specified period* as we discussed. We show how this connectivity reliability is calculated in the following sections.

3.1 Supply Chain in a Reliability Block Diagram

The network reliability is calculated for the given reliabilities of each component in a system. To calculate this, it is helpful to describe the structure of a system in the reliability block diagram (RBD). The RBD is an event diagram to denote which elements of the system are necessary for the fulfillment of the required function and which can fail without affecting it (Birolini, 2007). In the supply chain context, the elements are suppliers.

Consider an example of bill of material (BOM) and corresponding RBD described in a Figure 4. The product X is composed of the parts a and b, and b is composed of c and d. The part d is sourced from two suppliers. In RBD, the production of each component is described as 'block.' The branching operations between different parts (a and b, c and d) in a tree diagram are described as links in a *series* in RBD, because system fails if any of components fails. Likewise, the branching operation between same parts (d_1 and d_2) in a BOM is described as links in a *parallel*, because system fails if and only if all components fail. RBD with more complicated structure is discussed in Section 3.5, and RBD with multi-product case is discussed in Section 3.6.

3.2 Calculation of Network Reliability

Once the system is described in a RBD form, it is necessary to denote the condition of each player and the entire system. Here, let x_a be binary variable to denote whether player a is functional as:

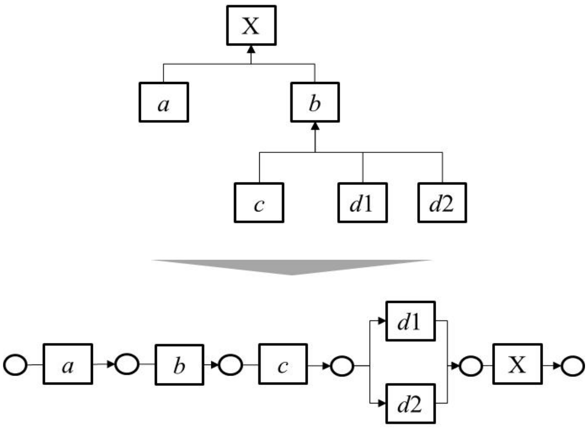

Figure 4. An example illustrating bill of materials and correspond reliability block diagram.

$$x_a = \begin{cases} 1, & \text{if link } a \text{ is functional} \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

Similarly, let $x = (x_1, \cdots, x_n)$ denote the state vector of the system and $\phi(x)$ be binary variable to denote whether the system is functional as in (5):

$$\phi(x) = \begin{cases} 1, & \text{if system is functional} \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

Using these variables, we show how the network reliability in different systems can be calculated.

If the suppliers are composed in a series system in RBD, there is only one path from the origin of supply chain to the customer. The network reliability R, therefore, is calculated as in (6):

$$R = \prod_{i=1}^{N} r_i \tag{6}$$

where r_i denotes the reliability of each component with $r_i = 1\text{-}p_i q_i$, p_i denotes breakdown probability and q_i denotes the recovery failure probability for supplier i.

On the other hand, if the suppliers are composed in a parallel system in RBD, the network reliability is calculated as in (7):

$$R = 1 - \prod_{i=1}^{N} (1 - r_i) \tag{7}$$

In a parallel system, the required function of the system is fulfilled if at least one of the elements works without failure.

Using these formulas (6) and (7), the supply chain reliability described in Figure 4 can be calculated as:

$$R = r_a r_b r_c [1 - (1 - r_{d1})(1 - r_{d2})] r_X \tag{8}$$

Therefore, disruption risk of supply chain is given as: $L \times (1 - R)$.

3.3 Probability Importance

In this section, we consider how to improve network reliability efficiently. In the supply chain, it is interpreted as which suppliers to select to reduce disruption risks efficiently. As an index of efficiency of improvement of network reliability, we introduce the 'probability importance' defined as in (9):

$$PI_i = \partial R / \partial r_i \tag{9}$$

This index has property $PI \geq 0$, and quantifies the impact of the improvement of link i on the entire supply chain protection against disruption.

In a series system composed of two suppliers with reliability r_1 and r_2, the supply chain reliability is calculated as in (10):

$$R = r_1 r_2 \tag{10}$$

The probability importance of each link is then calculated as in (11) and (12):

$$PI_1 = \partial R / \partial r_1 = r_2 \tag{11}$$

$$PI_2 = \partial R / \partial r_2 = r_1 \tag{12}$$

Without the loss of generality, provided $r_1 > r_2$, then $PI_1 > PI_2$ holds. From this analysis, we can see improving the weakest link in the chain gives the largest risk-reductions for the supply chain in a series system.

In a parallel system with two suppliers, the supply chain reliability is calculated as (13):

$$R = 1 - (1 - r_1)(1 - r_2) \tag{13}$$

The probability importance of each link is then calculated as in (14) and (15):

$$PI_1 = \partial R / \partial r_1 = 1 - r_2 \tag{14}$$

$$PI_2 = \partial R / \partial r_2 = 1 - r_1 \tag{15}$$

Provided $r_1 > r_2$, then $PI_1 > PI_2$ holds. From this analysis, we can see improving the strongest link in the chain gives the largest risk-reductions for a parallel system.

Likewise, we can calculate the probability importance for more complicated systems. Using these calculations, we can detect suppliers that need improvements to the entire supply chain reliability against disruption.

3.4 Complex Structure

In this section, we consider how to calculate the reliability of complex system. For example, consider the distribution network illustrated in Figure 5. There are two manufactures (1, 2), one depot (3), and two retailers (4, 5). In this example, products manufactured in 1 and 2 are delivered through depot 3 to retailers 4 and 5, but there are also direct delivery from manufactures to retailers.

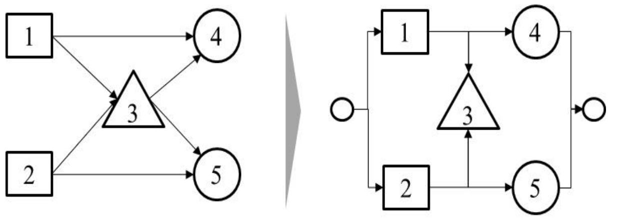

Figure 5. An example illustrating 'bridge' structure (box, manufacture; triangle, depot; circle, retailer).

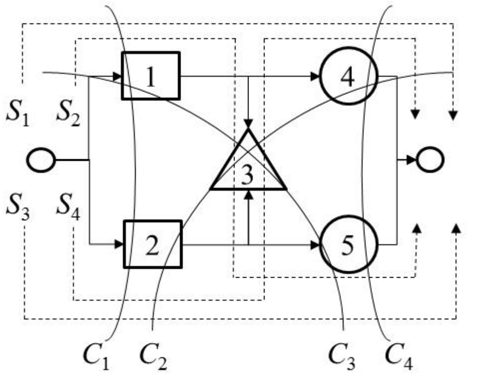

Figure 6. An example illustrating minimal path set and minimal cut set.

This structure is called 'bridge' structure, and it is known that this structure cannot be described in serial-parallel patterns unless at least one of their components appears more than once.

There are two ways to calculate the reliability of complex network, using '(*minimal*) *path set*', and '(*minimal*) *cut set.*' An example illustrating minimal path set and minimal cut set are shown in Figure 6. A set S_j is a minimal path set. Here system downs if any of components in S_j is down. In this example, we have $S_1 = \{1, 4\}$, $S_2 = \{1, 3, 5\}$, $S_3 = \{2, 5\}$, and $S_4 = \{2, 3, 4\}$. On the other hand, a set C_j is a minimal cut set. Here system downs if and only if all components in a cut are down. In this example, we have $C_1 = \{1, 2\}$, $C_2 = \{2, 3, 4\}$, $C_3 = \{1, 3, 5\}$, $C_4 = \{4, 5\}$.

The general formulas for network reliability using path set and cut set are given as in (16) and (17) respectively:

$$R = E\left[1-\prod_{j=1}^{J}\left(1-\prod_{i\in S_j} x_i\right)\right] \tag{16}$$

$$R = E\left[\prod_{j=1}^{J}\left(1-\prod_{i\in C_j}(1-x_i)\right)\right] \tag{17}$$

Where S_j denotes j-th path set, and C_j denotes j-th cut set. Evaluating this function require 2^N the binary operation.

However, there are several simple heuristics that work really well. For example, heuristics proposed in Iida *et al.* (1988) calculate the 16-nodes-24-arcs network reliability without Boolean operation with 99.99% accuracy.

3.5 Reliability of Multi-Product Supply Chain

We can also think of the multi-product case. For example, consider the supply chain network and corresponding RBD in a simplified manner, illustrated in Figure 7. There are six supply chain channels in RBD, each of which is a path in a series system with reliability R_k. Here let L_k denote the loss caused by supply disruption for product k. The expected losses, *i.e.* risks, are calculated by as in (18):

$$\sum_{k=1}^{K} L_k(1-R_k) \tag{18}$$

where, K denotes the number of supply chains.

Also, we should modify the probability importance in a weighted form as in (19):

$$\sum_{k\in K(i)} L_k PI_i = \sum_{k\in K(i)} L_k \partial R_k / \partial r_i \tag{19}$$

where, $K(i)$ denotes the set of products composed of the parts i. This index can be interpreted '*risk importance*', by which we can select the supplier that gives maximum efficiency of improvement in reliability.

3.6 Case Study

To get a clear understanding of risk assessment and risk importance, we consider an example illustrated in Figure 7. The risk event we consider in this example is earthquake. We assume reliability of each suppler as Table 2, loss for each supply chains (SCs) failure as A = 5, B = 3, C = 4, D = 2, E = 1, F = 4 ($, million). Failure probability in Table 2 is estimated by Poisson arrival.

Table 2. Reliability of each supplier

Suppliers	Failure frequency	Reliability
2, 11, 14, 21, 25	Once in 10 years	$r_i = 0.9$
The others	Once in 100 years	$r_i = 0.99$

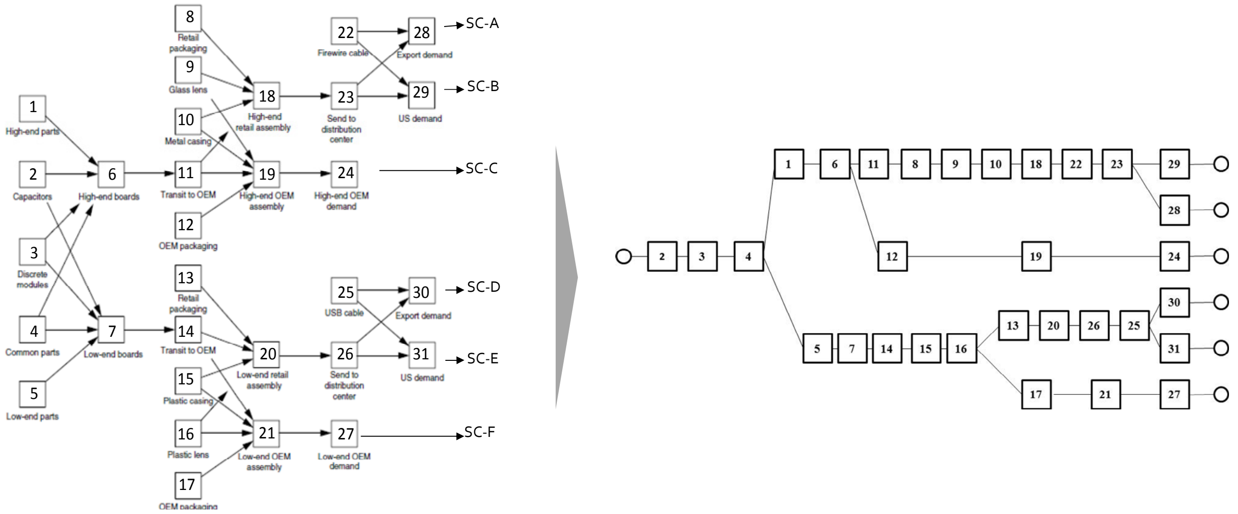

Figure 7. Supply chain of PC industry and correspond reliability block diagram. Taken from Humair and Willems (2006).

We define the planning period as 10 years. We assume the failure frequency is estimated as "once in 10 years" for suppliers 2, 11, 14, 21, 25, and "once in 100 years" for the other suppliers. Based on these estimation, we derive the probability of each supplier does not fail in next 10 years, using Poisson distribution.

The result of risk assessment is summarized in Table 3, and the result of risk importance is summarized in Figure 8. Since supplier #2 has the highest value of risk importance, supplier #2 is the improvement target. This is because the supplier #2, as well as #3, #4 is a source supplier, and is included in every supply chain. This is what is called the "diamond" structure, and known to be typical structure of automobile supply chain where one or a few key suppliers has link to much of other downward suppliers in a chain, and has huge impact on the overall strength of overall supply chain. Especially, supplier #2 has lower value of reliability compared to supplier #3, #4. This is considered to be one of the biggest reasons why the supplier #2 is selected as an improvement target.

Table 3. Result of risk assessment

Supply chain, i	Failure rate, P_i(%)	Loss, L_i ($, million)	Risk ($\sum_{i=1}^{6} P_i L_i$)
A	27	5	1.4
B	27	3	0.8
C	14	4	0.5
D	27	2	0.5
E	35	1	0.3
F	33	4	1.3

4. CHOOSING MITIGATION STRATEGIES

In this section, we discuss how to choose mitigation strategies for particular situations.

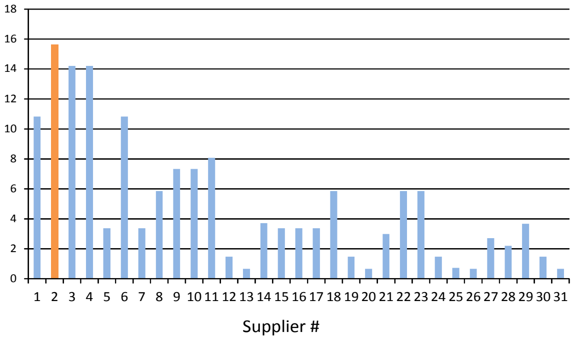

Figure 8. Result of risk importance.

4.1 Stabilization, Absorption, and Duplication

Once a particular supply chain risk is assessed, and selected for mitigation, it can be mitigated by decreasing breakdown probability, recovery failure probability or both. To do this, we propose three mitigation strategies: Stabilization, Absorption, and Duplication. Each gives different changes in network, works best in particular situations, and affects the supply chain risks in different ways.

Stabilization is an effort of increasing resistance of each supplier, which results in reduction of the breakdown probability for an existing player, i.e., $p_i \rightarrow p_i - \Delta p_i$. In the case of earthquake, enhancing quake-resistance is an example.

Absorption is an effort of softening negative effect of each supplier, which results in reduction of the recovery failure probability, i.e., $q_i \rightarrow q_i - \Delta q_i$ by building buffers. The most common example is adding inventories.

Duplication is an effort of preparing alternative options for each supplier, which results in reduction of reduce the breakdown probability by building redundancy, i.e., $p_i q_i \rightarrow (p_i q_i)^2$. An obvious example is duplicating suppliers. Another example is building self-manufacturing options.

Although this categorization may not be universal, it gives us great advantages when developing mitigation strategies in association with network reliability.

4.2 Discovering Trade-Off between Cost and Risk Covered

With risk-mitigation approaches to consider, managers must consider the tradeoff between the cost of mitigation and the risk coverage to construct a supply chain risk management strategy.

To get a clear understanding of relations between the cost and the risk, we consider again the case described in the Section 3.6. The improvement point is supplier #2. We compare three mitigation strategies: "quake-resistance reinforcement" as *stabilization*, "adding inventory" as *absorption*, and "dual-sourcing" as *duplication*.

For quake-resistance reinforcement, we assume investment cost $C = 1$ ($, million). The reliability improvement for the strategy is estimated as $r_2 = 0.9 \to 0.99$, which result in the risk coverage improvement as $\sum_{k=1}^{6} P_k L_k = 4.3 \to 3.4$ ($, million). Therefore, total cost become $C + \sum_{k=1}^{6} P_k L_k = 1 + 3.4 = 4.4$ ($, million).

For inventories addition, we assume unit inventory cost as $0.05 million. Recovery time t is estimated by beta distribution with $\alpha = 2, \beta = 5$ and target recovery time is given as $T = 10$. With x days amount of inventories, the deadline of recovery can be extended to $T + x$, therefore, we can calculate the new reliability of supplier 2 as: $r_2 = Prob[t < T + x\}$. With this new reliability under different inventory level, we can calculate the corresponding risk of overall supply chain, as well as cost for holding it, described as in Figure 9. The cost and risk trade-off is shown as follows. As the inventory added increases, the risk covered is reduced, but the investment cost increases, and thus, we can get the trade-off curve for total cost. Since this curve is a single-peak function, we can get the optimal point very easily. In this example, holding 10 days inventory yields the minimum total cost. Total cost become $C + \sum_{k=1}^{6} P_k L_k = 0.5 + 3.6 = 4.1$ ($, million).

Similarly, we assume unit duplication cost as $0.1 million, and using $p_i q_i \to (p_i q_i)^2$, we can obtain the cost-risk trade-off as Figure 10. Total cost become $C + \sum_{k=1}^{6} P_k L_k = 0.6 + 3.4 = 4.0$ ($, million).

Comparing the optimal value of total cost that is obtained by inventory addition, we can see that the dual-sourcing strategy is better. By doing so, we can choose the best mitigation strategies in a different settings very easily.

Finally, we conduct sensitivity analysis to compare these strategies in a different cost structures as Figure 11. We can see that dual-sourcing strategy is better if unit inventory cost is high and unit duplication cost is low (vice versa). We should do nothing if both costs are high. As such, depending on the cost structure, the best strategies can be different, and by using such sensitivity analysis, managers can choose the best strategy easily.

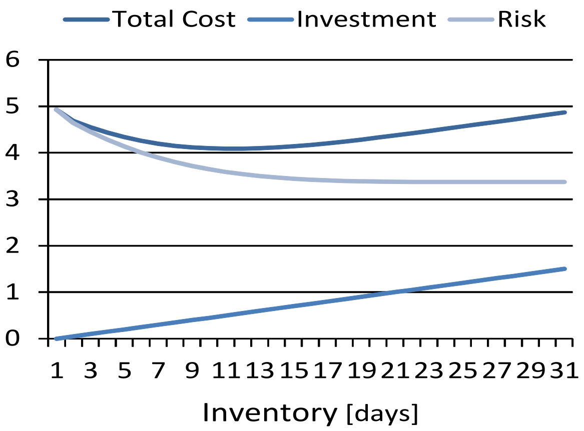

Figure 9. Cost-risk trade-off for inventory addition.

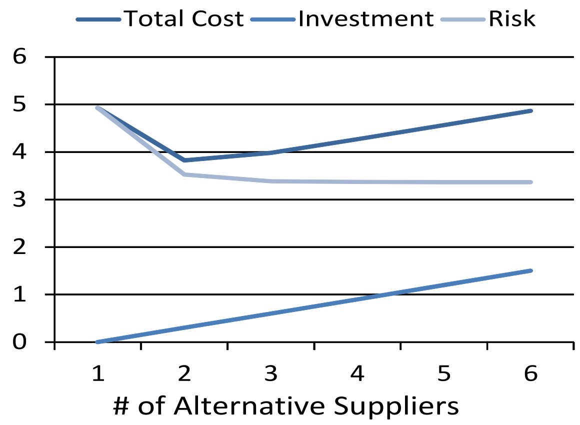

Figure 10. Cost-risk trade-off for dual-sourcing.

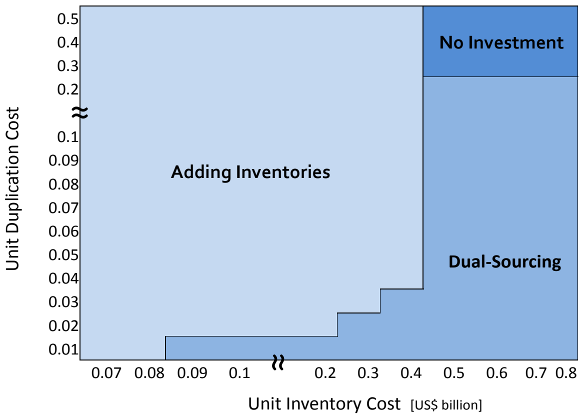

Figure 11. Result of sensitivity analysis.

5. CONCLUSION

This paper discussed how to manage supply chain disruption risks from natural disasters or other low-likelihood-high-impact risk drivers. We proposed the risk assessment and mitigation method for the supply chain disruption, using the network reliability theory. We have considered several features arising in the context of supply chain risk management. First, we have defined the loss (and risk) of supply chain disruption as to whether they can be recovered by the specified target time, not just whether they are simply broken down. Second, we have applied probability importance to detect the weakest link in the supply chain. By doing so, managers can invest mitigation strategies on a proper point. We analyzed the situation under which each of these strategies is the best suitable. With a clear understanding of relations between these mitigation strategies and the entire supply chain risks, mangers can select effective risk-reduction approaches to their supply chain.

While the application of network reliability in areas such as computer networks and transportation networks have been studied for about a few decades and successfully implemented, applications in supply chain network are not sufficiently well. We think that network reliability is an important enough tool that everyone who considers SCRM should know at least a little bit about it. In our opinion, network reliability is a natural next topic for managing risks to avoid supply chain disruption.

As a final comment, we should mention the potential future works. It is interesting to develop a stochastic programming model using our risk assessment model as a part of objective function or constraints. It is also interesting to calculate the mean time to repair of the supply chain to explicitly consider the degree of loss. There are also several indices used in the transport network security or computer network security: availability, capacity reliability, travel-time reliability. Although these indices are not straightforward, they have potential be-nefit in getting better understanding in several aspects of tradeoffs between costs and risks.

REFERENCES

Birolini, A. (2007), *Reliability Engineering: Theory and Practice*, Springer, Heidelberg, Germany.

Bundschuh, M. Klabjan, D., and Thurston, D. L. (2003), *Modeling robust and reliable supply chains, Working paper*, Department of Mechanical and Industrial Engineering, University of Illinois at Urbana-Champaign, Urbana, IL.

Garg, M. and Smith, J. C. (2008), Models and algorithms for the design of survivable multicommodity flow networks with general failure scenarios, *Omega*, **36**(6), 1057-1071.

Humair, S. and Willems S. P. (2006), Optimizing strategic safety stock placement in supply chains with clusters of commonality, *Operations Research*, **54** (4), 725-742

Iida, Y., Yoshiki, T., and Wakabayashi, T. (1988), An approximate evaluation of road network reliability with partial minimal path sets and cut sets, *Journal of Japan Society of Traffic Engineers*, **23**(4), 3-13.

Santoso, T. Ahmed, S. Goetschalckx, M., and Shapiro, A. (2005), A stochastic programming approach for supply chain network design under uncertainty, *European Journal of Operational Research*, **167**(1), 96-115.

Simchi-Levi, D. (2010), *Operations Rule*, MIT Press, Cambridge, MA.

Sodhi, S. and Tang, S. (2012), *Managing Supply Chain Risk*, Springer, New York, NY.