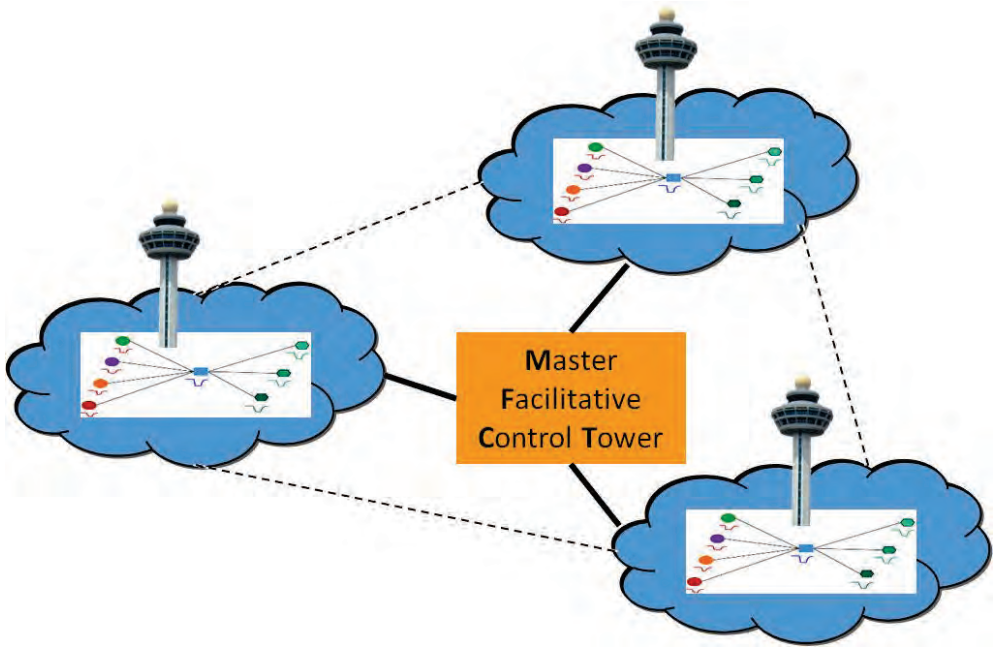
TLI – Asia Pacific White Papers Series

Master Facilitative Control Tower for Risk Management of Complex Supply Chains – An Overview

Volume 13-Nov-RISK



Institute of High Performance Computing
A*STAR

Singapore Institute of Manufacturing Technology
A*STAR

TLI THE LOGISTICS INSTITUTE ASIA PACIFIC

CONTENTS

Master Facilitative Control Tower for Risk Management of Complex Supply Chains – An Overview

1. INTRODUCTION

Risk management of complex supply chain networks has risen to the top of the corporate agenda, particularly, given an ever-increasing number of disasters and disruptions to business in the past decade. In this paper, we seek to capture and reflect the dynamic and complex nature of multiple supply chain networks (SCNs) through data collection, data analysis, network model building, simulation, and scenario appreciation to eventually enable the prediction and control of SCN behaviors in advance through the activity of a master facilitative control tower which facilitates a group of enterprise driven control towers serving various stakeholders in the SCN.

Supply chain risk can generally be categorized into four types according to their frequency of occurrence and consequence: low probability & low impact (LPLI), low probability & high impact (LPHI), high probability & low impact (HPLI), and high probability & high impact (HPHI). Among them, a LPHI risk is called disruption, which is the main focus in the current study.

As supply chain disruptions are unplanned and unanticipated events that severely disrupt the normal flow of goods and materials (Kleindorfer and Saad, 2005), the whole supply chain/network may not fully bolstered for the disruption. The disruption will directly lead to one or more stakeholders' capacity losses in terms of material acquisition, production, shipping, communication (IT system), demand, etc. Worse still, such disruptions may propagate through tightly connected networks.

Generally, for a focal company, the recovery from disruptions depends on the company's ability to find the back-up capacity in the supply chain before its remaining capacity is utilized. This back-up capacity either has been built up before hand as the focal company's effort to build resilience into its supply chain or just exists across supply chains as the excess capacity in other entities.

For the former case, the company needs to justify or optimize the investment on the back-up capacity through thorough understanding of its potential exposure to risks and their impacts; for the latter case, the company should have the ability to sense a disruption at the earliest possible time and react to locate the sources of back-up capacity in the SCN.

In summary, in order to manage supply chain risks, a company should be able to systematically identify potential risks/disruptions embedded in its supply chain, assess their impacts, build in mid- or long-term preparedness or mitigation strategies, monitor risks, and design quick antidotes to the occurrence of such disruptions (Figure 1).

Figure 1. Five phases in the supply chain risk management of a company

2. RISK IDENTIFICATION

In order to enable companies to systematically identify potential risks in their supply chains, a risk framework has been built to guide the risk identification process. Besides well-known risks stated in the existing literature, new types of supply chain risks have been identified when considering risk propagation, resource shortage, industrial clusters, and the relationship between stakeholders. The framework also reflects the facts that the impact of risks and their mitigations could involve interactions among entities located in the same supply chain, in the same industry, or the macro level (Figure 2).

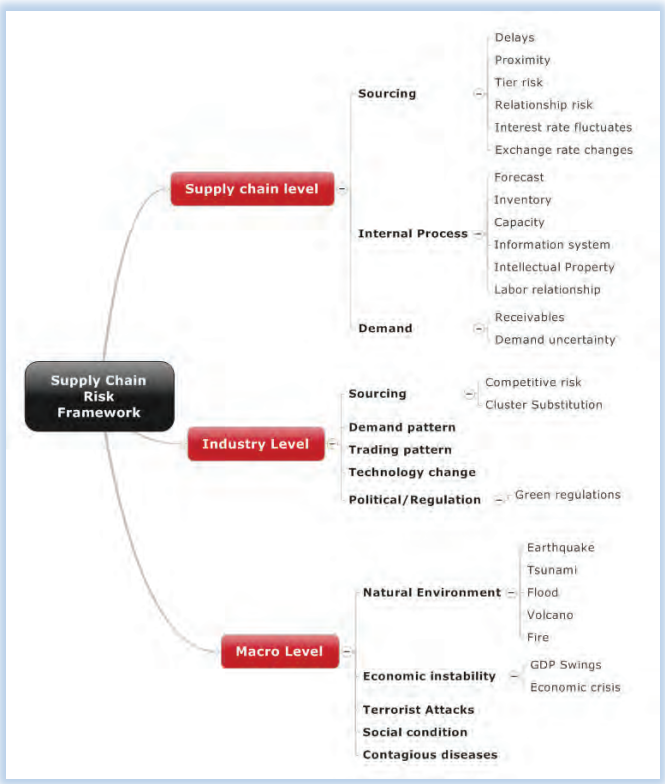


Figure 2. The supply chain risk framework

Furthermore, a network analysis approach is adopted to identify critical nodes through analyzing the structural attributes of a supply network. From a supply network perspective, the relative position of individual firms with respect to one another influences both strategy and behavior. In this context, it becomes imperative to study each firm's role and importance as derived from its embedded position in the broader relationship structure (Borgatti and Li, 2009). Furthermore, the structure of a supply network plays a vital role in both the evolution of the network and its response to disruption. The network structure's influence in determining the severity of a disruption, and the time taken by the network to recover are key components to be addressed in risk management surrounding disruptive events. Finally, network analysis also provides better understanding about the disruption propagation/cascading effects and the effects of the interactions among the supply chain entities both before and upon the occurrence of a disruption.

Figure 3. The phase of risk identification

3. RISK ASSESSMENT

Risk assessment involves assessing the risk exposure of a company/supply chain and the actual impacts of certain disruption to a company/a supply chain.

3.1 Assessment of risk exposure

It is important for a company to understand its risk exposure caused by itself and its partners before any risk actually occurs. The self-risk can be assessed considering only the company's internal influence factors like inventory level, production utilization, employee skill, etc. The risks caused by supply chain partners can be defined as connectedness risk, which may have depth and breadth between any two of linked partners. We developed the methodology to quantify the connectedness risk. Overall, the risk exposure of a company can be obtained by summing up the self-risk index and all of connectedness risk indices. With this information, the company can determine both its own influence factors and the partners which have most impact on its risk exposure. Then the company can make adjustment to improve itself. For the risky partners, the company can work on replacing them with safer ones.

Influence factors

An entity has various factors which determine its performance. The disruption is realized through the changes in those factors and we refer them as influence factors, which can be generally classified and categorized into four groups, namely, Product, Demand, Supply, and Cluster. As shown in Figure 4, the influence factors have a hierarchical structure. When a risk event occurs, some influence factors, which may belong to different categories (e.g., Product and Supply), are triggered simultaneously. In this sense, the direct effect of a risk can be interpreted by linking up the impact levels of influence factors against the risk.

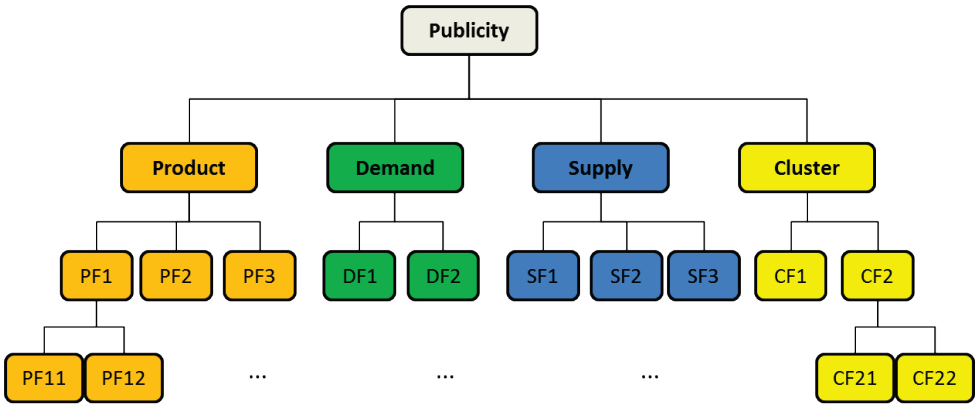


Figure 4. Variety and hierarchy of Influence factors

The values of influence factors would be estimated from historical data and determined by the decision makers though it is subjective. Suppose that Product factor PF1 has been influenced by a certain set of risk realizations, the distribution for the risk realization would represent PF1. Based on the distribution, the decision makers would determine the relative importance of PF1 compared to others.

As the influence factors represent the potential disruptions, an entity may not be exposed to the factors in the low levels. However an entity would show lower level influence factors when it builds serious relationship with partners.

Self-disruption of an entity

Quantifying the level of the influence factors is critical to estimate the direct effect on the performance of the entity. The risk may actually come from the internal process of the entity or external events. Influence factors turn out the disruption of the performance of the entity regardless of the causes of risk. Thus, we can use the influence factors to diagnose the self-disruption of the entity. The self-disruption is estimated by quantifying the impact level of the influence factors against the potential risk.

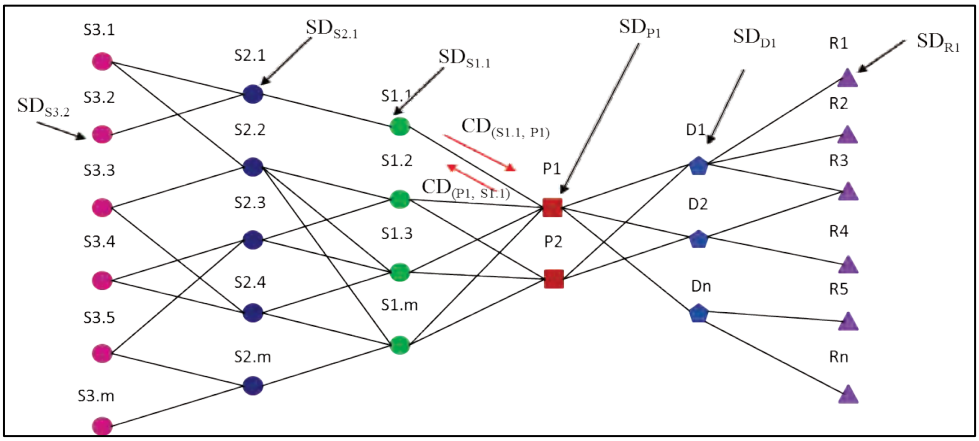


Figure 5. Supply chain risk network

Figure 5 shows the supply chain risk network that contains 3-tier suppliers, manufacturers, distributors, and retailers. The framework visualizes the potential disruption of each entity involving the supply chain network and the disruption relationship between entities. The self-disruption, depicted as SDP1, for example, can be represented as the value of the entity P1 (manufacturer) in the framework. However, SDP1 would be estimated by investigating its own influence factors without considering the partner entities. Thus, it is recommended to estimate the index representing the relationship with each partner entity so that the index would explain disruption caused by interacting with partners.

Connectedness disruption (CD) between linked entities

On the supply chain risk network (in Figure 5), there are two unidirectional arcs linking two entities P1 and S1.1, for example: one is from entity S1.1 to P1; and the other is from Entity P1 to S1.1. Thus, each arc represents the CD with directionality from an entity to the other. For P1 and S1.1, the connectedness risks are denoted as CD (S1.1, P1) and CD (P1, S1.1), respectively. The CD is a view of the potential risk on the influence factors of an entity by considering the exposure level of risk on the influence factors of the partner entity. Thus, the CD would have different values for different partner entities as those may have different values of influence factors or different exposure levels of risk. In order to estimate the CD, it is required to estimate the effect of the influence factors for Entity S1.1 on those for Entity P1 or vice versa.
(Suh, 2001) invented a functional design methodology by sequentially mapping the requirement of one domain to another. The author determined the design requirement from the relationship between two domains though the measurement is possibly subjective. We borrow the idea to estimate the CD of an entity by referring to the influence factors of the other entity. Figure 3 explains how we refer to the influence factors from one side to the other. It is assumed that the two entities share the same level of knowledge when they build a relationship to enhance the interaction/trades and to help anticipating potential disruptions.

According to (Myers and Cheung, 2008), knowledge sharing is recommended even though the knowledge sharing may be controversial. Note that knowledge sharing is a joint activity between supply chain partners; the parties share knowledge and then jointly interpret and integrate it into a relationship-domain-specific memory that influences relationship-specific behaviour.

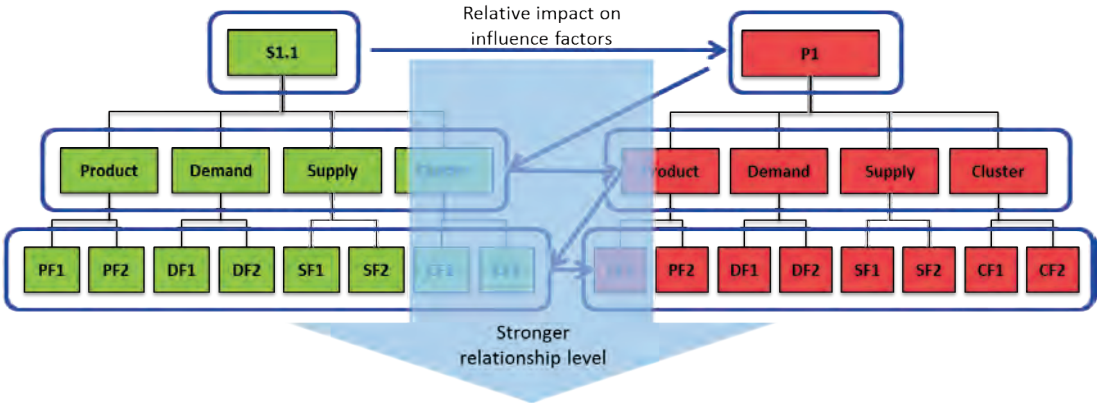


Figure 6. Mapping influence factors of a supplier (S1.1) for a manufacturer (P1)

Figure 6 gives us an example to estimate the connectedness risk from the influence factors of the two entities, S1.1 and P1. When the two entities build a serious relationship, they share the knowledge regarding the influence factors with the decision makers so as to anticipate the potential disruption for the partners. From the perspective of S1.1, in Figure 3, it only obtains CD from the public knowledge provided by P1 if they do not share the knowledge regarding influence factors. However, their relationship gets stronger, they share more knowledge for their influence factors and the decision makers in S1.1 possibly map their influence factors to those provided by P1. By integrating the impacts on the influence factors against to those of a partner entity, the connectedness risk would be determined. The estimated connectedness risk is depicted on arcs in the supply chain risk framework in Figure 5.

Calculation of risk exposure

A new definition of risk for an entity can be defined by estimating potential disruption levels from both internal and external disruptions based on influence factors. The new risk index would be beneficial to evaluate the current risk level, increase the resilience, or re-calibrate the supply chain network. It means that we can define the risk exposure index as

$$\text{RP1 (Risk)} = \text{SDP1 (self-risk)} + \sum_{i \in C} CD_{(i,P1)}$$

Note that C is the set of arcs connected to the focal entity, SD is the self-disruption, and CD is the connectedness disruption directing to the focal entity. The risk index consists of the self- disruption and the connectedness disruption from direct partner entities. The proposed risk exposure index has advantages to coordinate/design the supply chain network in the view of mitigating potential disruptions.

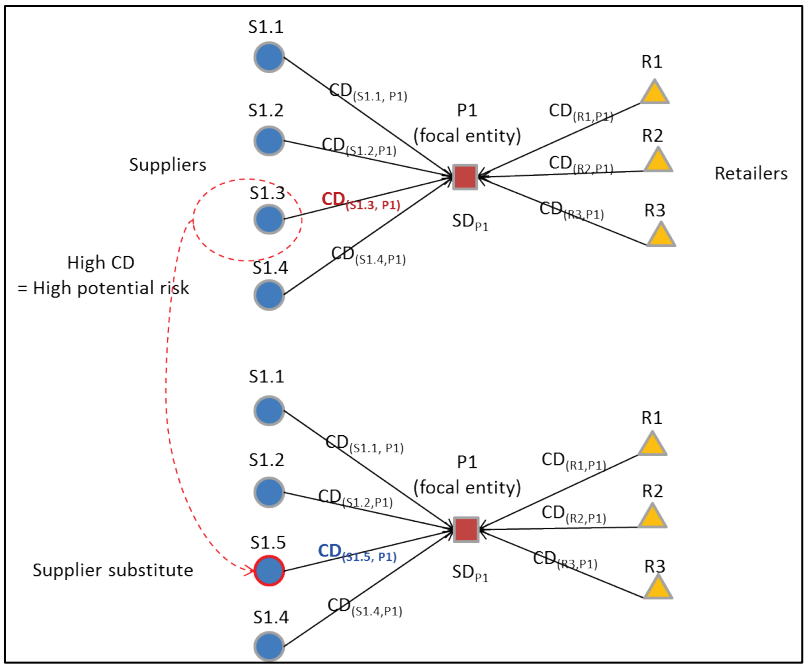


Figure 7. Supply chain coordination using the risk exposure index

When the focal entity P1 judges that a supplier has great expected risk exceeding a certain threshold to cause disruptions, for example, the entity may able to substitute the supplier S1.3 as drawn in Figure 7. Through this activity, the supply chain is redesigned and the supply chain risk framework would be updated by referring to CD provided by the new supplier S1.5. The proposed risk framework provides a systematic way to help each entity visualizing the potential disruption by estimating its own disruption level as well as the connectedness disruption caused from its partner entities. The risk framework would not only be helpful to evaluate the risk level but also applicable to better design the supply chain network.

3.2 Assessment of risk impact

For assessing the actual impacts of certain disruption to a company or a supply chain, we propose VaR (Value at Risk) and simulation. VaR is defined as a threshold value describing the amount of loss that will not be exceeded within a certain period of time and under a certain probability (Jorion, 2007). Simulation enables companies to analyze and evaluate their systems' performance in the occurrence of risks. A simulation model has to be built for the company based on its operational data. The former approach can be referred to (Zhang *et al.*, 2012) and the simulation approach is described as follows.

Disruption Profile

Although (Sheffi and Rice, 2005) identify eight typical stages of disruption which include preparation, the disruption event, first response, initial impact, full impact, preparation for recovery, recovery, and long-term impact, we group those stages into two categories: decay and recovery.

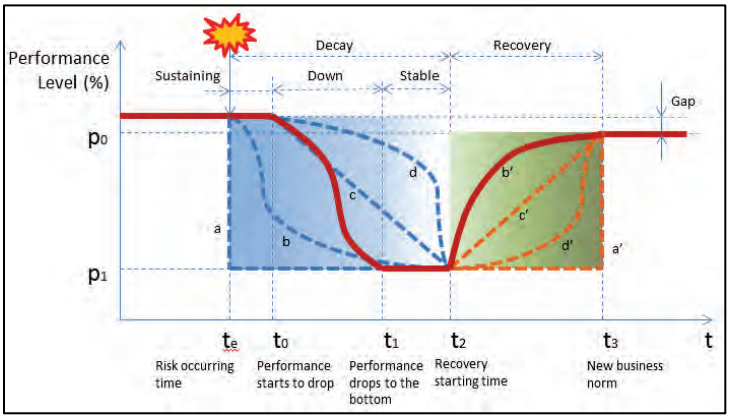


Figure 8. A generic disruption and recovery curve

Figure 8 refers to a generic disruption profile which tracks the performance or the yield level of a company from time t_e to t_3. After a risk occurs at time t_e, the yield of a company may be sustained for a while till time t_0; then it starts to drop to the bottom at time t_1. The yield level may stay at this bottom (p_1) for some time and then the recovery starts at time t_2. A new business norm are reached at time t_3 and the new yield level (p_2) of the company after the risk may be lower than the one before the risk (p_0).

In both stages of decay and recovery, there can be typically four types of decay/recovery patterns: abrupt, slow, normal, and fast. For example, decay patterns a, b, c, and d represent abrupt, slow, normal, and fast decay in yield/performance, respectively; similarly, recovery patterns a', b', c', and d' represent abrupt, slow, normal, and fast recovery, respectively (Figure 8).

Therefore, two types of disruption profiles can be generated for companies with good robustness and resiliency and for those do not have such characteristics. The robustness means that a company shows an acceptable performance in its Key Performance Indicators (KPIs) during and after an unexpected event. The resiliency refers to the company's ability to recover to the previous performance after disruptions.

Figure 9 shows the disruption profile of a robust and resilient company. The company's yield sustains for some time then starts to drop slowly to the bottom till time t_2; it immediately recovers at time t_2 along a fast cure and then reaches a new norm at time t_3. On the contrary, in Figure 10, a company's yield abruptly drops to the bottom right after the occurrence of a risk. It stays at the bottom until time t_3 for an abrupt recovery to a new norm. This company is fragile in facing a disaster and rigid in recovering back to a new norm.

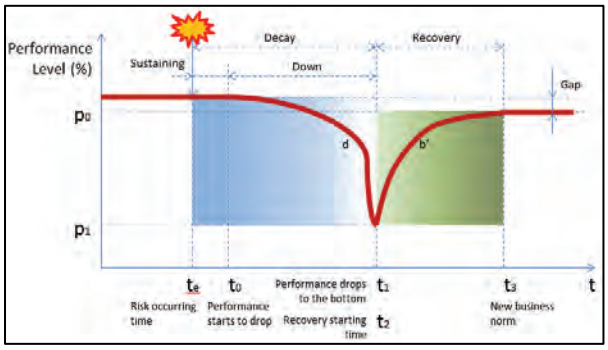


Figure 9 Disruption profile of robustness and resiliency

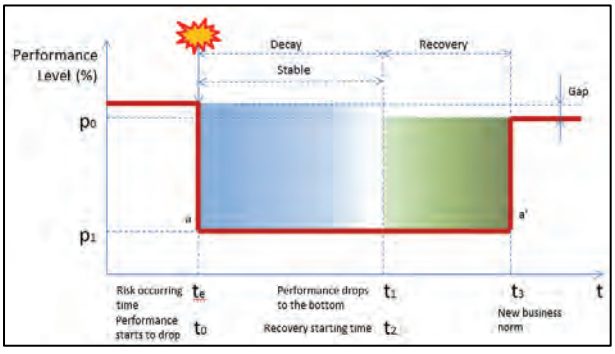


Figure 10. Disruption profile of no robustness and resiliency

Risk Propagation

We assume a tier one supplier S1.2 (in Figure 5) is hit by a disaster. We can observe that all nodes in the whole network are affected whenever one of them is under disruption through propagation. However, the disruption effect may be alleviated or reinforced along the way due to robustness and resiliency factors of nodes in the network.

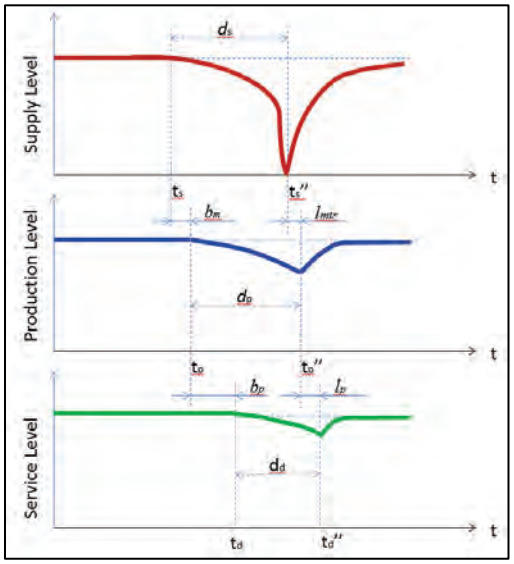


Figure 11. Disruption effect alleviated

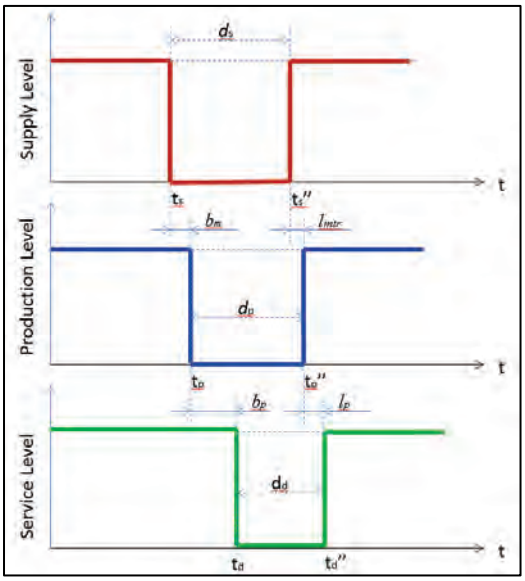


Figure 12. Disruption effect reinforced

For example, assuming nodes $S_{1.2}$, P_1, and D_2 represent robust and resilient companies with disruption profiles similar to the one in Figure 8. Figure 11 shows a disruption occurred in supplier $S_{1.2}$ is actually

alleviated when it is passed down from nodes $S_{1.2}$, P_1, to D_2. In contrary, if all those nodes are fragile and rigid, Figure 12 shows that the disruption in nodes $S_{1.2}$ is can be reinforced through nodes P_1 and D_2.

Risk Evaluation

For the disaster prone company

The impact of the disaster to the vulnerable company very much depends on the robustness and resiliency of the company. The disruption profile can range from Figurer 9 to Figure 10. We can then simulate to quantify the disruption impact.

Simulation enables companies to analyse and evaluate their systems' performance in the occurrence of risks. A simulation model has to be built for the company based on its operational data. Generally, the following data are required.

- The emerging pattern of the disruption profile/distribution
- The time of disruption
- The duration of the disruption
- Operational data e.g. inventory level, product unit cost, demand, etc.

For other vulnerable companies

For those companies that are affected through risk propagation, e.g. focal company P_1, and distributor D_2, their disruption profiles can be illustrated in Figure 13 in a time series. We assume that the focal company does not keep sufficient product inventory.

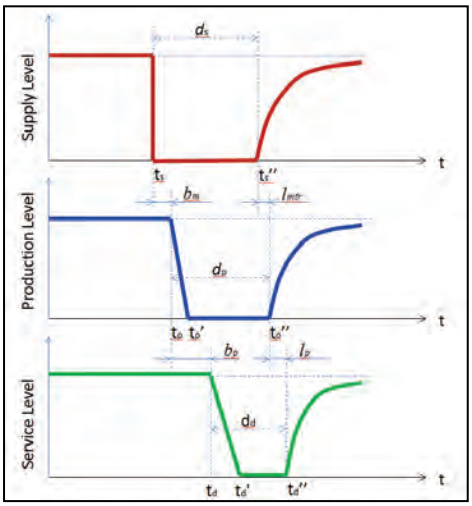


Figure 13. Risk propagation from supplier, manufacturer to distributor

The generic scenario is given assuming that supplier $S_{1.2}$ is hit by a disaster at time t_s and its yield drops to the bottom immediately. Manufacturer P_1 sustains its production for some time (b_m) buffered by its

material and pipeline inventories till time t_p before its production level drops to the bottom. Similarly, the distributor D_2 sustains its service level for some time (b_p) buffered by its product inventory till time t_d. The service level starts to drop at time t_d and then reaches to the bottom at time t_d'.

For manufacture P_1, the time of the disruption (t_p) and duration (d_p) can be calculated as follows.

$$t_p = t_s + b_m \quad (1)$$

$$d_d = d_s - b_m + l_{mtr} \quad (2)$$

Similarly, for distributor D_2, the time of the disruption (t_d) and duration (d_d) are:

$$t_d = t_s + b_m + b_p \quad (3)$$

$$d_d = d_s - b_m - b_p + l_{mtr} + l_p \quad (4)$$

Where l_{mtr} and l_p refer to the transportation lead times from the supplier to the manufacturer and from the manufacturer to the distributor, respectively.

Thus, the disruption triggered by supplier $S_{1.2}$ to focal company P_1 and distributor D_2 can be qualified using the basic approaches in section *a*. In this way, the effect of the disruption on the rest of the nodes in the network can be obtained.

For the whole supply chain network

Based on the calculations in sections *a* and *b*, the impact triggered by the disaster on supplier $S_{1.2}$ to each node can be tabulated. The overall impact on the supply chain network can be summed up in a risk effect matrix as in Table 1.

Disruption Origin Node	Node 1	Node 2	Node 3	Node 4	…	Node n	Overall Impact
Node 1	$I_{1.1}$	$I_{1.2}$	$I_{1.3}$	$I_{1.4}$	…	$I_{1.n}$	I_1
Node 2	$I_{2.1}$	$I_{2.2}$	$I_{2.3}$	$I_{2.4}$	…	$I_{2.n}$	I_2
Node 3	$I_{3.1}$	$I_{3.2}$	$I_{3.3}$	$I_{3.4}$	…	$I_{3.n}$	I_3
Node 4	$I_{4.1}$	$I_{4.2}$	$I_{4.3}$	$I_{4.4}$	…	$I_{4.n}$	I_4
…	…	…	…	…	…	…	…
Node n	$I_{n.1}$	$I_{n.2}$	$I_{n.3}$	$I_{n.4}$	…	$I_{n.n}$	I_n

Table 1. Risk effect matrix

From table 1, we can identify the critical node which has the greatest impact to each other and to the overall supply chain network. For example, $I_{1.3}$ is the qualified value of the effect of node 1 to node 3. From the column of Node 3, through the list of values, e.g. $I_{1.3}$, $I_{2.3}$, … to $I_{n.3}$, if $I_{4.3}$ is the greatest value in the column, then node 4 among all the node in the network has the biggest effect on node 3. This means node

4 can cause biggest disruption to node 3. Similarly, we may identify which node could cause the biggest disruption to the overall supply chain network.

Thus, the assessment for both risk exposure and risk impact can be quantified. In summary, the risk exposure is calculated based on influence factors, which determine the potential risk level of a node. A manager can use the risk exposure index to identify the most risky partners and may replace them before any risk actually occurs. The calculation of risk impact is based on the disruption profile, which considers how a risk event develops in a certain time period. The purpose of this index is to measure the loss of a risk may bring to a node during its decay and recovery stages.

Figure 14. The phase of risk identification

4. MID/LONG TERM MITIGATION

After investigating and assessing the possible risks, mitigation would usually dictate that managers take a proactive role in coordinated activities to manage and control supply chain risks. De Loach (2000) defines four categories of action plans: avoiding, reducing, retaining and transferring. Avoiding refers to not performing an activity that could bring risk; reducing involves lowering the impact and probability of a loss from occurring; retaining involves accepting any burden from loss or benefit of gain from a risk; transferring refers to sharing any burden from loss or benefit of gain for a risk with another party when an event occurs.

We focus on the first two approaches to design mitigation strategies for LPHI disruptions as the loss from an LPHI risk should not be ignored or transferred to other supply chain partners. Furthermore, mitigation strategies should be designed and applied both before and after disruption events. The mitigation strategies designed for pre-event actually aim to improve robustness and resiliency of a supply chain and they are referred to as mid- or long-term mitigation strategies in this study.

A mitigation strategy framework is built according to the generic disruption and recovery pattern, essentially, there are four mitigation directions: reduce disruption severity, reduce disruption duration, improve the recovered performance level, and postpone the disruption effecting time (figures 15 to 18).

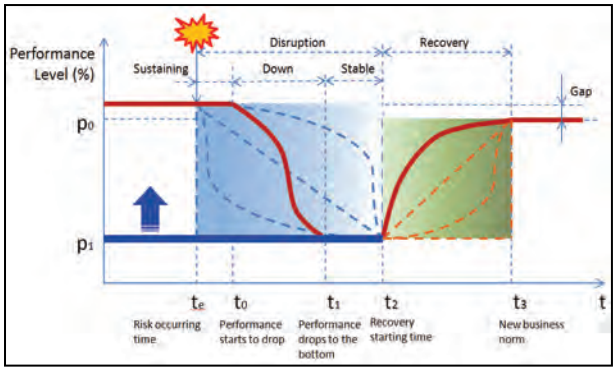


Figure 15. Reduce disruption severity

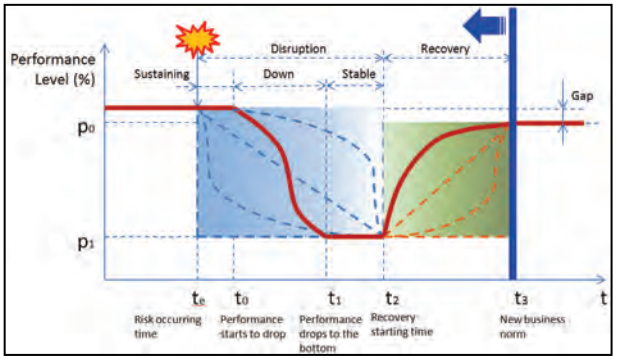


Figure 16. Reduce disruption duration

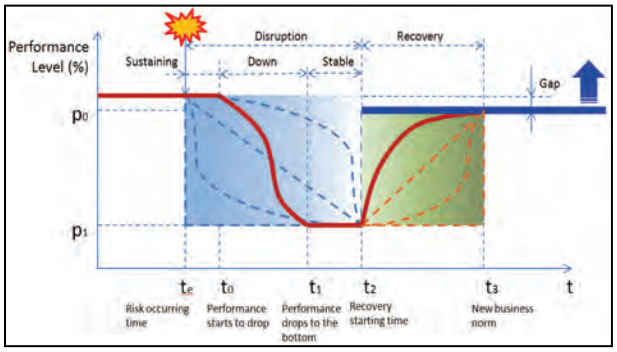


Figure 17. Improve recovered performance level

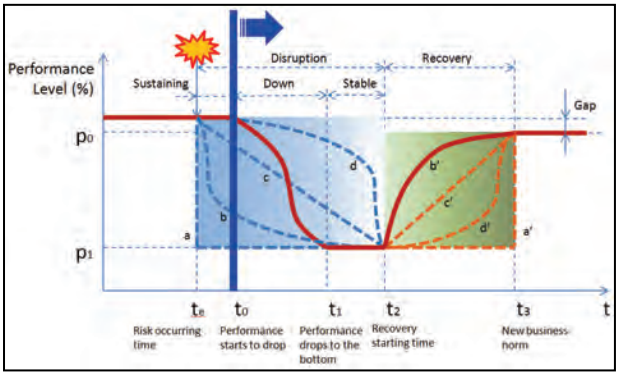


Figure 18. Postpone the disruption effecting time

The mitigation direction in Figure 15 is to reduce the performance drop level. The detailed mitigation methods could be multiple sourcing, backup production capacity, and others. The mitigation direction in Figure 16 is to shorten the disruption effect time. The mitigation strategies may involve seeking quick fixes through early detection of risks and prompt identification of alternative capacities. In Figure 17, the mitigation direction is to minimize the gap between the performance before the disruption and the one after the recovery. In Figure 18, the mitigation direction is to delay the decay phase as late as possible through increased inventory and quick risk fixes.

We study supply chain mitigation strategies by complex systems approaches, including agent-based approach, network theory, evolutionary algorithms, etc. Supply chain networks as adaptive complex systems are modeled using agent-based simulation based on case studies to test and verify the mitigation strategies for supply chain scenarios. The mitigation strategies to be considered include but not limited to:

- Optimized network topology: improve the network structure to make it more robust
- Redundant resources: to maintain redundant capacity and inventory in some critical points of the SC network.
- Resource pooling and aggregation: to do resource pooling and consolidation, so provide more alternatives as supply chain partners but at the same time can control the total supply chain cost.
- Transshipment: to allow transshipment of materials between the nodes in the same level of the supply chain. This will reduce material shortage risk in the network and control total backorder cost.
- Postponement and inventory positioning: to delay the finalizing of the product as later as possible to avoid risks of product outdating.
- Addition logistics routes and business channel: to setup alternative logistics routes and supply chain channel for improve robustness of the supply chain in case damage of some routes in the supply chain network.

In the approach, key performance index and fitness function for robustness will be defined to measure the operations performance and robustness of the supply chain. As shown in Figure 19, a SC is modeled as a complex adaptive system (CAS) with every company and the whole supply chain has a life (based on case data of a MNC).

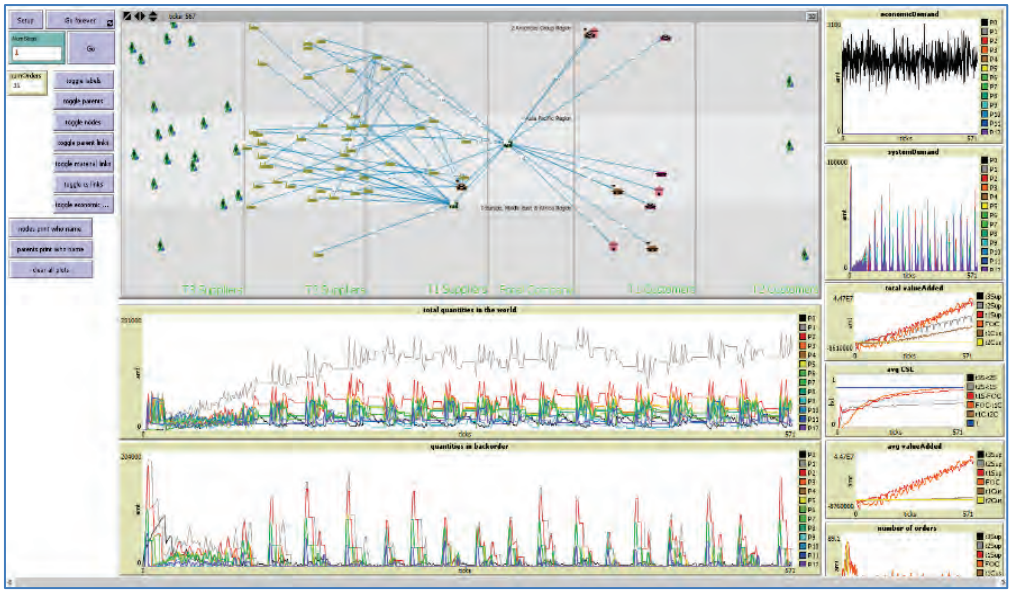


Figure 19. Mitigation evaluations by the agent-based simulation

Key indexes such as Value-added, CSL, Number of Living Players (companies) are defined to measure the performance of the organizations and the supply chain. Figure 19 includes three main parts. The first part is the control console of the simulation model; the second part is the simulation model and every link and nodes can be opened for showing detail features. The third part is the performance indexes, include Value-added, CSLs and the Number of Living Players in the Chain, Total Inventory and Backlog Costs etc. The purpose of the model is to study the effect of disruptions and also the mitigation polices.

Figure 20. The phase of risk mitigation

5. RISK MOINTORING

After identifying key risks, carefully choosing the right supply chain stakeholders, implementing mitigation strategies to improve robustness and resiliency, a company still needs to monitor its everyday operational processes for timely risk detection and early quick fixes. Thus, there is an immediate need of end-to-end visualization of its supply chain, especially, when the supply chain is complex. We have built a supply chain visualizer aimed at integrating different supply chain risk management components together on top of the

visualization of supply chain networks. Some key areas are identified to be closely monitored: critical supply, inbound and outbound logistics, inventory level, order fulfilment and manufacturing operations, natural disasters, etc.

Furthermore, the visualizer can be used to display what-if analysis. At the backend, simulations can be triggered to derive the near-term or long-term mitigation plans for various disruptions. The assessment of risks through simulations incorporating risk metrics and updated information from supply chain network monitoring process can continuously provide the evaluation of possible impacts of different key entities in the network. The results can be presented to managers for review of their strategy and facilitating dynamic supply chain risk management. In addition, risk mitigation strategies can also be simulated under network view and assessed for their robustness under different scenarios. The proposed visualization framework offers the following advantages, as illustrated in Figure 21:

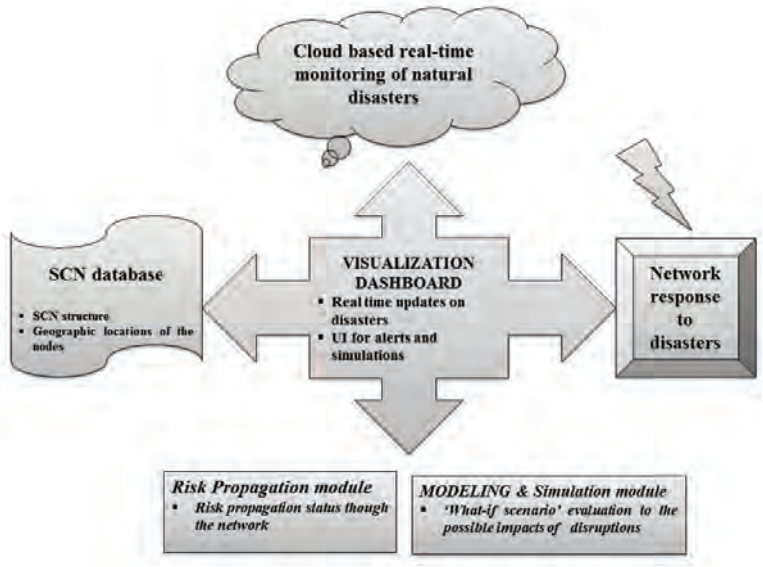


Figure 21 Salient features of the visualization framework

Figure 22 is a snap shot of the visualizer (named as RiskVis) which keeps track of natural disasters, e.g. earth quake. More LPHI events should be tracked and display using our RiskVis.

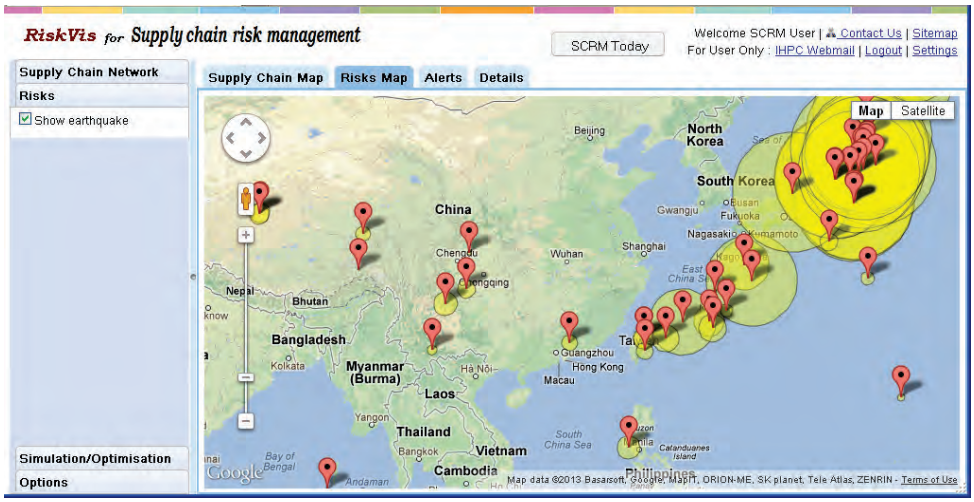


Figure 22. Display real-time nature disaster, such as earthquake

Figure 23. The phase of risk mitigation

6. RISK QUICK FIXES

Risk quick fixes refer to the immediate risk relief upon the occurrence of disruptions. The mitigation strategies used here aim to reduce the loss from the particular risk based on current status of the company and its embedded supply chain. The concept of the master facilitative control (MFC) is to design and develop risk tracking methodologies for risk identification, detection and classification. MFC is a network-based coordination organization constructed to enhance the visibility across supply chain networks and to provide insights for sustainable risk management over complex supply chains. Figure 24 illustrates the factors that influence the construction of an MFCT.

Figure 24. Factors influencing the construction of MFCT

A functional framework of MFCT is built (Figure 25) and the functions include providing insight for assisting supply chain disruption management, insight about cascading risk propagation, complete picture about connectedness in supply chains, inbound and outbound warning about risk propagation, identification of key linkages/nodes in the networks, etc.

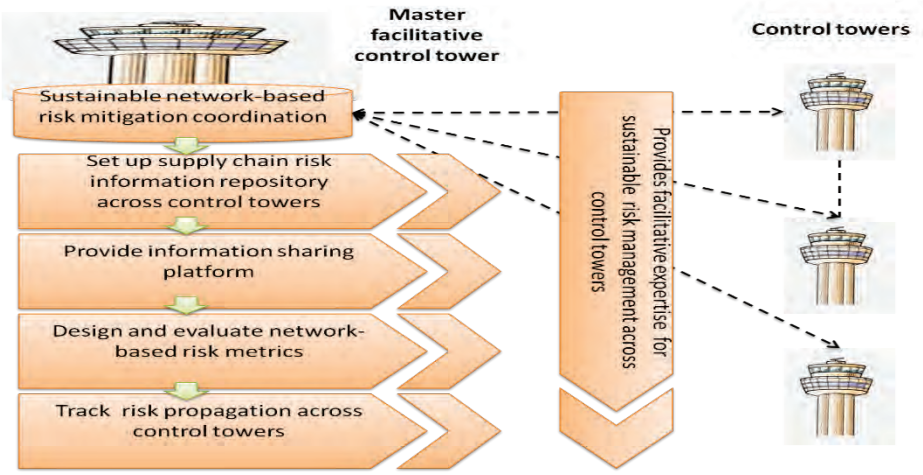


Figure 25. Functional framework of master facilitative control tower

With a MFCT to facilitate detection of risks at an early stage and by providing visibility of alternative locations of resources across SCNs, some quick fixes are studied. For example, a novel inventory refurbishment policy is proposed at the time of urgent disruption. Furthermore, a game-theory based approach is proposed for supply chain entities to choose right suppliers and order quantities when they face the competitive risk from competitors considering uncertain demand and price.

Figure 26. The phase of risk mitigation

7. CONCLUSION

The novelty of our study in each step of the supply chain risk management is summarized in Figure 27.

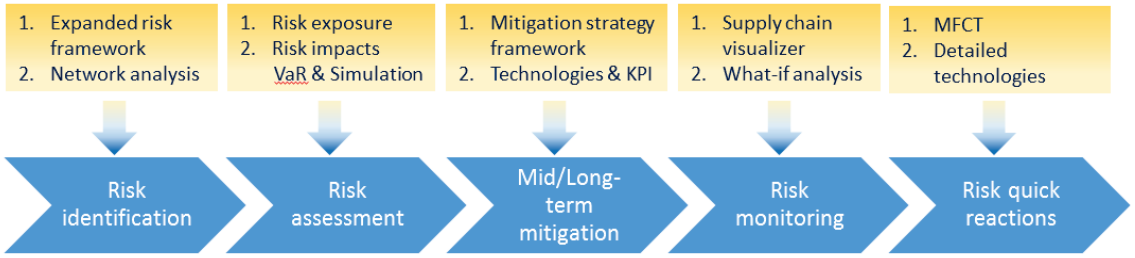


Figure 27. Novelty of study in each step of SCRM

Firstly, in the risk identification step, an expanded risk framework is built to guide the process of systematically identifying potential risks in a focal company's supply chain. The technology of network analysis is also adapted to identify key nodes and links in the supply network. Secondly, in the risk assessment step, we differentiate the assessment of risk exposure and risk impacts. In the former case, we propose a novel approach of connectedness index; in the latter case, we propose two approaches: VaR and simulation, for different data inputs.

Thirdly, in mid/long-term mitigation, a framework is built to identify key influence factors and the respective mitigation strategies; the technologies to validate appropriate strategies and key performance indicators (KPIs) are also reviewed. Fourthly, in the risk monitoring, we build a supply chain visualizer to oversee the end-to-end activities. The visualizer is also backed with several simulation engines for what-if analysis. The results of simulation can be displayed by the visualizer.

Finally, in the step of risk quick reactions, a novel MFCT is proposed to facilitate early risk detection, provide visibility of alternative resources, and coordinate partners across different supply networks in risk mitigation.

REFERENCES

Borgatti, S. P. and X. Li (2009). "On social network analysis in a supply chain context." Journal of Supply Chain Management **45**(2): 5-21.

Jorion, P. (2007). Value at Risk - The new benchmark for managing financial risk. New York, NY, McGraw-Hill.

Kleindorfer, P. R. and G. H. Saad (2005). "Managing Disruption Risks in Supply Chains." Production and Operations Management **14**(1): 53-68.

Loach, J. W. D. (2000). Enterprise-wide Risk Management: Strategies for linking risk and opportunity. London, Financial Times/Prentice Hall.

Myers, M. B. and M. S. Cheung (2008). "Sharing global supply chain knowledge." MIT Sloan Management Review **49**(4): 67-73.

Sheffi, Y. and J. B. J. Rice (2005). "A Supply Chain View of the Resilient Enterprise." MIT Sloan Management Review **47**(1): 41-48.

Suh, N. P. (2001). Axiomatic design: Advances and applications. New York, Oxford University Press.

Zhang, A. N., S. M. Wagner, M. Goh, M. Terhorst and B. Ma (2012). Quantifying Supply Chain Disruption Risk Using VaR. IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). Hong Kong. **1:** 272-277.

Institute of High Performance Computing

Fusionopolis
1 Fusionopolis Way,#16-16 Connexis , Singapore 138632
Tel: (65) 6419 1111
Fax: (65) 6463 0200
Email: gohsm@ihpc.a-star.edu.sg
URL: www.tliap.nus.edu.sg

Singapore Institute of Manufacturing Technology

71 Nanyang Drive, Singapore 638075
Tel: (65) 6793 8388
Fax: (65) 6790 6377
Email: ido@SIMTech.a-star.edu.sg
URL: http://wwwsimtech.a-star.edu.sg

The Logistics Institute – Asia Pacific

National University of Singapore
21 Heng Mui Keng Terrace, #04-01, Singapore 119613
Tel: (65) 6516 4842
Fax: (65) 6775 3391
Email: tlihead@nus.edu.sg
URL: www.tliap.nus.edu.sg