



PMG 663

Supply Chain Vulnerability and Disruptions Management

Lecture 5

Prepared by
Dr. Badur elgasim

Supply Chain Vulnerability definition

Simulation of Supply Chain Vulnerability

Disruptions in the Model

Difference between vulnerability analysis and risk analysis

During the last decade, improving efficiency and delivery times has become a key issue in many organizations. Supply chains have become a focal point for improving competitiveness in an increasingly global marketplace. While numerous trends (e.g., development of communications and other technologies, e-business outsourcing, and lean and agile logistics) have made it possible to develop complex international networks of industrial partners, they have also made organizations vulnerable to various risks arising from these networks

Many recent events have highlighted the vulnerability of long and complex service supply chains.

A risk realization affecting operations anywhere in the system can directly affect its ability to continue operations, thus endangering customer value creation where companies admitting to major supply chain difficulties lost 10% of their shareholder value on average.

These issues have become increasingly relevant as the global financial crisis emphasized the role of supply chain risk management in many companies

In international supply chains, interorganizational dependencies and relationships have become increasingly important, and while the network exposes organizations to various risks, it is difficult to be competitive in the modern world without them .

Therefore, organizations need to understand and analyze the causalities of network processes to ensure that the goals of the supply chain fit with their own organizational strategy y. It is essential for actors to collaborate and share information in their network to avoid interruptions in logistic flows

Indeed, supply chain management is undergoing continuous, considerable, and rapid changes leading to a high cost of vulnerability .

However, in the past decade, only a few studies have addressed the issue of vulnerability in the context of supply chains and even fewer studies have addressed the methodological issues faced therein

researchers have emphasized the need for integrated frameworks to support analyses for overcoming supply chain vulnerability and supply chain disturbances. Therefore, we aim to provide insights on supply chain vulnerability using analyses with a discrete-event-based simulation. Specifically, it shows how a simulation method can be used to gain a more holistic view of supply chain vulnerability. For this purpose, a conceptual framework is developed and tested to analyze supply chain vulnerability, and its feasibility is evaluated

A supply chain is defined as a system of suppliers, manufacturers, distributors, retailers, and customers in which material, financial, and information flows connect participants .a supply chain as consisting of a series of activities and organizations through which material moves on its journey from initial suppliers to final customers. Material can include everything that an organization moves and can be both tangible and intangible

To define supply chain vulnerability, it is essential to first examine the characteristics of risk. Risks have been defined in numerous ways: defined risks as a threat of disruption to normal activities that stop these activities from happening as planned.

A standard formula for the quantitative definition of supply chain risk is

$$\text{Risk} = P \times I$$

where P is the probability of a risk event, and I is the impact of the risk event.

Depending on the context, the sources of risk can be categorized in several ways. The sources of risk are generally categorized as endogenous and exogenous, depending on whether they derive from within or outside the system, which in this case is the supply network.

Risks can arise from organizations, supply chain partners, or the external environment. The sensitivity of a supply chain to these disturbances is measured by its vulnerability.

From the perspective of supply chain risk management, an organization incurs loss as a result of its supply chain's vulnerability to a risk event.

vulnerability defined as “the properties of a supply chain system; its premises, facilities and equipment, including human resources, human organization and all its software, hardware, Netware that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside system boundaries.

Previous definitions were somewhat different. For example, vulnerability described as an “exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain.” Furthermore, “supply chain vulnerability reflects the susceptibility of a supply chain to disruption and is a consequence of the risks to the chain.” supply chain vulnerability as the propensity of risk sources and risk drivers to outweigh risk-mitigating strategies, thus causing adverse supply chain consequences and jeopardizing the supply chain’s ability to effectively serve the end customer market.

Difference between vulnerability analysis and risk analysis

the difference between vulnerability analysis and risk analysis arises from the focus of the analysis. While vulnerability analysis focuses on the more holistic supply chain perspective in terms of the system's mission and supply security, risk analysis focuses more on the impacts of individual events.

from a quantitative perspective, the difference between risk and vulnerability arises from the exposure element, which reflects the extent of the impact with regard to a specific supply chain actor

The benefit of this type of

examination is that it allows the differentiation of both the general risk (e.g., for the supply chain) and an individual actor's vulnerability to a specific risk.

In doing so, the illustration of these different perspectives allows a better understanding of different actors' views on different risks and therefore allows mitigation actions to be adjusted accordingly in the entire supply chain.

Currency risk is a practical example of the benefit of adding the exposure element to risk management examination: if a company faces a currency risk in its supply chain, its risk exposure is determined by the risk management actions it conducts.

If the company acknowledges the risk but does not manage it in any way, its risk exposure can be considered to be 100%

Accordingly, we define supply chain vulnerability as follows:

$$\textbf{Vulnerability} = \textbf{P} \times \textbf{I} \times \textbf{E}$$

where E is the risk exposure. In reality, when considering supply chain vulnerability, the actors can better affect the probability of a risk event when they have control over the operations (risk arising inside the supply chain) or the exposure to risk events (risk that enters from outside the supply chain). Thus, when analyzing the proper responses to supply chain vulnerability, the origin of the risk event needs to be taken into account.

Simulation of Supply Chain Vulnerability

Simulations have been used for analyzing vulnerability-related issues in various applications during the last decade; studies have used various research approaches to this end.

- Conceptual approach refers to a purely conceptual contemplation of concepts and terms
- Hypothetical approach, to a simulation research conducted with hypothetical models (without real-world cases or data); and Empirical approach, to real-world case examples in which simulations are used in different ways

- The first case found analyzed only risks involving demand-side uncertainty.
- The second case concentrated on a portfolio of contracts for procuring strategic parts
- The third case studied the effect of transportation disruptions on the performance of different parts of the supply chain.
- The fourth case concentrated on the carpet manufacturing industry with a focus on reverse logistics

Supply chain risks can also depend on global issues. also there is developed a conceptual framework that can be used to enhance research on the impact of climate change on fresh produce supply chains. In this case, the risks are greatly different from those in most analyses where some physical disruption or demand uncertainty is evaluated.

Supply Chain Operations Reference (SCOR) used for constructing a simulation model. SCOR is a supply chain management tool used to address, improve, and communicate supply chain management decisions within a supply chain

In recent years, areas other than traditional supply chains have attracted interest in supply chain vulnerability simulations. For example evaluated the short-term security of natural gas supply with a contracts-based simulation model by representing different parts of the supply chain.

- concentrating on intermodal transport networks with a micro level perspective.
- analyzing a JIT-based cross-docking distribution center by minimizing supply uncertainty in the cross-docking activities proposed a generic tool that is based on a bill-of-materials and covers production disruptions and supply chain optimization

Overall, the above examples clearly show that simulations are mostly applied on the demand or supply side or from a single actor's perspective of the supply network; only a few studies take into account the supply chain vulnerability holistically.

Previous simulation-based analyses have typically concentrated on a specific part of a supply chain or a certain perspective of it.

Vulnerability Simulation

The supply chain consists of multiple suppliers, a manufacturing unit, distribution warehouses, and sales offices, as shown in Fig. 7.2. Two of the suppliers are located offshore. When the manufacturing unit places an order, the goods arrive in 30–41 days (Table 7.3); two of the suppliers had a delivery lead time of 7–14 days; and the last supplier had a lead time of 2–4 days.

We assume that the lead time is uniformly distributed and that it should reflect real operations as deliveries tend to be optimized.

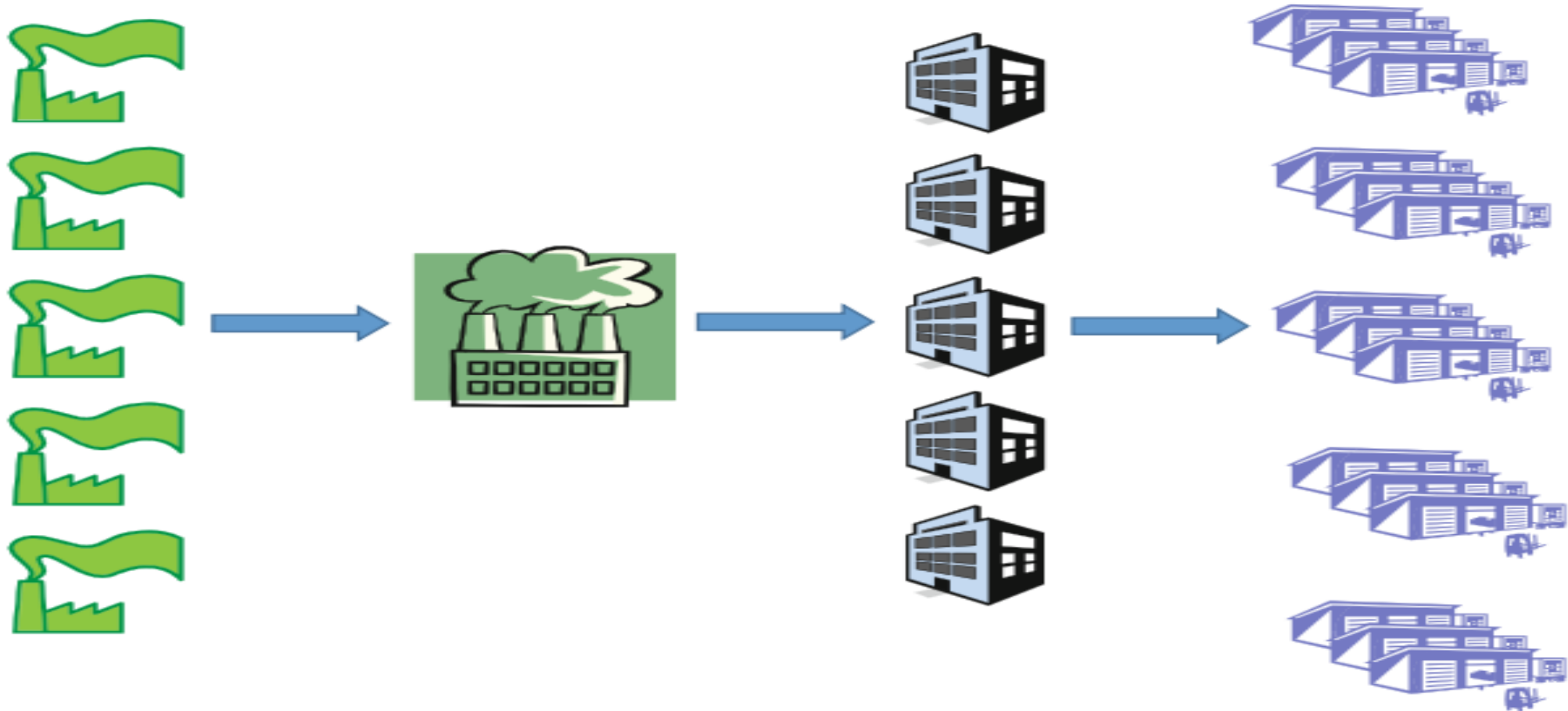


Fig. 7.2 Basic supply chain structure

The distribution warehouses also have different lead times; the last distribution warehouse had a lead time of 14 days. Each distribution warehouse serves three sales offices. These sales offices are supplied with a lead time of 1–3 days. The actual simulation is run for 11 years, in which the first year is a warm-up period and the last ten years are the actual simulation period.

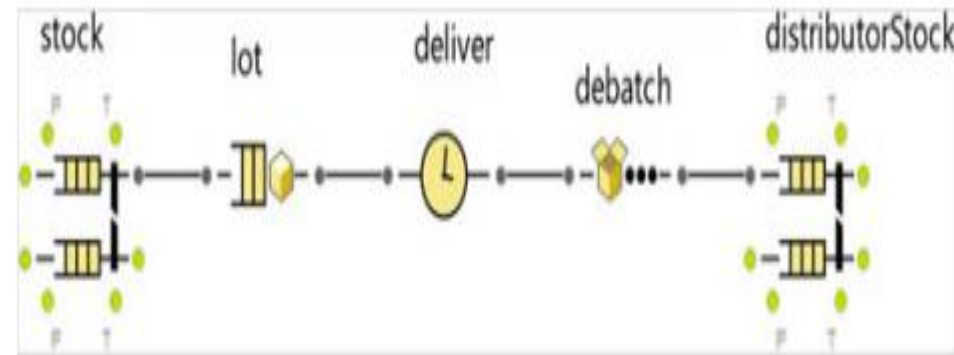


Fig. 7.3 Basic connections in simulation model

Both the factory and the distribution warehouse reserve their stock according to the orders received from the next tier in the supply chain.

All tiers inform the previous tier by using their own sales data. For instance, as soon as a sales office sells one product, it sends information to its own distribution warehouse, which in turn reserves one product from the warehouse for that particular sales office. As soon as an entire order is ready, the supplier/factory/distribution warehouse sends the delivery to the customer

Supply chain costs arise from three different sources: lost sales, warehousing costs, and ordering costs. These costs are location dependent, for example, an order from an offshore supplier has much higher cost than an order from a supplier located nearby. Warehousing costs start accumulating as soon as the raw materials arrive at the factory, and it is assumed that all raw materials have a similar cost. In addition to the supply chain nodes, simplified production is also modelled. Producing one unit takes 6 min, and the factory operates in two shifts per day from Monday to Friday. This is used to ensure that the production is not instant and that it reflects normal operating conditions

Table 7.3 Warehousing policy and distribution lead times

Node	Batch size (units)	Delivery lead time (days)
Suppliers 1 and 2	400	30–41
Suppliers 3 and 4	150	7–14
Supplier 5	30	2–4
Distribution warehouse 1	60	2
Distribution warehouses 2 and 3	75	5
Distribution warehouse 4	90	7
Distribution warehouse 5	120	14
Sales offices	30	1–3

Table 7.4 Cost elements in supply chain

Cost element	Amount
Cost of lost sales	\$1000/unit
Ordering cost from suppliers 1 and 2	\$3000/order
Ordering cost from suppliers 3 and 4	\$700/order
Ordering cost from supplier 5	\$200/order
Ordering cost for distribution warehouse 1	\$500/order
Ordering cost for distribution warehouses 2 and 3	\$625/order
Ordering cost for distribution warehouse 4	\$750/order
Ordering cost for distribution warehouse 5	\$1000/order
Ordering cost for sales offices	\$500/order
Warehousing cost	\$200/unit/year

The actual simulation model was constructed using Anylogic. The distribution warehouses and sales offices are almost identical, with the only difference between them being that the demand at the sales offices is stochastic and random whereas that at the distribution warehouses is dependent on the demand at the sales offices.

Figure 7.3 shows an example of these nodes. The suppliers' warehouses are not modelled and have infinite capacity; however, in the simulation model, they are completely dependent on the demand from the factory.

The factory has a simple assembly operation in which all goods from the suppliers are assembled to make final products. The factory itself operates on a push principle; however, the raw materials arrive based on a pull principle. The factory stock is then connected to the distribution warehouses.

“Stock” represents physical stock. Products arrive at the location and wait in the queue for an order. When an order arrives, they are moved to the “lot” element

. The “lot” element batches the products depending on the batch size, and when the correct batch size is reached, the goods are delivered. The “deliver” element contains a node-dependent delay. In the case of a disruption, the delay contains additional time in addition to the actual delivery lead time.

When the goods arrive, they are removed from the batch in the “debatch” element to become individual products. Finally, the products arrive at the next stock called “distributorStock.” The distributor has a similar chain for the sales offices.

Disruptions in the Model

to analyze how the supply chain behaves when different partners react to changes in the likelihood of disruptions. We analyze multiple different scenarios, in which either only one party will change their amount of safety stock or all parties will cooperate.

By doing so, we can understand the benefits that can be achieved when supply chain partners cooperate to manage changes in supply-chain-related risks

We assume that there is an inherent likelihood of having an excess delay between the raw material suppliers and the factor.

The actual disruption will double the delivery time to the factory.

The three scenarios use different likelihoods for this disruption: 5, 15, and 25%. In each case, we use the OptQuest optimization engine to minimize the supply chain costs

Overall, there are nine different scenarios. We use the scenario with a disruption likelihood of 5% as a baseline scenario. The baseline scenario defines the used safety stocks; these are used in the other scenarios as well. If all supply chain partners cooperate, we can allow all safety stocks to change. However, if only one tier tries to cope with the change in the environment, we assume that the other tiers do not change their safety stock policies but instead rely on the values optimized in the baseline scenario

Results

Table 7.5 presents the results in millions over a ten-year period. These results clearly show the benefits of cooperating in supply chain risk management. Depending on the scenario, different partners have a larger impact on the results.

In the scenario with 15% likelihood, the sales offices have the best tools to manage disruptions as they can keep their costs the lowest if the tiers do not cooperate. However, in the scenario with 25% likelihood, the factory has the best impact on the supply chain cost structure

Table 7.5 Supply chain costs in millions during ten-year period when different partners react to changes in the supply chain environment

	5%	15%	25%
Factory		8.387	8.473
Warehouse		8.339	8.475
Sales office		8.294	8.525
Cooperation	7.885	8.264	8.336

.

The nonlinear dependencies place different importance on different actors in different scenarios. Cooperation between supply chain partners should be encouraged.

This creates some issues with incentives as the tier that increases the amount of safety stocks has to carry more costs

Table 7.6 provides the optimized safety stocks when cooperation is used. In the 15% scenario, the sales offices hold lesser inventory than in the baseline scenario, whereas the factory and distribution warehouses hold more inventory. In the 25% scenario, the factory and sales offices hold more inventory. If a supply chain tier tries to mitigate the change alone, the safety stocks need to increase.

Table 7.6 Optimized safety stock levels in the scenario where different partners cooperate

	5%	15%	25%
Factory	200	450	350
Warehouse	125	175	125
Sales office	10	5	16

In particular, the sales offices need to hold much more inventory than in the cooperative scenario, as shown in Table 7.7. These values should be compared to the 5% likelihood scenario in the cooperative scenario as it serves as the baseline for the other scenarios.

Table 7.7 Optimized safety stock levels if only one tier mitigates

	15%	25%
Factory	450	500
Warehouse	150	200
Sales office	19	36

Theoretical perspective

From a theoretical perspective, we make three main contributions. First, we provide a definition for supply chain vulnerability using an integrated literature review. Second, we demonstrate the current state-of-the-art of using simulations in scientific studies. Finally, and most importantly, we develop and test our discrete-event simulation model that enables one to test the benefits of collaboration in supply chain risk management and thus reduce the overall vulnerability. Our method seemed to work particularly well when analyzing the key components of vulnerability, namely, disruptions and exposure risk.

From a practical perspective, we make two main contributions.

First, we demonstrate how simulations can be used to illustrate complex structures in long supply chains without losing process-level factors, which is especially important for gaining a holistic view of supply chain vulnerability.

Second, we illustrate how the model can be used to run “what-if” experiments and how it can be used to increase the supply chain performance by influencing the factors a supply chain is most sensitive to

Reference

Supply Chain Risk Management Advanced Tools, Models, and Developments

By: Yacob Khojasteh

-ISBN 978-981-10-4106-8 (eBook)

Chapter 5



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

