Hindawi Publishing Corporation
Scientific Programming
Volume 2016, Article ID 2819238, 10 pages
http://dx.doi.org/10.1155/2016/2819238

Research Article

An Integrated Method of Supply Chains Vulnerability Assessment

Jiaguo Liu,[1,2] Fan Liu,[3,4] Huan Zhou,[1] and Yudan Kong[1]

[1] *Transportation Management College, Dalian Maritime University, Dalian 116026, China*
[2] *Collaborative Innovation Center for Transport Studies, Dalian Maritime University, Dalian 116026, China*
[3] *School of Business Administration, Zhongnan University of Economics and Law, Wuhan 430073, China*
[4] *Post-Doctoral Research Center, Zhongnan University of Economics and Law, Wuhan 430073, China*

Correspondence should be addressed to Fan Liu; 462399289@qq.com

Received 2 May 2016; Accepted 28 August 2016

Academic Editor: Xiaofeng Xu

Supply chain vulnerability identification and evaluation are extremely important to mitigate the supply chain risk. We present an integrated method to assess the supply chain vulnerability. The potential failure mode of the supply chain vulnerability is analyzed through the SCOR model. Combining the fuzzy theory and the gray theory, the correlation degree of each vulnerability indicator can be calculated and the target improvements can be carried out. In order to verify the effectiveness of the proposed method, we use Kendall's tau coefficient to measure the effect of different methods. The result shows that the presented method has the highest consistency in the assessment compared with the other two methods.

1. Introduction

With the rapid development of economy and technology, the competition among enterprises has become competition between supply chain. Because of the frequency and intensity of terrorist attacks, SARS, hurricane, and series of other disasters and crises [1–3], supply chain management has aroused widespread concern. In 2011, Thailand suffered the worst flooding in the past fifty years which led to a fatal damage for some giant industrial park around Bangkok, and the flooding resulted in the supply chain disruption of motor industries, electronic components, and hard disk [4]. As the supply chain structure becomes more and more complicated, the supply chain capacity that respond to the disruption is weaker than before [5, 6], and thus the supply chain vulnerability is more serious [7]. Researches on the vulnerability originated in the 1970s when White (1974) first proposed the "vulnerable" concept and it is a new emerging research field in supply chain management. Christopher and Peck [8] defined supply chain vulnerability as "a kind of exposure to serious disturbance." In the researches of natural disasters and crisis management, Blaikie et al. [9] defined vulnerability as the ability of an individual or organization to predict, process, resist, and recover. In the researches of ship supply chain, Barnes and Oloruntoba [10] described the vulnerability as "a vulnerable constitution that leads to loss which caused by existing organizations or functional activity or external condition." Based on various definitions, we consider that the vulnerability is an instability and destructiveness that caused by supply chain external and internal risks. Supply chain vulnerability is an inherent trait of the supply chain, which is determined by the structure and characteristics of the supply chain itself.

Currently, researches on supply chain vulnerability mainly concentrated on its definition, connotation, influence factors, and other aspects, while little concern is paid to supply chain vulnerability assessment [11]. Based on interference, performance losses, the relationship between them, and other factors, Albino and Garavelli analyzed the sensitivity of supply chain systems under the condition that time is known and interference occurs randomly; then the supply chain vulnerability was evaluated [12]. Prater et al. [13] used five cases in the paper to achieve optimal coordination between agility and complexity through controlling supply chain risk factors and changing supply chain complexity. Zhong and Xie [14] proposed "3P" management principles and supply chain

vulnerability management principles to prevent and respond to damage at the tactical level. In the view of specialization of supply chain, Barnes and Oloruntoba [10] analyzed the characteristics of the entire supply chain using the special case, and they concluded that it is the complexity of the interaction between marine operations and supply chain that caused the vulnerability. In 2000, Svensson, representative scholar in the supply chain vulnerability, built a supply chain vulnerability theoretical framework and made a qualitative description and assessment of the vulnerability through the disturbance source, category, and logistics mode [15]. After two years, he calculated the vulnerability again based on time and relationship [16]. In order to enrich the study, he assessed the supply chain vulnerability from time, function, and relationship's three dimensions in 2004 [17]. Peck introduced the network theory and complex systems into the interactive production system supply chain conceptual model and analyzed the four levels from multiangles [18]. D. Bogataj and M. Bogataj [19] evaluated the vulnerability from the perspective of vulnerable point and analyzed the input-output tables and the relationship between storage and delivery, using the dynamic NPV method which can find the relationship of before and after items; then he concluded the weak link of the supply chain and predicted the vulnerability point. Based on the vulnerability index, Stephan and Wagner [20] proposed a method to confirm the validity of the policy by comparing different industry or enterprise vulnerability index. With the development of extensive, Fang et al. [21] proposed vulnerability assessment and early warning model for small and medium-sized enterprises intellectual property.

To sum up, the existing researches have established theoretical framework to evaluate the supply chain vulnerability. However, these basically are limited to the qualitative framework. Therefore, we utilize the FMEA (failure mode and effect analysis) method, which is a way for prospective reliability analysis and safety assessment. It analyzes every failure mode that existed in the system, and it calculated risk priority number (RPN) for the consequences of all failure modes [22]. According to the value of RPN, we make a quantitative assessment of the failure modes and take corresponding measures to prevent and avoid the potential failure mode if necessary. However, the traditional FMEA method does not recognize the importance of the relationship between all the failure modes and every decisive factor in the vulnerability, and the traditional FMEA method makes its evaluation effect limited when the experts' evaluation language is qualitative and subjective. Considering the above conditions, we present an integrated method using the fuzzy theory and the gray relational theory to solve the above problems. The present method can help business managers implement the improvements of supply chain vulnerability.

2. Methodology and Assessment Process

2.1. Methodology. FMEA, namely, failure mode and effect analysis, in fact, originated in the 1950s. Because of the significant value in safety and reliability assessment, FMEA has developed rapidly and has been widely used in many areas such as the nuclear industry, automotive, machinery, aerospace, electronics, and ships. It use three aspects for assessment. They are severity (S), occurrence (O), and detection (D) [23]. It is a powerful tool for defining, identifying, and eliminating potential failures from the system, design, process, or service before they reach the customer [24]. Severity is the degree of the effect of the potential failure mode on customers; occurrence refers to the possibility of the occurrence of the specific failure mode; detection describes the possibility that the current system cannot recognize the failure modes or reasons. The traditional FMEA method has two following disadvantages in practical application.

First, the traditional FMEA method to assess products or system risks merely depends on RPN which can lead to large problems in the actual situation. In the traditional FMEA, we get RPN simply through the product of the three factors: severity (S), occurrence (O), and detection (D). In traditional FMEA, the relative importance of each factor is not considered and the three factors are given the same weight. Meanwhile, the different factors may be multiplied to get the same RPN, but corresponding degree of risk is inconsistent, which makes the RPN inefficient in practical application in various failure modes of the level of risk assessment.

Second, the application effect of FMEA was limited because of the limited experience and knowledge that the experts have. To apply FMEA method, you should set up a committee of experts first, and experts grade every factor by their experience and knowledge. In this process, experts need to have a profound understanding, investigation, and research, but it is difficult to describe their experience and knowledge because the subjective of the language, so the traditional FMEA can not make accurate judgments; thus there is a limit to the effect of traditional FMEA.

From the preceding analysis, we can find that there are a lot of factors that influenced the supply chain vulnerability in the assessment index system, and many factors mutually affect each other, so we need a comprehensive approach to integrating the FMEA method to assess the vulnerability. Meanwhile, the comment that the FMEA expert team members assess often expressed ambiguous. In order to modify the defects of the traditional FMEA method and consider the characteristics of supply chain vulnerability influence factors, FMEA method is combined with fuzzy theory and gray Correlative Method to evaluate and rank the RPN.

2.2. Assessment Process. When using the FMEA method, we should first give the operational model a clear definition, then analyze the potential failure modes that existed in every process, and confirm the cause of potential failure modes. Next, we use the models to assess all failure modes, rank the vulnerability, take preventive measures according to the vulnerability value, and estimate the effect of the measures. In this paper, we give a special study on supply chain vulnerability which is based on traditional FMEA operation steps, so the supply chain based on FMEA vulnerability assessment process is shown as Figure 1.

3. Supply Chain Vulnerability Analysis

3.1. Supply Chain Vulnerability Analysis. We adopted the supply chain operations reference model (SCOR) that is

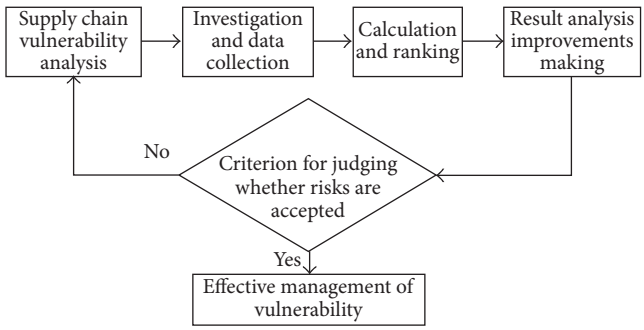

Figure 1: Assessment process.

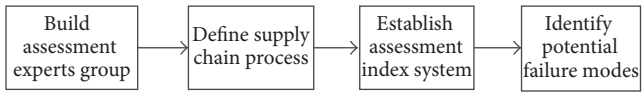

Figure 2: SC vulnerability analysis process.

developed and authorized by the Supply Chain Council, so that we can better identify failure modes existing in the supply chain process and assess the supply chain vulnerability. Based on the SCOR model, the supply chain vulnerability analysis process is given in Figure 2.

Ten experts from academia and industry fully aware of the supply chain operation in the manufacture industry are divided into two groups. Group 1 adapt the SCOR model to conceptualize the supply chain vulnerability analysis, and group 2 validate the results of group 1. They define the supply chain operation management processes as follows: Plan, Source, Make, Deliver, and Return, denoted as P, S, M, D, and R. And they establish competitive performance goals. The second configuration layer is composed of 26 kinds of core processes through a full discussion. In the third decomposition layer, the second layer is detailed and specific, which makes the process more specific and gives the company's competence ability in selected markets. At the third layer, the experts group analyze the process, identify failure modes, and conclude consequences.

3.2. Supply Chain Vulnerability Assessment Index System and FMEA Analysis. In reviewing the relevant research results, the experts group built a supply chain vulnerability assessment index system. We define the second layer as P_i, S_i, M_i, D_i, R_i, and its corresponding potential failure modes as P_iF_j, S_iF_j, M_iF_j, D_iF_j, R_iF_j, where $i = 1, 2, \ldots,\ j = 1, 2, \ldots$.

(1) Planning Process Failure Analysis. In the SCOR model, "Plan" is the processes that balance aggregate demand and supply to develop a course of action which best meets sourcing, production, and delivery requirements. The planning processes include confirming, ranking, and consolidating needs; confirming, evaluating, and integrating resources and capabilities; balancing resources, capabilities, and needs; and making plans.

(2) Sourcing Process Failure Analysis. "Source" is the processes that procure goods and services to meet planned or actual demand. Sourcing processes include confirming supply source; selecting vendors and negotiating procurement of raw materials; product distribution arrangement; accepting products; checking products; transferring products; authorizing payments; and other steps.

(3) Making Process Failure Analysis. "Make" is the processes that transform product to a finished state to meet planned or actual demand. The making processes include arranging production activities; distribution of raw materials and products; production and testing; packaging; storage.

(4) Delivering Process Failure Analysis. "Deliver" is the processes that provide finished goods and services to meet planned or actual demand, typically including order management, transportation management, and distribution management. The delivering processes include processing queries, offering, and receiving; registration and verification of orders; reserving inventory and determining distribution date; combining orders; distribution packaging; loading and generating and distributing records; transporting products; customer reception and checking products.

(5) Returning Process Failure Analysis. "Return" is the processes associated with returning or receiving returned products for any reason. These processes extend into postdelivery customer support. The return processes include acknowledging of customer returning products; disposal of returned products; requesting a return privilege; arranging distribution; recycling returned products; and other processes.

4. Model

The proposed integrated FMEA model can be described as the following steps in detail based on the basic FMEA model.

4.1. Establishment of Assessment Index System. According to the previous introduction to supply chain vulnerability identification, we could put forward the factors set as follows: $U = \{P, S, M, D, R\}$ and further divide them, and the next layer factor is set as $P = \{P_1, P_2, P_3\}$, $S = \{S_1, S_2\}$, $M = \{M_1, M_2, M_3\}$, $D = \{D_1, D_2, D_3\}$, $R = \{R_1, R_2, R_3, R_4\}$. If there is a next layer, we continue to define it.

4.2. Establishment of Assessment Set. We establish the assessment set by selecting, "very high," "high," "higher," "medium," "lower," "low," and "very low," seven semantic items [25].

$$V = \{\text{very high (VH)},\ \text{high (H)},\ \text{little high (VH)},\ \text{medium (M)},\ \text{little low (LL)},\ \text{low (L)},\ \text{very low (VL)}\}. \quad (1)$$

The corresponding meaning of all semantic items is shown in Table 6. By using the seven semantic items, experts assess the potential failure modes in the supply chain and give fuzzy scores to the severity S, occurrence O, and detection D. According to the seven semantic items, we obtain the corresponding clear number by using fuzzy mathematical

theory and method and establish the assessment set as shown in Table 6.

We used experts scoring method to determine the weight of each failure mode. Assuming that there are n experts and i failure modes, the weight of failure mode i given by expert k is recorded as υ. The corresponding fuzzy semantic value of triangular fuzzy number is through the use of the Delphi method; experts make decisions depending on their own experience and knowledge. The ability of expert k is defined as ∂_k and the fuzzy assessment of a certain critical factor in the failure mode is defined as x_k, which can be expressed by the triangular fuzzy number as $x_k = (a_k, b_k, c_k)$. According to the experts' experience, we can get the value of the key factor fuzzy triangles corresponding to the digital fuzzy semantic items by the following equation (note that $\sum_{k=1}^{n} \partial_k = 1$, $\partial_k \in (0, 1)$):

$$\begin{aligned} a &= \sum_{k=1}^{n} \partial_k a_k \\ b &= \sum_{k=1}^{n} \partial_k b_k, \\ c &= \sum_{k=1}^{n} \partial_k c_k. \end{aligned} \tag{2}$$

We use fuzzy theory to calculate the formula, which is proposed by Xiao and Li [26]. Formula is shown as follows:

$$\begin{aligned} C(x) = {} & \frac{1}{2(1+N)} * a + \frac{N + 2NM + M}{2(1+N)} * b \\ & + \frac{1}{2(1+M)} * c. \end{aligned} \tag{3}$$

For the basic factor set having three layers, we added variable h. Then, the weight of the failure mode i was calculated by

$$\begin{aligned} \pi_i &= \frac{1}{n} \sum_{k=1}^{n} {\pi_{ki}}^{h} \\ & (k = 1, 2, \ldots, n;\ i = 1, 2, \ldots, m;\ h = 1, 2, 3). \end{aligned} \tag{4}$$

4.3. Establishment of FMEA Table. In the previous section, we applied fuzzy number and fuzzy theory and obtained the corresponding number of fuzzy semantic items assessed by an expert team. Next, FMEA assessment team will assess the various failure modes by using the fuzzy semantic items. In this process, we need to establish an expert survey and statistics table in order to obtain the data.

After experts scored the failure mode, we can get every layer factor's weight which ups to the average scores. In the traditional FMEA, experts score in the condition that every layer factors unrelated. In fact, the factors of every layer exist hierarchical relationships. By using probability tree theory, we calculate the value of weight considering hierarchical relationships of factors. If we used θ to represent the RPN coefficient of every failure mode, then $\theta = {\pi_i}^{h} {\pi_i}^{h-1} {\pi_i}^{h-2}$ (${\pi_i}^{h}$ indicates the weight of the failure mode regardless of the hierarchical relationships, ${\pi_i}^{h-1}$ indicates the weight of the failure mode corresponding to the upper layer, and ${\pi_i}^{h-2}$ indicates weight of the failure mode corresponding to the next higher layer of the upper layer).

4.4. Determination of Vulnerability Level. According to the formula of improved risk priority number RPN $= \theta * S * O * D$, we can get RPN which indicates the level of risk of various failure modes. But the crux of the matter is that RPN can help managers make decisions. Then, the degree of gray correlation between the evaluation vectors of each scheme is calculated by the gray relational grade, and the decision and evaluation vector in the best scheme are obtained.

Step 1 (establishing comparison matrix). We assume that there are p types of failure modes. Each failure mode is expressed by i, and x_i illustrates failure mode i. When computing, there are S, O, D, three variables of each failure mode, so the data shows failure mode i represented as $x_i = \{x_i(t),\ t = 1, 2, 3\}$, whose values can be got by (3). On the basis of the method mentioned above, to reflect various of failure mode, we establish the comparison matrix as follows:

$$\begin{aligned} X_i(t) = \{x_i(t)\} &= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix} \\ &= \begin{pmatrix} x_1(1) & x_1(2) & x_1(3) \\ x_2(1) & x_2(2) & x_2(3) \\ \vdots & \vdots & \vdots \\ x_p(1) & x_p(2) & x_p(3) \end{pmatrix}. \end{aligned} \tag{5}$$

Step 2 (establishing reference matrix). Failure mode risk ranking should be based on certain reference standards. In general, we choose the best or worst value as a reference. The worst value of each variable is chosen to build a reference matrix as follows:

$$\{x_0(t)\} = \begin{pmatrix} \mathrm{VH} & \mathrm{VH} & \mathrm{VH} \\ \mathrm{VH} & \mathrm{VH} & \mathrm{VH} \\ \vdots & \vdots & \vdots \\ \mathrm{VH} & \mathrm{VH} & \mathrm{VH} \end{pmatrix}. \tag{6}$$

Step 3 (calculating gray correlation coefficients). When it comes to the gray correlation theory, the following formula can be obtained:

$$\begin{aligned} & \lambda(x_0(t), X_i(t)) \\ & = \frac{\min_i \min_t \left| x_0(t) - x_i(t) \right| + \upsilon \max_i \max_t \left| x_0(t) - x_i(t) \right|}{\left| x_0(t) - x_i(t) \right| + \upsilon \max_i \max_t \left| x_0(t) - x_i(t) \right|}, \end{aligned} \tag{7}$$

where υ is distinguishing coefficient, with the value in interval (0,1), normally $\upsilon = 0.5$.

Table 1: Planning process assessment index and failure mode analysis.

First-layer factors	Second-layer factors	Potential failure modes
Plan P	Strategy P_1	P_1F_1: unclear strategic positioning
		P_1F_2: high positioning
		P_1F_3: low positioning
		P_1F_4: inaccurate plan data
		P_1F_5: supply chain strategy adjustment
		P_1F_6: inconsistent strategic objectives among supply chain members
		P_1F_7: failed strategic investment
	Culture P_2	P_2F_1: insufficient understanding and emphasis of supply chain managers on the multicultural conflict risk
		P_2F_2: low quality of the staff cultural skills
		P_2F_3: weak risk awareness and corporate risk culture
		P_2F_4: inconsistent corporate cultural values
	Demand P_3	P_3F_1: customer loss
		P_3F_2: low satisfaction of customers' needs
		P_3F_3: demand fluctuations
		P_3F_4: poor sales reputation
		P_3F_5: many competitive alternatives

Step 4 (calculating gray correlations). Because of the different influence on risk, the variable of failure mode has different weights. Assuming the weight of variables is ξ_t, so the correlation degree is computed by the following equation [27]:

$$\mu(x_0, x_i) = \sum_{t=1}^{3} \xi_t \left\{\lambda\left(x_0(t), X_i(t)\right)\right\}. \quad (8)$$

Note that $\sum_{t=1}^{3} \xi_t = 1$, ξ_t is computed from the front expert questionnaire statistics.

Step 5 (ranking). Finally, according to formula $\theta * \mu(x_0, x_i)$, we could calculate the correlation degree in the case of considering single weight of failure mode and three critical factors of weight of each failure mode. Then, we sort the correlation degree in descending order. Determine the RPN and make target improvements.

5. Case Study

5.1. Case Introduction. Shipbuilding Yard RS was founded in 2005, which is mainly engaged in shipbuilding, marine engineering, marine engine manufacturing, and construction machinery, and it concentrates on the relevant customers and markets of oil and gas industry. According to the 2010 annual report, it had the largest proportion of business in Brazil, China, Germany, and Turkey, and it is the fastest growing private shipbuilding company in China. According to the British maritime agency Clarkson report, RS is also the largest shipbuilding enterprises at present in China by calculating hand-held orders. In October 2012, a RS's subsidiary, named RS Maritime, which aims to achieve the development strategy of its upgrading and transformation and develop the ocean engineering operations which are high value-added and rapidly increasing, was set up in Singapore.

The company attaches great significance to the vulnerability of the supply chain. As a result, the FMEA assessment team is set up to assess the enterprises' vulnerability. Because of the difficulty in obtaining the accurate risk factors, the semantic variables are used in Table 8 to score the potential failure modes. The FMEA assessment team includes 5 cross-department assessment members, and it is mainly used as the scoring expert group which is named Expert Group 1. Owing to the different expertise and background of the experts, the importance and ability of them are also different. On these grounds, different relative weights are given as follows: 0.3, 0.2, 0.2, 0.2, and 0.1. In order to verify the effectiveness of Expert Group 1 construction index and scoring results, we ask the company to set up another expert group, named Expert Group 2, which is mainly used as validation expert group.

5.2. Model Application

5.2.1. Establishment of Assessment Index System. We have a thorough initial assessment with a total of 68 third-layer factors and 15 second-layer factors (Tables 1–5). In this part, Expert Group 1 is provided with questionnaires to identify the most important variables in their opinion, from Tables 1–5. After a discussion of the Expert Group 1, they summarized a set of vulnerability assessment index system for the RS. Then, the index system is presented to an additional independent group (Expert Group 2) for the purpose of model and result validation, so the index system is corrected and improved, and eventually we obtained the most suitable index system for RS (see Appendix in Supplementary Material available online at http://dx.doi.org/10.1155/2016/2819238).

5.2.2. Establishment of Fuzzy Assessment Set. In order to get clear numbers of corresponding fuzzy semantic items, Expert Group 1 scores the fuzzy semantic items. According

Table 2: Sourcing process assessment index and failure mode analysis.

First-layer factors	Second-layer factors	Potential failure modes
Source S	Purchasing S_1	S_1F_1: high purchasing price
		S_1F_2: frequent fluctuations in exchange rates
		S_1F_3: inappropriate supplier selection
		S_1F_4: unable to deliver goods on time
		S_1F_5: low quality of procurement product
		S_1F_6: irresponsible purchase person
		S_1F_7: purchasing accident
		S_1F_8: acceptance lax of procurement materials
	Supply S_2	S_2F_1: key suppliers failing to bankruptcy or loss
		S_2F_2: supplier business outsourcing
		S_2F_3: suppliers' insufficient production capacity
		S_2F_4: unable to deliver goods on time
		S_2F_5: insufficient supplier technical innovation capability
		S_2F_6: shortages of raw materials market
		S_2F_7: inadequate supply elasticity of supplier

Table 3: Making process assessment index and failure mode analysis.

First-layer factors	Second-layer factors	Potential failure modes
Make M	Environment M_1	M_1F_1: macroeconomic fluctuation
		M_1F_2: political instability and government intervention
		M_1F_3: industrial policy constraints
		M_1F_4: natural disasters and so forth.
		M_1F_5: insufficient in public utilities supply
	Production M_2	M_2F_1: improper control of the production process
		M_2F_2: inelastic production capacity
		M_2F_3: low level of information sharing
		M_2F_4: technical level restrictions
		M_2F_5: labor cost Rising
		M_2F_6: talent loss and labor dispute
		M_2F_7: less rigorous of production inventory control
	Control M_3	M_3F_1: imperfect financial system
		M_3F_2: imperfect job security system
		M_3F_3: failed risk response mechanism
		M_3F_4: inappropriate product cost control
		M_3F_5: substandard product
		M_3F_6: intellectual property rights and other legal issues

Table 4: Delivering process assessment index and failure mode analysis.

First-layer factors	Second-layer factors	Potential failure modes
Deliver D	Relation D_1	D_1F_1: self-interested behavior of partners
		D_1F_2: distrust between partners
		D_1F_3: inequitable benefits distribution among partners
		D_1F_4: unfair competition between partners
	Transportation D_2	D_2F_1: inappropriate choice of transportation routes and means
		D_2F_2: immature delivery technology or distribution equipment failure
		D_2F_3: product damage or loss
		D_2F_4: unscientific delivery personnel management
		D_2F_5: inappropriate distribution model
		D_2F_6: errors or delays in delivery
	Origination D_3	D_3F_1: irrational supply chain structure
		D_3F_2: improper delegation of supply chain authority

Table 5: Returning process assessment index and failure analysis.

First-layer factors	Second-layer factors	Potential failure modes
Return R	Return way R_1	R_1F_1: no consensus with customer
		R_1F_2: no consensus with supplier
	Return route R_2	R_2F_1: improper return route
	Return procedure R_3	R_3F_1: imperfect return process and rules
	Return management R_4	R_4F_1: imperfect return asset management
		R_4F_2: imperfect return distribution management
		R_4F_3: improper return inventory management
		R_4F_4: incomplete return collection data

Table 6: Corresponding meaning of semantic items.

Semantic items	Severity	Occurrence	Detection
Very low	Products are not affected	Failure hardly occurs	Almost all detected
Low	Products are slightly affected	Failure rarely occurs	The probability that failure is not detected is low
Little low	Some characteristics are slightly affected but product function properly	Failure occurs less	The probability that failure is not detected is relatively low
Medium	Product can be used, but some important characteristics are affected, while there is no dissatisfied customer	Failure occurs occasionally	Failure is not occasionally detected
Little high	Product can be used, but some important characteristics are affected strongly, some customers are not satisfied	Failure occurs frequently	Failure cannot be detected occurs frequently
High	Product has problems and has lost basic function	Failure occurs repeatedly	Failure most cannot be detected
Very high	Products are complete lost basic function, and threaten personal safety or violate laws	Failure is almost inevitable	Failure is almost undetectable

Table 7: Rating levels for decision-making factor i of failure mode FM_i.

Expert	∂_k	Very low (VL)	Low (L)	Little low (LL)	Medium (M)	Little high (LH)	High (H)	Very high (VH)
1	0.3	(0,1.3,2.8)	(0.8,2.3,3.8)	(2.7,4.5,6.3)	(3.8,5.8,7.8)	(5.3,7.1,8.8)	(7.8,9.1,9.9)	(8.8,10,10)
2	0.2	(0,1.3,2.6)	(0.6,2.1,3.6)	(2.2,4.1,6.6)	(3.3,5.3,7.6)	(4.5,6.5,8.7)	(7.1,8.9,9.9)	(8.3,10,10)
3	0.2	(0,1.3,2.3)	(0.7,2.4,3.7)	(2.4,4.5,6.7)	(3.5,5.5,8.2)	(5.1,7.1,9)	(7.5,9.3,9.9)	(8.5,10,10)
4	0.2	(0,1.3,3)	(0.7,2.3,4)	(2.6,4.5,6.5)	(3.6,5.1,8)	(5.3,6.5,8.9)	(8.1,9.2,9.9)	(9.2,10,10)
5	0.1	(0,1.3,2.7)	(0.6,2.1,3.7)	(2.4,4.5,6.4)	(3.4,5.6,8)	(5,6.8,8.9)	(7.6,8.9,9.9)	(8.6,10,10)
Total	1	(0,1.3,2.7)	(0.7,2.7,3.8)	(2.5,2.4,6.4)	(3.6,5.6,7.9)	(5.1,6.8,8.9)	(7.6,9.1,9.9)	(8.7,10,10)

to the seven items proposed in the previous section, Expert Group 1 assesses fuzzy decision-making factor of each failure mode. The following table shows the expert scores, which are triangular fuzzy numbers. ∂ is the relative weight mentioned above.

Based on (3) and the scores in Table 7, clear numerical values of fuzzy semantics can be calculated. The results of these calculations are summarized in Table 8.

5.2.3. Establishment of FEMA Table and Weight Scoring Table. Owing to space limitations, detailed FMEA tables are not displayed in the body part but in Appendix A. In addition, FEMA scoring is shown in Table A1 and the weights at all layers scoring are shown in Table A2. When establishing FMEA table, we omit corresponding causes and results of failure modes on the basis of the practical needs, but we have improved the traditional FMEA table to be applicable for the macro supply chain system.

Table 8: Corresponding clear number of fuzzy semantic items.

Items	VL	L	LL	M	LH	H	VH
Clear number	1.3	2.3	4.5	5.7	6.9	9	9.8

5.2.4. Processing of Data. By summarizing statistics of expert scoring sheets, we got Tables B1 and B2 in Appendix B. On the basis of the clear number in Table 8, we get decision-making

Table 9: Risk ranking of third-layer factors based on FEMA and gray correlation.

Third-layer factors	Weight	Correlation	Ranking
P_1F_1	0.04	0.0260	11
P_1F_2	0.03	0.0198	14
P_2F_1	0.02	0.0128	20
P_2F_2	0.02	0.0116	22
P_3F_1	0.02	0.0163	16
P_3F_2	0.02	0.0136	19
P_4F_1	0.02	0.0119	21
P_4F_2	0.01	0.0062	25
P_4F_3	0.01	0.0069	24
P_4F_5	0.01	0.0064	26
S_1F_1	0.07	0.0433	5
S_1F_2	0.05	0.0315	9
S_2F_1	0.08	0.0501	3
S_2F_2	0.04	0.0255	12
M_1F_1	0.06	0.0432	8
M_1F_2	0.06	0.0385	6
M_1F_3	0.06	0.0482	4
M_2F_1	0.05	0.0373	7
M_2F_2	0.04	0.0267	10
M_2F_3	0.03	0.0197	15
D_1F_1	0.02	0.0145	17
D_1F_2	0.03	0.0208	13
D_2F_1	0.02	0.0137	18
D_2F_2	0.01	0.0055	27
D_2F_3	0.02	0.0106	23
R_1F_1	0.08	0.0506	2
R_1F_2	0.08	0.0630	1
Sum	1.0	—	—

factors set named B2. Owing to space limitations, we do not list the source data but show the average index weight set B3.

5.2.5. Determination the Level of Vulnerability

(1) Establishing Related Matrix. According to decision-making factor set obtained in the previous step, we establish a comparison matrix and choose the worst value including $x_i(t)$ and $x_0(t)$ to establish reference matrix.

(2) Calculating Gray Correlation Coefficient. Taking $\upsilon = 0.5$, we compute the gray correlation coefficient between decision-making factor variables and reference values by (7) and get $\lambda(x_0(t), X_i(t))$.

(3) Calculating Gray Correlation Degree. On the basis of (8) (ξ_t, available in Appendix), we can get the following data: (0.64964,0.65921,0.63872,0.58098,0.81740,0.68236,0.59689, 0.61506,0.69091,0.57574,0.61907,0.63095,0.62653,0.63831, 0.71990,0.64093,0.80330,0.74667,0.66641,0.65730,0.72529, 0.69363,0.68583,0.54514, 0.53203,0.56261,0.73313).

(4) Ranking Vulnerability Level. Again, according to $\theta * \mu(x_0, x_i)$, we obtain the risk ranking summarized in Tables 9, 10, and 11.

Table 10: Risk ranking of second-layer factors based on FEMA and gray correlation.

Second-layer factors	Weight	Correlation	Ranking
P_1	0.068	0.0458	6
P_2	0.04	0.0244	11
P_3	0.044	0.0299	9
P_4	0.048	0.0314	8
S_1	0.1248	0.0748	5
S_2	0.1152	0.0756	4
M_1	0.168	0.0867	2
M_2	0.112	0.0837	3
D_1	0.048	0.0353	7
D_2	0.052	0.0298	10
R_1	0.18	0.1136	1
Sum	1	—	—

Table 11: Risk ranking of first-layer factors based on FEMA and gray correlation.

First-layer factors	Weight	Correlation	Ranking
P	0.2	0.1315	3
S	0.24	0.1504	2
M	0.28	0.2136	1
D	0.1	0.0651	5
R	0.18	0.1136	4
Sum	1	—	—

5.3. Result Analysis. From Table 11, we conclude that five first-grade indicators ranking is make > source > plan > return > deliver. The vulnerability of RS is chiefly reflected in three aspects: make, source, and plan. The make risk is the largest so its weight is the heaviest. Meanwhile, factor of source is the second place in the secondary indicators of manufacturing, which indicates that the manufacturing process attaches great importance to the shipbuilding supply chain and it is the most vulnerable part and the most error-prone part, which have relations with the characters of the shipbuilding enterprises industry. Source is nearly as significant as make. Especially, the overcapacity of RS should be taken seriously. Furthermore, source is also important in the second part of the shipbuilding supply chain. Owing to the expanding scope of business and cost savings resulting from zero inventory, RS has higher and higher requirements for the raw materials. RS becomes increasingly dependent upon suppliers, but suppliers which lead to risk are among all failure modes that are ranking in the top place, which should concern more about the supply chain flexibility when pursuing efficiency and low cost at the same time. Large-scale shipbuilding overseas orders make the process of planning more crucial and higher request for the accurate strategic plan and the effective building. What requires more attention is that the weightof the last link of supply chain in return

Table 12: Comparison of τ value of various methods.

	Improved FMEA	Average	Only fuzzy theory FEMA
τ_1	0.69	0.16	0.45
τ_2	0.71	0.17	0.50
τ_3	0.70	0.36	0.46
τ_4	0.68	0.32	0.45
τ_5	0.65	0.33	0.37
τ_6	0.65	0.11	0.32
τ_7	0.71	−0.01	0.24
τ_8	0.69	0.00	0.43
τ_9	0.73	0.28	0.53
τ_{10}	0.75	0.13	0.64
τ	0.70	0.18	0.44

process is not big. It is calculated ranking top in the layer 3 risk factors, and they are company cancel the order and contract renegotiation, which is the first and second, respectively. The mismanagement between the firm and the demand side management causes that there is a large-scale overseas of invalid orders.

5.4. Comparison with Other Methods. In order to verify the validity of improved FMEA in evaluating the supply chain, Expert Group 2 is also requested to score the FMEA table and weight table. In this paper, we use Kendall's tau coefficient [28, 29] to verify the quality of order-preserving.

Given two rating score vectors $\{a_i\}_{i-1}^n$ and $\{b_i\}_{i-1}^n$, C_{ij} defined as

$$C_{ij} = \begin{cases} 1 & \text{If } \left(a_i < a_j \text{ and } b_i < b_j\right) \text{or } \left(a_i > a_j \text{ and } b_i > b_j\right) \text{or } \left(a_i = a_j \text{ and } b_i = b_j\right) \\ 0.5 & \text{If } \left(a_i = a_j \text{ and } b_i \neq b_j\right) \text{or } \left(a_i \neq a_j \text{ and } b_i = b_j\right) \\ 0 & \text{Other.} \end{cases} \tag{9}$$

Then, the number of concordant pairs is $C = \sum_{i-1}^{n} \sum_{j=i+1}^{n} C_{ij}$. Based on the above definition, Kendall's tau rank-correlation coefficient can be calculated, namely, τ. Besides, τ value has three properties: (1) if the two ratings imply the same ranking, $\tau = 1$. Otherwise, $\tau = -1$. (2) For all the cases, τ value lies between −1 and 1. (3) One property of τ index is as follows: the larger value τ that shows order-preserving is better and the method applied during sorting is more in line with the actual situation. Table 12 shows that the improved FMEA result is more in line with the actual situation compared with the other two methods.

6. Conclusions

In this study, an improved FMEA is provided to assess the supply chain vulnerability. The main results are as follows:

(1) With lots of expert interviews and investigations of related literature, we establish the supply chain vulnerability assessment index system, including 5 first-layer factors, 10 second-layer factors, and 27 potential failure modes. The assessment index system almost contains the whole process of supply chain and provides the corresponding potential failure modes, and it can enhance the operability of the assessment work.

(2) To solve the two shortcomings of traditional FMEA, we provide an improved FMEA that combined with gray correlation and fuzzy theory. In the improved FMEA, the weights consider every layer factor's correlation. Also we introduce the gray relational degree to rank which makes the scoring more scientific and reliable.

(3) In order to test applicability of the improved FMEA model, we choose a shipbuilding Yard that is called RS to study. The results showed that vulnerability is mainly concentrated on the manufacturing, procurement, excess capacity, and other links. We make some proposals to make vulnerability identification and assessment, which might be helpful for the similar shipbuilding enterprise.

(4) In order to verify the effect of the improved FMEA, the paper used Kendall's tau coefficient to assess the ten scoring methods, only fuzzy theory FMEA, and improved FMEA. The study found that the improved FMEA method is the best in isotonicity, which means that the improved FMEA method is more in line with reality.

Disclosure

The draft of this paper has been presented in 2014 International Joint Conference on Computational Sciences and Optimization [30].

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The authors are grateful for all the revision suggestions that were provided in the conference. And this paper is partly supported by Natural Science Foundation (71402038) and Higher Education Development Fund of Liaoning Province (20110116202). And thanks are due to all the references' authors.

References

[1] L. Coleman, "Frequency of man-made disasters in the 20th century," *Journal of Contingencies and Crisis Management*, vol. 14, no. 1, pp. 3–11, 2006.

[2] O. K. Helferich and R. L. Cook, *Securing the Supply Chain* , Council of Logistics Management, Oak Brook, Ill, USA, 2002.

[3] Re. Munich, *Annual Review: Natural Catastrophes* , Munich Re Publications, Munich, Germany, 2005.

[4] K. B. Hendricks and V. R. Singhal, "An empirical analysis of the effects of supply chain disruptions on long-run stock price performance and equity risk of the firm," *Production and Operations Management*, vol. 1, no. 14, pp. 35–52, 2005.

[5] Z. Lin, X. Zhao, K. M. Ismail, and K. M. Carley, "Organizational design and restructuring in response to crises: lessons from computational modeling and real-world cases," *Organization Science*, vol. 17, no. 5, pp. 598–618, 2006.

[6] G. A. Zsidisin, G. L. Ragatz, and S. A. Melnyk, "The dark side of supply chain management," *Supply Chain Management Review*, vol. 2, no. 9, pp. 46–52, 2005.

[7] M. Christopher and H. L. Lee, "Mitigating supply chain risk through improved confidence," *International Journal of Physical Distribution & Logistics Management*, vol. 34, no. 5, pp. 388–396, 2004.

[8] M. Christopher and H. Peck, "Building the resilient supply chain," *International Journal of Logistics Management*, vol. 2, no. 15, pp. 1–13, 2004.

[9] P. Blaikie, T. Cannon, I. Davis, and B. Wisner, *At Risk: Natural Hazards, People's Vulnerability, and Disasters*, Routledge, London, UK, 2014.

[10] P. Barnes and R. Oloruntoba, "Assurance of security in maritime supply chains: conceptual issues of vulnerability and crisis management," *Journal of International Management*, vol. 11, no. 4, pp. 519–540, 2005.

[11] L. Wang and Z. Y. Chu, "Literature review on vulnerability in supply chain," *Soft Science*, vol. 9, no. 25, pp. 136–139, 2011.

[12] V. Albino and A. C. Garavelli, "A methodology for the vulnerability analysis of just-in-time production systems," *International Journal of Production Economics*, vol. 41, no. 1–3, pp. 71–80, 1995.

[13] E. Prater, M. Biehl, and M. A. Smith, "International supply chain agility—tradeoffs between flexibility and uncertainty," *International Journal of Operations and Production Management*, vol. 21, no. 5-6, pp. 823–839, 2001.

[14] B. Zhong and T. Xie, "Research on the model of supply chain System's brittleness," *Chinese Journal of Management Science*, vol. 10, pp. 443–445, 2005.

[15] G. A. Svensson, "A conceptual framework for the analysis of vulnerability in supply chains," *International Journal of Physical Distribution & Logistics Management*, vol. 30, no. 9, pp. 731–749, 2000.

[16] G. Svensson, "A conceptual framework of vulnerability in firms' inbound and outbound logistics flows," *International Journal of Physical Distribution and Logistics Management*, vol. 32, no. 2, pp. 110–134, 2002.

[17] G. Svensson, "Sub-contractor and customer sourcing and the occurrence of disturbances in firms' inbound and outbound logistics flows," *Supply Chain Management*, vol. 8, no. 1, pp. 41–56, 2003.

[18] H. Peck, "Drivers of supply chain vulnerability: an integrated framework," *International Journal of Physical Distribution & Logistics Management*, vol. 35, no. 4, pp. 210–232, 2005.

[19] D. Bogataj and M. Bogataj, "Measuring the supply chain risk and vulnerability in frequency space," *International Journal of Production Economics*, vol. 108, no. 1-2, pp. 291–301, 2007.

[20] M. Stephan and N. N. Wagner, "Assessing the vulnerability of supply chains using graph theory," *Production Economics*, vol. 126, no. 1, pp. 121–129, 2010.

[21] Y. L. Fang, W. Song, and Z. Y. Wang, "Research of assessment and pre-warning of vulnerability of SMEs' independent intellectual property," *Economic Management Journal*, vol. 10, no. 31, pp. 141–146, 2009.

[22] F. Lolli, A. Ishizaka, R. Gamberini, B. Rimini, and M. Messori, "FlowSort-GDSS—a novel group multi-criteria decision support system for sorting problems with application to FMEA," *Expert Systems with Applications*, vol. 42, no. 17-18, pp. 6342–6349, 2015.

[23] F. Men and S. Q. Ji, "An improved FMEA based on fuzzy theory and gray Relational Theory," *Industrial Engineering and Management*, vol. 2, pp. 55–59, 2008.

[24] H.-C. Liu, P. Li, J.-X. You, and Y.-Z. Chen, "A novel approach for FMEA: combination of interval 2-tuple linguistic variables and gray relational analysis," *Quality and Reliability Engineering International*, vol. 31, no. 5, pp. 761–772, 2015.

[25] C. X. Zhang, "Improved QFD and integrated framework of FMEA," *Chinese Journal of Management*, vol. 2, no. 6, pp. 207–212, 2009.

[26] Y. Xiao and H. Li, "Improvement on judgment matrix based on triangle fuzzy numbe," *Fuzzy Systems and Mathematics*, vol. 2, no. 17, pp. 59–64, 2003.

[27] L. Liu, H. C. Liu, and Q. L. Lin, "An improved FMEA using fuzzy evidential reasoning approach and gray theory," *Fuzzy Systems and Mathematics*, vol. 2, no. 25, pp. 72–80, 2011.

[28] M. Vanhoucke, "Using activity sensitivity and network topology information to monitor project time performance," *Omega*, vol. 38, no. 5, pp. 359–370, 2010.

[29] Y. Li, P. Luo, and C. Wu, "Information loss method to measure node similarity in networks," *Physica A: Statistical Mechanics and its Applications*, vol. 410, pp. 439–449, 2014.

[30] J. Liu and Y. Zhou, "Improved FMEA application to evaluation of supply chain vulnerability," in *Proceedings of the 7th International Joint Conference on Computational Sciences and Optimization (CSO '14)*, pp. 302–306, Beijing, China, July 2014.