Analysis of vulnerability in ezship delivery process

YU-KAI HUANG [a], CHENG-MIN FENG [b], WEN-LING CHUNG [c]

[a] *Department of Culture & Creative Management, Nunhua University, Chiayi, 62249, Taiwan*
[a] *E-mail:osilo.huang@gmail.com*
[b, c] *Institute of Traffic and Transportation, National Chiao Tung University, Taipei, 10012, Taiwan*
[b] *E-mail: cmfeng@mail.nctu.edu.tw*
[c] *E-mail: orangesmile3.tt98g@nctu.edu.tw*

Abstract: Convenience stores in Taiwan have integrated e-commerce systems into their logistics systems to develop a new retail delivery model. ezShip is the one of the retail delivery systems served by CVS.com. Vulnerability is a new concept in risk analysis. The paper aims to discuss the vulnerabilities of the ezShip delivery process. This research is conducted with quantitative methodologies, Fault Tree Analysis (FTA), and Bayesian Network (BN). Firstly, we make interviews with experts to collect information of ezShip delivery system. Secondly, we map the FT of this system, and then convert it into BN. Finally, we evaluate BN and do predictive and diagnosis analyses to uncover the vulnerabilities in the ezShip process. With the results of the most vulnerable parts in ezShip delivery system, managers could add resources and formulate strategies to strengthen them and reduce the frequency of the events that have higher failure probabilities.

Keywords: Vulnerability, Store-to-Store delivery service, Fault tree analysis, Bayesian network

1. INTRODUCTION

The Internet is used widely as medium for social activities because information and communication technology (ICT) have been developed greatly. Retailers and customers use e-commerce systems because of it is convenient and inexpensive. Due to the dramatic growth of e-commerce, online shopping is becoming more and more popular. Online trading is not only business to customer (B2C), but also customer to customer (C2C). Internet users become the active players in the online C2C market. That is, people can trade with each other using e-commerce systems such as e-auctions.

Because online shopping is not constrained by space and timeliness, consumers from different places can use it at any time. This allows sellers to expand their markets easily. An efficient e-commerce system requires strong support from an efficient logistics system in order to send goods to customer quickly and securely. The difference between e-commerce development in Taiwan and in other countries is that there is a new logistics service called retail delivery or store-to-store service in Taiwan. This refers to customers shopping in an online store and then picking up the purchased goods in a convenience store. Taiwan has a high density of convenience stores. It is easy to find convenience stores in Taiwan. Also, most of stores in Taiwan provide 24-hours service. According to this operation model, they have already developed a mature retail delivery model. More and more famous e-commerce systems, such as KingStone, Yahoo, and PChome, cooperate with convenience stores to provide retail delivery service so that customers can pick up their products conveniently. There are two major companies serving retail delivery systems in Taiwan. One is 7-11.com, and the other is CVS.com. These systems receive more than one million orders per month online.

ezShip is the one retail delivery system that is served by CVS.com. CVS.com is a joint venture between three convenience store chains including FamilyMart, OK, and Hi-Life. In order to achieve proficiency, they should maintain reliability and efficiency. Nevertheless, the delivery process is complicated because different members and interfaces are involved. According to statistical data, there are over ten thousand problematic cases per month. This significantly increases their operating costs. Hence, it is necessary to understand the process well and engage in supply chain risk management to improve this system.

Vulnerability is a new concept in risk management. In recent years, a growing number of studies in different fields have examined this issue, particularly because of the recent series of catastrophes and hazards that impacted global economy causing large losses. Supply chain risk management (SCRM) is no exception. Although a substantial number of studies in supply chain vulnerability have been performed to date, most of them employed qualitative analysis. In addition, relatively little research has been conducted on a specific system or company. Therefore, this study is primarily concerned with the logistics of ezShip system and illustrates a quantitative approach to evaluating vulnerability. Overall, the objectives of this study are to examine all process used by ezShip and highlight all of the most vulnerable parts of the system, and then develop strategies to help improve system performance and, subsequently, reduce costs.

2. SUPPLY CHAIN VULNERABILITY

Because of increased frequency of hazard and catastrophe, risk management has been discussed in different fields. The influence of systems on risk consequences has been assessed in studies of climate change and natural hazard, and is characterized by the notion vulnerability (Zhang, 2007). The definition of vulnerability is various and depends on the different research field. Nick (2003) attempted to present a conceptual framework which may be applied consistently to the studies of vulnerability. He classified numerous definitions into two categories, biophysical vulnerability and social vulnerability. The former is broadly equivalent to the concept of risk, and the term “vulnerability” only refer to social vulnerability. On the whole, vulnerability represents the system sensitivity to external or internal disruptive events which remove the system from its standard working conditions (Albino & Garavelli, 1995).

Supply Chain disruption can have great impact on corporate financial performance, so it is widely accepted that supply chain risk management (SCRM) is necessary in today’s business (Wegner & Neshat, 2009). Supply chain vulnerability is a conceptual framework of supply chain risk management. Supply chain is exposed not only to the risks that come from external environment but also the risks caused by suboptimal interaction between the organizations within the network. That is, while a supply chain disruption is the situation that leads to the occurrence of risk, it is not the only determinant of the final result. However, the susceptibility of the supply chain to the harm of this situation seems significantly relevant. This leads to the concept of supply chain vulnerability. (Jutter *et al*., 2003, Wagner & Bode, 2006).

Wegner and Neshat (2009) interpreted the relationship between supply chain disruption and supply chain vulnerability, according to there point of view, corporate should identify the potential reasons that cause supply chain vulnerability. Hence, they can relocate their resource to improve supply chain performance and mitigate the risks of all system.

Even though there are different approaches to the construct “supply chain vulnerability”, Peck (2005) still appraises its conceptual basis as immature. Christopher and Peck (2004) define supply chain vulnerability as “an exposure to serious disturbance”. Svensson (2000) distinguishes between atomistic vulnerability (of a part of the supply chain) and holistic vulnerability (across the entire supply chain). Barnesand and Oloruntoba (2005) describe vulnerability as “a susceptibility or predisposition to loss because of existing organizational or functional practices or conditions” in their study in maritime supply chain. Wagner and Bode (2006) state that “supply chain vulnerability is a function of certain supply chain characteristics and the loss a firm incurs is a result of its supply chain vulnerability to a given supply chain disruption”. Wagner and Bode (2009) interpret further that supply chain characteristics are antecedents of supply chain vulnerability and have impact on both the probability of occurrence as well as the severity of supply chain disruptions.

In an overview of the definitions, we consider the definition by Wagner and Bode as reference. We define the delivery vulnerability that the properties of the delivery system construct the sensitivity of it. The sensitivity and loss of it when products delivering suffer from risks is considered as delivery system vulnerability.

3. EZSHIP

ezShip is an e-commerce RD system in Taiwan. It is provided by CVS.com, which is a joint venture run by three convenience store chains including FamilyMart, OK, and Hi-Life. It is the first system in Taiwan comprised of information and technology systems, and convenience stores chains and provides an integrated logistics service. The development of this logistics delivery model has provided a great deal of support to the C2C business model. Because the logistical cost of ezShip is lower than for home delivery, and almost the same as that of delivery through the post office, more and more customers are using this system. However, this system still has a lot of risks. That is because the different logistics system used by different convenience store chains need to be combined. Physical logistics systems and information systems need to be combined as well. Moreover, CVS.com promises quick delivery. They promise that “After the products are sent today, they will arrive at the selected CS before 6:00 a.m. the day after tomorrow.” All of these factors complicate the ezShip delivery process and increase the number of potential risks. There are more than ten thousand problematic cases per month on average. Those cases increase their operating costs. Hence, to reduce the risks in system, it is important to understand the process well.

As the upper part of Figure 1 shown, the process includes an information flow illustrated by thick dash lines and a product flow represented by solid lines. Firstly, sender can enter the receivers’ information and print the barcode attached to their products at home, or take products to a related convenience store using Familyport, which is an information kiosk provided by FamilyMart (only FamilyMart has this service). At this time, information is be uploaded to ezShip platform. After that, the sender takes the product and freight to the counter of the convenience store and then sends them. In the meanwhile, the information is transferred to IT, which is an outsourcing company that helps CVS.com to handle ezShip’s data and construct their database. Then, there are two different physical logistics system used by different companies. If senders send their goods to OK or FamilyMart convenience stores, the goods are dealt with by the Zi-Yi Corporation, which has their own fleet and distribution center. If the customer chooses a Hi-Life convenience store, the goods are handled by the

Hi-Life Corporation. When the goods are in the distribution center, the information is also uploaded to the ezShip system and IT identifies the data and volume of the products. Then a text message and e-mail are sent to inform the receiver when they can pick up their product from the store that they selected. These services depend on customers' requirements. They can request one of the services, or both. During this phase, IT is responsible for sending the text message and the e-mail is sent by the ezShip system. Finally, the product is delivered to the selected store, and the customer (receivers) can go to the store to pick up their product. If they don't go to pick up the product within a week, it will be considered returned goods. The products will be sent back to the distribution center.

To measure the system precisely and clearly, we assumed a goods delivery scenario (the lower part of Figure. 1). We specifically focus on the service, which includes all possible steps taken to deliver goods. Sellers (senders) deal with their orders and attach tags with barcode on the products at home. They may send multiple products at one time to the closest Hi-Life store. The products are then sent to the distribution center by a courier from Hi-Life distribution center. If there are some cases from Hi-Life to FamilyMart, they will be transferred to Zi-yi distribution center at this time. After that, products are distributed to the selected FamilyMart convenience store, and then buyers (receivers) will get their products at last. In addition, information is updated any time during the process.

In our hypothetical scenario we clearly identify all members involved and the tasks they must implement. The task of each member in ezShip delivery process is interpreted in Appendix 1. We will conduct our research with quantitative methods, fault tree analysis (FTA) and Bayesian network (BN), based on members' tasks, and analyze potential vulnerable parts in ezShip delivery process as well. In the next section, we will introduce our methodology to evaluate where the most vulnerable parts are in this system.

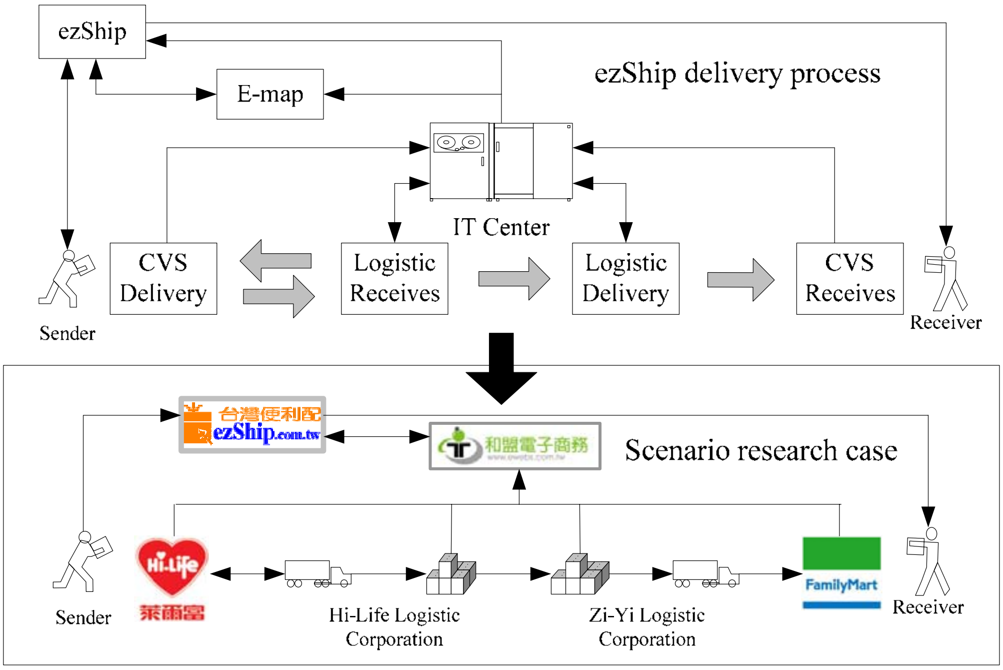

Figure 1. ezShip delivery process

4. METHODOLOGY

FTA is an inferential technique for dependability modeling and evaluation of an undesired event. FT is constructed in a top-down fashion. The Top Event (TE) is a critical situation that causes system failure. After that, each event that causes the root event is developed until all the basic components that cannot be developed further are reached. This methodology is based on four assumptions: 1. events are binary events (working or not-working). 2. events are statistically independent. 3. relationships between events and causes are represented by means of logical AND (as its symbol) and OR gates (as its symbol). 4. the root of FT is the undesired top event, to be analyzed. However, the third assumption is relaxed to allow the inclusion of the related gates.

An FT was used to analyze a single fault event. That means that only one event could be analyzed in a single fault tree. To construct and analyze an FT involves five steps.

1) Define the undesired event to study.
2) Obtain an understanding of the system.
3) Construct the fault tree.
4) Evaluate the fault tree
5) Control the hazards identified

Fault trees are built using gates and events. The two most commonly used gates in an FT are the AND and OR gates. For example, we considered a situation in which two events lead to a TE to occur. If the occurrence of either event caused the TE to occur, these events were connected using an OR gate (). Alternatively, if both events need to occur to cause the TE, they were connected by an AND gate ().

A Bayesian Network (BN) (Pearl, 1988) is a probability-based knowledge representation method, which is appropriate for the modeling of causal processes with uncertainty. It is based on the Baye' theorem, and can be used to denote causal inference. A BN is a directed acyclic graph (DAG) whose nodes represent random variables and whose links define probabilistic dependencies between variables. The nodes with arrows directed into them are called "child" nodes; and the nodes from which the edges depart are called "parent" nodes; and nodes without arrows directed into them are called "root" nodes. The DAG represents the structure of causal dependence between nodes and shows the qualitative part of causal reasoning in a BN. Thus, the relations between variables and the corresponding states provide the quantitative part, which consists of a conditional probability table (CPT) (Trucco *et. al.*, 2007). Diagnosis or prediction using BN is composed of fixing the values of the observed variables and computing the posterior probabilities of some of the unobserved variables (Kao *et. al.*, 2005).

Many learning techniques rely heavily on data. A BN, which is a knowledge representation, can provide new knowledge by combining expert domain knowledge with statistical data. The chain rule says that a BN is a representation of the joint distribution over all the variables represented in the DAG. Marginal and conditional probabilities can be computed for each node in the network.

Let BN be a Bayesian network over $U = \{X_1, X_2, X_3 ..., X_n\}$. BN specifies a unique joint probability distribution $P(U)$ given by the product of all conditional probability tables specified in BN:

$$P(U) = \prod_{i=1}^{n} P(X_i \mid Pa(X_i)) \tag{1}$$

where,

$Pa(X_i)$: the parents of X_i in BN,

$P(U)$: reflects the properties of BN.

Therefore, various marginal and conditional probabilities can be computed given an evidence *e*, as the following shows. The evidence is information received from external sources about the possible states of a subset of the variables of the network.

$$P(X_1, X_2, ..., X_n \mid e) = \frac{P(X_1, X_2, ..., X_n, e)}{P(e)} \quad (2)$$

A probabilistic inference is given that is capable to updating our belief about events given observations, and then it is possible to perform a sensitivity analysis of probabilities given different subsets of evidences. A mapping algorithm includes graphical and numerical tasks (Khakzad *et. al.*, 2010). In graphical mapping, the conversion algorithm proceeds along the following steps (Bobbio *et. al.*, 2001):

1) For each leaf node (i.e. primary event or system component) of the FT, create a root node in the BN; however, if more leaves of the FT represent the same primary event (i.e. the same component), create just one root node in the BN.
2) For each gate of the FT, create a corresponding node in the BN.
3) Label the node corresponding to the gate whose output is the TE of the FT as the Fault node in the BN.
4) Connect nodes in the BN as corresponding gates are connected in the FT

In numerical mapping, it is practiced with the following steps:

1) Assign to root nodes in the BN the prior probability of the corresponding leaf node in the FT (computed at a given mission time t).
2) For each gate (OR, AND) in the FT assign the equivalent CPT to the corresponding node in the BN.

Due to the very special nature of the gates appearing in a FT, non-root nodes of the BN are actually deterministic nodes and not random variables and the corresponding CPT can be assigned automatically. The prior probabilities on the root nodes are coincident with the corresponding probabilities assigned to the leaf nodes in the FT. However, in terms of complicated systems, uncertainty exists in causal relationships. The probability of occurrence of working or not working is not simply assigned a value of 1 or 0. Dependency among variables in a BN is not limited to being deterministic. This corresponds the ability to model uncertainty in the behavior of the gates by suitably specifying the conditional probabilities in the CPT entries. Probabilistic gates may reflect an imperfect knowledge of system behavior, or may avoid the construction of a more detailed and refined model.

When specifying CPT entries one has to condition the state of a variable on every possible instantiation of its parent variables. This makes the number of required entries exponential in terms of the number of parents. This is difficult and may result in the bias of relying on experts' knowledge to give all prior conditional probability when the structure of the BN is large and complex. Therefore, we modeled the BN using e risk analysis software, AgenaRisk.

AgenaRisk provides three approaches to input prior probability, Manual, Expression, and Partitioned Expression. If BN modeling is too complicated the prior probability has been obtained from experts and input manually, we can generate CPT by parameters setting and operations with functions which is supported by the function, expression. To generate the CPT, the weight of the parent nodes as evaluated by experts should be input in to the software. After doing this, we chose the most appropriate function for calculating the CPT. There are two ways to measure the vulnerability of the ezShip delivery system. First, we implemented predictive analysis. This was measured by means of the difference in conditional probability of failure occurrence of TE when different states, working or not-working are given. Second, we conducted a diagnostic analysis. We computed the result of each basic event when the different states of the top event were instantiated. Finally, we examined the most vulnerable parts in the system and then proposed strategies for improving them.

5. MODEL AND ANALYSIS RESULTS

5.1 Inference via FT and BN

CVS.com, which provides the ezShip service, promises that a product sent today will arrive at selected convenience store at 6:00 a.m. the day after tomorrow. Therefore, the most severe and undesired failure of this system one in which this commitment is broken. That is, the receiver waits longer than the promised amount of time to receive their goods. We collected information about the ezShip process through in-depth interviews. We interviewed experts including an ezShip general executive, two system engineers, and a scholar who understand the whole system well, and obtained failure probabilities for all of the basic events in the FT. The failure probability of each basic event was given based on the number of occurrences per month. To figure out the vulnerability of the ezShip delivery process, our study constructed an FT of the ezShip delivery process.

As shown in Figure 2, we set the most undesired event, which is "Buyers cannot get their goods on the third day" as the TE. It may be caused by either information flow or product flow problems, so there were two leaf events: Information failures and Physical logistics failures. Both leaf events were connected to the TE with the OR gate. That is, either of the two would lead to the TE. Two events were developed further according to the former analysis until either basic events or undeveloped events were reached. Undeveloped events such as unusual errors during the delivery process, problems with system scheduling, and unusual information system errors or breakdown, remained undeveloped because either attribute could cause any of these events, which places them beyond the scope of our scenario, or there was insufficient information. Table 1 contains descriptions of basic and undeveloped events, and their failure probability based on experts' experience. The failure probabilities we collected from experts were consistent, so we used the values given by the scholar.

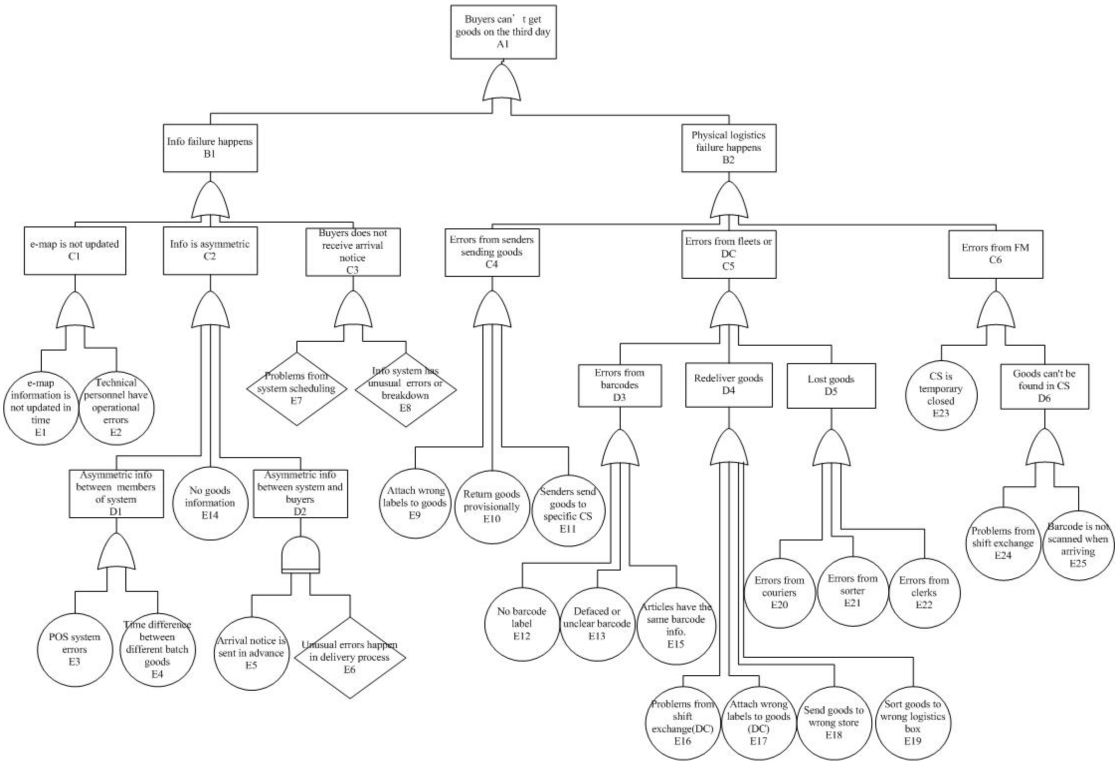
Buyers can' t get goods on the third day A1
Info failure happens B1
Physical logistics failure happens B2
e-map is not updated C1
Info is asymmetric C2
Buyers does not receive arrival notice C3
Errors from senders sending goods C4
Errors from fleets or DC C5
Errors from FM C6
e-map information is not updated in time E1
Technical personnel have operational errors E2
Problems from system scheduling E7
Info system has unusual errors or breakdown E8
Errors from barcodes D3
Redeliver goods D4
Lost goods D5
CS is temporary closed E23
Goods can't be found in CS D6
Asymmetric info between members of system D1
No goods information E14
Asymmetric info between system and buyers D2
Attach wrong labels to goods E9
Return goods provisionally E10
Senders send goods to specific CS E11
Problems from shift exchange E24
Barcode is not scanned when arriving E25
Errors from couriers E20
Errors from sorter E21
Errors from clerks E22
POS system errors E3
Time difference between different batch goods E4
Arrival notice is sent in advance E5
Unusual errors happen in delivery process E6
No barcode label E12
Defaced or unclear barcode E13
Articles have the same barcode info. E15
Problems from shift exchange(DC) E16
Attach wrong labels to goods (DC) E17
Send goods to wrong store E18
Sort goods to wrong logistics box E19

Figure 2. FT framework of ezShip delivery process

Table 1. Descriptions of basic and undeveloped events

	Event	Description	Prob.
E1	e-map information is not updated in time	Technical personnel do not update e-map information in time.	0.48%
E2	Technical personnel operational errors	Mistakes by technical personnel cause inaccurate e-maps.	0.24%
E3	POS system errors	Time lag between terminal computers and central computers, so data entry does not conform to the pieces sent to CS.	0.13%
E4	Time difference between different batches of goods	Data is updated by batching, so it causes goods delay processing.	0.19%
E5	Arrival notice is sent in advance	The goods arrival date does not conform to arrival notice.	0.29%
E6	Unusual errors during delivery	Unexpected events, such as natural hazards, delay goods.	0.45%
E7	Problems with system scheduling	Buyers do not receive the arrival notice in time because of system design and scheduling.	0.19%
E8	Unusual information system error or breakdown	Buyers do not receive arrival notice because the system breaks down.	0.17%
E9	Wrong labels attached to goods	Barcode labels are attached improperly, so barcode information doesn't match the goods.	0.34%
E10	Goods provisionally returned	Senders get their goods back provisionally. This causes imprecise information because the data in the IT system is not canceled.	0.13%
E11	Senders send goods to a specific CS	Buyers cannot receive goods on the third day because LF, OK, and some remote CSs don’t deliver goods on weekends	0.69%
E12	No barcode label	Barcode label is missing.	0.51%
E13	Defaced or unclear barcode	Barcode label is unrecognizable during scanning.	0.82%
E14	No goods information	Because of incomplete data entry there is missing information, such as receiver’s name or destination, when the barcode is scanned.	0.16%
E15	Articles have the same barcode info.	Barcodes with different articles show the same information.	0.12%
E16	Problems from shift changes (DC)	Errors occur during good processing because of shift changes.	0.79%
E17	Wrong labels attached to goods (DC)	The barcode labels are improperly attached when being switched from the sending to the receiving side, so the barcode information doesn't match the goods.	0.39%
E18	Goods sent to the wrong store	Courier sends goods to the wrong store.	0.55%
E19	Goods sorted to the wrong logistics box	Sorter sorts some goods to the wrong logistics box	0.61%

Table 1 (con.). Descriptions of basic and undeveloped events

Event		Description	Prob.
E20	Couriers errors	Goods are lost because of operational errors or carelessness.	0.15%
E21	Sorter errors		0.21%
E22	Clerk errors		0.55%
E23	CS is temporarily closed	CS is temporary closed.	0.17%
E24	problems from shift changes	Errors in goods processing cause by the clerk because of shift changes.	1.00%
E25	Barcode not scanned on arrival	Clerk does not scan the barcode of each package, so they cannot be found when receivers come to take them.	0.18%

For each basic event or undeveloped event on the FT, we created a root node in the BN, and created a corresponding node in the BN for each gate as well. Our BN framework was then constructed, as Figure 3 shown. Any event in the same level was assumed to be independent from the other ones in the FTA. However, there would be dependency between events in the same level because this system is too complicated. To construct a more practical and reliable BN, we interviewed experts to evaluate whether there are horizontal links between nodes. The red links in Figure 3 illustrate the relationship:

1) C1→C4：e-map is not updated→ Errors from senders sending goods.
2) C2→C5：Information is asymmetric→ Errors from fleets or DC.
3) D3→D4：Errors from barcodes→ Redeliver goods.
4) D5→D4：Lost goods→ Redeliver goods.
5) E3→E14：POS system errors →No goods information.
6) E16→E12：Problems from shift changes →No barcode label.
7) E16→E13：Problems from shift changes →Defaced or unclear barcode.
8) E21→E19：Sorter errors→ Goods sorted to the wrong logistics box.
9) E22→E17：Clerk errors→ Wrong labels attached to goods (DC).
10) E22→E25：Clerks errors→ Barcode not scanned upon arrival.

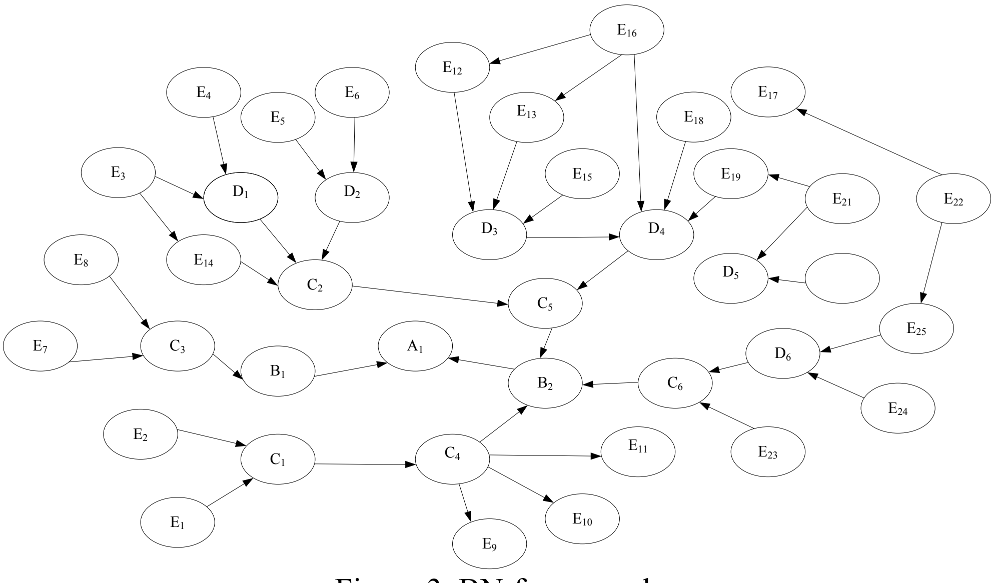

Figure 3. BN framework

The failure probabilities of the basic events in the FT were used as the prior probabilities of root nodes, and then the weight of each parent node was input into the properties of their non-root nodes. Our study attempts to measure the BN using different function types to find the closest result in relation to the real data. We learned that the best result came from using the WeightedMean to calculate the CPT of the nodes, which were converted from OR gate in the FT, and using the WeightedMin to calculate the CPT of the nodes that were converted from the AND gate in the FT.

5.2 THE RESULTS OF BN

Figure 4 shows the results of the BN. The marginal probabilities of all events are illustrated using a bar chart. Each event has two states. The upper blue bar of any event is the state *True*, which means there is a marginal probability of failure occurrence, and the lower blue bar of each event is the state of *False*, which means there is a marginal probability of no failure occurrence. The values of all probabilities are marked beside the bars.

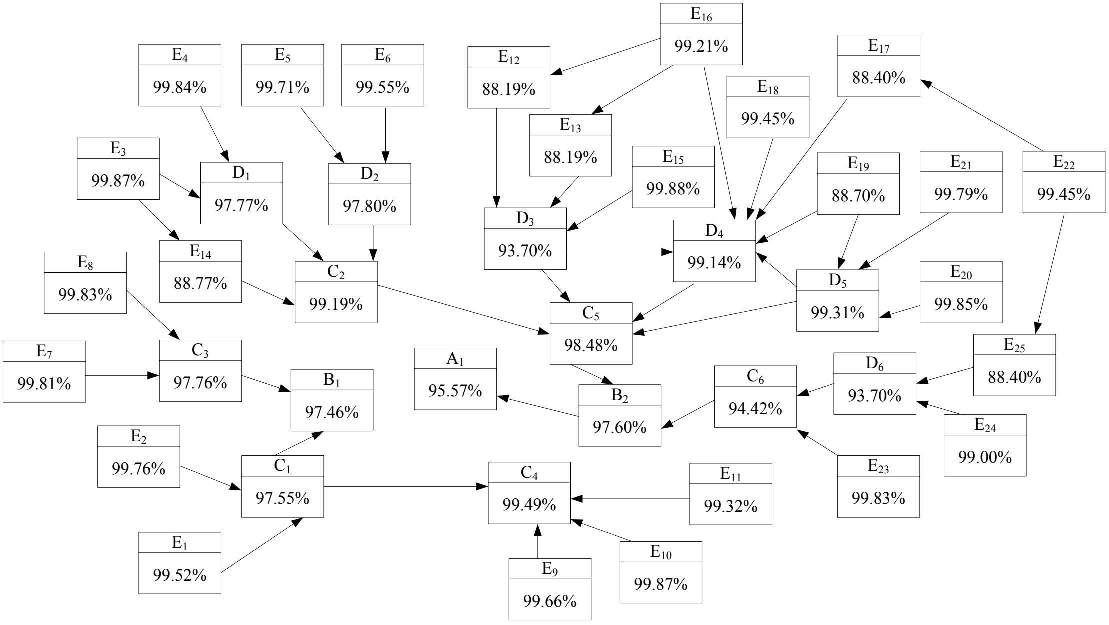

Figure 4. The result of BN

As the results show, the marginal probability that buyers do not receive goods on the third day (A_1) occurs, which is the TE for the FT, is 4.429%. It is slight underestimate, but quite similar to the real data, which was 5.94%. There may be a bias in the short-term data collected. In addition, the probabilities given by experts' were based on their long-term experience, so it is more stable and close to a normal situation compared to the real data. Therefore, we considered it to be a valid result and did an analysis using this framework.

Because of the factors which cause information and physical logistics failure, errors from FM (C_6) had the highest conditional probability, 5.584%, followed by asymmetric information (C_2), 4.807%, e-map not updated (C_1), 2.447%, buyer does not receive arrival notice (C_3) 2.238%, errors from fleets or DC (C_5), 1.518%, and errors from senders sending goods (C_4), 0.514%. This means that problems will happen more easily when receivers go to FamilyMart to pick up their goods. Additionally, failure caused by asymmetric information has higher conditional probability of occurrence. This is caused by things such as lack of goods information, and errors caused by unmatched receivers' information.

It should be noted that that the marginal probability of failure occurrence of information failure (B_1) is a little higher than physical logistics failure (B_2), which are 2.541% and 2.404% respectively. These results are very different from those of the FTA due to inclusion of uncertainty and potential dependency. In the next section, vulnerability of root nodes will be discussed.

5.3 Predictive analysis of conditional probability of A$_1$

A predictive analysis was conducted on the basis of the prior probabilities of the root nodes and the conditional dependency of each node. In order to discuss the relationships between the root nodes (Ei) and $A1$, $P(A1 = True \mid Ei = True)$ and $P(A1 = True \mid Ei = False)$ were calculated. They are presented in Table 2. Our study attempts to compare the conditional probabilities of failure occurrence of A$_1$ given evidence that Ei is $True$. We also try to figure out the impact on A$_1$ when the state of Ei changes from $False$ to $True$.

We specifically focused on the relationship between $P(A_1 = True \mid E_i = True)$ and $P(E_i = True)$. Figure 5 illustrates the relationship between them combined with their sensitivities. It is indicated whether or not a higher probability of failure occurrence for the root node contributes to a higher probability of failure occurrence for buyers do not receive goods on the third day. In Figure 6, the horizontal axis depicts the probabilities of the root nodes, $P(E_i = True)$, and the vertical axis depicts the conditional probabilities of A$_1$ given the evidence that Ei is $True$, $P(A_1 = True \mid E_i = True)$. Additionally, the radius of every circle is represented as a sensitivity, which is the difference in conditional probability from $False$ to $True$. We simply separated them into four areas by the averages of $P(E_i = True)$ and $P(A_1 = True \mid E_i = True)$, which are shown by the grey lines in the figure.

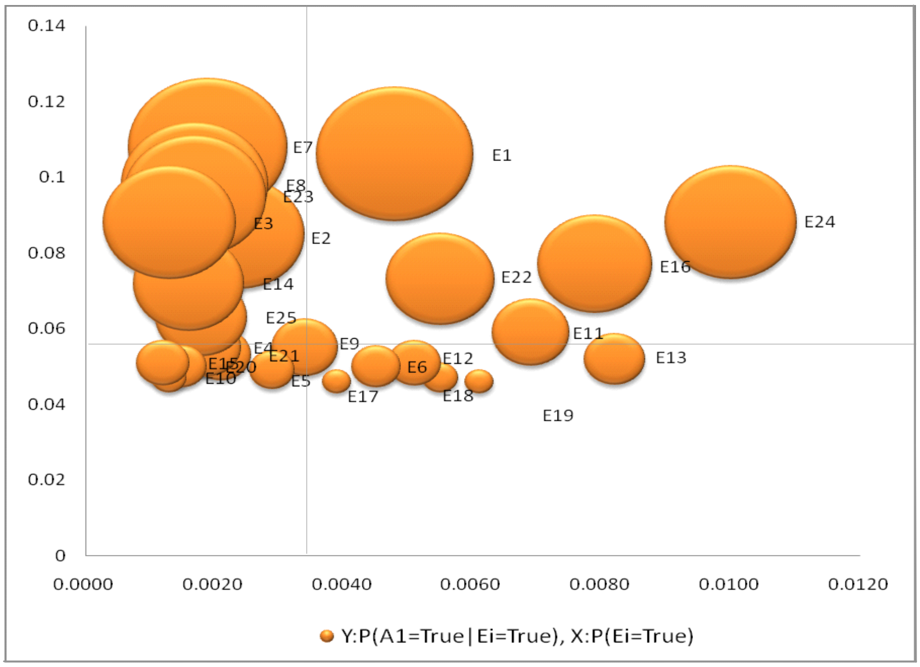

Figure 5 The relationship between root nodes and A1

The events in the upper area are considered to be the vulnerable parts because they lead to great increases in the conditional probability of an A$_1$ failure. It also indicates that the root nodes in upper right area have higher failure probabilities, and also cause higher conditional probabilities of failure occurrence of A1. They include: e-map information is not updated in time (E$_1$), problems from shift changes (E$_{24}$), problems from shift changes (DC) (E$_{16}$), and clerk errors (E$_{22}$). They also have higher conditional probabilities variations than average when the state of Ei changes from $False$ to $True$. This indicates that these events occur much easily, and have a considerable impact on A1 that we should not ignore.

Table 2. The result of $P(A_1 = True \mid E_i = True)$ and $P(A1 = True \mid Ei = False)$

No.	$P(A_1 = True \mid E_i = True)$	$P(A1 = True \mid Ei = False)$
E1	0.121	0.056
E2	0.101	0.058
E3	0.091	0.058
E4	0.068	0.058
E5	0.076	0.058
E6	0.077	0.058
E7	0.124	0.058
E8	0.114	0.058
E9	0.072	0.058
E10	0.064	0.058
E11	0.075	0.057
E12	0.080	0.054
E13	0.082	0.054
E14	0.083	0.055
E15	0.071	0.058
E16	0.102	0.055
E17	0.066	0.058
E18	0.067	0.058
E19	0.069	0.058
E20	0.070	0.058
E21	0.066	0.058
E22	0.069	0.058
E23	0.112	0.058
E24	0.101	0.054
E25	0.080	0.058

It is worth focusing on the root nodes in upper left area because they may be more vulnerable than the other ones. That is because their failure probabilities are lower, but they have a higher conditional probability of A1 failure occurrence. Problems with system scheduling (E_7), unusual information system errors or breakdown (E_8), CS is temporarily closed (E_{23}), POS system errors (E_3), technical personnel operational errors (E_2), and no goods information (E_{14}) are included in this area. In addition, their circles have the largest radiuses on average. This means they have greatest impact on A_1, although their failure probabilities are lower. If any of these events happen, it is more likely that buyers will not receive their goods on the third day.

5.4 Diagnostic analysis of conditional probability of Ei

A diagnostic analysis was done to compute the posterior probability of any given set of variables given some evidence. It was represented as instantiation of some of the variables to one of their acceptable values. This study computed the conditional probability of failure occurrence of each root node given $A1 = False$, which represents buyers do not receive goods on the third day does not happen ($P(Ei = True \mid A1 = False)$). Therefore, we can figure out the conditional probabilities of the failure occurrence of any event that we should maintain to ensure that buyers to receive their goods on time. $P(Ei = True \mid A1 = True)$ was also calculated in order to find variations. Table 3 lists the results.

Table 3. The result of $P(Ei = True \mid A1 = False)$ and $P(Ei = True \mid A1 = True)$

No.	$P(Ei = True \mid A1 = True)$	$P(Ei = True \mid A1 = False)$
E1	0.01146	0.00449
E2	0.00459	0.00230
E3	0.00257	0.00124
E4	0.00188	0.00158
E5	0.00322	0.00289
E6	0.00505	0.00447
E7	0.18205	0.10903
E8	0.00467	0.00177
E9	0.00375	0.00160
E10	0.00425	0.00336
E11	0.00139	0.00130
E12	0.00901	0.00670
E13	0.13571	0.11728
E14	0.13865	0.11711
E15	0.00139	0.00119
E16	0.01365	0.00763
E17	0.12155	0.11572
E18	0.00578	0.00549
E19	0.11810	0.11273
E20	0.00170	0.00149
E21	0.00254	0.00208
E22	0.00901	0.00534
E23	0.00366	0.00161
E24	0.01998	0.00954
E25	0.16475	0.11373

The conditional probabilities of the root nodes given that $A1 = False$ and $A1 = True$ are illustrated in Figure 6. The horizontal axis is represented as $P(Ei = True)$ and the vertical one is $P(Ei = True \mid A1)$. The curve with the diamond is the result of $P(Ei = True \mid A1 = True)$ and the one with the square is the result of $P(Ei = True \mid A1 = False)$. The variation in the conditional probability of failure occurrence in each root node when the state of A1 changes from $False$ to $True$ can then be seen.

Our study also separated the root nodes into four areas with mean values represented by the black lines shown in Figure 6. The events in the lower area are considered the vulnerable parts of the system because we have to keep these events at low conditional probabilities if we don’t want A_1 to occur. In the lower right area, it can be seen that the root nodes have higher failure probabilities and little change in their conditional probabilities of failure occurrence will cause the event, buyers do not receive goods on the third day. Problems from shift changes (E_{24}), Problems from shift changes (DC) (E_{16}), Senders send goods to a specific CS (E_{11}), clerk errors (E_{22}), goods sent to the wrong store (E_{18}), e-map information is not updated in time (E_1), unusual errors during delivery (E_6), and wrong labels attached to goods (E_9) are included in this area.

We also observed that the root nodes in the lower left area had lower failure probabilities, but only a small increase in their conditional probabilities of failure occurrence would cause the event, buyers do not receive goods on the third day. Articles have the same barcode information (E_{15}), POS system errors (E_3), goods provisionally returned (E_{10}), courier errors (E_{20}), CS is temporarily closed (E_{23}), unusual information system errors or breakdown (E_8), problems with system scheduling (E_7), time difference between different batches of goods (E_4), Sorter errors (E_{21}), technical personnel operational errors (E_2), and arrival notice sent in advance (E_5) are in this area.

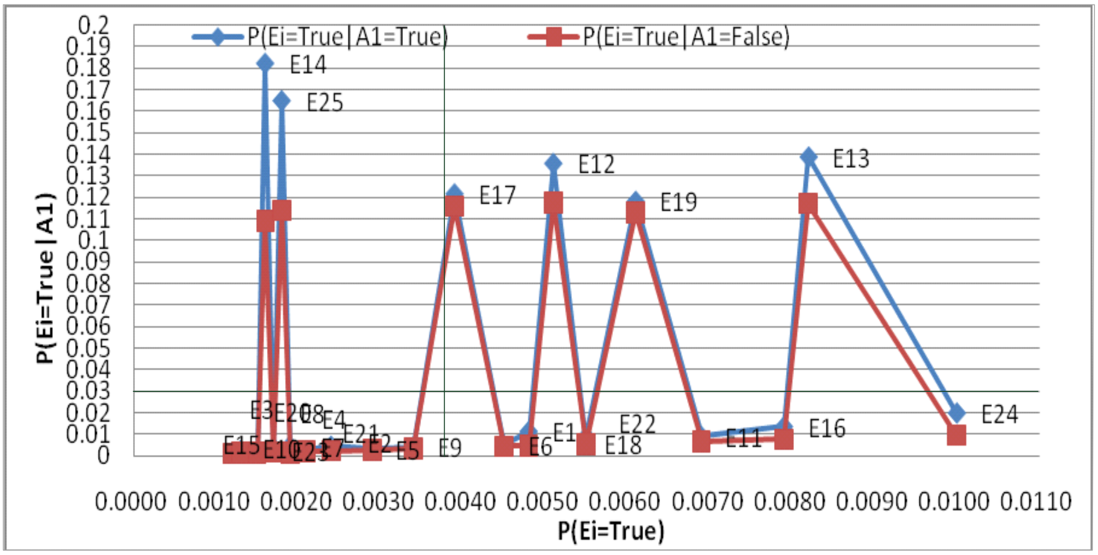

Figure 6 The result of $P(Ei = True \mid A1 = False)$ and $P(Ei = True \mid A1 = True)$

6. DISCUSSION

The real failure probability of buyers do not receive goods on the third day, 5.94%, is the average rate of problematic cases from August to October in 2010. It is apparent that the failure probability of A_1 in the FTA was a little higher than that of the real data. This is acceptable because the states of the gates are deterministic, working and not-working, do not include inherent uncertainty in the system. The conditional probability of failure occurrence of A_1 in BN is a little lower than that in the real data. This can be attributed to the time period of our data collection. Our real data was the average of problematic cases from three months. There may be bias caused by small amount of data. In addition, the probabilities were based on experts’ long-term experience, so they are more stable and closer to a normal situation compared to the data we collected. Therefore, we consider this result valid, which is better than that of the FTA.

In accordance with the result of BN from predictive analysis and diagnosis analysis, we can find out the most vulnerable root nodes. Our study classifies the result into four categories by the level of failure probability and two main causes of vulnerability in ezShip. e-map information is not updated in time (E_1) was categorized as information failure, and problems from shift changes (DC) (E_{16}), clerk errors (E_{22}), and problems from shift changes (E_{24}) were categorized as physical logistics failure. They all have higher failure probabilities and contribute to a higher conditional probability of failure occurrence of A1. Additionally, just small change in their conditional probabilities of failure occurrence, given the evidence of A_1, will lead to an occurrence of A_1. To sum up, these events have high failure probabilities and a great effect on A_1 occurrence.

These events are the most vulnerable parts in the ezShip delivery process, and most of them are caused by physical logistics failures, especially human mistakes, so ezShip managers should pay more attention to improving staff’s skills and implementing SOP intensively in order to reduce their failure probabilities.

The events that have lower failure probabilities are worth mentioning. Technical personnel operational errors (E_2), POS system errors (E_3), problems with system scheduling (E_7), and information systems have unusual errors or breakdown (E_8) belong to information failure, and CS is temporary closed (E_{23}) belongs to physical logistics failure. All of them had low failure probabilities, but they all greatly increase the conditional probability of A_1 occurrence than those that have higher failure probabilities. In addition, only a small change in their conditional probabilities of failure occurrence gives evidence that A_1 will occur. In brief, although these events do not happen easily, when any of these events happens they have a great impact on A_1 occurrence. They have a strong influence on buyers do not receive goods on the third day. Therefore, these events are also the most vulnerable parts in the ezShip delivery process.

These events are the most vulnerable in ezShip delivery system and most of them belong to information failure, so it is so important that managers of ezShip allocate more resources to maintaining the reliability and stability of information systems. With respect to CS is temporary closed, the ezShip website should provide this information in advance, or close this option to avoid customers choosing it.

7. CONCLUSSION AND SUGGESTIONS

Supply chain vulnerability is a new concept in risk management. There have been few studies that measure the vulnerability of local supply chains. Consequently, our study is aimed at discussing the vulnerability of the ezShip delivery process, which is part of a supply chain. FTA is a very popular technique for safety-critical systems. It provides a logical expression of casual relationships to construct a framework from TE to basic events. However, it has some limitations in practice. BN have become a widely used for representing uncertain knowledge in probabilistic systems. It expresses casual relationships based on a set of conditional probabilities. It can include uncertainty and be carried out in predictive and diagnostic analysis, but it is not easy to construct BN and obtain all probabilities directly from experts’ domain knowledge. Therefore, our study combined the two methodologies. We first constructed the FT logically, and then converted it into BN.

We consider researching the vulnerability of a system using both FT and BN to be feasible because FT provides a logical and simple way to construct a framework for a large, complicated system, and the results of the BN are reasonable and close to real data. Through predictive and diagnostic analyses, e-map information is not updated in time, problems from shift changes (DC), clerk errors, and problems from shift changes are the most vulnerable parts, with high failure probabilities in the ezShip delivery process. It was also found that technical personnel have operational errors, POS system errors, problems with system scheduling, has unusual information system errors or breakdown, and CS is temporarily closed were the most vulnerable parts with lower failure probabilities in the ezShip delivery process. Once any of them occurs, there will be a great impact on buyers do not receive goods on the third day. Moreover, little change in their conditional probabilities of failure occurrence will cause A1 to occur.

To summarize, it was found that most of the vulnerable parts with higher failure probabilities belonged to physical logistics failure. On the other hand, most of the vulnerable parts with lower failure probabilities belonged to information failure. This analytical result favors to CVS.com managers finding solutions. Then, ezShip can achieve good performance. For those vulnerable events that have higher failure probabilities, ezShip managers should pay more attention to improving staff's skills and implementing SOP intensively. We suggest that analyst should try to accumulate statistical data to evaluate the BN in order to achieve more objective results. In addition, BN allows events to include multiple states. Considering multiple states can increase the depth of the study. In our research, we only analyzed the relationship between A1 and each event. In the further research, we can consider events jointly to infer posterior probabilities and observe the relationships.

ACKNOWLEDGEMENTS: This work is supported by the National Science Council of Taiwan for providing the research grant (NSC 100-2410-H-343-027-).

REFERENCES

Albino, V., Garavelli, A.C. (1995) A methodology for the vulnerability analysis of just-in-time production systems. *International Journal Production Economic*, 41, 71-80.

Barnes, P., Oloruntoba, R. (2005) Assurance of security in maritime supply chains: conceptual issues of vulnerability and crisis management. *Journal of International Management*, 11(4), 519–540.

Bobbio, A., Portinale L., Minichino M., Ciancamerla E. (2001) Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety*, 71, 249-260.

Christopher, M., Peck, H. (2004) Building the resilient supply chain", *International Journal of Logistics Management*, 15(2), 1–13.

Jüttner, U., Peck, H., Christopher, M. (2003) Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), 197–210.

Kao, H.Y., Huang, C.H., Li, H.L. (2005) Supply chain diagnostics with dynamic Bayesian networks. *Computers and Industrial Engineering*, 49(2), 339-347.

Pearl, J. (1988). Probabilistic reasoning in intelligent systems, Morgan Kaufmann, San Mateo.

Peck, H. (2005) Drivers of supply chain vulnerability: an integrated framework. *International Journal of Physical Distribution & Logistics Management*, 35 (4), 210–232.

Svensson, G. (2000) A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management*, 30(9), 731–749.

Trucco, P., Cagno, E., Ruggeri, F., Grande, O. (2008) A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation. *Reliability Engineering and System Safety*, 93, 823-834.

Wagner, S.M., Bode, C. (2006 An empirical investigation into supply chain vulnerability. *Journal of Purchasing & Supply Management*, 12, 301–312.

Wagner, S.M., Bode, C., Koziol, P. (2009) Supplier default dependencies: empirical evidence from the automotive industry. *European Journal of Operational Research*, 199(1), 150–161.

Appendix 1 Functions of each member in ezShip

Member	Description of Function
Information Technology Corporations	1. Receive logistics information 2. Maintain and update e-map information 3. Set logistics information schedules 4. Transmit logistics information 5. Send arrival notices to receivers 6. Plan daily delivery routes in DC 7. CVS provide the new, deleted, and corrected information for stores
Senders	1. Enter the required delivery information into the platform 2. Print barcode labels online 3. Attach the label to the corresponding article 4. Send goods to LF
Hi-Life	1. Scan the barcode of each article 2. Store goods 3. Help sender attach barcode label 4. Print the waybill when an LF courier comes to receive goods 5. Take goods to the LF courier
Distribution Center	1. Scan the barcode of each article in LF DC 2. Sort goods into different CVSs (goods to FM are gathered) 3. Send Goods which destinations are to FM stores to FM DC 4. Switch barcode labels from the sending side to the receiving side 5. Package goods with specific package bags 6. Sort goods into different logistics boxes according to their destinations 7. Send goods to FM stores via courier
Family Mart	1. Receive and store goods 2. Scan barcodes 3. Give goods to receivers
Receivers	1. Choose the store where they want pick up their goods 2. Pick up their goods after receiving the arrival notice