International Journal of Automation and Computing 1 (2005) 85-92

A Subjective Risk Analysis Approach of Container Supply Chains

Zai-Li Yang, Jin Wang*, Steve Bonsall
School of Engineering, Liverpool John Moores University, Liverpool, L3 3AF, UK

Jian-Bo Yang
Manchester Business School, The University of Manchester, Manchester, M60 1QD, UK

Quan-Gen Fang
Merchant Marine College, Shanghai Maritime University, Shanghai, 200135, PRC

Abstract: After the 9/11 terrorism attacks, the lock-out of the American West Ports in 2002 and the breakout of SARS disease in 2003 have further focused mind of both the public and industrialists to take effective and timely measures for assessing and controlling the risks related to container supply chains (CSCs). However, due to the complexity of the risks in the chains, conventional quantitative risk assessment (QRA) methods may not be capable of providing sufficient safety management information, as achieving such a functionality requires enabling the possibility of conducting risk analysis in view of the challenges and uncertainties posed by the unavailability and incompleteness of historical failure data. Combing the fuzzy set theory (FST) and an evidential reasoning (ER) approach, the paper presents a subjective method to deal with the vulnerability-based risks, which are more ubiquitous and uncertain than the traditional hazard-based ones in the chains.

Keywords: Container supply chains, risk assessment, evidential reasoning, fuzzy sets, vulnerability.

1 Introduction

Container supply chains (CSCs), with many complex physical and information flows, have contributed themselves to economic prosperity and also rendered themselves uniquely vulnerable by many risks. In the past decade, some specific events closely related to the risks include the Kobe earthquake which affected supply chains across the globe in 1995; the Asian economic crisis in 1997; the Y2K-related IT problems at the end of the 20^{th} century; the fuel protest of September 2000 across Europe; the terrorist attacks of 11^{th} September 2001 in USA; the lock-out of American West Ports of October 2002; the breakout of SARS disease in the world in 2003; and the blasts of Madrid commuter trains in 2004[1,2]. These accidents showed that the definitions of the risks existing in the chains have changed and broadened forever. They, together with the complexity of CSCs in nature, have stimulated the research and development of novel risk analysis methods in the supply chain context.

A method for quantifying the reliability of supply chains for contingent logistics systems was developed based on a reliability interference theory[3]. Introducing the concept of Six Sigma into the field of supply chains, Garg et al.[4] developed and applied an innovative approach for designing Six Sigma supply chain networks to qualify reliable supply chains with synchronized delivery. After reviewing the existing techniques used in decision making for risk analysis, Pai et al.[5] presented a modelling and analysis framework for assessing logistics risks and evaluating safeguards to secure supply chains. Svensson[6] generated a framework for managing vulnerability in supply chains and analysed the vulnerability from firms' inbound and outbound logistics flows. Chapman et al.[1] identified supply chain vulnerability and used an advanced "3-P" approach to manage risks in logistics supply chains.

Although prior research has greatly increased our understanding that a) the risks in CSCs originate from vulnerability; b) effectively preventive actions may significantly reduce the frequency and damage of the risks, few studies have considered the vulnerability in the chains as the marriage of hazards and threats and also generated an appropriate approach to deal with highly uncertain situations resulting from those threats.

Many typical safety assessment approaches (such as a Qualitative Risk Assessment (QRA) approach), identified as deductive risk assessments, have been widely used and easily conducted based on historical data. However, such historical data is not always available, and its collection is time-consuming and expensive as well as depends on many uncertainties. Consequently,

Manuscript received August 27, 2004; revised July 13, 2005.

*Corresponding author. *E-mail address*: J.Wang@livjm.ac.uk

they may not be well suited for dealing with the CSC systems in situations of having a high level of uncertainty. One realistic way to cope with imprecision is to use linguistic assessments. However, such linguistic descriptions define risk assessment parameters to a discrete extent so that they can at times be inadequate. Fuzzy set theory is well suited to model such subjective linguistic variables and deal with discrete problems[7]. In the theory, such linguistic variables can be characterised by their membership functions to a set of categories, which describe the degrees of the linguistic variables.

From the viewpoint of risk analysis, a CSC can be regarded as a complex engineering system, which is constructed by some subsystems (i.e. ports and containerships) with the support of many components (i.e. cranes and engines). In such a hierarchical structure, it is usually the case that safety analysis at a higher level makes use of the information produced at lower levels. It is therefore extraordinarily important to synthesise the risk evaluations of the components in a rational way so as to obtain the risk evaluations of the subsystems and the whole system. Actually, the importance of such a synthesis means is further enforced by the requirements of combining all judgements of multiple experts on either one component or the whole system.

Unlike the risk evaluations in QRA, which are precisely expressed by some numerical values (e.g. potential loss of life), the risk evaluations using fuzzy sets are impossibly synthesized by using normal mathematic logical operations. An Evidential Reasoning (ER) approach is well suited to model subjective credibility induced by partial evidence. The kernel of this approach is an ER algorithm developed on the basis of the Dempster-Shafer (D-S) theory, which requires modelling the narrowing of the hypothesis set with the requirements of the accumulation of evidence[8].

The current study aims at developing a subjective risk assessment method by combining fuzzy set theory and an ER approach to deal with the uncertainty in CSCs. In order to achieve this purpose, the paper identifies the major problems of CSC risk analysis; creates four parameters to assess threat-based risks; applies a Fault Tree Analysis (FTA) method to construct a hierarchical structure so as to enable the application of the ER approach in the realm of supply chains; and validates its feasibility by a case study of terrorists attacking ports.

2 Major problems in the CSC risk analysis

The proposed subjective approach consists of the solutions of three major problems, which outline the necessary steps required for risk analysis using fuzzy set and ER methods.

2.1 Complex CSCs

Modern CSCs are very large and complex. A typical door-to-door journey using a shipping container will involve the interaction of approximately 25 different participants, generate 30-40 documents, use 2-3 different modes and be handled at as many as 12-15 physical locations[9]. Compared to other logistics systems, CSCs have two distinctive features. One is that both physical and information flows move in the same direction, although the information flow should always be ahead of the physical flow. The other is that another sub-flow – custody flow is identified under the umbrella of the physical flow in order to attempt critical assessment of the risks in the systems as comprehensively as possible.

Facing the complexity of the chains, the effective risk analysis requires a generic model to describe the functions, features, characteristics and attributes, which are common to all CSCs. The generic model is therefore not a 'typical' container transport chain considered in isolation but the hub of a chain of systems – with a physical cargo flow system at the centre, following an information flow system at the beginning and deciding a custody flow system at the end. Each of these systems interacts dynamically with the others at and across all levels to constitute a comprehensive picture of the CSC operation process, as shown in Fig.1.

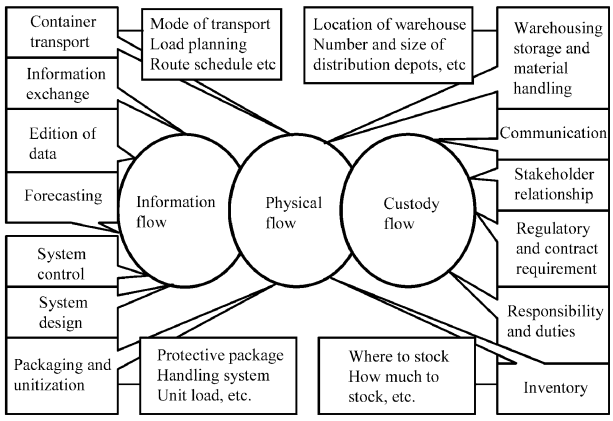


Fig.1 The generic model of CSCs

2.2 Definition of vulnerability

Although the vulnerability concept has been in use for more than twenty years since Timmerman's conceptualisation[10], presently, there is still no common conceptualization of vulnerability, and the meanings of vulnerability are still ambiguous and fuzzy[11]. Many of the discrepancies in the meanings of vulner-

ability arise from different epistemological orientations and subsequent methodological practices. In a supply chain context, vulnerability can be defined as 'an exposure to serious disturbances, arising from risks within the supply chain as well as risks external to the supply chain[1]'. However, the current research has indicated that either internal or external risks would originate from a hazard or threat. Thus, the vulnerability will be considered from another viewpoint – its nature and consequently is defined as 'an exposure to serious disturbances, arising from a hazard or threat'. Compared with Chapman et al.'s concept, the analysis from vulnerability nature will more redound to the risk analysis. After all, the first step to achieve any effective risk analysis is to better understand the true nature of those risks.

Further studying the definition of the vulnerability of the chains, one will appreciate the distinction between hazards and threats. Differing from the definition of a hazard, a threat can be defined as an action or a potential action rather than a physical situation likely to cause damage, harm or loss[12]. Threat-based risks are potentially greater than hazard-based risks because they are sometimes not within the focal companies' direct control. Furthermore, it may be difficult or even impossible to precisely determine the probability distribution of the parameters for a practical/potential action. Therefore, the emphasis of this container supply chain risk analysis is placed on those threat-based risks.

2.3 Application of FTA

FTA is a diagrammatic method used to evaluate the probability of an accident resulting from sequences and combinations of faults and failure events[13]. Because of its many advantages, specially in the combination of the qualitative and quantitative analysis to provide decision makers with an objective means of measuring the risk levels of a targeting system, FTA has been widely applied to the risk analysis of various industries, including logistics chains. The application of FTA to the current study, however, is worth noting the following:

i) *The qualitative FTA diagram is considered as a hierarchical structure to apply an ER approach.*

The hierarchical structure should be a qualitative FTA diagram, which means that the fault tree has been reduced to a logically equivalent form (minimal cut sets) by using the Boolean algebra in terms of the specific combination of basic events sufficient for the undesired top event to occur[14].

ii) *The weights of all events are distributed according to a specifically defined rule.*

The weights of all events in applying the ER method are determined considering that the fault tree, which can be considered as a hierarchical diagram, consists of many '*OR*' and '*AND*' gates. Therefore, a specific rule is required to assign the weights on a rational basis and defined as 'all input events of an '*OR*' gate are given the same weight equal to that of the output event of the gate, and the weights of all input events of an '*AND*' gate are assigned through dividing the weight of the output event of the gate by the number of the input events.

3 Subjective risk assessment of CSCs

3.1 Risk analysis using fuzzy sets

After the study of traditional quantitative safety methods like Failure Mode, Effects and Criticality Analysis (FMECA), it can be seen that there are three basic parameters – failure likelihood, consequence severity and failure consequence probability (i.e. the probability that possible consequences happen, given the occurrence of the failure), which are used in assessing the safety associated with each failure mode of a component and in determining safety level through "Safety scores"[7]. Given that the consequence severity of a threat is determined by its own damage capability and external recall ability, four new parameters are proposed to carry out threat-based risk estimation. They are "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*". The "*Will*" decides the failure likelihood of a threat-based risk. The combination of "*Damage capability*" and "*Recall difficulty*" responds to the consequence severity of the threat-based risk. The "*Damage probability*" represents the failure consequence probability of the risk.

In fuzzy set theory, linguistic variables that are used to describe the probability of the four parameters, can be characterised by their fuzzy set membership functions to a set of categories which describe the degrees of "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*" and which are usually graduated from low to high. The typical linguistic variables and their membership functions for the four parameters of a threat may be defined and characterised as shown in Tables 1-4. It is obviously possible to have some flexibility in the definition of membership functions to suit different situations.

Table 1 Will

Linguistic variables	Categories						
	1	2	3	4	5	6	7
Highly strong	0	0	0	0	0	0.75	1
Strong	0	0	0	0	0.75	1	0.25
Reasonably strong	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Reasonably weak	0	0.25	1	0.75	0	0	0
Weak	0.25	1	0.75	0	0	0	0
Very weak	1	0.75	0	0	0	0	0

Table 2 Damage capability

Linguistic variables	Categories						
	1	2	3	4	5	6	7
Extremely big	0	0	0	0	0	0.75	1
Big	0	0	0	0	0.75	1	0.25
Moderately big	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately small	0	0.25	1	0.75	0	0	0
Small	0.25	1	0.75	0	0	0	0
Extremely small	1	0.75	0	0	0	0	0

Table 3 Recall difficulty

Linguistic variables	Categories						
	1	2	3	4	5	6	7
Very difficult	0	0	0	0	0	0.75	1
Difficult	0	0	0	0	0.75	1	0.25
Moderately difficult	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately easy	0	0.25	1	0.75	0	0	0
Easy	0.25	1	0.75	0	0	0	0
Very easy	1	0.75	0	0	0	0	0

Table 4 Damage probability

Linguistic variables	Categories						
	1	2	3	4	5	6	7
Definite	0	0	0	0	0	0.75	1
Highly likely	0	0	0	0	0.75	1	0.25
Reasonably likely	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Reasonably unlikely	0	0.25	1	0.75	0	0	0
Unlikely	0.25	1	0.75	0	0	0	0
Absolutely unlikely	1	0.75	0	0	0	0	0

If W, D, R and P represent respectively "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*", the fuzzy safety score S can be defined by using the following fuzzy set manipulation, which is developed on the basis of Karowski's formula[15,7]:

$$S = (R \times D)^{\circ}(P \times W) \tag{1}$$

where the symbol "$\circ$" represents composition operation and "$\times$" the Cartesian product operation in the fuzzy set theory. The membership function of S is thus described by:

$$\mu_S = \mu_{(R\times D)^{\circ}(P\times W)}. \tag{2}$$

Judging from the above formula, the membership function of S is denoted by the membership values of four parameters (R, D, P and W) respectively. Suppose the membership values for the elements in S, R, D, P and W can be expressed as follows:

$$\begin{aligned}
&\mu_S = (\mu_S^1, \mu_S^2, \cdots, \mu_S^7)\\
&\mu_R = (\mu_R^1, \mu_R^2, \cdots, \mu_R^7)\\
&\mu_D = (\mu_D^1, \mu_D^2, \cdots, \mu_D^7)\\
&\mu_P = (\mu_P^1, \mu_P^2, \cdots, \mu_P^7)\\
&\mu_W = (\mu_W^1, \mu_W^2, \cdots, \mu_W^7).
\end{aligned} \tag{3}$$

Then, those fuzzy operations in Equation (2) can be analysed and described as follows:

i) Cartesian product. Two Cartesian product operations can be separately defined by:

$$\begin{aligned}
&\mu_{R\times D} = (\mu_{R\times D}^{ij})_{7\times 7}\\
&\mu_{P\times W} = (\mu_{P\times W}^{ij})_{7\times 7}
\end{aligned} \tag{4}$$

where $\mu_{R\times D}^{ij} = \min(\mu_R^i, \mu_D^j)$, $\mu_{P\times W}^{ij} = \min(\mu_P^i, \mu_W^j)$, both i and $j = 1, 2, \cdots, 7$.

ii) Composition. The composition operation can be defined by:

$$\mu_S = \mu_{(R\times D)^{\circ}(P\times W)} = (\mu_S^j)_{1\times 7} \tag{5}$$

where $\mu_S^j = \max(\max(\min(\mu_{R\times D}^{1i}, \mu_{P\times W}^{ij})), \max(\min(\mu_{R\times D}^{2i}, \mu_{P\times W}^{ij})), \cdots, \max(\min(\mu_{R\times D}^{7i}, \mu_{P\times W}^{ij})))$, both i and $j = 1, 2, \cdots, 7$.

However, μ_S obtained only presents a relative safety level, which can be measured in terms of the defined fuzzy safety expressions (i.e. "*Poor*", "*Fair*", "*Average*" and "*Good*"). In another word, the risk of a threat is required to be expressed by degrees to which it belongs to the safety expressions. The safety expressions defined on the basis of Tables 1-4 can be shown in Table 5 through satisfying the following conditions:

i) The expressions are exclusive for each category by normalizing the membership values of the variables.

ii) $S_{Poor} = (R_{Very\ difficult} \times D_{Extremely\ big})^{\circ}$ $(P_{Definite} \times W_{Extremely\ strong})$.

iii) $S_{Fair} = (R_{Moderately\ difficult} \times D_{Moderately\ big})^{\circ}$ $(P_{Reasonably\ likely} \times W_{Moderately\ strong})$.

iv) $S_{Average} = (R_{Moderately\ easy} \times D_{Moderately\ small})^{\circ}$ $(P_{Reasonably\ unlikely} \times W_{Moderately\ weak})$.

v) $S_{Good} = (R_{Very\ easy} \times D_{Extremely\ small})^{\circ}$ $(P_{Absolutely\ unlikely} \times W_{Extremely\ weak})$.

Table 5 Safety expressions

Linguistic variables	Categories						
	1	2	3	4	5	6	7
Poor	0	0	0	0	0	0.75	1
Fair	0	0	0	0.5	1	0.25	0
Average	0	0.25	1	0.5	0	0	0
Good	1	0.75	0	0	0	0	0

Using the Best-Fit method[7], the obtained fuzzy safety score description S_i of a threat judged by assessor i can be mapped onto one (or all) of the defined safety expressions. The method uses the distance between S_i and each of the safety expressions to represent the degree to which S_i is confirmed to each of them. For example, the distance between S_i and the safety expression "*Poor*" can be shown as follows:

$$d_{i1}(S_i, Poor) = \left[\sum_{k=1}^{7}(\mu_{S_i}^k - \mu_{Poor}^k)^2\right]^{1/2}. \tag{6}$$

The analyses for other distances between S_i and other safety expressions can be conducted in a similar way. The smaller the distance is, the closer S_i to the corresponding safety expressions. When the distance $d_{ij}(j = 1, 2, 3 \text{ or } 4)$ is equal to zero, S_i is just the same as the jth safety expression in terms of membership functions. Because each d_{ij} is an unscaled distance, in order to more clearly express the safety level of S_i, the reciprocals of the relative distances between S_i and each safety expression d_{ij} are normalised into a new index $\alpha_{ij}, (j = 1, 2, 3, 4)$. If $d_{ij} = 0$ it follows that α_{ij} is equal to 1 and the others are equal to 0. The α_{ij} can be defined as follows in other situations:

$$a_{ij} = \frac{1/d_{ij}}{\sum_{j=1}^{4} 1/d_{ij}}, \ j = 1, 2, 3, 4. \tag{7}$$

Each $\alpha_{ij}(j = 1, 2, 3, 4)$ represents the extent to which S_i belongs to the jth defined safety expression. Thus, the safety levels of threat-based risks determined by using a fuzzy set can be expressed as follows:

$$S(S_i) = \{(\alpha_{i1}, \text{“}Poor\text{”}), (\alpha_{i2}, \text{“}Fair\text{”}), (\alpha_{i3}, \text{“}Average\text{”}), (\alpha_{i4}, \text{“}Good\text{”})\}.$$

To produce the risk degree of a threat for ranking purposes, it is necessary to describe the four safety expressions using numerical values. The numerical values associated with the defined safety expressions can be calculated by studying the categories and membership values in Table 5. Suppose W'_p, W'_f, W'_a and W'_g represent the unscaled numerical values associated with “*Poor*”, “*Fair*”, “*Average*” and “*Good*”, respectively. W'_s, W'_m, W'_p and W'_g can be calculated as follows:

$$\begin{aligned}
W'_p &= [0.75/(0.75+1)] \times 0.83 + [1/(0.75+1)] \times 1 = 0.927 \\
W'_f &= [0.5/(0.5+1+0.25)] \times 0.5 + [1/(0.5+1+0.25)] \\
&\quad \times 0.67 + [0.25/(0.5+1+0.25)] \times 0.83 = 0.644 \\
W'_a &= [0.25/(0.25+1+0.5)] \times 0.17 + [1/(0.25+1+ \\
&\quad 0.5)] \times 0.33 + [0.5/(0.25+1+0.5)] \times 0.5 = 0.356 \\
W'_g &= [1/(1+0.75)] \times 0 + [0.75/(1+0.75)] \times 0.17 = 0.073.
\end{aligned} \tag{8}$$

The above values give numerical relations between the safety expressions. The reciprocally normalized vector $[w_p, w_f, w_a, w_g]$ is then obtained as follows, where “Good” takes the largest value of 1 (i.e. $w_g = 1$):

$$[w_p, w_f, w_a, w_g] = [0.079, 0.384, 0.695, 1].$$

Naturally, a numerical risk degree of the threat, can be obtained by the following calculation:

$$P_{S(Si)} = \alpha_{i1} \times 0.079 + \alpha_{i2} \times 0.384 + \alpha_{i3} \times 0.695 + \alpha_{i4} \times 1. \tag{9}$$

3.2 Synthesis of safety evaluations by hierarchical ER

The $S(S_i)$ obtained represents only the piece of estimation from one assessor. When more pieces of estimation from different assessors emerge, they can be effectively synthesized by using an ER approach. The approach has been widely applied to risk and safety assessment[7]. In continuously researching and practicing processes, the evidential reasoning algorithm has been developed, improved and modified toward a more rational way[8]. The algorithm can be analysed by the following pathway.

Let A represent the set of the four safety expressions, which has been synthesized by two subsets A_1 and A_2 from two different assessors. Then, A, A_1 and A_2 can separately be expressed by:

$$\begin{aligned}
A &= \{\alpha^1 \text{“}Poor\text{”}, \alpha^2 \text{“}Fair\text{”}, \alpha^3 \text{“}Average\text{”}, \alpha^4 \text{“}Good\text{”}\} \\
A_1 &= \{\alpha_1^1 \text{“}Poor\text{”}, \alpha_1^2 \text{“}Fair\text{”}, \alpha_1^3 \text{“}Average\text{”}, \alpha_1^4 \text{“}Good\text{”}\} \\
A_2 &= \{\alpha_2^1 \text{“}Poor\text{”}, \alpha_2^2 \text{“}Fair\text{”}, \alpha_2^3 \text{“}Average\text{”}, \alpha_2^4 \text{“}Good\text{”}\}.
\end{aligned}$$

Suppose the normalized relative weights of two safety assessors in the safety evaluation process are given as ω_1 and $\omega_2(\omega_1 + \omega_2 = 1)$ and ω_1 and ω_2 can be estimated by using established methods such as simple rating methods or more elaborate methods based on pair-wise comparisons.

Suppose M_1^m and M_2^m $(m = 1, 2, 3 \text{ or } 4)$ are individually degrees to which the subsets A_1 and A_2 support the hypothesis that the safety evaluation is confirmed to the four safety expressions. Then, M_1^m and M_2^m can be obtained as follows:

$$M_1^m = \omega_1 \alpha_1^m, \quad M_2^m = \omega_2 \alpha_2^m \tag{10}$$

where $m = 1, 2, 3, 4$. Therefore,

$$\begin{aligned}
M_1^1 &= \omega_1 \alpha_1^1, \quad M_2^1 = \omega_2 \alpha_2^1 \\
M_1^2 &= \omega_1 \alpha_1^2, \quad M_2^2 = \omega_2 \alpha_2^2 \\
M_1^3 &= \omega_1 \alpha_1^3, \quad M_2^3 = \omega_2 \alpha_2^3 \\
M_1^4 &= \omega_1 \alpha_1^4, \quad M_2^4 = \omega_2 \alpha_2^4.
\end{aligned} \tag{11}$$

Suppose H_1 and H_2 are the individual remaining belief values unassigned for M_1^m and $M_2^m (m = 1, 2, 3, 4)$. Then, H_1 and H_2 can be expressed as follows[8]:

$$H_1 = \bar{H}_1 + \tilde{H}_1, \quad H_2 = \bar{H}_2 + \tilde{H}_2 \tag{12}$$

where $\bar{H}_n (n = 1 \text{ or } 2)$, which represents the degree to which the other assessor can play a role in the assessment, and $\tilde{H}_n (n = 1 \text{ or } 2)$, which is caused due to the

possible incompleteness in the subsets A_1 and A_2, can be described as follows respectively:

$$\bar{H}_1 = 1 - \omega_1 = \omega_2, \quad \bar{H}_2 = 1 - \omega_2 = \omega_1 \tag{13}$$

$$\tilde{H}_1 = \omega_1(1 - \sum_{m=1}^{4} a_1^m) = \omega_1[1 - (\alpha_1^1 + \alpha_1^2 + \alpha_1^3 + \alpha_1^4)]$$

$$\tilde{H}_2 = \omega_2(1 - \sum_{m=1}^{4} a_2^m) = \omega_2[1 - (\alpha_2^1 + \alpha_2^2 + \alpha_2^3 + \alpha_2^4)].$$

Suppose $\alpha^{m'}(m = 1, 2, 3 \text{ or } 4)$ represents the non-normalized degree to which the safety evaluation is confirmed to the four safety expressions as a result of the synthesis of the judgments produced by assessors 1 and 2. Suppose H'_U represents the non-normalized remaining belief unassigned after the commitment of belief to the four safety expressions as a result of the synthesis of the judgments produced by assessors 1 and 2. The evidential reasoning algorithm can be stated as follows:

$$\begin{aligned} \alpha^{m'} &= K(M_1^m M_2^m + M_1^m H_2 + H_1 M_2^m) \\ \bar{H}'_U &= K(\bar{H}_1 \bar{H}_2) \\ \tilde{H}'_U &= K(\tilde{H}_1 \tilde{H}_2 + \tilde{H}_1 H_2 + H1 \tilde{H}_2) \\ K &= [1 - \sum_{T=1}^{4} \sum_{\substack{R=1 \\ R \neq T}}^{4} M_1^{\mathrm{T}} M_2^R]^{-1}. \end{aligned} \tag{14}$$

After the above aggregation, the combined degrees of belief are generated by assigning $\bar{H}'_U$ back to the four safety expressions using the following normalization process:

$$\begin{aligned} a^m &= a^{m'}/1 - \bar{H}'_U (m = 1, 2, 3, 4) \\ H_U &= \tilde{H}'_U/1 - \bar{H}'_U \end{aligned} \tag{15}$$

where H_U is the unassigned degree of belief representing the extent of incompleteness in the overall assessment.

The above gives the process of combining two fuzzy sets. If three fuzzy sets are required to be combined, the result obtained from the combination of any two sets can be further synthesized with the third one using the above algorithm. In a similar way, multiple fuzzy sets from the judgements of multiple assessors or the safety evaluations of lower level risks in the chain systems (i.e. components or subsystems) can also be combined. The two different and noteworthy points are that the relative weights of every assessor will be normalized first; and the relative weights of the lower level risks should satisfy the requirements of the specific rule in Section 2.3 and a normalized distribution.

4 A risk analysis of terrorists attacking ports

The American West Coast Ports 11-day lock-out in October 2002 has caused a growing concern on how serious the impacts of a major sophisticated attack related to container ports can be. Such a concern has further been underscored by progressive terrorism groups' activities. Therefore, in this section, risk analysis is carried out to assess the safety level of ports in CSCs and identify the major factors causing the risk on a proritised list.

Terrorists attacking ports would highly likely happen through two ways: to attack the channel/ waterway or bomb the quayside infrastructures/ facilities of the terminals. Using the FTA method, a fault tree related to a terrorism threat in ports can be constructed in Fig.2.

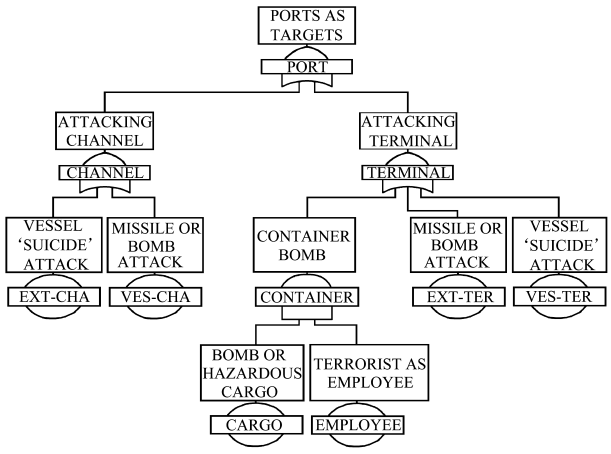


Fig.2 A fault tree of terrorists attacking ports

Following the fault tree, the basic events can be ranked in terms of their risk levels using the fuzzy set approach described. The risk level of the top event can be calculated using the ER approach. The estimation and calculation of the risk levels can be conducted as follows:

Step 1. assigns the relative weights of the events in Fig.2 using the rule in Section 2.3, where the top event is assigned value 1 as its weight. The results of the assignments are shown in Table 6.

Table 6 The weight assignments of all events

Events	Weights	Events	Weights
PORT	1	CONTAINER	1
CHANNEL	1	EXT-TER	1
TERMINAL	1	VES-TER	1
EXT-CHA	1	CARGO	0.5
VES-CHA	1	EMPLOYEE	0.5

Step 2 calculates the safety scores of the basic events on the basis of the fuzzy estimations of the four parameters from Tables 1-4. The safety scores are calculated by using the fuzzy operations of the formula

'$\mu_S = \mu_{(R\times D)\circ(P\times W)}$' and the Best-Fit method in Section 3.1. The ranking of the basic events can then be obtained using the method of studying the fuzzy membership values and categories. The results of the calculation are shown in Table 7.

Step 3. applies the ER approach and its attached software IDS (Intelligent Decision System via Evidential Reasoning)[8] to calculate the safety level of the top event which can be expressed by its safety score shown in Fig.3:

$$S_{Terrorism} = \{0.276, \text{“}Poor\text{”}, 0.461, \text{“}Fair\text{”}, 0.17, \text{“}Average\text{”}, 0.093, \text{“}Good\text{”}\}.$$

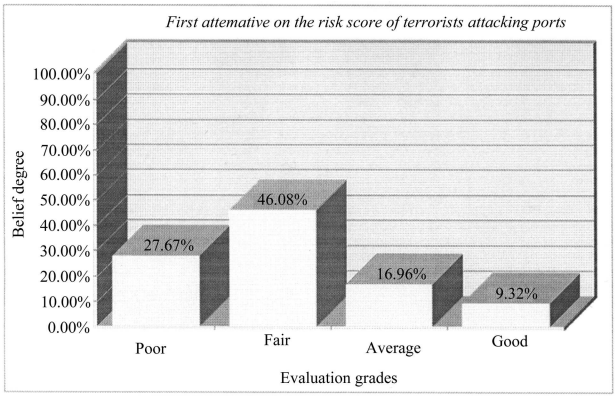


Fig.3 The safety level expressed by safety score

From the above results, it is obvious that the six basic events (i.e. EXT-CHA and VES-CHA) have been assessed as 'Good' to a quite small extent. For example, the event EXT-CHA has been assessed as 'Good' with a belief of 13.9 percent; the event VES-CHA has been evaluated to a significantly smaller extent as 'Good' with 1.8 percent. Since the safety of the top event is determined by the safety of each basic event, the top event safety should be evaluated as 'Good' to a small extent. This is in harmony with the results obtained above as the safety of the top event has been assessed as 'Good' to the extent of 9.3 percent.

The above gives an overall picture of the safety estimate of this top event. The safety score representing the safety level of the top event can be seen as a reference for considering the effectiveness of risk control options and the comparison with other hazardous events for making decisions if necessary.

5 Conclusion

The safety consciousness in the supply chain industry has been significantly growing over the last several years. This paper providing a subjective risk assessment method for the organisations involved in CSCs enables them to assess the vulnerability of the chains and to support the safety planning for both mitigating and continuity actions. The marriage of fuzzy sets and ER to deal with uncertainty can also facilitate risk assessment and be tailored and applied to more management-related industries, where risks usually arise from threats rather than hazards.

References

[1] P. Chapman, M. Christopher, U. Jüttner, H. Peck, R. Wilding, Identifying and managing supply-chain vulnerability, *Logistics & Transport Focus*, vol. 4, no. 4, pp. 17, 2002.

[2] Z. L. Yang, S. Bonsall, W. Alan, J. Wang, Reliable container line supply chains - a new risk assessment framework for improving safety performance, *WMU Journal of Maritime Affairs*, vol. 4, no. 1, pp. 107–122, 2005.

[3] M. U. Thomas, Supply chain reliability for contingency operations, *Annual Reliability and Maintainability Symposium*, pp. 61–67, WA, USA, 2002.

[4] D. Garg, Y. Narahari, N. Viswanadham, Design of Six Sigma supply chains, *Proceedings - IEEE International Conference on Robotics and Automation*, pp. 1737–1742, Taibei, 2003.

[5] R. R. Pai, V. R. Kallepalli, R. J. Caudill, M. C. Zhou, Methods towards supply chain risk analysis, *Proceedings of the IEEE International Conference on Systems*, Man and Cybernetics, vol. 5, pp. 4560–4565, 2003.

[6] G. Svensson, A conceptual framework of vulnerability in firms' inbound and outbound logistics flows, *International*

Table 7 The risk estimation of all basic events

Basic events	Parameters				Safety Scores	Risk Rank
	W	D	R	P		
EXT-CHA	W = {0, 0.25, 1, 0.75, 0, 0, 0}	D = {0, 0, 0.5, 1, 0.5, 0, 0}	R = {0, 0, 0.5, 1, 0.5, 0, 0}	P = {0, 0, 0, 0.75, 1, 0.25, 0}	S = {0.139, “Poor”, 0.361, “Fair”, 0.361, “Average”, 0.139, “Good”}	0.44 4
VES-CHA	W = {0, 0, 0, 0, 0.75, 1, 0.25}	D = {0, 0, 0, 0, 0, 0.75, 1}	R = {0, 0, 0, 0, 0,75, 1, 0.25}	P = 0, 0, 0, 0.75, 1, 0.25, 0	S = {0.021, “Poor”, 0.934, “Fair”, 0.027, “Average”, 0.018, “Good”}	0.31 1
CARGO	W = {0, 0, 0, 0, 0, 0.75, 1}	D = {0, 0, 0, 0, 0.75, 1, 0.25}	R = {0, 0, 0.5, 1, 0.5, 0, 0}	P = {0, 0, 0.5, 1, 0.5, 0, 0}	S = {0.444, “Poor”, 0.199, “Fair”, 0.184, “Average”, 0.173, “Good”}	0.4115 3
EMPLOYEE	W = {0, 0, 0.5, 1, 0.5, 0, 0}	D = {0, 0.25, 1, 0.75, 0, 0, 0}	R = {0, 0.25, 1, 0.75, 0, 0, 0}	P = {0, 0, 0, 0.75, 1, 0.25}	S = {0.139, “Poor”, 0.361, “Fair”, 0.361, “Average”, 0.139, “Good”}	0.44 4
EXT-TER	W = {0, 0.25, 1, 0.75, 0, 0, 0}	D = {0, 0, 0.5, 1, 0.5, 0, 0}	R = {0, 0, 0.5, 1, 0.5, 0, 0}	P = {0, 0, 0, 0.75, 1, 0.25, 0}	S = {0.139, “Poor”, 0.361, “Fair”, 0.361, “Average”, 0.139, “Good”}	0.44 4
VES-TER	W = {0, 0, 0, 0., 0.75, 1, 0.25}	D = 0, 0, 0, 0, 0.75, 1, 0.25	R = {0, 0, 0.5, 1, 05, 0, 0}	P = {0, 0, 0, 0, 0.75, 1, 0.25}	S = {0.686, “Poor”, 0.119, “Fair”, 0.101, “Average”, 0.094, “Good”}	0.324 2

Journal of Physical Distribution and Logistics Management, vol. 32, no. 2, pp. 110–134, 2002.

[7] J. Wang, J. B. Yang, P. Sen, Multi-person and multi-attribute design evaluations using evidential reasoning based on subjective safety and cost analyses, *Reliability Engineering and System Safety*, vol. 52, no. 2, pp. 113–128, 1996.

[8] J. B. Yang, D. L. Xu, On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty, *IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans*, vol. 32, no. 3, pp. 289–304, 2002.

[9] OECD, Security in maritime transport: risk factors and economic impact, *Maritime Transport Committee of OECD Report*, France, 2003.

[10] P. Timmerman, Vulnerability, resilience and the collapse of society, *Institute of Environmental Studies*, University of Toronto, Toronto, 1981.

[11] J. Weichselgartner, Disaster mitigation: the concept of vulnerability revisited, *Disaster Prevention and Management*, vol. 10, no. 2, pp. 85–94, 2001.

[12] H. T. Burns, P. Cordire, T. Eriksson, *Security Risk Assessment and Control*, Perpetuity Press Ltd., Leicester, UK, 2003.

[13] A. Pillay, J. Wang, *Technology and Safety of Marine Systems*, Elsevier Science Ltd., Oxford, UK, 2003.

[14] E. J. Henley, H. Kumarnoto, *Probability Risk Assessment*, IEEE Press, NY, USA, 1992.

[15] W. Karwowski, A. Mital, Potential applications of fuzzy sets in industrial safety engineering, *Fuzzy Sets and Systems*, vol. 19, no. 2, pp. 105–120, 1986.

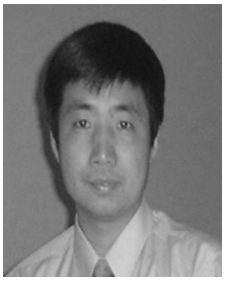
Zaili Yang received his BSc in Foreign Trade Transportation from Dalian Maritime University, China in 2001 and MSc in International Transport from Cardiff University, UK in 2003, respectively. Since 2003, he has been a PhD student in the School of Engineering of Liverpool John Moores University, UK. His research interests include risk assessment of container supply chains, in particular, subjective risk analysis using fuzzy set and Bayesian probability theories.

Jin Wang received his BSc in Marine Automation from Dalian Maritime University, China in 1983, MSc in Marine Engineering and PhD in Maritime Safety Engineering from the University of Newcastle upon Tyne in 1989 and 1994, respectively. He is Professor of Marine Technology at the School of Engineering of Liverpool John Moores University, UK.

Professor Wang's major research interests include safety and reliability based design and operations of large marine and offshore systems.

Steve Bonsall received his BSc in Marine Science from Liverpool Polytechnic, UK in 1977 and PhD in Maritime Technology from Liverpool John Moores University, UK in 2001, respectively. He is currently the maritime programme coordinator and principal lecturer at the School of Engineering of Liverpool John Moores University, UK.

Dr. Bonsall's major research interests include container terminal operations, container supply chains and developments in maritime leisure.



Jian-Bo Yang received his BEng and MEng degrees in Control Engineering at North Western Polytechnic University, Xi'an, China in 1981 and 1984, and PhD degree in Systems Engineering at Shanghai Jiao Tong University, Shanghai, China in 1987. He is Chair of Decision and System Sciences at the Manchester Business School, The University of Manchester, UK.

Professor Yang's main research interests include intelligent decision analysis and support under uncertainties, multiobjective optimisation, system modelling, simulation and control with applications in both engineering and management systems.

Quangen Fang received his BSc in Navigation from Shanghai Maritime University, China in 1976 and MSc in Maritime Education and Training from World Maritime University, Sweden in 1991, respectively. He is currently a professor and Director of the Navigation Simulator Training Centre of Shanghai Maritime University, China.

Professor Fang's major research interests include ship simulation, navigation studies and ship operations.