© Marine Technology, Vol. 46, No. 2, April 2009, pp. 61–73

Marine Technology

The Risk Assessment and Management of Port Security Using Fuzzy Modeling

S. T. Ung,[1] **V. Williams,**[2] **S. Bonsall,**[2] and **J. Wang**[2]

A security assessment is considered to be a difficult mission because of the characteristically unpredictable outcomes associated with high consequences. This study offers an illustration using different approaches both in thinking about and in dealing with this issue. The security risk can be modeled and a risk ranking can be obtained based on the concept of "Failure Mode, Effects, and Criticality Analysis" (FMECA) using a fuzzy rule base method. The model presented in this study is based on the assumption that the elements of criticality at each port facility, and of the vulnerability of the security measures associated, are more important than the elements of probability of occurrence the threat associated and also of its severity. This is because the former two elements are the only factors that can be fully under control by the port authority. The priority of the order in implementing the modified security measures proposed to enhance the security level of each scenario is determined using "Expanded Failure Mode and Effects Analysis" (EFMEA), taking into account their feasibility and effect.

Keyword: port facilities

1. Introduction

SINCE the terrorist attack in the United States on September 11, 2001, even greater heed has been paid to matters relating to maritime security. In December 2002, the International Maritime Organization (IMO) adopted the International Ship and Port Facility Security Code (ISPS), which came into force on July 1, 2004. The Code is based on the concept of risk management, with the prime purpose of ensuring that international trade, as conducted by the shipping industry, could be safely expedited without undue threat or fear from terrorists or any other intentional criminal activity. Such an assessment is basically a risk analysis of all operational aspects of a port to determine which facilities in the port area are more susceptible and more likely to be the target of attack. It treats the security risk as identical to others caused by either natural hazards or human errors. When developing a port security assessment model four elements are introduced, namely, the criticality of each asset (C), the probability of occurrence of each threat against a specific asset or target (P), the severity of each adverse attack against that specific asset (S), and the vulnerability of each asset or facility (V). C is defined as the relative importance of each facility, taking into account its function, location, costs, and allowable time for returning operational. P would be a measure of the likelihood that a specific type of attack will be initiated against a specific target (Ung et al. 2004). S is either the amount of expected loss or damage, or it is the negative effects in the shipping industry should the attack be successful. V would be the likelihood that various types of safeguard measures against a scenario would fail (Ung et al. 2004).

In the model, a scenario is defined as a specific type of attack that would be initiated against a specific target. Therefore, when assessing a scenario the four elements mentioned previously are taken into account. The security risk in this study is evaluated using Failure Mode and Effects Analysis (FMEA) based on fuzzy theory. A risk ranking for all scenarios based on defuzzified values is then proposed. This is followed by the preparation of a list of modified security measures aimed at reducing the security risk for each scenario. Since the modified security measure designed to reduce the highest security risk for a specific scenario may not always be the effective one, a model based on Expanded Failure Mode and Effects Analysis (EFMEA) capable of identifying practicable-preferred measures is developed. By taking into consideration the feasibility of each modified security measure provided by the EFMEA model, the priority order for the modified measures can be identified. Consequently, the modified measures are implemented and the periodic review of the security risk enables the measures to be continually effective.

2. Background

2.1. Failure mode, effects, and criticality analysis

FMEA was first adopted as a formal design methodology in the 1960s by the aerospace industry seeking to enhance the safety and reliability level (Sankar & Prabju 2000). Since then, it has been applied to ensure the safety and reliability of products in many industries, mainly including aerospace, automotive, nuclear, and medical technologies. In the automotive industry for example, most companies divide FMEA into two processes, design FMEA and process FMEA (Aldridge et al. 1991) (Ford Motor Company, 1988). Design FMEA is a procedure to ascertain that the right materials are being used to conform to customer specifications and to ensure that government regulations are being met before

[1] Department of Merchant Marine, National Taiwan Ocean University, Keelung, Taiwan.
[2] Offshore & Transport Research Group, School of Engineering, Liverpool John Moores University, Liverpool, United Kingdom.
Manuscript received at SNAME headquarters November 2007.

finalizing the product design. Process FMEA deals with the manufacturing and assembly processes. Several variations of FMEAs have been developed. These include the use of a knowledge-based system for the automation of the FMEA process (Price et al. 1992, 1995, Russomano et al. 1992), the introduction of a causal reasoning model for FMEA (Bell et al. 1992). An improved FMEA has also been proposed using a single matrix to model the entire system and a set of indices derived from a probabilistic combination reflecting the importance of an event relating to the indenture under consideration and to the entire system (Kara-Zaitri et al. 1991, 1992). Usually, FMEA is applied to evaluate the system behavior in terms of identifying potential failure modes and their impact on every system component.

FMECA is an extension of FMEA capable of ranking each potential failure mode according to the combined impacts from the parameters such as severity, probability of occurrence, and detectability. The criticality assessment of each failure mode is traditionally performed by either calculating its criticality number (CN) or developing a risk priority number (RPN). The first method was proposed in U.S. MIL-STD-1629A *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis (FMECA)* presenting a well-known criticality assessment methodology based on the calculation of a CN for each system failure mode i. That is, $CN_i = \alpha_i\beta_i\lambda_p t$, where β_i is the failure effect probability, α_i the failure mode ratio, λ_p the failure rate, and t the operating time. The procedure includes the determination of β_i, α_i, λ_p, and t and the calculation of the values determined to obtain a CN for each failure mode. However, there are some shortcomings raised when applying the CN calculation method (Bowles & Pelaez 1995):

- The CN may be underestimated as a failure mode has multiple effects in different severity categories since only the severest effect is considered in the calculation.
- The determination of β_i, α_i, λ_p, and t is based on qualitative assessment using expert predictions or generic apportionments, making the calculation less precise.

An alternative approach for criticality assessment capable of prioritizing failures for corrective actions is based on a RPN. When assessing a risk level of a specific failure mode, the RPN method uses linguistic priority terms to rank the elements of probability of occurrence (S_f), severity (S), and detectability (S_d) on a numeric scale from 1 to 10. These rankings are subsequently multiplied to give the RPN; i.e. $RPN = S_f \times S \times S_d$. Failure modes with higher RPN are deemed to be more risky and give a higher priority than those having a lower RPN. Tables 1 to 3 show how traditional FMEA employs linguistic priority terms to rank (S_f), (S), and (S_d) (Pillay & Wang 2002).

However, some criticisms have been raised with regard to the application of the RPN method (Ben-Daya & Raouf 1996, Deng 1989, Gilchrist 1993, Pillay & Wang 2003):

- There is no precise algebraic rule to assign a score to the possible failure occurrence rate and detection rate. Although the application of the traditional FMECA scales for probability of occurrence, severity, and detectability as shown in Tables 1 to 3 simplify the calculation, there can nevertheless be problems. The reason for that is because the relationship between detection rate and its corresponding score is linear, whereas the failure rate and its score do not follow the linear law.
- Although the risk ranking based on the RPN values enables management to allocate the limited resources to the most risky events, there is no rationale in obtaining it as a product of the elements of (S_f), (S), and (S_d).
- In the situation where various sets of (S_f), (S), and (S_d) produce an identical value of RPN, however, the risk implication may be totally different. For example, if considering two different sets of (S_f), (S), and (S_d) with values of 1, 4, 6 and 2, 3, 4, respectively, the RPN value of these two sets is identical (24). However, the risk implication is different. When such a circumstance occurs, a misjudgment could take place; consequently, the more risky event would become unnoticed.
- The RPN value does not consider the relative importance between (S_f), (S), and (S_d); that is, these three elements are assumed to have the same importance. However, this may not always be the case, and sometimes it is regarded as impractical.

Table 1 Traditional FMECA scale for probability of occurrence (S_f)

Criteria	Score	Possible Failure Occurrence Rate (Operating Days)
Remote	1	<1/20,000
Low	2	1/20,000
	3	1/10,000
Moderate	4	1/2,000
	5	1/1,000
	6	1/200
High	7	1/100
	8	1/20
Very high	9	1/10
	10	1/2

Table 2 Traditional FMECA scale for severity (S)

Criteria	Score
Remote	1
Low	2, 3
Moderate	4, 5, 6
High	7, 8
Very high	9, 10

2.2. Fuzzy logic FMECA

Fuzzy theory was first proposed by Zadeh in 1965, and its objective is to help in making decisions characterized by imprecise information. In a fuzzy logic based FMECA, linguistic variables such as the probability of occurrence and severity can be represented as members of a fuzzy set, described using linguistic priority terms associated with corresponding membership values (fuzzy inputs) and combined by matching them against rules in a rule base. The input and output membership functions as well as the rules are developed based on expert judgment. The outcome of such a combination is referred to as a set of fuzzy conclusions. By introducing the defuzzification method taking into account the consequent membership functions, the risk level of an event in terms of defuzzified value can be realized. If there are many events in question, a list of risk priority

Table 3 Traditional FMECA scale for detectability (S_d)

Criteria	Score	Possible Detection Rate (%)
Remote	1	86–100
Low	2	76–85
	3	66–75
Moderate	4	56–65
	5	46–55
	6	36–45
High	7	26–35
	8	16–25
Very high	9	6–15
	10	0–5

of these events are then developed based on their defuzzified values. Bowles and Pelaez evaluated a stopper valve on the water tank leveling system and illustrate the idea well (Bowles & Pelaez 1995). The method has also been used to perform reliability assessment of electronic devices (Zafiropoulos & Dialynas 2004). A modified method proposed by Braglia and Bevilacqua outlines how analytical hierarchy process (AHP) may assist the practitioners in establishing the numerousness fuzzy rules (Braglia & Bevilacqua 2000). This is because it has several advantages:

- It provides a tool for directly working with the linguistic priority terms used in assessing risks. Thus, fuzzy theory enables analysts to evaluate risks in a natural way.
- Ambiguous, qualitative, or imprecise information as well as quantitative data can be used in the assessment and can be handled in a consistent manner.
- It is capable of providing a flexible structure for combining the elements of criticality, probability of occurrence, severity, and vulnerability. In other words, these elements can be evaluated taking into account their individual importance.

However, the method described previously mainly focuses on the risk assessment aspect. In this study, an approach proposed based on the fuzzy logic takes into account not only the risk assessment but also the risk management aspects. By applying EFMEA, the elements of feasibility and effect of measures are considered. Furthermore, the traditional method only allows for three elements in the fuzzy logic FMECA model, whereas this study evaluates four. In addition, the work presented here demonstrates how a fuzzy rule base can be established as each element has its own degree of importance. Figure 1 clearly illustrates the idea of risk assessment and management using fuzzy modeling proposed in this research. Further details of the framework are presented in the next section.

3. Methodology

The traditional FMEA contains three elements, namely, the probability of occurrence, severity, and detectability. However, the framework proposed incorporates four different categories of criteria to evaluate the overall risk associated with each asset. The categories include the criticality of each asset (C), the probability of occurrence of each threat against a specific asset or target (P), the severity of each adverse attack against that specific asset (S), and the vulnerability of each asset or facility (V). Five linguistic priority terms describing these four elements are used, namely, Remote, Low, Moderate, High, and Very High. A scenario associated with these four elements is then established, representing the primary risk characteristics. Each scenario cannot be compared until the following steps are taken. The first step is to establish the membership function for the linguistic priority terms using a triangular distribution based on expert judgments. The values of the membership function associated with the linguistic priority terms of each of these four elements involved in a specific scenario are then determined. This is followed by the development of a rule base that is also based on expert judgments. An element called Priority Level comprising the value of weight associated with a defined linguistic priority term is introduced with respect to combinations of C, P, S, and V. The first three steps are regarded as

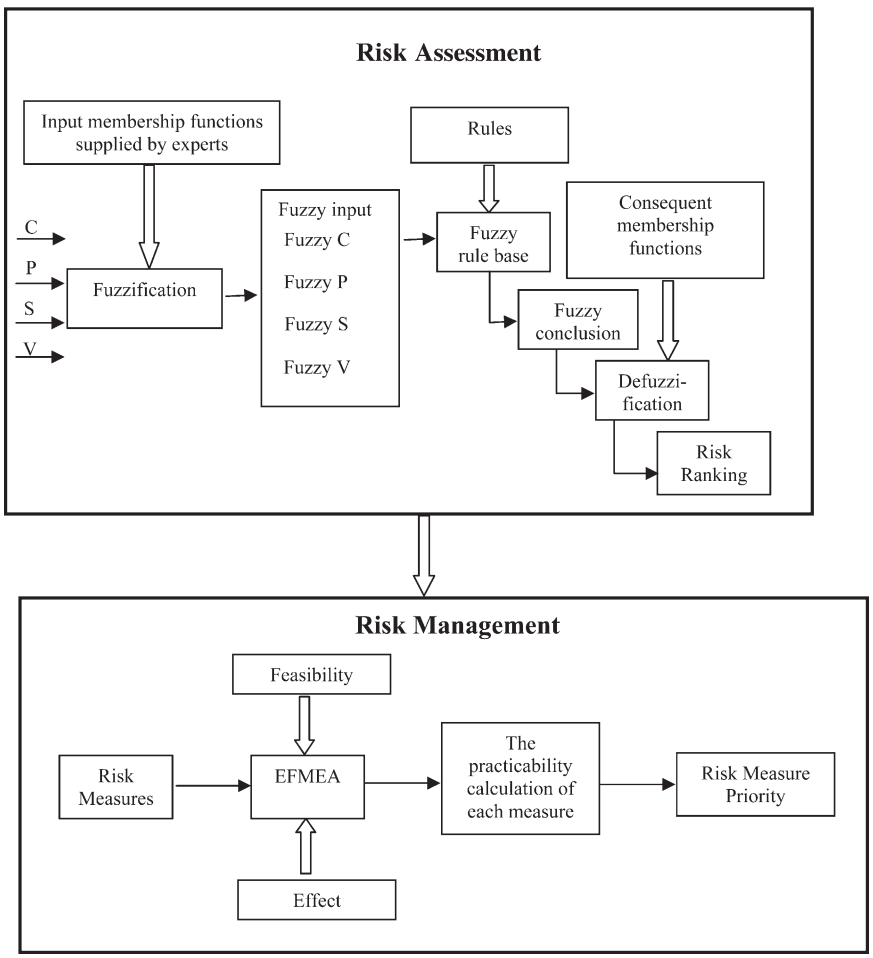

Fig. 1 The proposed idea of risk assessment and management using fuzzy modeling

a fuzzification process of expressing how well the input belongs to the linguistic priority terms used in the rules. A defuzzification process is then adopted by employing appropriate algorithms. A value of the overall risk to a scenario is obtained, and therefore a risk ranking of all scenarios can be produced. Based on the risk ranking generated, the list of modified security measures aimed at reducing or eliminating risks is presented. By applying the Expanded Failure Mode, Effects, and Analysis (EFMEA) taking into account the feasibility of the measures, the priority of modified security measures are finally developed. The modified measures are implemented and reviewed periodically to maintain the risk on the acceptable level. Figure 2 shows the process of the research methodology.

3.1. The establishment of membership function for linguistic priority terms of each element

The membership function is established for linguistic priority terms describing the linguistic variables C, P, S, and V using multiple experts. The experts involved in a port security project should be appropriately selected so that an unrealistic and biased membership function are avoided (Kuusela et al. 1998). Each expert is asked to evaluate a proposition "x belongs to A?." Suppose A is a fuzzy set on X that represents a linguistic priority term associated with a given linguistic variable and $a_i(x)$ is a value of scores within a certain range in X; i.e., $a_i(x) \in$ X (in this study, X follows the same pattern the traditional FMEA adopts, 1 to 10 categories). In the situation where there are n experts and each of them has equal competence, the following formula is applied (Klir & Yuan 1995):

$$\mathrm{A}(x) = \frac{\sum_{i=1}^{n} a_i(x)}{n} \tag{1}$$

where A(x) is the final answer (value) after n experts' judgments are synthesized, and $a_i(x)$ is the answer (value) given by the ith expert, $i \in n$.

In the case where the experts have different degrees of competencies, equation (1) is modified as:

$$\mathrm{A}(x) = \sum_{i=1}^{n} Comp_i a_i(x) \tag{2}$$

where $Comp_i$ is the degree of competency of the ith expert, and

$$\sum_{i=1}^{n} Comp_i = 1 \tag{3}$$

It is important to note that the degree of competency for each of the experts should be determined based on his knowledge and experience in risk assessment and management as well as in the port security field.

The triangular membership function is adopted since it has a smooth transition from one linguistic priority term to the other. On the other hand, it facilitates easy defuzzification of each linguistic priority term. The membership function for each linguistic priority term is evaluated within its limits on an arbitrary scale from 0 to 1.

Prior to the determination of the membership function for C, it is important to conduct a criticality assessment since it is capable of identifying and evaluating significant assets and infrastructure in terms of various factors. The following factors should be taken into account when evaluating the criticality of facilities within port areas:

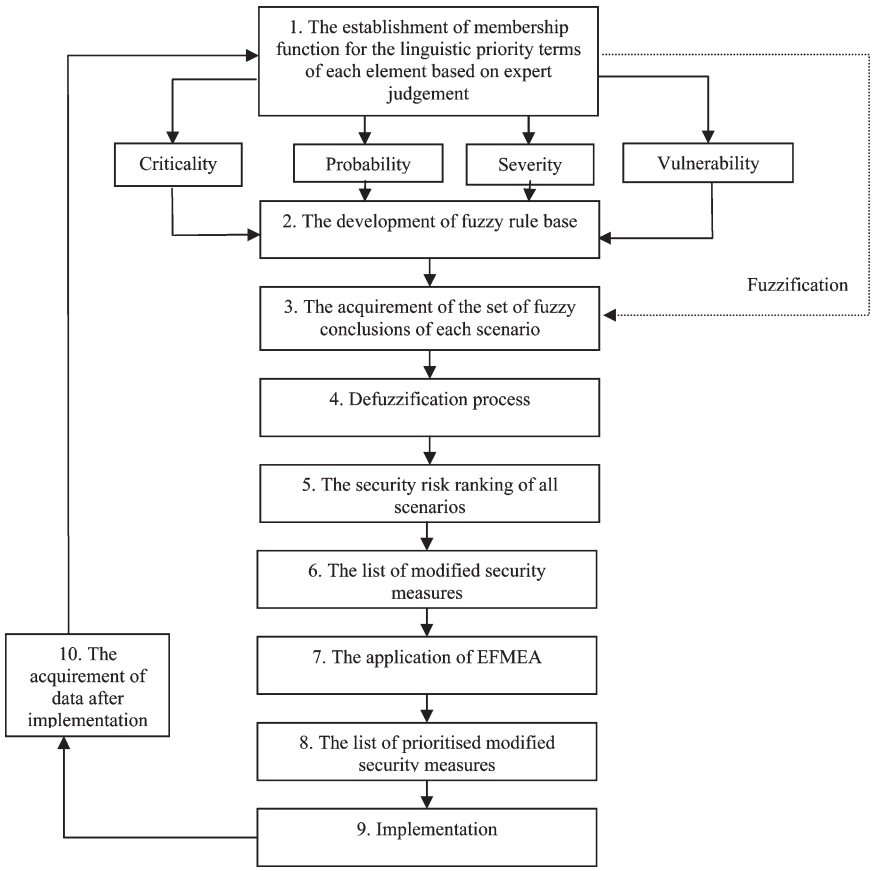

Fig. 2 The flowchart of the research methodology

- The importance of each facility's function in terms of overall port operations
- The location of the facility
- The allowable time for returning the facility to operational capability if attacked (U. S. Department of Veteran Affairs 2002)
- The costs of permanent replacement and temporary substitute as well as the loss of income in the downtime period (ASIS International Guidelines Commission 2003).

The traditional risk assessment and management in evaluating the element of likelihood of occurrence is often based on failure rates obtained from daily operations. When assessing the likelihood of occurrence of potential threats in port security, however, there is usually no such data available. It may only be possible to rely on complicated factors such as politics, religion, intelligence, the capability, intention, and past activities of potential criminal organizations, etc. to determine the likelihood of occurrence level using linguistic priority terms. Additionally, the level of severity would depend on the extent to which the negative effects impose on the port operations once an attack or intentional crime was initiated. The criteria of evaluating such effects may include the number of injuries and fatalities as well as the damage to the facility.

A vulnerability assessment is a process that identifies weaknesses in physical structures, personnel protection systems, the security processes aimed at surveilling the passage of cargoes and personnel, and some other measures designed to prevent attacks that may be exploited by terrorists or criminals. By conducting drills periodically, the data available for the vulnerability assessment can be collected and analyzed. In general, the assessment is performed by teams of experts specializing in engineering, intelligence, security, etc.

In addition, as stated earlier, five linguistic priority terms are employed to describe the linguistic variables of each scenario, whose interpretations are given in Tables 4 to 7.

It is worth noting that the more quantified the data supporting the criteria adopted in each of these four elements are, the more precise the acquired outcome. The output of this step is that each element of a scenario has at least one membership function value associated with one linguistic priority term.

Table 4 Interpretation of the linguistic priority terms for criticality

Linguistic Priority Term	Interpretation
Remote	The importance of the facility is near none. Its location is much further away from the central administration. Its costs and time for returning to operational capability would be extremely low if attacked.
Low	The importance of the facility is low. Its location is far away from the central administration. Its costs and time for returning to operational capability would be low if attacked.
Moderate	The importance of the facility is moderate. Its location is not far away from the central administration. Its costs and time for returning to operational capability would be moderate if attacked.
High	The importance of the facility is high. The location is near the central administration. The costs and time for returning to operational capability would be high if attacked.
Very high	The importance of the facility is very high. The location is very near or in the central administration. The costs and time for returning to operational capability would be extremely high if attacked.

Table 5 Interpretation of the linguistic priority terms for probability of occurrence

Linguistic Priority Term	Interpretation
Remote	It would be very unlikely for the scenario in question to occur even once in the facility's lifetime.
Low	It would be unlikely for the scenario in question to occur once in the facility's lifetime.
Moderate	It would be likely for the scenario in question to occur more than once in the facility's lifetime.
High	It would be very likely for the scenario in question to occur at least once in the facility's lifetime.
Very high	It would be almost certain for the scenario in question to occur several times in the facility's lifetime.

3.2. The development of fuzzy rule base

Fuzzy logic systems are constructed from human knowledge in the form of fuzzy IF/THEN rules (Sii et al. 2001, Wang 1997). A fuzzy IF/THEN rule is an IF/THEN statement in which some words are characterized by continuous membership functions (Pillay & Wang 2002). It provides a systematic procedure transforming a knowledge base into nonlinear mapping. The first part of an IF/THEN rule is the input variables, including the elements of C, P, S, and V. The second part is the consequent describing the risk level based on a value of weight established by experts and a linguistic priority term attached. In this paper, the consequence is referred to as Priority, and five linguistic priority terms are introduced to interpreting it, namely, Low, Fairly Low, Moderate, Fairly High, and High.

The fuzzy rule base is developed in the fashion where the selected experts are asked to group the various combinations of linguistic priority terms describing C, P, S, and V of each scenario into one of the five linguistic priority terms reflecting the Priority Level. Since there are four elements associated with five linguistic priority terms, the total number of the rules is 625. The membership function for the fuzzy rule base can be determined by applying equations (2) and (3). When developing the rule base in this paper, the authors decided to put more weight onto the elements of criticality and vulnerability, i.e., 0.3 each for C and V and 0.2 each for P and S. This is because the criticality determines the relative importance of each asset, whereas the vulnerability is the only element that the administration can fully control when encountering intentional crimes.

Table 6 Interpretation of the linguistic priority terms for severity

Linguistic Priority Term	Interpretation
Remote	The scenario in question would have nearly no effect on port operations.
Low	The scenario in question would have low effect on port operations, e.g., a few people slightly injured and/or little damage to the facility.
Moderate	The scenario in question would cause moderate effect on port operations, e.g., a limited amount of injuries and a limited amount of damage to the facility.
High	The scenario in question would have high effect on port operations, e.g., a certain amount of injuries and fatalities and serious damage to the facility.
Very high	The scenario in question would have extremely high effect on port operations, e.g., serious injuries and fatalities and complete damage of the facility.

Table 7 Interpretation of the linguistic priority terms for vulnerability

Linguistic Priority Term	Interpretation
Remote	It is extremely unlikely that the security measures designed to prevent the intentional crimes would fail once attacked.
Low	It is unlikely that the safety and security measures designed to prevent the intentional crimes would fail once attacked.
Moderate	It is likely that the safety and security measures designed to prevent the intentional crimes would fail once attacked.
High	It is very likely that the safety and security measures designed to prevent the intentional crimes would fail once attacked.
Very high	The safety and security measures designed to prevent the intentional crimes would definitely fail once attacked.

3.3. The acquisition of the set of fuzzy conclusions of each scenario

The Priority Level of a specific scenario is decided on the basis of the fuzzy rule base developed. Using a "min-max" approach, the set of fuzzy conclusions of the scenario is obtained in terms of membership function values associated with linguistic priority terms. When applying the "min-max" approach, the following steps are taken:

1. Identify the possible combinations of C, P, S, and V in which the membership values associated with the corresponding linguistic priority terms are not zero. The outputs of such combinations can be obtained from the fuzzy rule base developed.
2. Determine the minimum value of each combination by comparing the values obtained from each element and the value of the belief degree established in the Priority Level.
3. Determine the highest minimum values obtained from step 2 with respect to each linguistic priority term.

If there is only one rule that can be applied to the scenario in question, then the minimum value of the membership function and the linguistic priority term associated are the set of fuzzy conclusions. In the above, each maximum value and its associated linguistic priority term is a fuzzy conclusion; each set of fuzzy conclusions of each scenario is defuzzified using the method proposed in the next section.

3.4. Defuzzification process

The defuzzification process creates a single crisp ranking from the fuzzy conclusion set, i.e., the Priority Level of scenarios to express the inherent security risk. Several defuzzification algorithms have been developed (Runkler & Glesner 1993). The one selected for use in this paper is the Weighted Mean of Maximums (WMoM). The algorithm averages the points of maximum possibility of each Priority Level of scenarios, weighted by their degree of truth at which the membership functions reach their maximum values (Andrew & Moss 2002, Pillay & Wang 2002). The formula of WMoM is as follows:

$$WMoM = \frac{\sum w_i x_i}{\sum w_i} \tag{4}$$

where w_i is the degree of truth of the membership function of the ith linguistic priority term, and x_i is the risk rank at maximum value of the membership function of the ith linguistic priority term.

3.5. The security risk ranking of all scenarios and the list of modified security measures

It is in this step that the security risk ranking of all scenarios are presented. Based on the values obtained from the defuzzification process, the scenarios with relatively higher risks are identified. The higher defuzzified values the scenarios have, the more the attention that should be paid.

3.6. The list of modified security measures

The list of modified security measures (MSM) designed to enhance the security level of each scenario are proposed in this step according to the security risk ranking presented. The list of the modified measures can be regarded as risk-based since it is produced based on the defuzzified value that each scenario has. In addition, it may be possible that one specific modified measure proposed is capable of reducing the risks imposed on two or more scenarios. However, it is not the case in this research.

3.7. The application of EFMEA

The list of modified security measures is proposed based on the risk assessment. However, the measures and correct actions aimed at reducing the scenarios with higher risks are not always the optimal ones appreciated by the administration. Therefore, the element of the feasibility of security measures should be considered. This is an outstanding feature of the EFMEA that differs from the traditional FMEA since it is capable of incorporating such an element providing various viewpoints other than the risk aspect. In this paper, a ranking of the feasibility of security measures from 0.1 to 1 based on expert judgment is proposed (Bluvband et al. 2004). When evaluating the feasibility, the availability of resources, cost and time consumption, success rate, and the probability of undesirable impacts are taken into account. The interpretation of the criteria of the feasibility is shown in Table 8.

Table 8 Interpretation of feasibility criteria

Criteria	Score
Fully available resources, very low cost and time consumption, near 100% success rate, and near zero probability of undesirable impact.	0.1
Highly available resources, low cost and time consumption, high success rate, and low probability of undesirable impact.	0.2
Rather high available resources, rather low cost and time consumption, rather high success rate, and rather low probability of undesirable impact.	0.3
Moderate availability of necessary resources, cost, time consumption, success rate, and probability of undesirable impact.	0.4
Rather low availability of necessary resources and/or rather high cost and/or time consumption and/or rather low success rate and/or rather high probability of undesirable impact.	0.5
Low availability of necessary resources and/or high cost and/or time consumption and/or low success rate and/or high probability of undesirable impact.	0.6
Very low availability of necessary resources and/or very high cost and/or time consumption and/or very low success rate and/or very high probability of undesirable impact.	0.7
Remote availability of necessary resources and/or near unacceptable cost and/or time consumption and/or remote success rate and/or near 100% probability of undesirable impact.	0.8
Very remote availability of necessary resources and/or almost unacceptable cost and/or time consumption and/or almost zero success rate and/or almost 100% probability of undesirable impact.	0.9
No available resources and/or unacceptable cost and/or time consumption and/or zero success rate and/or 100% probability of undesirable impact.	1.0

Since the evaluation of the feasibility is based on expert judgments and the opinion from each expert may be different, two formulas similar to equations (1) and (2) are introduced. In the situation where there are n experts and each one has equal degree of competencies:

$$F(x) = \frac{\sum_{i=1}^{n} f_i(x)}{n} \tag{5}$$

where $F(x)$ is the final answer (value) of n experts, and $f_i(x)$ is the value of scores within a certain range F (0.1 to 1.0), i.e., $f_i(x) \in \mathrm{F}$ from the ith expert, $i \in n$.

In the case where the experts have different degrees of competencies, the following equations are applied:

$$F(x) = \sum_{i=1}^{n} Comp_i f_i(x) \tag{6}$$

where $Comp_i$ is the degree of competency of the ith expert, and

$$\sum_{i=1}^{n} Comp_i = 1 \tag{7}$$

After obtaining the value of feasibility of each security measure, the estimated result of the risk level of each scenario since implementing the security measure in terms of expected defuzzification values are developed. The differences between the original and expected defuzzification values are then obtained. The optimal security measures are therefore appreciated by the value obtained from equation (8). The security measures with higher quotients are more preferable than the others.

$$\mathrm{P}(x)_j = \frac{Def_{j\mathrm{Original}} - Def_{j\mathrm{Expected}}}{F(x)_j} \tag{8}$$

where $P(x)_j$ is the value of practicability of the modified security measure designed to reduce or eliminate the risk of the jth scenario, $Def_{j\mathrm{Original}}$ is the original defuzzified value of the jth scenario whereas $Def_{j\mathrm{Expected}}$ is the expected defuzzified value estimated after the security measure has been implemented, and $F(x)_j$ is the feasibility of the security measure designed to reduce or eliminate the risk of the jth scenario.

3.8. The list of prioritized modified security measures

A list of prioritized modified security measures are proposed based on the values calculated using equation (8) taking into account the element of the practicability of each modified measure. Therefore, the list of the priority of the modified security measures are more acceptable than if obtained merely based on risk assessment since it allows for the aspects of the availability of resources, cost and time consumption, success rate, and the probability of undesirable impacts.

3.9. The implementation of the prioritized modified security measures

In this step, the modified security measures based on the practicability assessment are implemented. After the implementation, the data compilation with regard to daily operations is highly recommended as it facilitates the mission conducted in the next step.

3.10. The acquirement of data since implementation

The data collection step seems to be necessary because terrorist activities are complex. They are dependent on the political situation, the capabilities of terrorists, and accuracy of the intelligence gathered etc. so that the elements of C, P, S, and V may change significantly. Therefore, the only way to keep the security measures effective is to view, collect, and analyze the data periodically after they come into force.

4. Case Study

The aim of this study is to demonstrate how the methodology can be applied to port security. A difficulty exists, however, in that data are difficult to acquire, and thus they are assigned by the experts specializing in risk assessment and port operations. Therefore, the methodology is applied to a hypothetical port.

4.1. The establishment of the membership functions for linguistic priority terms of C, P, S, and V

As described in section 3, five linguistic priority terms are introduced for modeling C, P, S, and V, namely, Remote, Low, Moderate, High, and Very High. Using equations (2) and (3) provided that the weight of each expert is given, the values capable of fully representing each linguistic priority term (that is, the limits where the membership function reaches 1 or becomes 0) can be determined. The value ($\mathrm{A}(x)$) that fully represents the linguistic priority term when the membership function reaches 1, e.g., Remote, can be obtained as follows (provided there are five experts with the weights of 0.3, 0.3, 0.2, 0.1, and 0.1 associated with their individual answers as to the value that can fully describe the linguistic term, Remote, when the membership function reaches 1, 1.5, 1.5, 1, 2, and 2, respectively):

$$\mathrm{A}(x) = \sum_{i=1}^{n} C_i a_i(x) = 0.3 \cdot 1.5 + 0.3 \cdot 1.5 + 0.2 \cdot 1 + 0.1 \cdot 2 + 0.1 \cdot 2 = 1.5 \tag{9}$$

The values of two limits of the linguistic priority term, Remote, as the membership function reaches 0, can also be calculated using the pattern illustrated above. Figure 3 illustrates the assumed membership functions for the five linguistic priority terms of elements C, P, S, and V based on expert judgments. In reality, the establishment of membership functions and the collection of data when determining the linguistic priority terms and its associated values depend on the factors already stated in the research methodology.

4.2. The development of fuzzy rule base

As stated in the previous section, since there are four linguistic variables and each has been assigned five linguistic priority terms, the number of fuzzy rules developed is 625 ($5 \times 5 \times 5 \times 5$). As already described in the research methodology section, because the criticality and vulnerability assessments are the internal factors that can be fully controlled by the administration, the weight assigned to each is 0.3, which is higher than the other two, 0.2. The consequent (the column of Priority Level) is determined by five linguistic priority terms (Low, Fairly Low, Moderate, Fairly High, and High) and an arbitrary value based on the combination of the weights assigned and the level of each linguistic priority term describing the four elements. The procedure of determining a Priority Level is indicated below.

If Criticality is Remote, Probability of Occurrence is Remote, Severity is Remote, and Vulnerability is Remote, then the Priority Level is Low (1). The value of 1 is obtained by the sum of the weights of each element, i.e., ($0.3 \times 1 + 0.2 \times 1 + 0.2 \times 1 + 0.3 \times 1$). The weight of each element is determined by the product of the individual weight assigned (that is, Criticality = 0.3, Probability of Occurrence = 0.2, Severity = 0.2, and Vulnerability = 0.3) and the level of each linguistic priority term describing these four elements (Remote = Level 1, Low = Level 2, Moderate = Level 3,

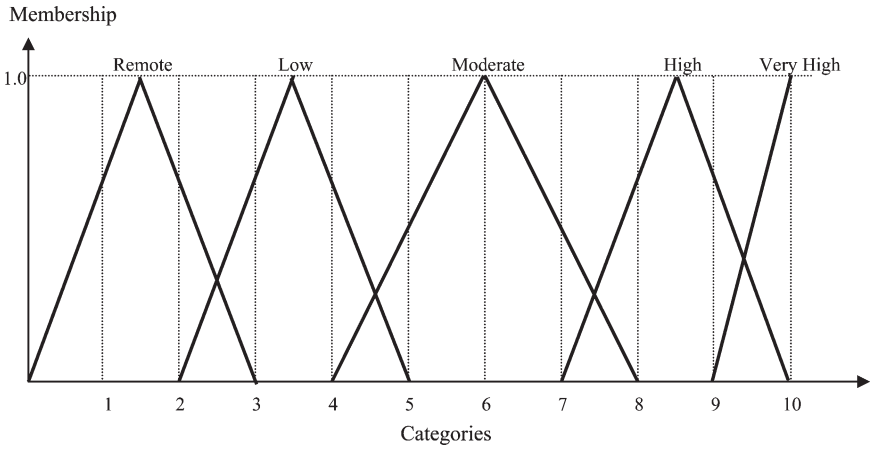

Fig. 3 Membership function for linguistic priority terms reflecting C, P, S, and V

High = Level 4, and Very High = Level 5). The value of threshold of each linguistic priority term describing Priority Levels is set up to be 1 (that is, Remote = 1, Fairly Low = 2, Moderate = 3, Fairly High = 4, and High = 5). If Criticality is Remote, Probability of Occurrence is Remote, Severity is Low, and Vulnerability is Remote, e.g., the sum of the weights is 1.2 ($0.3 \times 1 + 0.2 \times 1 + 0.2 \times 2 + 0.3 \times 1$). Therefore, the linguistic priority term and its associated value adopted to describe the Priority Level is Fairly Low (0.2). By applying equations (2) and (3), the membership functions of the fuzzy rule base developed can be obtained. Appendix 1 shows a selected list of combinations used in this case study. Figure 4 shows the assumed membership functions for the five linguistic priority terms reflecting Priority Levels on the basis of expert judgments. It is proposed in a similar way to that in which Fig. 3 was developed.

4.3. The determination of risk levels for C, P, S, and V of each scenario and the acquirement of its fuzzy conclusion

In order to obtain a security risk ranking, two steps are required. Firstly, the linguistic priority terms and the membership values associated reflecting the risk levels for C, P, S, and V of each scenario should be carefully decided. Secondly, the fuzzy set conclusion of each scenario is obtained based on the fuzzy rule base using the "min-max" approach. Since the purpose of this research is to demonstrate how the security risk can be modeled, in the first step 10 scenarios are assumed based on the knowledge of the authors. Such hypothetical scenarios are listed in Table 9, and it is noted that the hypothetical port in this case study is set to be capable of handling dry bulk, oil, chemical, and containerized cargoes. Suppose the risk category of the Criticality of scenario 1 falls within categories 7 and 8, 7.3, for example. The level for C is described as Moderate 0.38 and High 0.18 as shown in Fig. 5. In a similar way, the descriptions of C, P, S, and V for all scenarios can be produced as shown in Table 10.

In Table 10, Scenario 1 (maritime terrorist attack to chemical facilities) is set under circumstances where:

> the criticality of the chemical facilities in question was Moderate 0.38 and High 0.18; the probability of occurrence of maritime terrorist attack against such facilities was Low 0.42 and Moderate 0.14; the severity should such an attack occur was Very High 0.8 and High 0.1; and the vulnerability of the chemical facilities was High 0.41 and Moderate 0.17.

The rest of the scenarios in Table 10 can be expressed using the similar pattern aforementioned based on their individual circumstances established.

By applying the "min-max" approach, the set of fuzzy conclusions of Scenario 1 is obtained as follows:

i. List the membership function values according to the rules developed.
   - If C = Moderate 0.38, P = Low 0.42, S = Very High 0.8, and V = High 0.41, then the Priority Level is Fairly High 0.5 according to rule 299.
   - If C = High 0.18, P = Low 0.42, S = Very High 0.8, and V = High 0.41, then the Priority Level is Fairly High 0.8 according to rule 424.

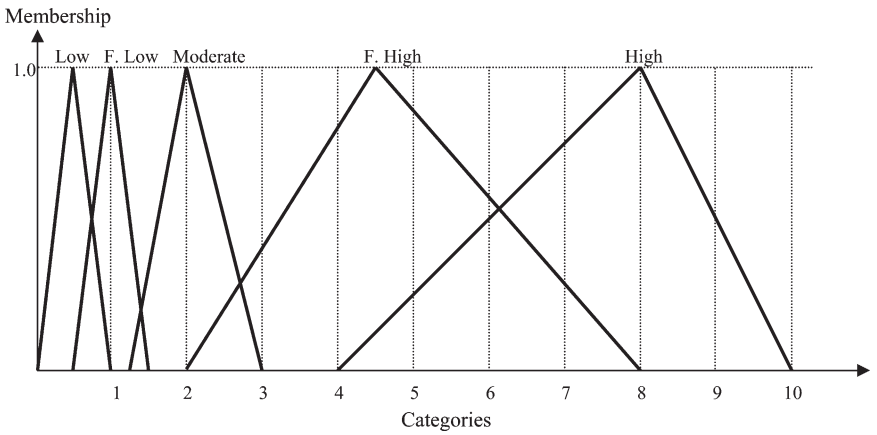

Fig. 4 Membership function for linguistic priority terms describing the fuzzy rule base

Table 9 Details of hypothetical scenarios

Scenario No.	Hypothetical Details
1	Maritime terrorist attack to chemical facilities
2	Vandalism of inappropriate use of dry bulk terminals
3	Terrorist attack to oil terminals
4	Smuggling explosive against container facilities
5	Terrorist attack to oil deports
6	Intrusive assault against unmanned areas
7	Stowaways against dry bulk facilities
8	Cargo theft against container yard
9	Armed assault and robbery against warehouses
10	Opportunistic crime to the headquarter of the port authority

- If C = Moderate 0.38, P = Moderate 0.14, S = Very High 0.8, and V = High 0.41, then the Priority Level is Fairly High 0.7 according to rule 324.
- If C = High 0.18, P = Moderate 0.14, S = Very High 0.8, and V = High 0.41, then the Priority Level is Fairly High 1 according to rule 449.
- If C = Moderate 0.38, P = Low 0.42, S = Moderate 0.1, and V = High 0.41, then the Priority Level is Fairly High 0.1 according to rule 289.
- If C = High 0.18, P = Low 0.42, S = Moderate 0.1, and V = High 0.41, then the Priority Level is Fairly High 0.4 according to rule 414.
- If C = Moderate 0.38, P = Moderate 0.14, S = Moderate 0.1, and V = High 0.41, then the Priority Level is Fairly High 0.3 according to rule 314.
- If C = High 0.18, P = Moderate 0.14, S = Moderate 0.1, and V = High 0.41, then the Priority Level is Fairly High 0.6 according to rule 439.
- If C = Moderate 0.38, P = Low 0.42, S = Very High 0.8, and V = Moderate 0.17, then the Priority Level is Fairly High 0.2 according to rule 298.
- If C = High 0.18, P = Low 0.42, S = Very High 0.8, and V = Moderate 0.17, then the Priority Level is Fairly High 0.5 according to rule 423.
- If C = Moderate 0.38, P = Moderate 0.14, S = Very High 0.8, and V = Moderate 0.17, then the Priority Level is Fairly High 0.4 according to rule 323.
- If C = High 0.18, P = Moderate 0.14, S = Very High 0.8, and V = Moderate 0.17, then the Priority Level is Fairly High 0.7 according to rule 448.
- If C = Moderate 0.38, P = Low 0.42, S = Moderate 0.1, and V = Moderate 0.17, then the Priority Level is Moderate 0.8 according to rule 288.
- If C = High 0.18, P = Low 0.42, S = Moderate 0.1, and V = Moderate 0.17, then the Priority Level is Fairly High 0.1 according to rule 413.
- If C = Moderate 0.38, P = Moderate 0.14, S = Moderate 0.1, and V = Moderate 0.17, then the Priority Level is Moderate 1 according to rule 313.
- If C = High 0.18, P = Moderate 0.14, S = Moderate 0.1, and V = Moderate 0.17, then the Priority Level is Fairly High 0.3 according to rule 438.

ii. Determine the minimum value of each combination in terms of comparing the values obtained from each element and the value of weight established in the Priority Level.
- In the first combination, C = Moderate 0.38, P = Low 0.42, S = Very High 0.8, and V = High 0.41 and the Priority Level is Fairly High 0.5. Therefore, the minimum value of C, P, S, and V is 0.38, which is associated with the linguistic priority term Fairly High according to the fuzzy rule developed. The minimum values of the other 15 combinations can be determined in a similar way as shown in Table 11.

iii. Determine the maximum value of the minimum values obtained from step 2 that have the same category of linguistic priority term.
- In the first scenario, there are 16 combinations and two different categories of linguistic priority terms, Moderate and Fairly High. The membership values in the Fairly High category are 0.38, 0.18, 0.14, 0.1, and 0.17, respectively. Therefore, the maximum membership value is 0.38 as shown in Table 12. Likewise, the values in the Moderate group are 0.1 in 13th combination and in 15th combination. Thus, the maximum membership value in the Moderate category is 0.1.
- The set of fuzzy conclusions of the other 9 scenarios can be obtained in a similar way, which is defuzzified in the next section. Table 13 shows the set of fuzzy conclusions of the 10 scenarios.

4.4. The defuzzification process

By applying equation (4) in the defuzzification process, taking into account the risk ranks at maximum value of the membership function as shown in Fig. 4, the defuzzified value of scenario 1 can be detailed as:

$$WMoM = \frac{\sum w_i x_i}{\sum w_i} = \frac{0.1 \cdot 2 + 0.38 \cdot 4.5}{0.1 + 0.38} \cong 3.98 \qquad (10)$$

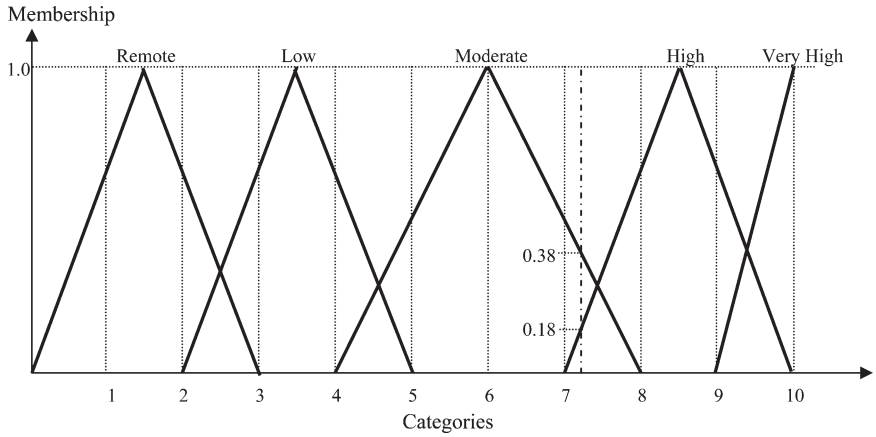

Fig. 5 The determination of membership function for the criticality element

Table 10 Levels of C, P, S, and V of each scenario

Scenario No.	Criticality	Probability of Occurrence	Severity	Vulnerability
1	Moderate 0.38, high 0.18	Low 0.42, moderate 0.14	Very high 0.8, high 0.1	High 0.41, moderate 0.17
2	Remote 0.5	High 0.6, very high 0.1	Moderate 0.7	High 0.55, moderate 0.09
3	Very high 0.4, high 0.4	High 0.4, moderate 0.18	Moderate 0.5	Very high 0.52, high 0.29
4	Moderate 1	Low 0.28, moderate 0.28	High 0.65	Very high 0.9, high 0.05
5	Very high 0.9, high 0.05	Low 0.39, moderate 0.19	Moderate 0.39, low 0.12	Very high 0.81, high 0.12
6	Low 0.39, moderate 0.19	Very high 0.805, high 0.12	Very high 0.9, high 0.05	Moderate 0.39, low 0.12
7	Low 0.5, remote 0.17	Low 0.31, remote 0.31	Moderate 0.44, low 0.08	Remote 1
8	Moderate 0.38, high 0.18	High 0.65	Low 0.39, moderate 0.19	Moderate 0.7
9	Low 0.42, moderate 0.14	High 0.6, very high 0.1	High 0.4, moderate 0.18	Low 0.28, moderate 0.28
10	Very high 0.9, high 0.05	Remote 0.5	Remote 0.5	Very high 0.81, high 0.12.

Table 11 Minimum value of each combination

1	Fairly high 0.38	2	Fairly high 0.18	3	Fairly high 0.14	4	Fairly high 0.14
5	Fairly high 0.1	6	Fairly high 0.1	7	Fairly high 0.1	8	Fairly high 0.1
9	Fairly high 0.17	10	Fairly high 0.17	11	Fairly high 0.14	12	Fairly high 0.14
13	Moderate 0.1	14	Fairly high 0.1	15	Moderate 0.1	16	Fairly high 0.1

In a similar way, the defuzzified values of all scenarios are obtained as shown in Table 14. The scenarios with higher defuzzified values are considered to be more risky.

4.5. The security risk ranking of all scenarios and the modified security measure list

The security risk ranking of all scenarios can be determined based on the defuzzified values calculated. The modified security measures for each scenario are then proposed. These modified measures are designed to enhance the security level of each scenario. If the risk associated with a specific scenario, e.g., the checkpoint of a port area is relatively higher than the others, then modified security measures such as the proposition of additional port security personnel in the site could enhance the security level. Table 15 contains the details of the 10 hypothetical scenarios and the modified security measures (MSMs) proposed accordingly.

4.6. The application of EFMEA

The final score of the feasibility of each MSM can be obtained by applying equation (5) or equations (6) and (7), depending on the situation. As the experts are evaluating their own score of a specific MSM, the interpretation of feasibility criteria in Table 5 shall be taken into consideration. However, in this case study, because of the scarcity of data, the feasibility score of each MSM, $F(x)_j$, is arbitrarily determined.

In addition, the expected levels of C, P, S, and V of each scenario after implementing the modified security measure should be established. The expected levels of each element are evaluated based on the membership function for the five linguistic priority terms in Fig. 5. It should be noted that since the criticality assessment is based on the importance of each facility's function, location of the facility, allowable time for returning the facility to operational capability if attacked, costs of permanent replacement and temporary substitute, and the lost of income in downtime period, the MSMs designed cannot reduce its level. Therefore, the authors decide to keep the Criticality level of the 10 scenarios unchanged. When obtaining the fuzzy expression of the expected level for the probability of occurrence of Scenario 1, suppose the category value falls within categories 2 and 3, that is, 2.5. The appropriate linguistic priority term and the membership value describing the level for P is described as Remote 0.32 and Low 0.32 as shown in Fig. 6. In a similar way, the status of the elements of S and V for scenario 1 can be acquired. The fuzzy descriptions of C, P, S, and V for all the scenarios after the implementation of the modified security measures can also be obtained using the similar pattern aforementioned, which are shown in Table 16.

The practicability of each MSM designed to reduce or eliminate the risk can be determined by applying equation (8). The value of $P(x)_j$ for MSM1 is obtained as follows provided $F(x)_j$ is 0.3 determined arbitrarily as aforementioned:

$$\mathrm{P}(x)_j = \frac{Def_{j\mathrm{Original}} - Def_{j\mathrm{Expected}}}{F(x)_j} = \frac{(3.98 - 2.6)}{0.3} = 4.6 \qquad (11)$$

The values of $P(x)_j$ from MSM 2 to MSM 10 can be calculated in a similar way as shown in Table 16. It can be seen that the most preferable modified measure is MSM 10 since its $P(x)_j$ value, 18.2, is the highest. The modified measure that would incur maximum negative impacts is MSM 7 associated with the value of $P(x)_j$, 0.13. An MSM with a higher difference between the original defuzzified value and expected defuzzified value and a smaller feasibility value is more desirable

Table 12 Maximum value associated with the same category of linguistic priority terms

Category of Linguistic Priority Terms	Maximum Values
Moderate	0.1
Fairly high	0.38

Table 13 Set of fuzzy conclusions of the 10 scenarios

Scenario No.	Set of Fuzzy Conclusions
1	Moderate 0.1, fairly high 0.38
2	Moderate 0.5, fairly high 0.1
3	Fairly high 0.29, high 0.4
4	Fairly high 0.28
5	Fairly high 0.39, high 0.19
6	Moderate 0.12, fairly high 0.39
7	Fairly low 0.31
8	Moderate 0.38, fairly high 0.19
9	Moderate 0.28, fairly high 0.14
10	Moderate 0.05, fairly high 0.4

Table 14 Defuzzified values of the 10 scenarios

Scenario No.	Defuzzified Values
1	3.98
2	2.42
3	6.53
4	4.5
5	5.65
6	3.91
7	1.0
8	2.83
9	2.83
10	4.22

than the others. This is demonstrated by MSMs 10, 9, and 7 whose differences between the original and expected defuzzified values are 1.82, 0.83, and 0.12 corresponding to the feasibility values of 0.1, 0.2, and 0.9, respectively. Their positions in priority ranking are 1st, 5th, and 10th as shown in Table 17. It should be noted that if the difference of practicability values between MSMs is comparatively small, i.e., MSM 2 and MSM 6 in the case study, further study should be conducted to investigate the priority order with care.

4.7. The implementation of the prioritized MSMs and the acquisition of data after implementation

The preference of the MSMs has been determined based on the practicability assessment as shown in Table 16. It is produced, taking into account diverse aspects, including risk assessment, the availability of resources, the costs and time consumption, success rate, and the probability of undesirable impact once implemented. The MSMs could subsequently be implemented according to their priority order. Furthermore, to ensure that the port security risk assessment model presented could be capable of dealing with the missions desired by the administration at any time, it is important to keep it updated. Therefore, a periodic collection and analysis of the security data is suggested.

5. Conclusion

The security assessment is usually difficult to model since its characteristic has been regarded as an unpredictable likelihood but with a high consequence. In this study, the port security is evaluated based on the concept of risk assessment and management using fuzzy modeling illustrating a different thinking of assessing security. Within the FMECA framework, the risk level of each scenario can be appreciated. The modified security measures are then proposed based on the risk assessment aspect. The feasibility and effect of these measures are subsequently considered using EFMEA to ensure that the modified measures proposed based on risk assessment are practically and cost effectively acceptable. Although the model proposed in this study is capable of dealing with the security risk in ports when there is not much precise information in hand, the quantification of the data compiled and collected from daily operations associated with security is still recommended.

Table 15 Details of hypothetical scenarios and modified security measures proposed

Scenario No.	Hypothetical Details	Modified Security Measures
1	Maritime terrorist attack to chemical facilities	MSM 1: Deployment of waterway management initiatives
2	Vandalism of inappropriate use of dry bulk terminals	MSM 2: Landside patrol
3	Terrorist attack to oil terminals	MSM 3: Deployment of an emergency response team
4	Smuggling explosives against container facilities	MSM 4: Procurement of nonintrusive inspection (NII) facilities
5	Terrorist attack to oil deports	MSM 5: Improved monitoring of access and egress control from depots
6	Intrusive assault against unmanned areas	MSM 6: Procurement of closed circuit television (CCTV)
7	Stowaways against dry bulk facilities	MSM 7: Establishment of transportation security cards for port personnel
8	Cargo theft against container yard	MSM 8: Use of tamper-evident containers
9	Armed assault and robbery against warehouses	MSM 9: Procurement of detecting equipment
10	Opportunistic crime to the headquarter of the port authority	MSM 10: Deployment of security personnel

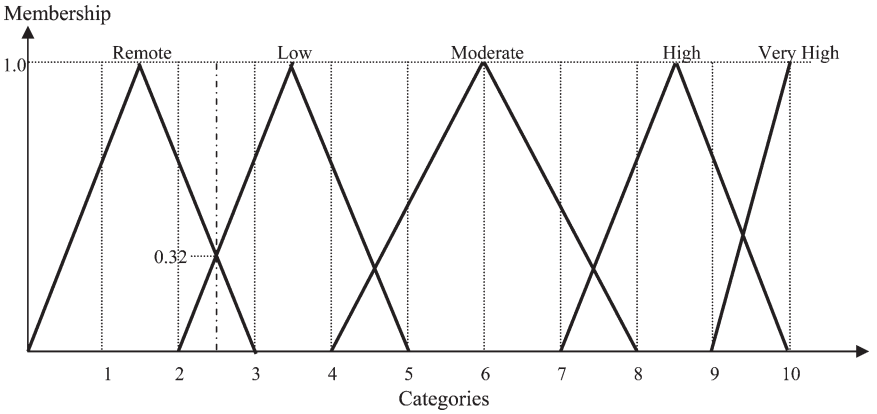

Fig. 6 The determination of membership function for the probability of occurrence

Table 16 Expected levels of C, P, S, and V of each assumed scenario after the modified security measures in place

Scenario No.	Criticality	Probability of Occurrence	Severity	Vulnerability
1	Moderate 0.38, high 0.18	Remote 0.32, low 0.32	Moderate 0.42, high 0.11	Low 0.5, moderate 0.1
2	Remote 0.5	Moderate 0.41, low 0.1	Low 0.68	Low 0.46, remote 0.19
3	Very high 0.4, high 0.4	Low 0.51, moderate 0.8	Low 0.68	Moderate 0.8
4	Moderate 1	Low 0.51, remote 0.11	Moderate 0.65	Moderate 0.42, high 0.07
5	Very high 0.9, high 0.05	Remote 0.32, low 0.32	Low 0.55, moderate 0.06	Moderate 0.5
6	Low 0.39, moderate 0.19	Moderate 0.41, low 0.11	Moderate 0.7	Low 0.51, remote 0.11
7	Low 0.5, remote 0.17	Remote 0.32, low 0.32	Low 0.53, remote 0.1	Remote 1
8	Moderate 0.38, high 0.18	Moderate 0.67	Low 0.41, remote 0.25	Moderate 0.6
9	Low 0.42, moderate 0.14	Moderate 0.4, high 0.12	Moderate 0.7	Low 0.55, remote 0.1
10	Very high 0.9, high 0.05	Remote 0.5	Remote 0.5	Moderate 0.42, high 0.08

Table 17 MSM priority

Scenario No.	Original Defuzzified Values	Modified Security Measures Designed	Expected Defuzzified Values	$F(x)_j$	$P(x)_j$	MSM Priority
1	3.98	MSM 1	2.6	0.3	4.6	4
2	2.42	MSM 2	1	0.6	2.37	8
3	6.53	MSM 3	3.25	0.5	6.56	2
4	4.5	MSM 4	2.36	0.4	5.35	3
5	5.65	MSM 5	2.96	0.7	3.84	6
6	3.91	MSM 6	1.8	0.8	2.64	7
7	1.0	MSM 7	0.88	0.9	0.13	10
8	2.83	MSM 8	2.52	0.5	0.62	9
9	2.83	MSM 9	2.0	0.2	4.15	–5
10	4.22	MSM 10	2.4	0.1	18.2	1

References

Aldridge, J., Taylor, J., and Dale, B. 1991 The application of failure mode and effects analysis at an automotive components manufacturer, *International Journal of Quality & Reliability Management*, **8**, 3, 44–56.

Andrew, J. D., and Moss, T. R. 2002 Reliability and Risk Assessment, 2nd ed., Professional Engineering Publishing Limited, Suffolk, U. K., 107.

ASIS International Guidelines Commission 2003 *The General Security Risk Assessment Guideline*, ASIS International, Alexandria, VA, 703-519-6200.

Bell, D., Cox, L., Jackson, S., and Schaefer, P. 1992 Using causal reasoning for automated failure modes and effects analysis (FMEA), *Proceedings of Annual Reliability and Maintainability Symposium*, Jan 21-23, Las Vegas, NV, 343–353.

Ben-Daya, M., and Raouf, A. 1993 A revised failure mode and effects analysis model, *International Journal of Quality & Reliability Management*, **13**, 1, 43–47.

Bluvband, Z., Grabov, P., and Nakar, O. 2004 Expanded FMEA (EFMEA), *The IEEE Proceedings of Annual Reliability and Maintainability Symposium*, Jan 26-Feb 29, Los Angeles, CA, 31–36.

Bowles, J. B., and Pelaez, C. E. 1995 Fuzzy logic prioritisation of failures in a system failure mode, effects and criticality analysis, *Reliability Engineering & System Safety*, **50**, Part 2, 203–213.

Braglia, M., and Bevilacqua, M. 2000 Fuzzy modelling and analytical hierarchy processing as a means of quantifying risk levels associated with failure modes in production systems, *Technology Law and Insurance*, **5**, 125–134.

Deng, J. 1989 Introduction to grey system theory, *Journal of Grey System*, **1**, 1, 1–24.

Ford Motor Company 1988 *Instruction Manual Process FMEA*.

Gilchrist, W. 1993 Modelling failure modes and effects analysis, *International Journal of Quality & Reliability Management*, **10**, 5, 16–23.

Kara-Zaitri, C., Keller, A. Z., Barody, I., and Fleming, P. V. 1991 An improved FMEA methodology, *Proceedings of Annual Reliability and Maintainability Symposium*, Jan 29-31, Orlando, FL, 248–252.

Kara-Zaitri, C., Keller, A. Z., and Fleming, P. V. 1992 A smart failure mode and effect analysis package, *Proceedings of Annual Reliability and Maintainability Symposium*, Jan 21-23, Las Vegas, NV, 414–421.

Klir, G. J., and Yuan, B. 1995 *Fuzzy Sets and Fuzzy Logic, Theory and Application*, Prentice Hall Inc., Upper Saddle River, NJ.

Kuusela, H., Spence, M. T., and Kanto, A. J. 1998 Expertise effects on pre-choice decision processes and final outcomes: a protocol analysis, *European Journal of Marketing*, **32**, 5/6, 559–576.

Pillay, A., and Wang, J. 2002 Risk assessment of fishing vessels using fuzzy set approach, *International Journal of Reliability Quality and Safety Engineering*, **9**, 2, 163–181.

Pillay, A., and Wang, J. 2003 A risk ranking approach incorporating fuzzy set theory and grey theory, *Engineering Reliability & System Safety*, **79**, 1, 61–67.

Price, C. J., Hunt, J. E., Lee, M. H., and Ormsby, R. T. 1992 A model-based approach to the automation of failure mode effects analysis for design, *Proceedings of IMechE*, Part D, Automobile Engineering, 285–291.

Price, C. J., Pugh, D. R., Wilson, M. S., and Snooke, N. 1995 The flame system: automating electrical failure mode and effects analysis (FMEA), *Proceedings of Annual Reliability and Maintainability Symposium*, Jan 16-19, Washington, D.C., 90–95.

Runkler, T. A., and Glesner, M. A. 1993 A set of axioms for defuzzification strategies toward a theory of rational defuzzification operators, *Proceedings of the Second IEEE International Conference on Fuzzy Set System*, New York, 1161–1166.

Russomanno, D. J., Bonnel, R. D., and Bowles, J. B. 1992 A blackboard model of an expert system for failure mode and effects analysis, *Proceedings of Annual Reliability and Maintainability Symposium*, Jan 21-23, Las Vegas, NV, 483–489.

Sankar, N. R., and Prabju, B. S. 2000 Modified approach for prioritisation of failures in a system failure mode and effects analysis, *International Journal of Quality & Reliability Management*, 18, 3, 324–335.

Sii, H. S., Ruxton, T., and Wang, J. 2001 A fuzzy-logic-based approach to qualitative safety modelling for marine systems, *Engineering Reliability & System Safety*, **73**, 1, 19–34.

U.S. Department of Veteran Affairs 2002 Physical security assessment for the Department of Veteran Affairs facilities. Available at http://www.va.gov/facmgt/standard/etc/vaphysicalsecurityreport.pdf. Accessed July 10, 2004.

Ung, S. T., Williams, V., Bonsall, S., Wall, A., and Wang, J. 2004 An introduction of risk-based maritime security, *The Journal of the UK Safety & Reliability Society*, **24**, 2, 13–22.

Wang, L. X. 1997 *A Course in Fuzzy Systems and Control*, Prentice Hall Inc., Upper Saddle River, NJ.

Zadeh, L.A. 1965 Fuzzy sets, *Information and Control*, **8**, 338–353.

Zafiropoulos, E. P., and Dialynas, E. N. 2004 Reliability prediction and failure mode effects and criticality analysis (FMECA) of electronic devices using fuzzy logic, *International Journal of Quality & Reliability Management*, **22**, 2, 183–200.

Appendix 1. The Fuzzy Rules Applied in the Case Study

No.	Criticality	Probability of Occurrence	Severity	Vulnerability	Priority Level
299	Moderate	Low	Very high	High	Fairly high (0.5)
424	High	Low	Very high	High	Fairly high (0.8)
324	Moderate	Moderate	Very high	High	Fairly high (0.7)
449	High	Moderate	Very high	High	Fairly high (1)
289	Moderate	Low	Moderate	High	Fairly high (0.1)
414	High	Low	Moderate	High	Fairly high (0.4)
314	Moderate	Moderate	Moderate	High	Fairly high (0.3)
439	High	Moderate	Moderate	High	Fairly high (0.6)
298	Moderate	Low	Very high	Moderate	Fairly high (0.2)
423	High	Low	Very high	Moderate	Fairly high (0.5)
323	Moderate	Moderate	Very high	Moderate	Fairly high (0.4)
448	High	Moderate	Very high	Moderate	Fairly high (0.7)
288	Moderate	Low	Moderate	Moderate	Moderate (0.8)
413	High	Low	Moderate	Moderate	Fairly high (0.1)
313	Moderate	Moderate	Moderate	Moderate	Moderate (1)
438	High	Moderate	Moderate	Moderate	Fairly high (0.3)