JOURNAL OF CURRENT RESEARCH IN SCIENCE
ISSN 2322-5009
CODEN (USA): JCRSDJ
Available at www.jcrs010.com

JCRS
4 (3), 2016: 94-103

Elaborating the vulnerability of seaports and providing their security pattern under emergency conditions

Jalal Mohammadi Baghmollaei [1], Habibollah Sahami[2*]

1. Ports and Maritime Organisation, Bushehr. Iran
2. Assistant Professor, Malek Ashtar University of Technology, Tehran, Iran
Corresponding Author email: hsahami15@gmail.com

K E Y W O R D S: Ports; Risk Assessment; Vulnerability Assessment; Threats; Maritime Security; Passive Defense.

ABSTRACT: The geostrategic status of Iran, especially having long coastal borders in the vicinity of the most vital economic lifeline of the world (Persian Gulf) has rendered it to a dependent country on seaports, economically and strategically. Seaports aren't military fortresses and have vulnerable infrastructure as open industrial and business centres, and an effective threats against them can cause extensive economic disorders and damages at national levels. Considering ports' as vital assets, their vulnerable points must be identified and appropriate actions should be performed to repair or strengthen these points. Therefore a coherent pattern must be provided in order to identify vulnerabilities and port security. Regardless of the relative importance weights of the evaluation criteria, it appears to be an urgent need for critical infrastructures to develop a risk assessment methodology to manage the effective components. The main purpose of this paper is to provide a developed framework with the aim to overcome limitations of the classical approach to build a more secure and resilient critical infrastructures. The proposed framework extends conventional RAMCAP [1] through introducing new parameters the effects on risk value. According to the complexity of problem and the inherent uncertainty, this research adopts a fuzzy multi criteria decision making technique to determine the weights of each criterion and the importance of alternatives with respect to criteria. Case analysis is implemented to illustrate the capability and effectiveness of the model for ranking the risk of critical infrastructures. The proposed model demonstrates a significant improvement in comparison with conventional RAMCAP.

Introduction

The unique diversity of activities taking place in seaports and rapid technological changes in this sector, their relationship and the process of economic and social developments, have all made it so sensitive and complex that economic experts, refer seaports as the driving force of development. They also consider its effectiveness and capabilities, as the ground for the comprehensive development of country (Alidoosti, A, etall.2012). According to experts, strategic success in the field of economic growth and development is indebted to massive investment in maritime infrastructures and equipments in seaports. Accordingly, countries that do not invest in this critical issue and neglect or forget it, gradually stay away from the development caravan and advancement and even fail to meet their basic needs. Iran at present having more than 6500 km. maritime borders with neighbouring countries and the possibility of invasion by the country's main adversaries (US, Israel regime and their allies) indicate that special attention must be paid to the assets of seaports and their vulnerability.

The geostrategic position of our country, especially having long coastal areas in the vicinity of the most vital economic lifeline of the world (Persian Gulf) has converted Iran to a dependent country on coastal borders and ports, economically and strategically. It is obvious that an offensive attack against maritime infrastructures can cause major disruption and huge volume of losses and damages . (Van klink.A. 1995) Therefore particular attention should be focused to the vulnerability of seaport's assets. (Chen, Sh-M. and Sanguansat, K., 2010).

Coastal borders in Iran, especially the Persian Gulf are considered as centres of high and growing tension over the country's security because of the presence of fixed and mobile foreign bases and existence of country's vital infrastructures. Stress born Politics of foreign forces in the region indicate the effectiveness of the degree of threats. Warships and naval vessels represent the offensive activity of the adversary forces in the southern waters are certainly faced with various constraints, but these limitations, according to the dynamic and changing technology of invasion can be reduced and overcome. Due to extremely wide possibilities in how the invasion and defence is conceivable, maintaining

[1] RAMCAP (Risk Analysis and Management for Critical Asset Protection)

the security and reducing the vulnerability of ports and maritime infrastructure, is unavoidable through the implementation of their safety procedures against the threats based on the principles of passive defence.

During the Iran-Iraq war, Iranian repeatedly faced with military threats by the US naval on their coastal borders and ports , thereby achieving lessons from the past that, attention should be paid to the new asymmetrical military threats. In this paper, the issue of protection of seaports and maritime infrastructures in the new asymmetric against the threats are analyzed , while presenting an appropriate model for assessing the vulnerability of ports, based on scientific advices and valuable guidelines to determine how to countermeasure the threats with an emphasis on the principles of civil defence.

Background research

Although various experts have provided detailed investigative reports about the importance of seaports and their impacts to the country's economy and development, as well as their safety particularly how to cope with emergency situations. It should be noted that after the September 11 attacks, the Americans forced to evaluate and analyse the vulnerability of their seaports in the event of vandalism incidents. While currently available analytical reports, somehow indicate appropriate approaches to assessing the vulnerability of ports but Iran's strategy in immunization and countering the threat of its kind should be indigenous and based on the principles of passive defense requirements. Although scientific and research documentation and reports collection as the institution's risk assessment and management by FEMA, especially after the events of September 11 were released. But they mainly highlight analytical - scientific and guidelines on the design of critical infrastructure and facilities against terrorist threats (Bajpai, Sh. et all., 2010). In these documentary and scientific collections, threat assessment methods, risk analysis, are determined based to needs of a particular type of threat that is called terrorism. (Nieto-Morote, A. and Ruz-Vila, F., 2011).

Research Methodology

The appropriate research method used in this study, is descriptive research method. It should be noted that in this study, the MATLAB software is used to build the knowledge base which will be discussed with the help of experts points of view. Deduction system to assess the risk from the type of Mamdani is selected, which is one of the most applicable methods in creating inference system. The following steps are taken to carry out this investigation.

To study the relevant books and journals, interviews with experts, specialists and experienced.
Formulate hypotheses and design research methodology.
Design techniques and methods needed for research, pilot implementation
Choosing the candidate samples to be investigated.
Fieldworking collection and receiving information and data.
Coding and data processing.
Statistical analysis.
Collect results and testing the hypotheses.
Coding in Software Environment
Check the output of the application
Analysis of the results

Research Findings

Adequate knowledge and comprehensive data base on a number of different problems are required to analyse critical infrastructures. There are a close relationship between complexity and certainty, so that; increasing the complexity lead to decrease the certainty. Fuzzy logic , introduced by Zadeh (1965) - can take into account uncertainty and solve problems where there are no sharp boundaries and precise values. Fuzzy logic provides a methodology for computing directly with words (Zadeh, 1996).

Fuzzy set is a powerful mathematical tool for handling the existing uncertain in decision making. A fuzzy set is general form of a crisp set. A fuzzy number belong to the closed interval 0 and 1, which 1 addresses full membership and 0 expresses non-membership. Whereas, crisp sets only allow 0 or 1. There are different types of fuzzy numbers that can be utilized based on the situation. It is often convenient to work with triangular fuzzy numbers (TFNs) because they are computed simply, and are useful in promoting representation and information processing in a fuzzy environment (Torlak et al, 2011).Fuzzy Inference System for the design should four network structures, namely: (1) the construction phase, (2) the fuzzy rule base, (3) the fuzzy inference engine and (4) defuzzification, designed and built.

For this purpose, with using MATLAB software package to build a knowledge base on the policies if ... then ... with the use of experts has been paid.

The first step in making model is to determine the input variables in order to find out the relationship between these input and the output which is security risk. In RAMCAP methodology, three main criteria of consequences, vulnerabilities and threats for obtaining risks are used. Therefore, in this study all outcome measures, vulnerabilities, threats and risks as fuzzy are presented.(Yazdani. M. etall, 2012)

Risk assessment is a methodology to determine the nature and extent of risk by analyzing potential hazards and evaluating existing conditions of vulnerability that could pose a potential threat or harm to people, property, livelihoods

and the environment on which they depend. The Standards defines Risk as the chance of something to happen that will have an impact upon objectives. It is measured in terms of consequences and probability.
Risk = Consequences x Likelihood

The term Consequence can be defined as the outcome of an event or situation, such as a loss, injury or even as a gain. The loss events could include: Death, Serious injury, First aid treatments, Acute or chronic disease, Loss of production, Equipment damage, Environmental damage, Loss of reputation etc.
Likelihood: Is used as a qualitative description of probability and frequency.
Likelihood = Probability x Frequency
Probability: Is the likelihood of a specific outcome, measured by the ratio of specific outcomes to the total number of possible outcomes.
Frequency: Is a measure of likelihood expressed as the number of occurrences of an event in a given time.

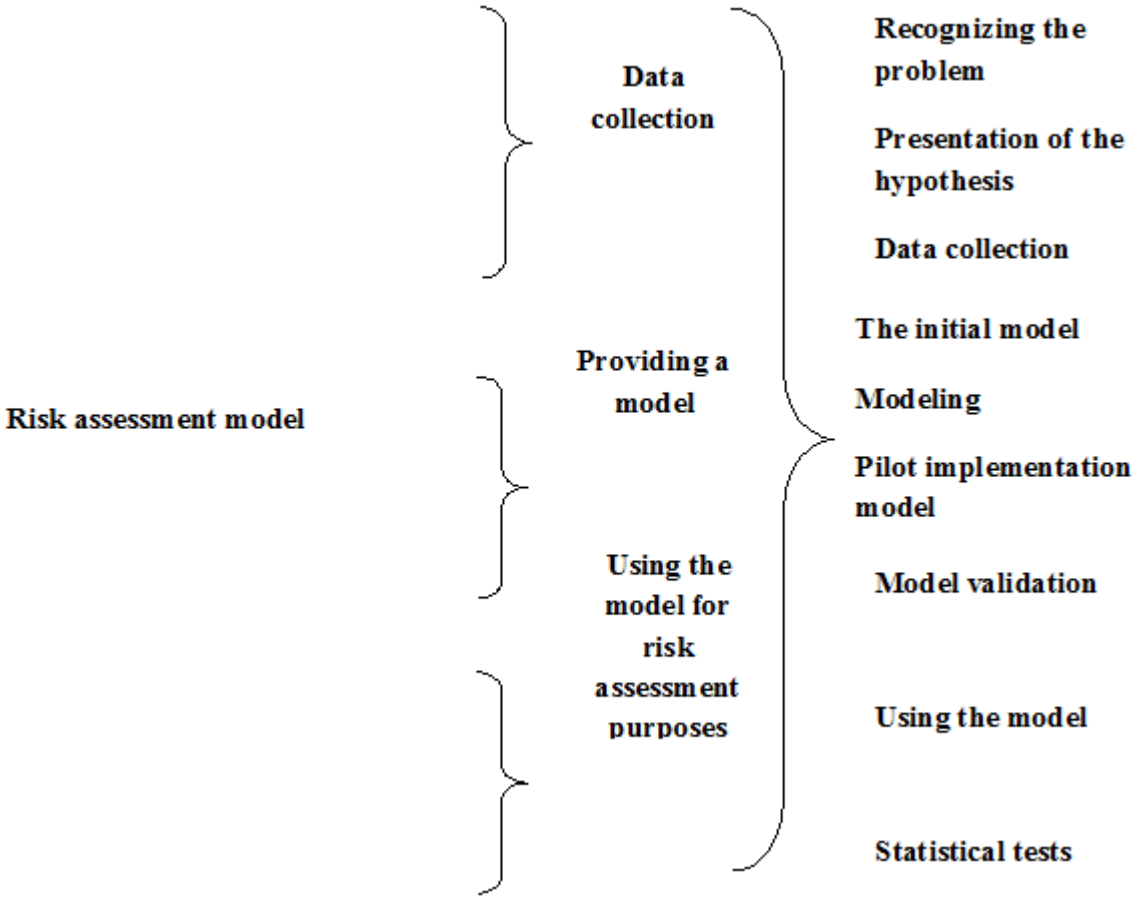


Figure 1. Process of making a risk assessment model

Fuzzy logic
Fuzzy set

A fuzzy set is a collection of elements in a universe of information where the boundary of the set contained in the universe is ambiguous, vague and otherwise fuzzy. Each fuzzy set is specified by a membership function, which assigns to each element in the universe of discourse a value within the unit interval [0, 1] (Sun, Ch.. 2010) Unlike crisp (or ordinary) sets, fuzzy sets have no sharp or precise boundaries (Liu, K. etall. , 2009). The concept of a fuzzy set provides mathematical formulations that can characterize the uncertain parameters involved in particular risk analysis method. Contrary to classical sets, fuzzy sets accommodate various degrees of membership on continuous interval [0,1], where '0' conforms to no membership and '1' conforms to full membership. So, even the most sophisticated, precise, and well constructed quantitative model may give misleading results if uncertainties are not treated at some level. Uncertainty in risk analysis can range from modeling uncertainties, to incomplete and unreliable information. Data uncertainties are a major source. Any system under study has dominant risk contributors in addition to the dependent failures usually studied (Singh, R.K., & Benyoucef, L. 2011)

There are different states in a secure set depicted in Fig. and it shows smooth change from secure to insecure state in fuzzy set under consideration. Vice versa, Boolean logic only takes into account two values 0, 1, where 1 addresses full membership for set under consideration and 0 addresses element do not belong to the set (Alidoosti et al., 2011).

Fuzzy inference systems

Fuzzy inference is the process of mapping from a given input set to an output set using fuzzy logic. Membership functions, fuzzy logic operators and if-then rules are used in this process. (Elsayed .2009). The basic idea of a fuzzy inference system is to use fuzzy logic to define an output as a function of measured inputs (Horgby. 1998). The basic advantage of such system is its tolerability to linguistic/imprecise data.

In this study, according to the structure of the study is to assess and manage security risks from the type of Mamdani which is one of the most used methods used in creating inference system

Membership function of vulnerability, threat and risk parameters based on RAMCAP methodology, contain five membership functions which include the linguistic values from very low (VL), low (L), medium (M), high (H) and very high (VH). While the Consequence membership functions for parameter including five membership function with little linguistic value (N), low (Mi), moderate (Mo), high (S) and very high (C) are shown. In order to better understand each of these fuzzy variables, these membership functions are provided In Figures 3 to 7.

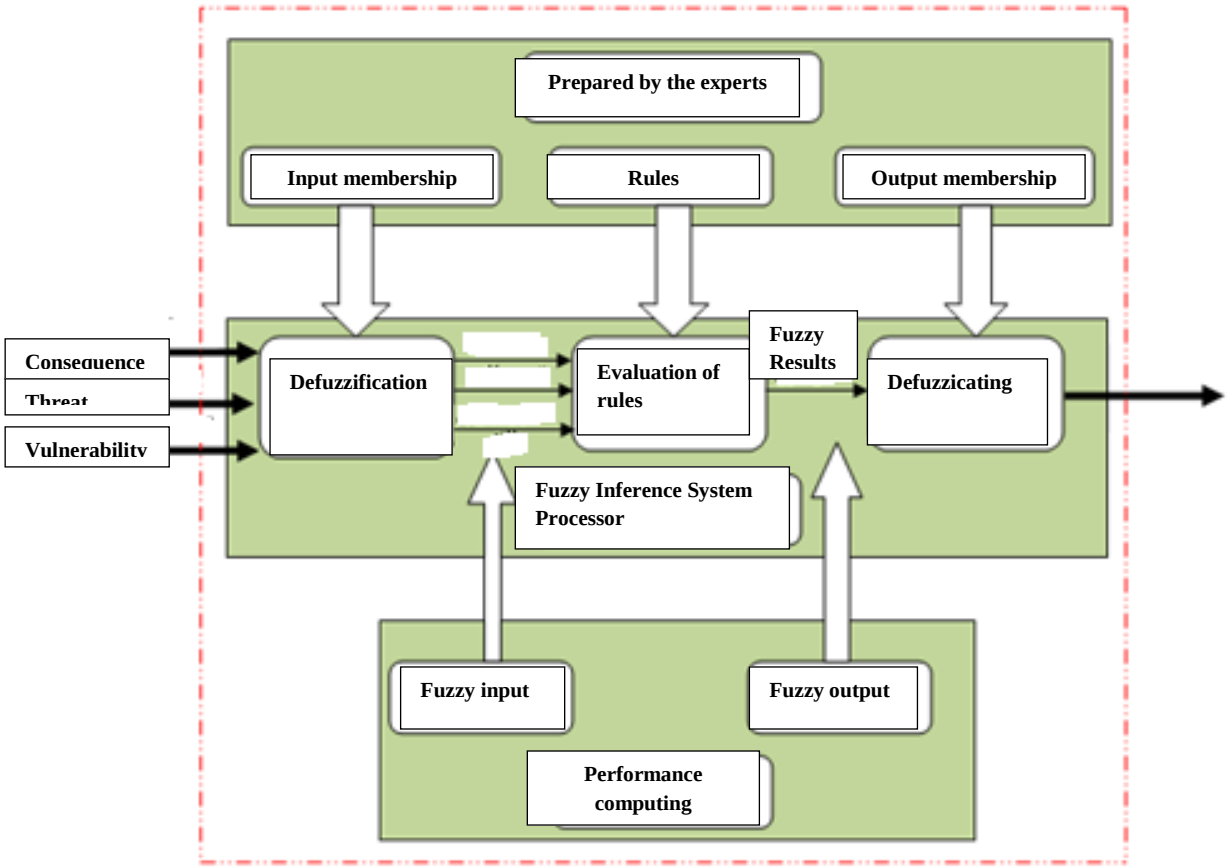


Figure 2. Process of obtaining risk

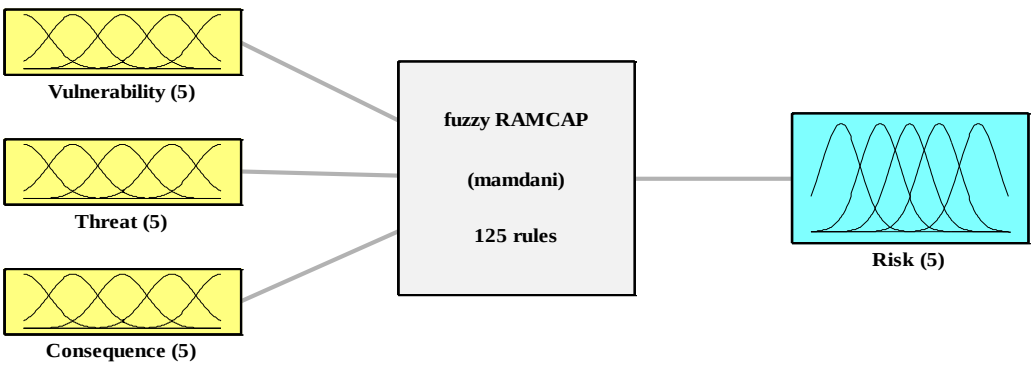


Figure 3. The architecture of the fuzzy inference system

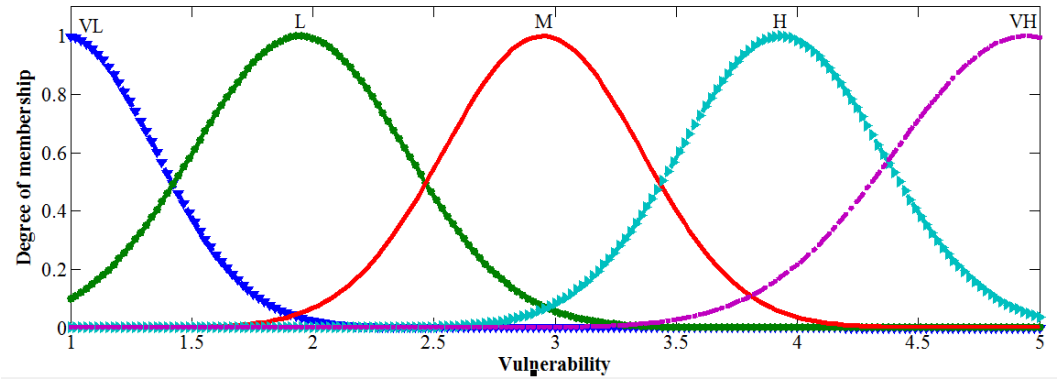


Figure 4. Membership functions of Vulnerability

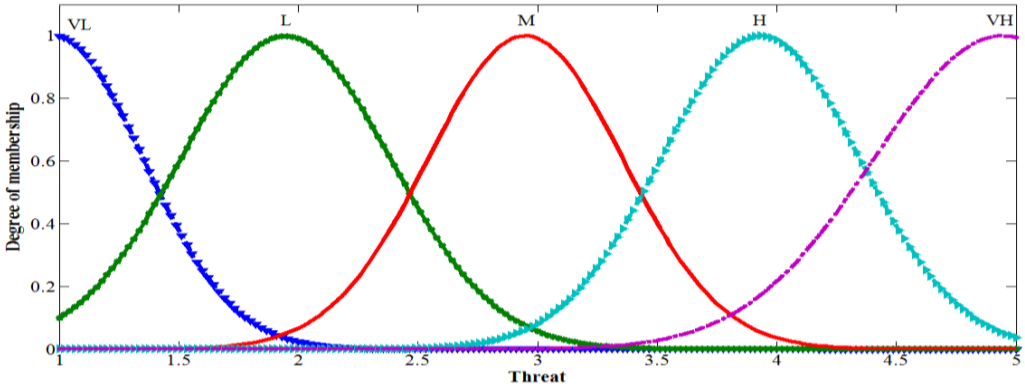


Figure 5. Membership functions of threat

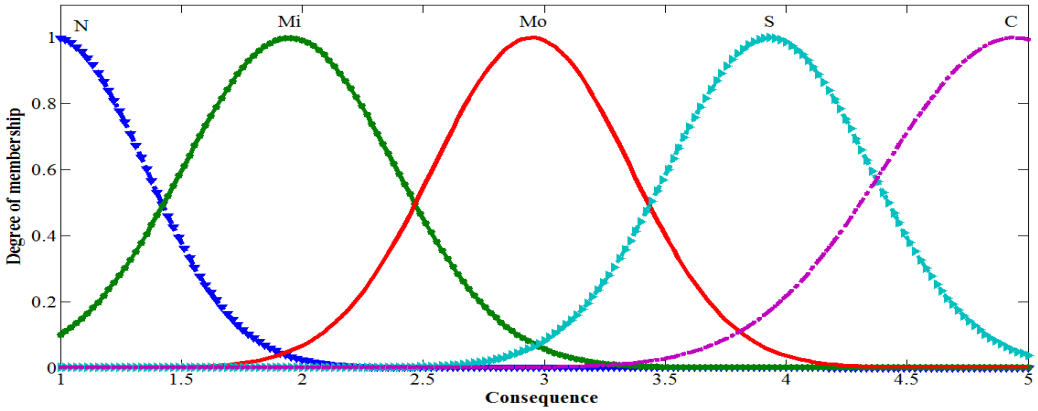
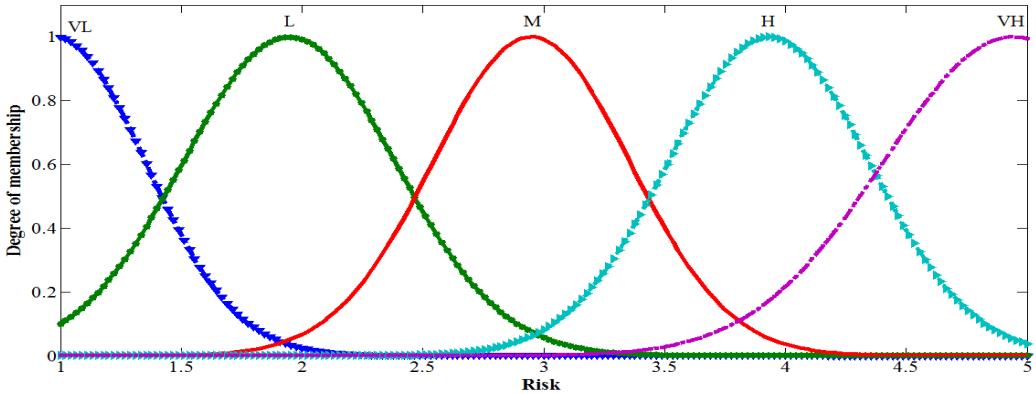


Figure 6. membership functions of consequence



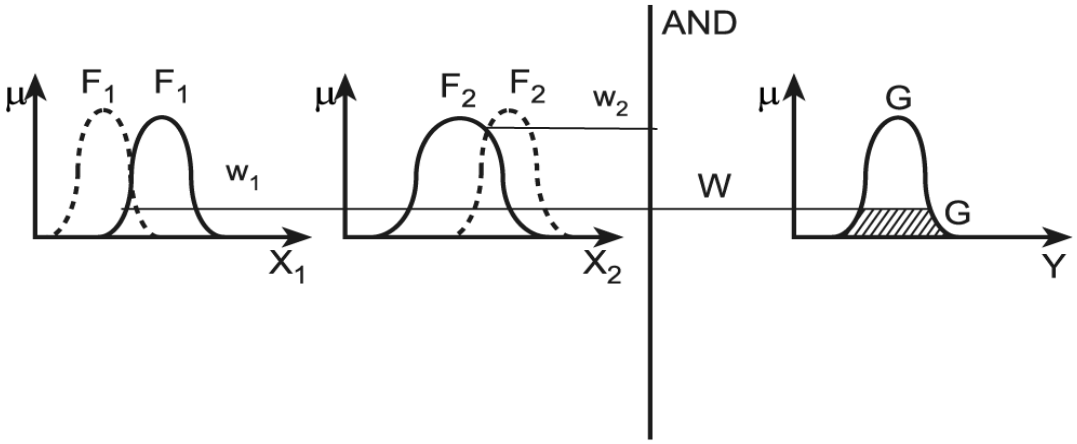
7. Membership functions of risk

Implementation of method

As the figures above indicate, membership functions used in this study is of Gaussian type. Since these membership functions simply display the mathematical characteristic. Moreover, Gaussian functions are considered as linkage mode that makes these functions smoothly and are non-zero. Gaussian membership function can be shown as follows:

$$Gaussion(x;c,\sigma) = e^{-\frac{1}{2}(\frac{x-c}{\sigma})^2}$$

Where c and σ are respectively the center and width of the membership function. In this study, for example, for each input variable, vulnerability, c has a fixed value of 0 for expression first language and 5 for expression final language and others, the center of expression language. Parameter is adapted so that each member function in approximately 50% overlaps. This causes the risk related to the lack of consideration of a special occasion to be removed. Figure 8 shows the fuzzy inference system with fuzzy membership functions that affect the operator AND (intersection of two fuzzy sets).



8. Fuzzy Inference System with Gaussian functions

To form a knowledge base, 125 laws if.... then.... written an example of the rules on risk for the law if... then, is provided graphically in Figure 9.

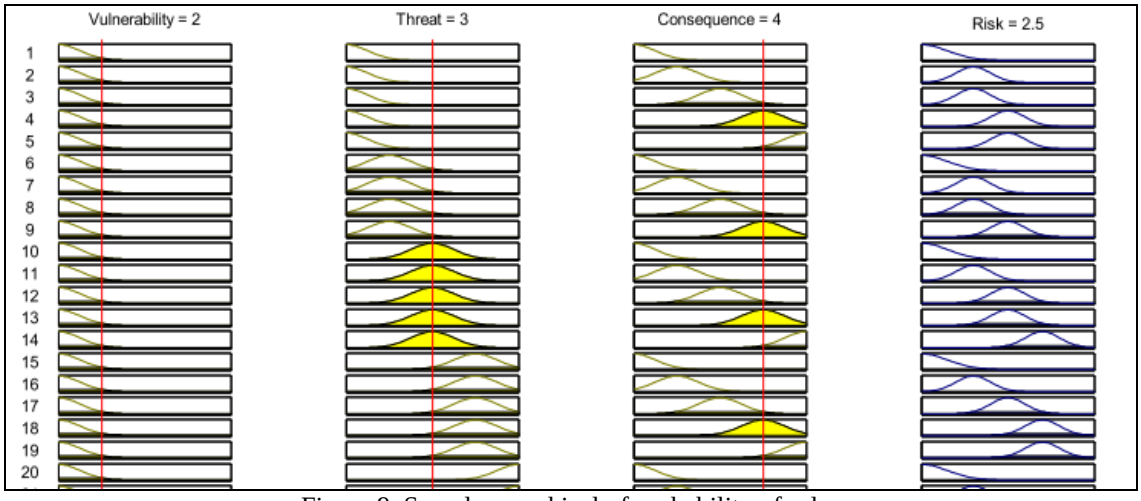


Figure 9. Samples graphical of probability of rules

Figures 10 to 12 show the output sensitivity risk model by using changes in threats, vulnerabilities and threats. As can be seen from Figure 10 risk behavior is associated with two inputs vulnerability and threat in such a way that an increase in the level of risk, increases the vulnerability and threat,.

Figure 11 shows the simultaneous impact of the increased threat and consequences taking into account the fixed amount for vulnerabilities Show on the risk. So that it is clear from this figure, an almost linear increase between the two inputs variables are evaluated on the level of risk. Figure 12 also increases the amount of risk increasing the consequences and vulnerability rates when variables are constant threats, show.

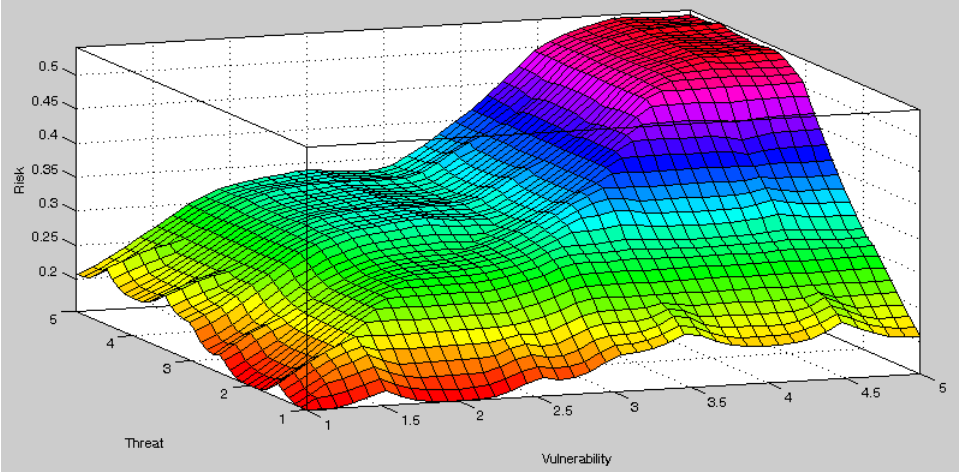


Figure 10. The sensitivity of risk to changes in vulnerability and threat

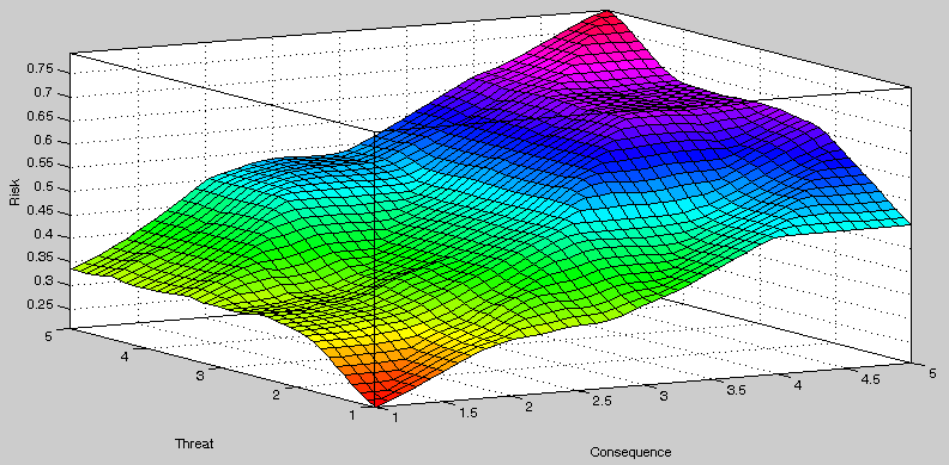


Figure 11. The sensitivity of risk to changes in the threat and consequences

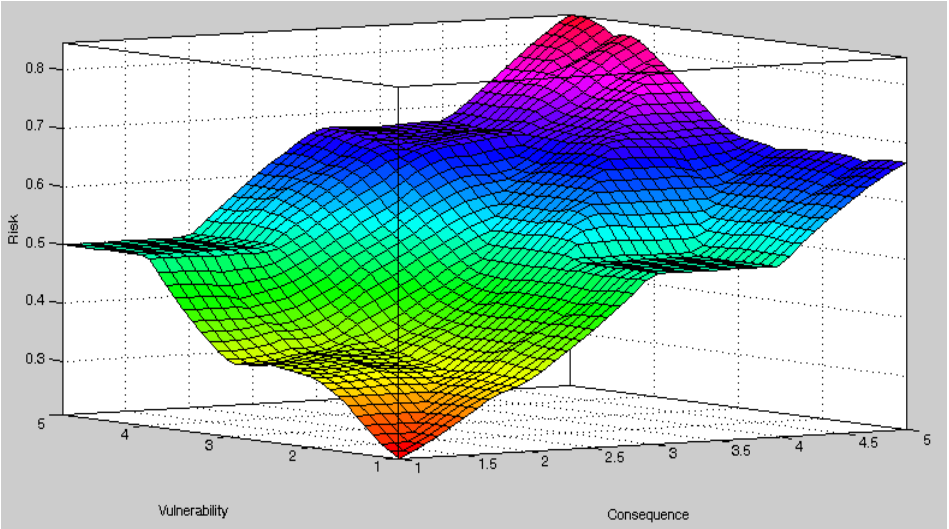


Figure 12. The sensitivity of risk to changes in vulnerability and consequences

Case Study

Seaport activities which mailnly include goods loading and unloading, operate relying upon the management activities of human resources, facilities and navigation equipment. The facility consists of berthing space for cargo vessels, cargo handling and storage, and a channel and turn-around area for vessels up to 175 feet in length with a draft of up to 12 feet. administrative building which houses the dock master's office and public restrooms..

Perceived threats and levels of the effects

In investigations perceived threats for ports based on the origin of influences threaten these are divided into three categories:

Internal threats (performance)

The scope of these threats in the field of ports activities and in different events related to the performance of collection include: Accidents warehouse fire, collision of ships to wharf and closing the internal communication ports congestion caused by trailers and other vehicles and pedestrians.... The impact of these threats, are limited to some of the ports.and has little effect on ship traffic in general trend activities of ports

Internal threats (subversive and terrorism)

The scope of these threats are imaginable in both land and sea. In the field of sea, the risk of sinking in pond input channel in order to disable ports activities are reported. This can have a significant impact on ports activities in the normal process and the general trend., The risk of bombings and explosions; by domestic factors or trailer load carrier and by small arms , mortars and shoulder-fired , are imaginable in the field of land . This occurs only to reduce the level of security in the region and consequently causing fear and panic in the hearts of goods and ships owners.

External threats

The scope of this threat are imaginable in both hard and soft. In the field of software, through pressure and economic sanctions or creating a psychological war as well as a variety of non-destructive weapons such as cyber-attacks, electromagnetic, threat occurs, whereby in addition to creating the consequences of psychological, social and economic threats ,the whole country, in the field of ports, and also a decrease in activity levels due to decreased vessel traffic and to reduce commodity exchange (import and export) are expected

In the field of hardware, known adversaries to the country creating numerous problems, provided the conditions to impose their demands and invade if their demands are not met, by creating the relative consensus among their allies.

Ranking of threats in ports (in order of preference)

The followings are the priority (ranking) of the threats on ports (from probability of high threat to low threats) that was conducted by experts:

Illegal traffic (hypocrites' relationship with staff and crew of vessels)
Passenger smuggled (pedestrian of unauthorized)
Assemble and strike (provocation by infiltrators)
Arson (by Kieran balance and unhappy)
Theft property responsible (by haters and people dissatisfied)
Release of hazardous materials and toxic (by the infiltrators)
Drug trafficking
Sabotage (bombs, explosion, shipwreck in channel, etc.)
Hostage taking
Theft and seizure of ships
Disruption of communication (cyber and electromagnetic, etc.)
Unauthorized access to information.
Military attack
Bandit / piracy

Scenario of threats

Invasion, or any threat to destroy, delete or inflict inefficiency to the system, activities or human resources such as mental phenomena, have all a plan and program support basis. In other words, different stages of beginning of threats until the end of an invasion, possess a wide range of potential vulnerabilities in the international macro scale to the national and regiona levell.

Threatening factor or Invading country, set different threat's plan, according to its policy and objectives,.In addition to the geographical scope and the extent of the target range, threat intensity and the rate of invasion, are considered among the strategies and objectives of macroeconomic policy strategy of the attacker which will determine the severity of threat. Other factors in the hierarchy of threats and attacks, which is to be considered, especially is based on a theory of Wordan,. (National leadership, key products, arteries of communication infrastructure, people and armed forces). While all attacks in a country can not necessarily adhere to the idea of such orientation process. For this reason, in addition to the physical characteristics and objective of threat levels and different sectors, goals and policies of higher levels will also be considered. In other words, setting the scenario or the process of intimidation and aggression are based on goals and policies involved

Evaluation of risks in seaports

In this example, eight critical assets, including office and administrative building collection (A1), receiving installations, power generation and transmission (A2), collection radio and telecommunications (A3), docks (A4), Input channels and ponds (A5), loading and unloading equipment (A6), gate and security guard (A7), internal and external access (A8), tanks of oil Company (A9), warehouses (A10), desalination and water Tanks (A11), collection of services and amenities (A12) and anchorage (A13) are investigated.

In risk assessment calculation tables, the three components of risk, threat and consequence based on "calculated risk priority numbers", are evaluated, and the by multiplying the three factores of risk, threat and consequence, the main risk index is obtained. The evaluation team consisted of 6 experts with a high degree of knowledge in the field of risk analysis.They assessed the existing assets under the three components of vulnerability, threat and consequences, such that the highest value is given the highest risk. Due to problems related to the uncertainty of the assessment of risk factors and their associated weights, the evaluation team agreed to assets evaluated using linguistic variables and then compare the output with the output of conventional method of RAMCAP .

Conclusion

In this study, after presenting an overview of risk, especially in the field of security risks in the seaports and emphasizing the important role of ports on the dynamics of country's economy, the importance of anticipating risks associated with this sector and the various methods ,are discussed. This paper developed an extended framework to analyze risk for critical assets in seaports

The main purpose was to investigate the major security risk items in order to allocate the limited resources and time using fuzzy set theory through fuzzy RAMCAP. The proposed methodology is able to solve some inherent imperfection of the RAMCAP. In contrast with the RAMCAP, the Fuzzy RAMCAP considers the relative importance among vulnerability, threat, and consequence. Application of linguistic terms in the input and output information also can be more realistic and flexible by fuzzy RAMCAP. Fuzzy RAMCAP can result a more accurate risk analysis for protection of critical assets in seaports.

In conclusion, seaports security risk modelling by using the system of fuzzy has been conducted. In general, two scenarios are as follows:

The security risk assessment at seaports with an approach of classical risk assessment using RAMCAP.

Ports security risk assessment by using proposed combination of Fuzzy and RAMCAP. Based on the results of these two approaches findings would be concluded as the following table.

Table 1. Risk assessment Security at seaports

Assets	Input						Output			
	Crisp			fuzzy			Traditional RAMCAP	Rank	Fuzzy RAMCAP	Rank
	V	T	C	V	T	C				
A1	5	1	2	4.38	1.06	2.37	10	9	2.12	10
A2	3	2	4	3.02	2.53	3.96	24	3	3.05	5
A3	2	3	4	2.57	3.15	4.05	24	3	3.11	4
A4	4	3	5	3.84	3.22	4.53	60	1	3.78	1
A5	3	2	4	2.65	2.33	3.69	24	3	2.84	7
A6	2	3	2	1.69	3.14	2.21	12	8	1.79	11
A7	2	4	3	1.87	4.00	3.63	24	3	2.75	8
A8	3	3	4	2.95	2.84	4.07	36	2	3.27	2
A9	2	1	1	2	1.11	1.24	2	13	1.12	13
A10	1	3	2	1.23	2.67	1.98	6	11	2.23	9
A11	2	4	2	1.58	4.21	1.69	16	7	3.03	6
A12	1	1	3	1.21	1.09	2.87	3	12	1.67	12
A13	2	1	5	2.12	1.32	4.91	10	9	3.23	3

The findings of this study are as follows

The proposed method is based on fuzzy systems compared to classical RAMCAP have a high potential in modeling complex systems.

Fuzzy Systems are proper tools for modeling uncertainty caused by the lack of information or where the data cannot be measured.

Fuzzy Systems is a knowledge-based tool that is able to model the complex processes based on verbal or linguistic variables and also knowledge of experts.

Suggestions

Fuzzy approach, is a powerful method in modeling the security risk. It is therefore suggested to be used in other infrastructures.

In this study, two methods RAMCAP and Fuzzy were evaluated. It is recommended that other methods available for security risk assessment were undertaken to compare for future research.

Presenting a computer program by using current techniques and the proposed methods can be considered as a new research work for future investigations.

References

Alidoosti, A., Yazdani, M., & Basiri, M., 2012. Fuzzy logic for pipelines risk assessment, Management Science Letters 2 , 1707–1716.

Ashtiani, B., Haghighirad, F., Makui, A., & Montazer, G. 2009. Extension of fuzzy TOPSIS method based on interval-valued fuzzy sets. Applied Soft Computing, 9: 457–461.

Awasthi, A., Chauhan, S. S., & Omrani, H. 2011. Application of fuzzy TOPSIS in

Bajpai, Sh., Sachdeva, A., Gupta, J.P., 2010. Security risk assessment: Applying the concepts of fuzzy logic, Journal of Hazardous Materials 173, 258–264.

Chen, Sh-M., Chen, J-H., 2009a. Fuzzy risk analysis based on similarity measures between interval-valued fuzzy numbers and interval-valued fuzzy number arithmetic operators, Expert Systems with Applications 36, 6309–6317.

Chen, Sh-M., Sanguansat, K., 2010. Analyzing fuzzy risk based on a new fuzzy ranking method between generalized fuzzy numbers, Expert Systems with Applications.

Cox, L.A.J. 2009. Risk Analysis of Complex and Uncertain Systems. Springer Science+Business Media, LLC, (Chapter 15).

evaluating sustainable transportation systems. Expert Systems with Applications, 38 (10): 12270-12280. http://dx.doi.org/10.1016/j.eswa.2011.04.005

Feng, L-H., Luo, G-Y., 2009. Analysis on fuzzy risk of landfall typhoon in Zhejiang province of China, Mathematics and Computers in Simulation 79, 3258–3266

Flores, W. C., Mombello, E., Jardini, J. A., Rattá G., 2009. Fuzzy risk index for power transformer failures due to external short-circuits, Electric Power Systems Research 79, 539–549.

Grassi, A., Gamberini, R., Mora, C., Rimini, B, 2009. A fuzzy multi-attribute model for risk evaluation in workplaces, Safety Science 47, 707–716.

Gürcanli, G. E., Müngen, U., 2009. An occupational safety risk analysis method at construction sites using fuzzy sets, International Journal of Industrial Ergonomics 39, 371–387.

Iranmanesh, H., Shirkouhi,S.N., Skandari,M.R., 2008. Risk Evaluation of Information Technology Projects Based on Fuzzy Analytic Hierarchal Process, World Academy of Science, Engineering and Technology 40, pp.351- 357.

Liu, K., Hao, J., Pang, Y., 2009. Algorithm Research on Project Risk Fuzzy Evaluation, First International Workshop on Database Technology and Applications, pp. 160-164.

Markowski, A. S., Mannan, M. S., Bigoszewska, A., 2009. Fuzzy logic for process safety analysis, Journal of Loss Prevention in the Process Industries 22, 695–702.

Nieto-Morote, A., Ruz-Vila, F., 2011.A fuzzy approach to construction project risk assessment, International Journal of Project Management, 29: 220–231.

Seçme, N. Y., Bayrakdaroglu, A., & Kahraman, C. 2009. Fuzzy performance evaluation in Turkish Banking Sector using Analytic Hierarchy Process and TOPSIS. Expert Systems with Applications, 36: 11699–11709.

Singh, R.K., & Benyoucef, L. 2011. A fuzzy TOPSIS based approach for e-sourcing. Engineering Applications of Artificial Intelligence, 24: 437–448.

Sun, Ch. Ch. (2010). A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods. Expert Systems with Applications, 37: 7745–7754.

Sun, Ch.Ch., & Lin, G.T.R. 2009. Using fuzzy TOPSIS method for evaluating the competitive advantages of shopping websites. Expert Systems with Applications, 36:11764–11771.

Torlak, G., Sevkli, M., Sanal, M., & Zaim, S. 2011. Analyzing business competition by using fuzzy TOPSIS method: An example of Turkish domestic airline industry. Expert Systems with Applications, 38: 3396–3406.

Van klink.A. 1995. Towards the borderless maikportRoterdam: An analysis of functional . Spatial and administrative dynamics in port system.Tinbergen Institute Resesch Seriesno:104

Yang, T., & Hung, C. C. 2007. Multiple-attribute decision making methods for plant layout design problem. Robotics and Computer-Integrated Manufacturing, 23(1): 126-137.

Yu, V.F., & Hu, K.J. 2010. An integrated fuzzy multi-criteria approach for the performance evaluation of multiple manufacturing plants. Computers & Industrial Engineering, 58:269–277.

Yue, Zh. 2011. An extended TOPSIS for determining weights of decision makers with interval numbers. Knowledge-Based Systems, 24: 146–153.

Zadeh, L. A. 1965. Fuzzy sets. Information and control, vol. 8, pp. 338–353

Zadeh, L. A. 1996. Fuzzy Systems, IEEE Transactions on 4 (2), 103-111