Varazdin Development and Entrepreneurship Agency
in cooperation with
Megatrend University, Serbia
University North, Croatia
Faculty of Management University of Warsaw, Poland
Faculty of Law, Economics and Social Sciences Sale - Mohammed V University in Rabat

Economic and Social Development

30th International Scientific Conference on Economic and Social Development

Editors:
Khalid Hammes, Igor Klopotan, Milica Nestorovic

ISSN 1849-7535

Book of Proceedings

Belgrade, 25-26 May 2018

Varazdin Development and Entrepreneurship Agency
in cooperation with
Megatrend University, Serbia
University North, Croatia
Faculty of Management University of Warsaw, Poland
Faculty of Law, Economics and Social Sciences Sale - Mohammed V University in Rabat

Editors:
Khalid Hammes, Igor Klopotan, Milica Nestorovic

Economic and Social Development

30th International Scientific Conference on Economic and Social Development

Book of Proceedings

Belgrade, 25-26 May 2018

CONTENTS

FUZZY LOGIC INFERENCE SYSTEM MODEL FOR RISK ASSESSMENT IN INFORMATION TECHNOLOGY AND SERVICES ENVIRONMENT

Olivera Milutinovic
Faculty of Law, Megatrend University, Serbia
omilutinovic@megatrend.edu.rs

Marija Kerkez
Faculty of Business Studies, Megatrend University, Serbia
majap@rcub.bg.ac.rs

Biljana Mladenovic Vojinovic
Faculty of Technical Science, University of Novi Sad, Serbia
biljana.mv@uns.ac.rs

ABSTRACT

Achieving security in ITS environment is a difficult task, one that is constantly evolving. With the development of technology over the last decades, risk assessments have become increasingly more complex. Availability of information for numerous risk parameters, affects the reliability of the risk assessment in information security processes. Due to that reason there is a need to develop a model that can contribute to increase of reliability of risk evaluation and reduction of subjectivity of the decision-maker regarding the risk level. In the paper, the authors proposed a concept to model the risk of specific processes in the system applying fuzzy logic and by using a procedure of expert valuation of weights of previously defined risk elements, their interrelation and relative importance compared to the total risk. ITS security process data for a specific company are incorporated into proposed model and validated with an example case.

Keywords: *fuzzy logic, ITS, modelling, risk assessments*

1. INTRODUCTION

Advances in information technology has a significant impact on security systems. Processes within systems are exposed to many risks that may occur due to negative scenarios and consequences that can be caused by various events. Frequently, they have significant uncertainty which is associated with their complexity, information reliability and estimation of statistical parameters from the past period of time. Fuzzy logic (FL) is often used to model complex systems, where appliance of other methods and techniques that determine interdependencies between particular variables is very difficult and cannot provide satisfying results. Fuzzy logic, as a mean to model uncertainty and imprecision in risk assessments, is suggested by number of authors, because FL offers a mathematically more precise way of modelling vague preferences. Subject of this paper is an analysis of the total risk in ITS environment, which is determined by five sets of data (basic risk elements). Each of the main risk elements consists of a number of sub-elements that permeates the entire system. Connections between main elements and their sub-elements are also problematic. Therefore, a precise classification is essential, in accordance with different criteria and perceptions of the expert. Consequently, a mathematical model for total risk evaluation, based on fuzzy logic, has been developed.

2. QUALITATIVE AND QUANTITATIVE EVALUATION

As a sets of models, methods and techniques, risk analysis and risk assessment could be qualitative and quantitative (Campbell and J. Stamp, 2004; Patel et al., 2008), but in recent years both approaches are combined (Markovic-Petrovic and Stojanovic, 2014; Ten and Liu, 2010; Wang and Zeng, 2010). Some, often used assessment tools for managing risks in information systems are: NIST, OCTAVE®, FRAP COBRA, Risk Watch etc. Qualitative risk assessment are based on experts' estimation by rating the various factors on a scale which could be, more or less, subjective. For example, that subjectivity is commonly reflected on linguistic variables, such as "very low risk" etc. For the same data, experts can give different linguistic values, which is inherent with a different human perception. For the same data, experts can provide different linguistic values, which are inherent with a different expert's perception, based on their relation to risk, experience etc. On the contrary, in some cases, expert opinion is easily available and may even be more valuable and accurate than historical data. However, risk assessment methods, which rely on expert opinion, must devote more attention to techniques for capturing, formalizing and ultimately turning into numeric values expert knowledge. Mathematically, quantitative risk can be expressed as:

$$\text{Annualized Loss Expectancy} = [\text{Single Loss Expectancy}] \cdot [\text{Annualized Rate of Occurrence}]$$

The formula is clear and logical, however, there are problems in its application in information systems. The most common causes for this are:

1. difficulties in identification and assigning a value to assets,
2. inability to determine the frequency, as a result of the lack of statistical data,
3. qualitative impact is exposed to many factors that can be potentially harmful,
4. difficulties in establishing mathematical principles and relations between assets.

However, estimating the cost of secondary effects is especially difficult because of the uncertainty associated with the ultimate impact on such intangible factors. For example, cost of a system may be easy to define, but this is not a case with the indirect costs, such as value of the information, loss of production activity and recovery cost. In information systems, the assessments is based on the formula: Risk = Probability x Impact, where probability and impact are values expressed in percentages, which is not mathematically correct, but helpful in ranking and determining risks priority.

Alternative formula in use is Risk = Threat x Vulnerability x Impact, in case there is sufficient historical data available, so that values can be assigned more often to frequent incidents (such as malware, spam, data entry errors, etc.). In the Table 1 is presented a hypothetical example (in illustrated purpose) of 4 risk and the procedure for calculating the rating of each individual risk. Raw probability and impact are specified by the persons responsible for monitoring and risk analysis, as a percentage value in the case of untreated risk. Raw risk rating is a product of those values. After evaluation treatment cost, status, probability and impact, current risk rating can be calculate as

$$\textit{Raw risk rating} - \left[\textit{Treatment status} \cdot \left(\textit{Raw risk rating} - \textit{Target risk rating}\right)\right].$$

Table following on the next page

Table1: Current risk rating calculation

Risk	Raw			Treated				Target risk rating	Current risk rating
	Probability	Impact	Risk rating	Cost	Status	Probability	Impact		
Insider incident	35%	65%	23%	$1.000	50%	82%	81%	66%	45%
Malware	85%	78%	66%	$450	50%	25%	40%	10%	38%
Spam	85%	44%	37%	$200	90%	10%	44%	4%	8%
New regulatory compliance	90%	15%	14%	$300	90%	5%	10%	1%	2%

In the next table are guidance of scoring. The values assigned to each category are *arbitrary* and the colors green, amber and red corresponding to the values 0%, 50% and 100%.

Table2: Guidance of scoring

Impact/Probability		**Extreme**	**Major**	**Moderate**	**Minor**	**Insignif.**
		100%	**80%**	**60%**	**25%**	**1%**
(Almost) certain	**100%**	100%	80%	60%	25%	1%
Probable	**80%**	80%	64%	48%	20%	1%
Possible	**60%**	60%	48%	36%	15%	1%
Unlikely	**25%**	25%	20%	15%	6%	0%
Rare	**1%**	1%	1%	1%	0%	0%

The difficulties of the quantitative measurement of security which hold in the risk quantification context are discussed in Verendel, 2009. IT-risk-related data are always linked to the subjective expert evaluation. Complex quantitative methods mostly use limited datasets. That usually leads to an incomplete picture about risks, but on the other hand, simplistic methods can also lead to unreliable expectations about risk. The risk register should be based on a combination of qualitative and quantitative methods to leverage their advantages and avoid some of the disadvantages and encourage quantitative methods where it is possible. Despite that, the expected quality of data for the register is fairly low.

Natural extension to probability risk assessments involves the use of fuzzy concepts (Ralston et al., 2007). Hybrid models in information security, that is apply the fuzzy and hierarchy analysis model to security risk assess were presented in works of (Chang and Hung, 2005; Goel and Chen, 2005). Recently, a lot researches have been published trying to achieve, through a combination of fuzzy techniques and different mathematical methods, an acceptable solution in evaluating ITC risks in different systems (Jiang, 2016; Anikin, 2016; Dai et al., 2015). Quantitative and qualitative techniques have some advantages and disadvantages. Among these techniques, the application of proposed model for risk assessment in information security processes seems appropriate. Accuracy of expert's assessment and quality of output results could be improved by application of fuzzy mathematics.

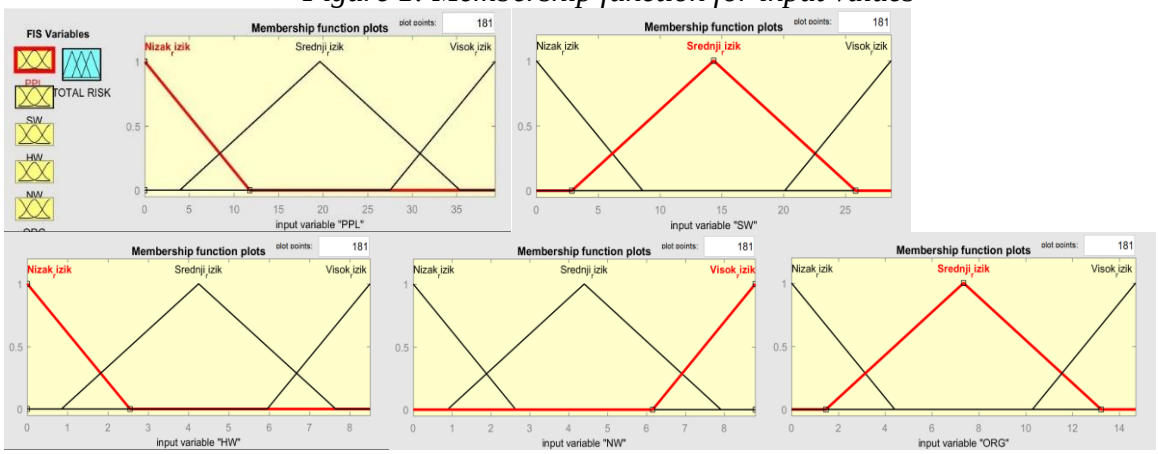
3. MODEL DESCRIPTION

ISO27005 standard[1] proposes but substantiates the risk modelling process by providing the best practices for managing the risks related to information security. Standard distinguish primary and supporting assets. Considering the fact, that data on risk realization during the previous period often are not available or sufficiently reliable, expert knowledge about the risks and elements of risk, experience and intuition are a must in assessment of model value. For the purpose of work on this paper and on the base of available information, authors distinguish five basic risk groups of the ITS environment: Hardware (HW), Software (SW), Network (NW), Organization (ORG), People (PPL). Initial data, knowledge about processes and treats are from the packaging company from Serbia. Team of employees, in charge for different processes in the Company, in accordance with Company procedures, formed a risk matrix. That is the starting point for implementation of data in the proposed model. Basic matrix is in the form of language variables. For the purpose of this work, in cooperation with the company's team (experts), risks are transform in crisp numbers in accordance with the Saaty's scale (Saaty, 2008). The team assigns a risk level of high, moderate, or low for each assets area, based on values of assets, the most likelihood threats, identified vulnerabilities and implemented security controls for each assets area. In the next phase authors formed triangular fuzzy numbers from the experts evaluation. There are several types of fuzzy sets depending on the set of values of the corresponding membership function. In the basic type of the set, the membership function has values in the interval [0, 1]. If X is an arbitrary non-empty set, fuzzy set A with values in the interval [0, 1] defined on X is characterized by a function $\mu_A : X \rightarrow [0,1]$. The function μ_A is called the membership function of the fuzzy set A. The value $\mu_A(x)$ is interpreted as the degree of membership of element x to the set A. Furthermore, the membership functions for selected risk elements are defined. Membership functions for each element are shown in figure 1. Each risk element are described by low risk, moderate risk and a high risk. MATLAB Fuzzy Logic Designer is used to calculate output values. The output value of the fuzzy system is the total risk in specific process (TR) and membership functions of fuzzy sets Y_{VL} - Very low risk, Y_L - Low risk, Y_M - Moderate risk, Y_H - High risk and Y_{VH} - Very high risk, are shown in Figure 2 (a).

Figure following on the next page

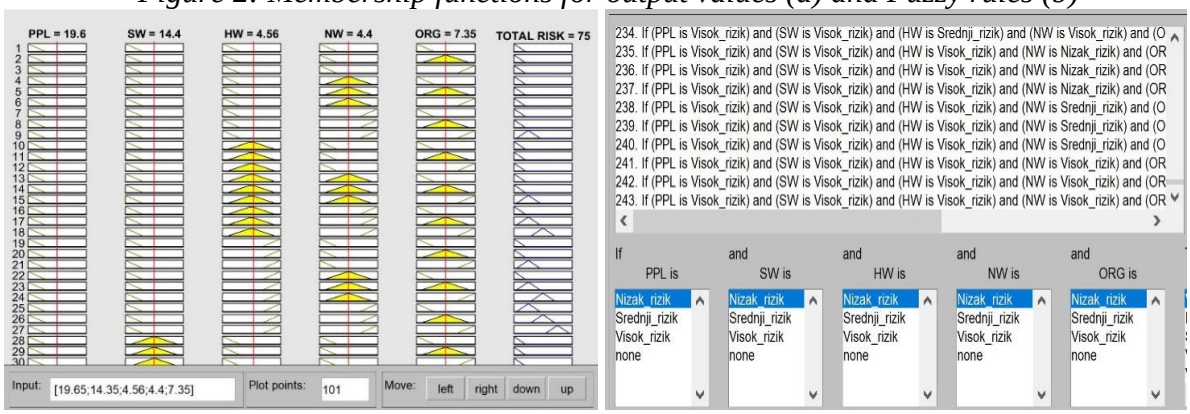
[1] ISO. BS ISO/IEC 27005:2011

Figure 1: Membership function for input values



Proposed model is a fuzzy system based on application of FL and an approximate reasoning algorithm. Fuzzy rules of all risk elements and levels of risk (very low, low, moderate, high and very high) are formed. System used the Mamdani technique and the rules are defined as in figure Figure 2 (b). System allows the application of different methods of defuzzification, bisector, centroid, mom, lom, som or customizes new method. For the purpose of this work authors applied centroid method.

Figure 2: Membership functions for output values (a) and Fuzzy rules (b)



In the next phase simulation is prepared on a large number of hypothetical data with input parameters obtained by generating random numbers. Output values of Fuzzy system simulation are shown in Table 2. The highest priority for the observed class of particular processes has PPL with 38,40% of influence, and the lowest priority has Nw with 8,60% of influence on total risk. The obtained results represent the total risk value, and their analysis included measuring of the relative weighting factors of each risk element and share in the total risk. The elements of membership functions for all input variables of fuzzy system are shown in Table 1. The output of the system (Table 2) is the total risk assessment of each specific process. Risk managers can make decision on the based on significance of every risk element. Their decision of acceptance, elimination or minimization of potential consequences of risk being evaluated are based on more precise and systematized data.

Table following on the next page

Table1: Input variables for fuzzy system (Author's calculations)

Risks	PPL	SW	HW	NW	ORG
Input values	0,384	0,288	0,087	0,086	0,155
Low risk	0,000	0,000	0,000	0,000	0,000
	0,000	0,000	0,000	0,000	0,000
	11,520	8,640	2,610	2,580	4,650
Moderate risk	3,840	2,880	0,870	0,860	1,550
	19,200	14,400	4,350	4,300	7,750
	34,560	25,920	7,830	7,740	13,950
High risk	26,880	20,160	6,090	6,020	10,850
	38,400	28,800	8,700	8,600	15,500
	38,400	28,800	8,700	8,600	15,500

Table2: Result of the model (Author's calculations)

Risks	PPL	SW	HW	NW	ORG
Output values	0,3901	0,2944	0,08	0,0778	0,1575

The highest impact on the total risk in observed processes has People (39.01%). The reasons are the insufficient users' security awareness and luck of general security culture. Then follow software, 28.6% due to none consistent patch management process. Organization risk has 15% of total risk, due to failures in compliance and contractors management. The less impact on total risk have Hardware and Network risks have the less impact on company risk, both due to a failure in assets management. The model enables a relatively easy implementation of expert knowledge, that is, the collected data from the indicated processes of the company. When implementing the risk, it is possible to use different linguistic scales of evaluation. Fuzzy logic designer makes it possible to convert these values into different fuzzy numbers, that is, different membership functions, triangular, trapezoidal, Gaussian, and other. Through the presented model, the degree of subjectivity of decision makers is minimized and a greater accuracy is achieved.

4. CONCLUSION

Authors presented a model based on fuzzy logic, which integrates a qualitative and quantitative approach, for risk assessment. Model enabled risk assessment in each specific process in the company. The methodology of the model can be applied to different companies and certain processes, in accordance with the needs of the decision maker. This is extremely important in a dynamic environment with many different influences and risks.

LITERATURE:

1. Anikin, I.V. (2016). Information security risks assessment in telecommunication network of the university, *in 2016 IEEE Int. Conf. on Dynamics of Systems, Mechanisms and Machines (Dynamics)*, Omsk, Nov. 15–17, pp. 1 – 4.
2. Campbell, P and Stamp, J. (2004). *A classification scheme for risk assessment methods*. Sandia National Laboratory; X SAND2004-4233.
3. Chang, P. T and Hung, K. C. (2005). Applying the fuzzy weighted average approach to evaluation network security systems. *Computers and Mathematics with Application*, 49, pp. 1797-1814.
4. Dai, F., Hu, Y., Zheng, K and Wu, B. (2015). Exploring risk flow attack graph for security risk assessment. *IET Information Security*, 9 (6) , pp. 344 – 353.

5. Goel, S and Chen, V. (2005). Information security risk analysis - a matrix-based approach, *in Proc. of the 2005 Information Resources Management Association International Conference*, University at Albany, SUNY.
6. ISO. BS ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management.
7. Jiang, D., Liu, X., Li, Y and Zhao, Y. (2016). The implementation and application of security evaluation system of Electric Power Communication Network, *in 2016 2nd IEEE Int. Conf. on Computer and Communications (ICCC),* Chengdu, Oct. 14-17, pp. 1162 – 1165.
8. Markovic-Petrovic, J. D and Stojanovic, M.D. An improved risk assessment method for SCADA information security. *Elektron Ir Elektrotech,* 20(7), pp. 69–72, 2014.
9. Patel, S., Graham, J and Ralston, P. (2008).Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements, *International Journal of Information Management*, vol. 28, no. 6, pp. 483–491.
10. Ralston, P. Graham, P and Hieb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions,* 46(4), pp. 583–94.
11. Saaty, T.L. (2008). Decision making with the analytic hierarchy process. *Int. J. Services Sciences*, 1(1), pp. 83-98.
12. Ten, C-W., Manimaran, G and Liu, C-C. (2010). Cybersecurity for critical infrastructures: attack and defense modeling," in *Conf.Rec. 2010 IEEE Int. Conf. on Systems, Man and Cybernetics*, 40(4), pp. 853–65.
13. Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions, in *Proc. of the 2009 workshop on new security paradigms workshop. ACM*, Oxford, pp. 37–50.
14. Wang, Z and Zeng, H. (2010). Study on the risk assessment quantitative method of information security. in *Conf.Rec. 2010 3rd Int. Conf. on Advanced Computer Theory and Engineering (ICACTE)*.6, pp. V6-529 - V6-533.