THE PROPOSAL OF SECURITY AND SAFETY MANAGEMENT SYSTEM WITH FUZZY LOGIC SUPPORT

Lucia Duricova[(a)], Martin Hromada[(b)], Jan Mrazek[(c)]

[(a),(b), (c)]Tomas Bata University in Zlin

[(a)] duricova@fai.utb.cz, [(b)] hromada@fai.utb.cz, [(c)] jmrazek@fai.utb.cz

ABSTRACT

This paper presents the implementation of the fuzzy logic into the security and safety solution in the soft targets. The primary structure of safety and security tool is described in the first part. This tool has been implemented into specific object; for example, for object without security and safety solution (soft targets). In the next part, the primary rules for the use of fuzzy logic are defined. The aim of this paper is to define the primary layout for software which could help operators with decision-making process. The article also proposes and describes the solution for system application of security requirements by understanding the soft targets threats. The system solution is different for each organization and object; however, the main structure is the same.

Keywords: object security, safety, soft targets, solution

1. INTRODUCTION

Soft targets are objects that do not have special security and safety measures in place. Soft targets are specified as objects with a large number of visitors in one place at the same time, and special security measures are not implemented into those locations. One of the main causes of danger is uncontrolled visitors movement in soft targets. People, who visit soft targets, are a source of risk. Soft targets include cinemas and theatres, shopping centres, schools, universities and other buildings (Duricova, L. Hromada, M. 2016). In safety category, special safety requirements are defined and this category is specified with categorization. Safety requirement for schools, authorities, cinemas, theatres and others. In this paper, the requirements for software proposal are specified.

This research concentrates on the system implementation, which has been applied into soft targets. The current situation could be different in other countries. In the Czech Republic, the current state could be presented as a system without any special security requirements. The soft targets have problems with financial resources that could be used towards security techniques and with knowledge about efficient measures. These statements are based on studies which have been done in soft targets such as shopping centrums, schools, hospitals and others (Fennely, L. Perry, M. 2016 and Duricova, P. L. Hromada, M. 2015 and Duricova, L. Hromada, M. 2016).

Soft targets could apply basic principles of management to manage processes because the structure is similar as a commercial and industrial organization aiming to gain/earn a profit. The management processes are implemented into organization because of the certification defining organization quality. The certification is based on definition rules for management and guaranteed fulfillment of standard which is authorized; for example, British Standard BS OHSAS 18001/2007, Occupational Health and Safety Management Systems. Risk is a subjective concept that needs to be viewed and quantified on an individual basis (Sennewald, Ch. Nailie, C. 2016). This research defines processes which could be implemented into software. The level of security and safety situation at soft target depends on the correct setting of measures. The software has to know the processes that occur at the soft target on daily basis and also the ideal situation. The ideal situation is represented by the values that are used for the fuzzy statements. The fuzzy statements are used for the decision making process (Duricova, P. L. Hromada, M. 2016).

The reminder of this paper is organized as follows. In Section 2, we defined the elementary principal of the proposal software solving. This part describes analytical tool which will be used in software as supported software tool. In Section 3, we defined elementary principles of fuzzy logic which will be used in the proposal. This section is divided into three parts (fuzzy logic principles, algorithmic examples and the defuzzification methods). Algorithmic examples describe the implementation of the security and safety principals into fuzzy logic. The last section concludes this research paper.

The paper proposes one system solution that could effectively manage security and safety situation in the soft targets. The software could supply missing knowledge to management of the soft targets. The fuzzy logic is the modern theory which belongs to artificial intelligence field (Ross, T. J. 2010).

2. THE PROPOSAL OF THE SECURITY AND SAFETY SOFTWARE

The proposal of software is divided into three parts. The first part analysis the current conditions and state. After that, the system could derive parameters which define security and safety state in object. These objects are categorized into groups which will be implemented in a risk state. The risk state can occur in object in the future. Firstly, the object must be evaluated, and then the object can be included into the software. The next part defines immediately corrective actions and also permanent corrective actions which have to be done by the operator.

The groups of these objects are specified with similar characteristics. The integration is based on law requirements, owner or manager requirements and technical requirements. Occupational Health and Safety (OHS) and Fire Protection (FP) is defined in law requirements (Duricova, L. Hromada, M. Mrazek, J. 2016). Each safety and security measure has tie with one of the next category:

- People and animals – this category is about life and health protection. First is human life, then animal life (Duricova, L. Hromada, M. Mrazek, J. 2016).
- Surrounding and environment – it is about requirements for safety and security in the surrounding. It is divided in different sections: environment, work places, public places, crowded places and others (Duricova, L. Hromada, M. Mrazek, J. 2016).
- Material things and machines – it is about using machines and working with things, and about requirements for use and development. Development of things, buildings, machines, as well as product requirements are included in specific requirements (Duricova, L. Hromada, M. Mrazek, J. 2016).
- Information – this section is about classification, use, transfer and about removing information as well (ISO/IEC 27001:2013).

The next part explains the principle of analytical tool. Analytical part specifies elementary requirements for analytical tool which can derive inputs parameters for the main software tool.

2.1. Analytical part

The analytical part considers the state identification of object which derives the inputs to the software. After this analytical part, the object is valued with characteristic number and coefficient. In this process, the objects are not evaluated by fuzzy rules because it is supported action for software.

RPE - Risk Probability and Effect				
	Interval	The Explanation	The definition	The advantage
Risk	1 - 10	What kind of negatives event is threatened?	The description of negatives events. It depends on the kind of event. It is precisely identified by the same distinguishing features. We will define this identify project from characteristics.	It can be applied in some others specifics object by the purpose.
Probability	1 - 10	How much percent is probably that this event can happen?	For this analytical part we must prepare analytical tools from analytical methods, which will be prepared assessment of the probability, based on past incidents and other contexts.	We can use some others analyses from others specialists. It will be compatible.
Effect	1 - 10	What happens it after the event?	We can identify some other risk after the first security incident. We anticipate response from others stakeholders and we must prepare scenarios. Precautions will must be lest financing costs as corrective actions or repair.	We must make the linking with other analytical tools and we make it compatible.
		How is damage?		
		How is hard to repair it?		

Figure 1: The description of RPE calculation (Duricova, P. L. Hromada, M. 2015)

The calculation of the RPE is based on similar foundations as calculation in systems of quality and it is called RPN. RPE is about Risk, Probability and Effect. These three indicators have values in interval from 1 to 10. Risk represents kind of event or security threat. The Probability represents percentual probability of event that can occur in the object. The Effect describes what consequences for object and visitors, or society this event could have. The RPE is non-dimensional quantity. This tool could be transferred into software which is based on fuzzy logic (Duricova, P. L. Hromada, M. 2015).

The inputs for RPE analysis are focused on the primary identification of the problem and surrounding where the problem is. This problem has main causes, and causes have special conditions where it makes problem.

The specification document defines state and location of the object. It is suggested with numerical value. This numerical value will be calculated by equation which we will determine by examining in the future research.

The object of analyses	Specification	Coefficient
State	CZ	*It must be specify for the future*
	SK	
The town / City	Prag	*It must be specify for the population and attractiveness for attackers*
	The large city	
	The medially city / town	
	The small town	
	The village	
The surroundings	With the presence of a potential offender	*It must be define analytical process for special location in town*
	With the possibility of a potential offender	
	It is clean surround	
	It is surround with security option	
The object	The specification	*It is individual*

Figure 2: The specification of the object, surrounding, town and state (Duricova, P. L. Hromada, M. 2015)

The specification and coefficient are connected in analyses. We use numerical value for better valuation for further processes and we could make this processes more practice than before.

3. FUZZY LOGIC IN THE PROPOSAL

It is necesery to examine every object; however, the aim is to examine and determine the security parameters. The fuzzy logic can be used, because it is necessary to know and work with a lot of plans and a lot of experts in one system. There is also a wide range of numerical values, and technical components. It is important to define parameters and a lot of values, that is main reason to use fuzzy logic (Takagi, T., Sugeno, M. 1985).

This system will be compatible with other methods, therefore every input and mechanism can be set up. Then it is the implementation of results from other groups of security to support solutions.

This proposal will be used in computers and will be connected with other objects in network. It depends on categorization that will be defined in the first part of analytical process. This software have to accept input parameters directly from the object in real time. The groups are for example: cinemas, shops, schools and other. On the other side, next group of inputs are requirements from law requirements and other standards that company have to accept. The software consists from a lot of subsystems. These subsystems consider the technical components and processes. Firstly, each expert has to know a lot of information about domain such as region, building, and situation. Then the expert needs to connect it. The proposed solution is a one system that will make decisions based on skills of experts. The proposal of system should be user friendly. We choose fuzzy logic because of reasons which are described in the previous section (Duricova, L. Hromada, M. Mrazek, J. 2016).

3.1. Fuzzy logic principles

Fuzzy logic is the logic that can work with a lot of values. The fuzzy logic examines whole range of values. It is important to implement expert findings and translate it to fuzzy logic. That means, we must define a range for the decision support.

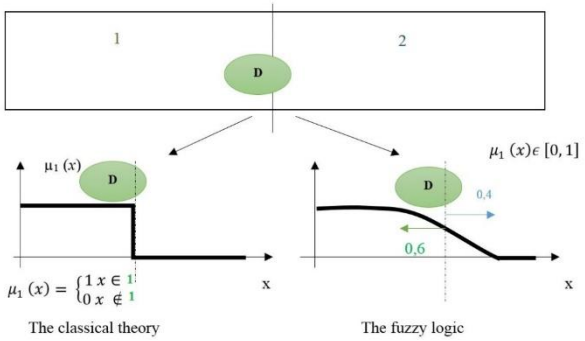

Figure 3: Basics of fuzzy logic (Duricova, L. Hromada, M. 2016).

The differences between fuzzy logic and classical theory can be seen in figure 3. In the classical theory, we can have only two values (1 or 0). It means, element D belongs or does not belongs to group 1. On the other hand, the fuzzy logic knows about each value in the interval from 0 to 1. Fuzzy logic has special rules and symbols operating with mathematical operations. They are called fuzzy statements. The truth of statement depends on value which is defined in interval between 0 and 1. In fuzzy logic, we use linguistic variables. The values of linguistic variables can be marked as element of plurality (Zadeh, L. A., 1965).

Inputs are numeric values which are in fuzzy process transferred to fuzzy sets. With fuzzy sets, we can make special fuzzy operations which are represented by rules. The process is reversed on the end. We have fuzzy set in which the numeric values must be defined (see Figure 4). We know more methods for defuzzification. For example, the center of gravity, the mean of maxima and other methods (Driankov, D. Hellendoom, H. Reinfrank, M., 1993).

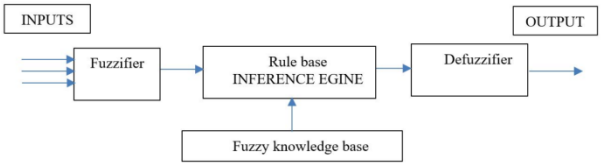

Figure 4: The main principle of fuzzy logic (Duricova, L. Hromada, M. 2016)

Classical theory uses two values and it is based on binary logic (0, 1). On the other hand, the security and safety solving is not based only on two values. These two values describe ideal situation in security and safety solving; however, operator in building needs more values for the definition of real situation. The real situation is more difficult and the decision making is based on more information and values. These values represent the degree of support (Duricova, L. Hromada, M. Mrazek, J. 2016).

3.2. Algorithmic examples

Fuzzy rule is mentioned in the next text: "if (fuzzy statement) and (fuzzy statement) then (fuzzy statement)" (Driankov, D. Hellendoom, H. Reinfrank, M., 1993).

- If (temperature=high) and (oxygen=low) then (ventilation= high).
- If (door4=open) and (mode=secret) then (camera4=start recording) and (voice prompts=on).

These examples describe using of linguistic variables in the proposal.

When we have been working with the statement, we will use logical operators. It will describe the interrelationship between these groups of variables; in security solutions known as special characteristics. Each object has a property with certain values. It is not about binary system; however, it indicates a relation between the object and characteristics. It is obvious that in each object is a risk; therefore, we have to determine the value which represents this risk. On the other hand, when we know about law requirements, we can set up normal interval by legislative. The limits can be set by the subsystem in the proposal (Klir, G. J., Yuan, B., 1995).

Interpreting if-then rules is a three-part process. This process is explained in detail in the next section (Rohan, 2016):

- Fuzzify inputs: Resolve all fuzzy statements in the antecedent to a degree of membership between 0 and 1. If there is only one part to the antecedent, this is the degree of support for the rule.
- Apply fuzzy operator to the multiple part antecedents: If there are multiple parts to the antecedent, apply fuzzy logic operators and resolve the antecedent to a single number between 0 and 1. This is the degree of support for the rule.
- Apply implication method: Use the degree of support for the entire rule to shape the output fuzzy set. The consequent of a fuzzy rule assigns an entire fuzzy set to the output. This fuzzy set is represented by a membership function that is chosen to indicate the qualities of the consequent. If the antecedent is only partially true, (i.e., is assigned a value less than 1), then the output fuzzy set is truncated according to the implication method.

In general, one rule by itself does not do much good. What the proposal need are two or more rules that can respond another. The output of each rule is a fuzzy set. The output fuzzy sets for each rule are then aggregated into a single output fuzzy set. Finally, the resulting set is defuzzified or resolved to a single number (Rohan, 2016).

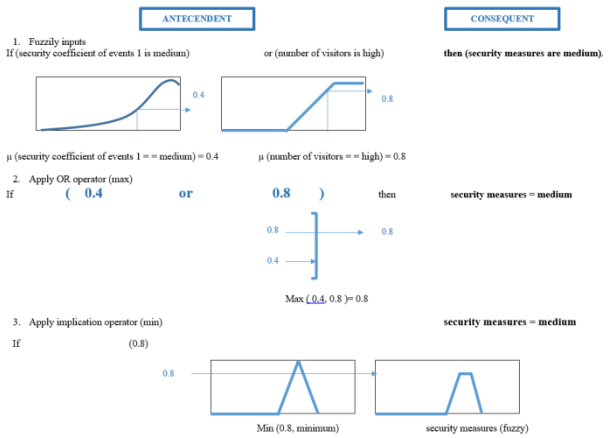

Figure 5: The principle of the fuzzification

Software will detect safety and security measures and it will optimize it for more effectively.

- If (security coefficient of event X is high) and (number of visitors is high) then (security measures are high).

The degree of support for the variable "security measures" is defined by fuzzy set "high". The degree of support for the variable "security coefficient" is defined by fuzzy set "high" and the degree of support for the variable "number of visitors" is defined by fuzzy set "high". The underlying idea, with increasing number of checks of propositions in premise; the more suggestions could be derived. For the degree of support for the truth of the fuzzy proposition "security measures are medium", the fuzzy implication must be defined. The fuzzy statement defines the degree of support for the fuzzy rule. The defuzzification is process in which the numeric value is determined from the interval (Duricova, L. Hromada, M. Mrazek, J. 2016).

3.3. The defuzzification methods

For defuzzification, different methods are possible to choose among several possible definitions. In this paper, one of the primary methods of defuzzification will be presented.

Defuzzification is based on converting fuzzy grade to on a single number. This is the last part of the process.

One of the defuzzification method is based on weighted average method which is valid for symmetrical output membership functions. In figure 6, we can see formed maximum membership value in each function (Duricova, L. Hromada, M. 2016).

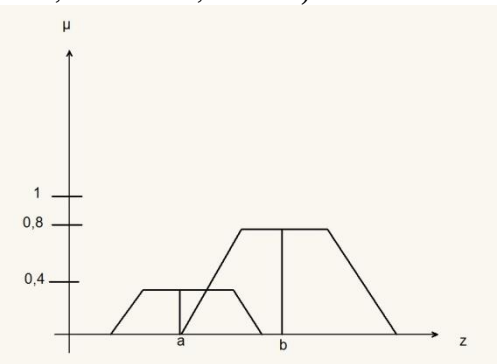

Figure 6. Defuzzification with Weighted Average Method (Duricova, L. Hromada, M. 2016)

The next equation formulates principle of this defuzzification method (Duricova, L. Hromada, M. 2016).

$$z^* = \frac{\sum \mu_c(\bar{z}) \times \bar{z}}{\sum \mu_c(\bar{z})}. \quad (1)$$

In the next equation, the example of a model that is depicted in graph.

$$z^* = \frac{a(0,4) + b(0,8)}{0,4 + 0,8}. \quad (2)$$

In this process, more methods, which are not described in paper, can be used. For example:

- Centre of gravity.
- Height method.
- Middle of maxima.
- Centre of sums.
- Centre of the largest area.
- First or last of maxima.

4. CONCLUSION

Detectors have special functions and works at technical bases. These detectors can be based on infrared, electrical, roentgen or other physical measurements.We

can use detectors and linked them to the proposed system. It is, for example, system from company NICE. After the integration of detectors, the system will be more efficient. However, we must understand physical phenomena of these detectors because we have to know the state of normal or alarm situation, and state of threaten. We propose a set of rules that consists of technical rules and also law rules. The conditions in object will be defined and then we can optimally set the security and safety parameters. The impact of this solution is system solving of situation with technical and management support. Object managers can make decisions with this solution which contains expert knowledge of each object. Therefore, it is possible to make decisions quickly and more efficiently (Rosenberg, F., 2014).

In the further research, the subsystem for analyzing incidents in the soft targets will be defined. The parameters in this subsystem can be also defined and will be used in the main software. These parameters will identify the probability of the incident in soft target.

ACKNOWLEDGMENTS

This project is realized as the research with doctoral student and it is the basic input for further research which we will develop in next term. This work was supported by Internal Grant Agency of Tomas Bata University under the project No. IGA/FAI/2016/012.

REFERENCES

Bishop, C.M., 2006. Pattern recognition machine learning, Springer.

British Standard BS OHSAS 18001/2007, Occupational Health and Safety Management Systems-Requirements.

Driankov, D. Hellendoom, H. Reinfrank, M., 1993. An introduction to fuzzy control, Springer Verlag.

Duricova, L. Hromada, M. Mrazek, J., 2016. Security and Safety Requirements for Soft Targets in Czech Republic, SECURWARE 2016 The Tenth International Conference on Emerging Security Information, Systems and Technologies, IARIA, pp. 271-275, ISBN: 978-1-61208-493-0.

Duricova, L. Hromada, M. Mrazek, J., 2016. Security and Safety Processes in Czech Republic Universities, SECURWARE 2016 The Tenth International Conference on Emerging Security Information, Systems and Technologies, IARIA, pp. 105-110, ISBN: 978-1-61208-493-0.

Duricova, P. L. Hromada, M. The Proposal of the Soft Targets Security. Advences in Intelligent Systems and Computing, Automation Control Theory Perspectives in Intelligent Systems. Proceedings of the 5th Computer Science On-line Conference 2016 (CSOC2016), Vol3, Springer, pp.: 337-345. ISSN 2194-5357, ISBN 978-3-319-33387-8, DOI 10.1007/978-3-319-33389-2.

Duricova, P.L., Hromada, M., 2015. The proposal system for the safety assessment of soft targets with focus on school facilities. Proceeding of 3rd CER Comperative, vol. 2, pp. 30-33. Sciemcee Publishing, London.

Fennely, L. Perry, M. " The Handbook for School Safety and Security," 1st ed., Elsevier, 2014, ISBN: 978-0-12800568-2.

ISO/IEC 27001:2013, Information Technology-Security Techniques- Information Security Management Systems – Requirements.

Jura, P., 2004. Some remarks on mathematical models, WSEAS Transactions on information science and application, 1 (5), 1426-1429.

Klir, G. J., Yuan, B., 1995. Sets and fuzzy logic In: Theory and application, Prentice Hall, New Jersey.

Rohan, 2016, If than rules. In: http://www.rohan.sdsu.edu/doc/matlab/toolbox/fuzzy/fuzzytu5.html

Ross, T. J. "Fuzzy logic with engineering applications" 3rd Edition, John Wiley & Sons, Ltd. 2010, ISBN: 978-0-470-74376-8.

Rosenberg, F., 2014. Nice solution for critical facilities, Nidam, Nice.

Sennewald, Ch. Baillie, C. "Effective Security Management," 6th ed.,Amsterdam: Elsevier, 2016, ISBN: 9780-12-802774-5.

Takagi, T., Sugeno, M. 1985. Fuzzy Identification of Systems and Its Application to Modeling and Control. IEEE Trans. on System, Man, and Cybernetics, 15 (1), 116–132.

Zadeh, L. A., 1965. Fuzzy Sets. In: Information and Control, vol. 8, 338–353.

AUTHORS BIOGRAPHY

Authors belong to Department of Security Engineering at Faculty of Applied Informatics. Lucia Duricova is a doctoral student at Tomas Bata University. Her thesis is: Soft targets as specific object in population protection. Martin Hromada is a consultant and supervisor of this thesis. He is an expert in critical infrastructure protection.