Libor Hadacek - Lenka Sivakova - Radovan Sousek - Mikael Zeegers

ASSESSMENT OF SECURITY RISKS IN RAILWAY TRANSPORT USING THE FUZZY LOGICAL DEDUCTION METHOD

The aim of the paper is to inform about the possibilities of using a fuzzy logical deduction in security practice. The fuzzy logic deduction allows to record the management experience in IF - THEN rules and does not require a precise description of the parameters of the controlled function. This property is an important asset for risk assessment in an incompletely defined environment. The application of the method is demonstrated in the security risk assessment of the physical protection of the national railway with a focus on the corridor railway lines and with regard to the future construction of high-speed railway lines in the Czech Republic. At present, it is a generally accepted fact that securing basic transport functions is a prerequisite for successful crisis management. These functions can be specified as road and rail negotiability.

Keywords: *fuzzy logic deduction, security, safety, rail, crisis management*

1 Introduction

Security management activities in an organization involve a great amount of decision-making on strategy and tactics of risk management [1-3]. Security managers have to make decisions despite uncertainties, inaccuracies, or incompleteness of input data [4-5]. They use quantitative tools to make decisions that require a certain level of input data precision. Furthermore, they can also apply semi-quantitative analytical methods based on a point scale. In the case of more independent variables, their point values are usually obtained using binary operations. This results in the value of the output dependent variable being the same for a different combination of values of the input variables.

A possible method of making decisions with uncertainty or incompleteness of input data is the application of fuzzy logic. Fuzzy logic isused in controlling processes of industrial products. For example, their principles control the image processing processes or automatic washing machines programs.

To control processes in an incompletely defined environment, it is appropriate to use a fuzzy logical deduction. Fuzzy logical deduction (FLD) is a part of fuzzy logic in a broader sense. FLD was described by prof. V. Novak in [6] in 1995 with the aim of creating an exact formal theory.

2 Model of risk assessment using the fuzzy logical deduction method

In common life, an event can be described by the two-state logic. Individual values can be assigned a value of 1 or 0 that corresponds to states such as on and off. Fuzzy logic expands the two-logic logic to multi-valued logic. An example of the difference between two-state logic and fuzzy logic is shown in Figure 1.

The fuzzy logical deduction is based on the basic rule of human logical thinking. Deduction, i.e. drawing conclusions, is implemented through formulas. The most important rule used is the modus ponens rule. Formally, it is possible to write it as follows:

$$\frac{A, A \Rightarrow B}{B}. \tag{1}$$

In this rule, there are A, B formulas. The rule modus ponens says that if we know the fact labeled by formula A and we know that the fact B is based on fact A, then we can assume that the fact B is valid. In classical logic, true and false formulas are examined in models, while fuzzy logic examines formulas whose truth value in models is different [7]. The principle of fuzzy logic deduction is illustrated by the general fuzzy controller shown in Figure 2. The general fuzzy controller consists of blocks of fuzzification, knowledge base, inferential mechanism, and defuzzification.

In the fuzzification process, the input independent variable is assigned a language expression. It is a variable whose values can be words or some natural language expressions [7]. An example of the names of selected language expressions is given in Table 1.

The extensions of evaluation predictions are constructed identically in all contexts. Typical elements have a degree of competence in the given extension of the evaluation prediction equal to 0.9 or 1. The example of the

Libor Hadacek[1,*], Lenka Sivakova[2], Radovan Sousek[1], Mikael Zeegers[3]
[1]Faculty of Transport Engineering, University of Pardubice, Czech Republic
[2]Faculty of Security Engineering, University of Zilina, Slovak Republic
[3]Security Risk Watch, Voorthuizen, Netherlands
*E-mail of corresponding author: libor.hadacek@gmail.com

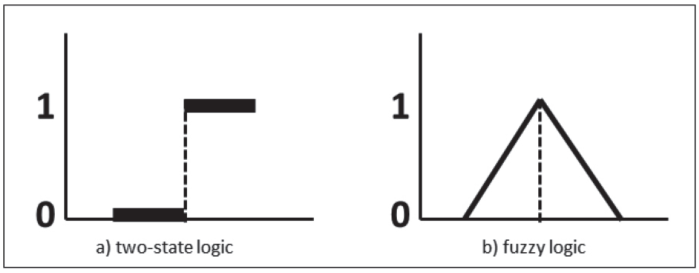

Figure 1 *Difference of two stage logic and fuzzy logic*

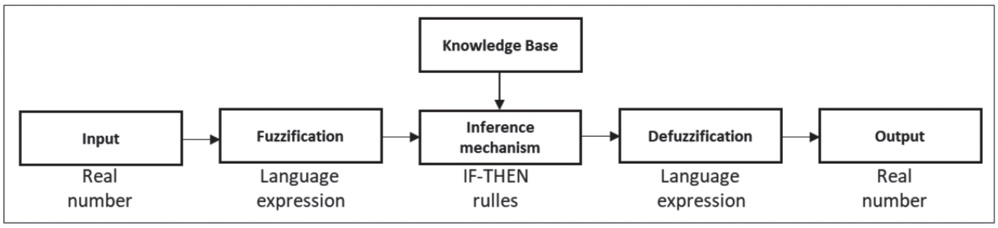

Figure 2 *General scheme of fuzzy controller [7]*

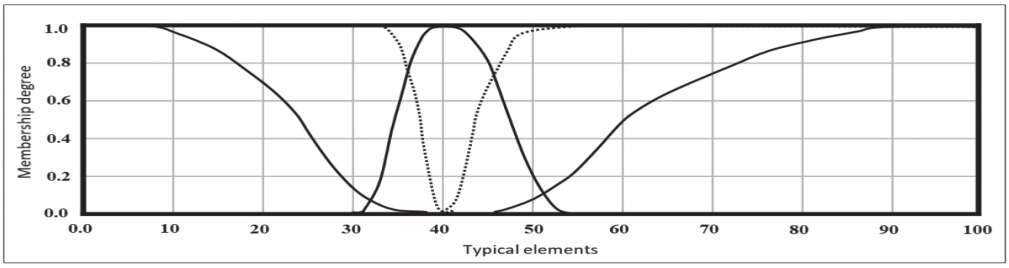

Figure 3 *Extension of evaluation predictions [7]*

Table 1 *Names of selected language expressions [7]*

Number	Languge expression	Abbreviation
1	Small	Sm
2	Roughly Small	Ro sm
3	Midle	Me
4	Roughly Big velky	Ro Bi
5	Big	Bi

Table 2 *Example of IF-THEN rules*

Number	X_1 is A_i	&	X_2 is B_i	=>	Y_1 is C_i
1	sm		Ze	|	ze
2	sm		Sm	|	sm
3	sm		ro sm	|	ro sm

course of selected extensions of the evaluation predictions for the context $\langle 0,40,100 \rangle$ is given in Figure 3 [7].

A set of rules is stored in the knowledge base. An approximate knowledge of the regulatory strategy is sufficient to create the rules. The strategy is described using the IF-THEN fuzzy set of rules [7]:

$$R_n = IF\ X\ is\ A\ THEN\ Y\ is\ B\,, \tag{2}$$

where:
R_n is the rule and n is the rule number,
X is the assessed object,
A is object property,
Y is a dependent variable,
B is object property.

In order to develop a controlling strategy, the expressions of a natural language, whose meaning is generally known, are used. The individual rules are made up of vague statements characterizing the properties of the input variables based on the results of the controlled process observation. An example of creating rules is given in Table 2.

In the inference mechanism, logical deduction is applied in the decision on the input variables according to the respective rule.

The conversion of a language expression into a real number occurs in the defuzzification process. Defuzzification is an operation that assigns an element from its carrier to the fuzzy set.

$$DEF(A) \in Supp(A)\,. \tag{3}$$

For defuzzification, the method of DEE (Defuzzification of Evaluative Expressions) is applied in combination with the fuzzy logical deduction. The reason for using it is a smoother course of the resulting function. The method is described in detail in [8].

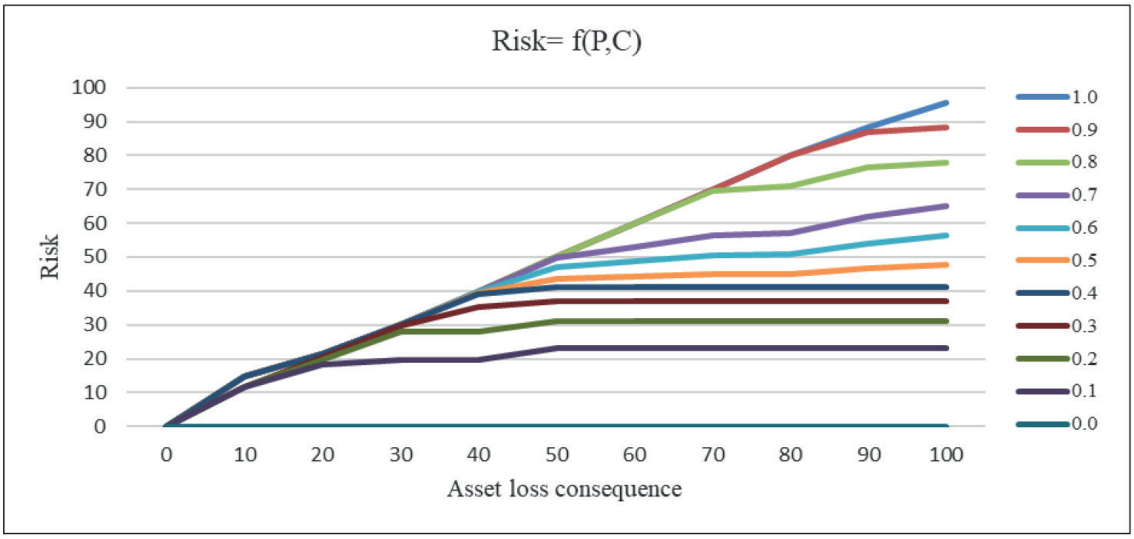

Figure 4 *The value of the risk is a function of an event probability and an asset loss consequence*

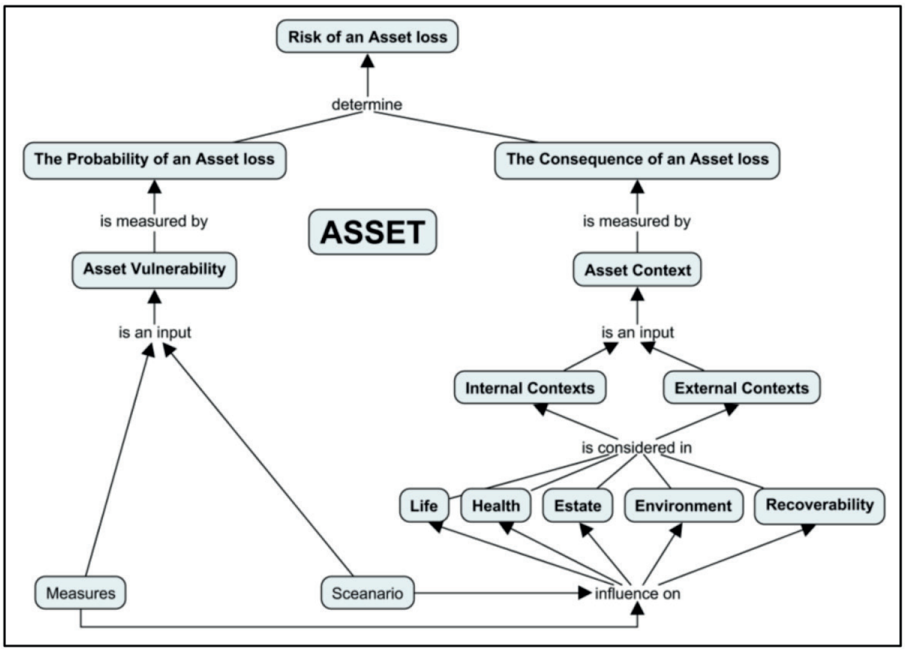

Figure 5 *The model of fuzzy controllers system for determining of the risk of an asset loss*

Determining the value of the risk by the FLD method is based on the same principles as the traditional method of determining the risk value, as described in the technical standard [9]. The risk values presented in Figure 4 are based on Table 5. The method of determining the values changes the established linear perception of the course of risk values. The created lines of risk are similar to those of the output characteristics of the transistor.

The proposed procedure eliminates the lack of a traditional risk-setting method. For example, with a probability value of 0.1 and the consequence value of 100, the resulting value of risk is 10. If the probability is 1 and the magnitude of consequence is 10, then the risk value is again 10. When applying the FLD method to determine the risk values, in the first case the risk value is 23.1 and in the second case, the result is 14.7, as can be seen in Table 5.

Fuzzy controllers can be connected together. This feature allows you to solve a complex task when only one set of rules is not sufficient. Assessing security risks is a complex task, the result of which supports the decision-making process of security management on the use of risk management strategies. Security risks are, by their nature, intentional, thoughtful and purposeful acts of a person who implements a scenario of an attack [10]. Due to the uniqueness of the location of the protected object, a number of uncertainties and incompleteness of the input data can be considered. A model of the fuzzy controller system for determining the value of the risk of an asset loss is shown in Figure 5.

The asset is related to the internal and external context. Contexts include the number of casualties. Other contexts include damage to property and the environment. The time context is the period of recovery of the asset to its original state after the effects of the scenario. The level, scope, and effectiveness of asset risk management measures are influenced by the scenario. The relationship between measures and scenarios is applied in an expert judgement on asset vulnerability. A measure of the asset‘s vulnerability is the probability of its loss. The consequence of the loss of an asset is a measure of the asset‘s context. The risk of loss of an asset depends on the probability of loss of the asset and the consequence of its loss.

For the purposes of the risk assessment procedures outlined in this text, we applied definitions of the event, occurrence, possibility or probability of occurrence, risk, and risk levels as set out in the technical standard [11].

Vulnerability means the property of any material object, technical means or social entity to lose the ability to fulfill its natural or established function due to external or internal threats of different nature and intensity. [12]

It can be concluded that the vulnerability characterizes the ability of the physical protection system to prevent the loss, damage or destruction of the protected object. It qualitatively or quantitatively expresses the degree of probability that something will happen, i.e. probability of loss of a protected subject. It follows that the probability of asset loss is a function of vulnerability.

3 Assessment of the risks of physical protection of high-speed rail

The software application „Analysis of Specific Risks of Physical Endangerment of the High-Speed Railway Infrastructure“ was developed for the solution of the security risks of high-speed railway lines using the fuzzy logical deduction method. For the purposes of this paper, the issue of high-speed lines has been reduced to the level of corridor tracks where the speed is 160 km/h.

3.1 Asset

According to the technical standard [13], the asset is anything that has value for the organization. The definition can be extended to the importance of the asset for its owner. The types of railway infrastructure assets can be considered, for example, a bridge, a tunnel [14], a station head, a grade separation structure or a track section [15]. Assets are entered into the database manually or from pre-prepared xls files.

For the purpose of assessing the risks of physical protection of the high-speed rail infrastructure, the infrastructure asset is characterized by the following fields:

a) Type - general designation of the group of assets,
b) Asset name - a closer unique identification of the asset,
c) Asset location - place, premises, space (regional headquarters, track section, ID),
d) GPS coordinates - the location of the asset in map coordinates,
e) Description of the asset - where other asset properties are specified.

3.2 Scenario

The scenario is a set of conditions and/or events that can cause a security incident. A deliberate anthropogenic threat is an individual or group of individuals with motivation and ability to act deliberately to cause loss or damage to the asset. The method of the threat manifestation is described by the scenario. The list of threats is specified in the threat catalog. When creating the threat catalog, legal provisions and the experience of experts from previous events are used. For each scenario, the following characteristics are given:

a) Threat,
b) Direction of an attack - it is important for the choice of preventive measures,
c) Time Attributes (seasons, time, opening hours),
d) Method attributed (tools, weapons, vehicles),
e) Description - other data supporting the expert judgment on the vulnerability of the asset.

3.3 Installed measures

For the purpose of physical protection, it is important to know the security features used to deter, slow, detect, and interrupt the attacker‘s progress. In particular, these include the construction of windows, doors, roof skylights, ventilation ducts and other openings of the building shell that can facilitate unauthorized entry [16]. For buildings with a perimeter, knowledge of fences, gates, barriers etc. is important. Details of current measures are listed in the following fields:

a) Asset - the name of the asset,
b) Safety / Security region - the area of safety or security, e.g. physical protection,
c) Type - general designation of the measure, eg. fencing,
d) The title of the measure - closer measure specification,
e) Level - the quality of the measure, e.g. burglary resistance,
f) Place of use - name of the security barrier, e.g. perimeter,
g) Purpose - which part of the security system is protected,
h) Date of commissioning - significant for systems degrading with time,
i) Description - a more detailed description of the measure, the item is not indexed,
j) Photo - this item allows you to attach a digital photo to the description.

3.4 Asset context

The process of determining the asset context, based on the technical standard [11], consists of subprocesses:

Table 3 *Formalized vulnerability sentences and language expressions*

Number	Semantics of Vulnerability	Language expression	Abbreviation
1	Not assessed	Zero	Ze
2	Protection multiply exceeds the requirements	Small	Sm
3	Protection exceeds the requirements	Roughly small	Ro Sm
4	Protection meets the requirements	Very Roughly small	VR Sm

Table 4 *Groups of risk values*

Number	Groupe title	Extent
1	Low risk	0.0-30.0
2	Moderate risk	30.1-36.9
3	Very high risk	37.0-60.0
4	Extreme risk	60.1-100.0

Table 5 *Risk values determined from the characteristic values of the input variables [18]*

Asset loss probability	1.0	0.0	14.7	21.3	30.2	39.9	50.0	60.0	69.9	79.8	88.2	95.6
	0.9	0.0	14.7	21.3	30.2	39.9	50.0	60.0	69.9	79.8	86.8	88.3
	0.8	0.0	14.7	21.3	30.2	39.9	50.0	60.0	69.5	71.1	76.5	78.0
	0.7	0.0	14.7	21.3	30.2	39.8	49.7	52.8	56.3	57.1	61.9	65.2
	0.6	0.0	14.7	21.3	30.2	39.8	47.2	48.6	50.6	50.9	54.0	56.3
	0.5	0.0	14.7	21.3	30.2	39.4	43.7	44.1	45.0	45.0	46.6	47.6
	0.4	0.0	14.7	21.3	30.2	39.0	41.3	41.3	41.3	41.3	41.3	41.3
	0.3	0.0	11.7	20.2	29.8	35.2	36.9	36.9	36.9	36.9	36.9	36.9
	0.2	0.0	11.7	19.8	27.9	27.9	31.1	31.1	31.1	31.1	31.1	31.1
	0.1	0.0	11.7	18.3	19.8	19.8	23.1	23.1	23.1	23.1	23.1	23.1
	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
		0	10	20	30	40	50	60	70	80	90	100
		Asset losss consequence										

determining contexts and determining risk criteria. The context is defined as the goal the organization seeks to achieve in its internal and external environments. The external and internal contexts justify the reason why preventive measures are planned and applied for the asset.

For the purpose of assessing the risks of physical protection, the targets are set as the number of casualties, the economic impact on property and the environment and the time necessary to restore the asset‘s function. External target values are as the same as internal target values, exept restoration. Restoration in external means the restoration of damage in external area or the reputation of the asset owner. The organization considers the importance of goals in both environments to be equivalent.

In the created SW application, three experts separately assess the level of achieving the context objectives of the context. Answers are formulated in numerical ranges or a formalized sentence. By selecting a predefined answer, it is possible to answer the question „what maximum value of the given context can the attack scenario achieve?“ An example of formalized sentences for recording the vulnerability analysis results, including associated language expressions, is given in Table 3.

In the risk criteria identification subprocess, the organization, besides other aspects, determines the levels of risk. According to the technical standard [17], the risk levels can be divided into three groups (low, large, extreme), four groups (low, medium, very large, extreme) or five groups (low, medium, large, very large, extreme). For the purpose of assessing the risks of physical protection, it is appropriate to use the four groups of risk levels, as listed in Table 4.

A four-level risk classification allows security management to select an appropriate security strategy for risk management.

3.5 Security risk assessment

The resulting risk value is the output of the fuzzy controller - the value of the risk. The rules for the determination of risk values using FLD were adopted

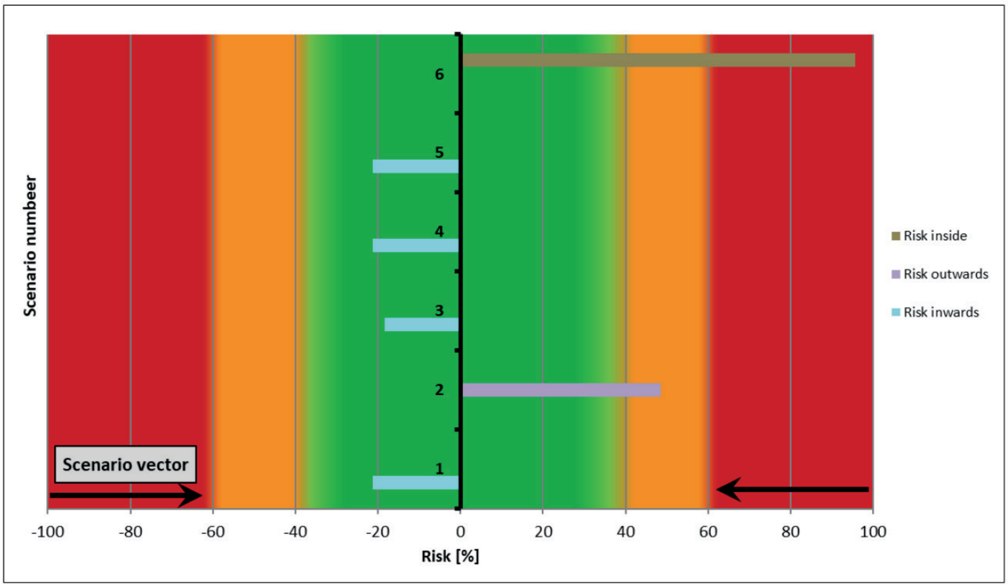

***Figure 6** Results of risk analysis*

***Table 6** Summary of links of terms for risk solution*

Risk treatment	Example
Risk treatment strategy	restriction, mitigation, transfer, preservation, avoidance
Safety / Security region	Physical Protection, Fire Protection, Information Security
Measures group	routine security precautions, physical security etc.
Typ of measure	fence, gate, door, PIR detector, detection camera, site security
Safety / Security element	door RC 3, switchboard 3
Reason of measure	mechanical barriers, detection systems, camera systems

from [18], where was for the calculations used the LFLC[1] program. The risk values determined by the FLD method are shown in Table 5.

The input variable „Consequence of the asset loss“ and the input variable „Probability of asset loss“ are defined by the characteristic values corresponding to the range of the minimum and maximum risk values.

3.6 Risk evaluation

The last step of the risk assessment, according to [11], is the risk evaluation. An example of a possible graphical representation of the risk values is shown in Figure 6.

The x-axis shows the risk values. Risk values with a „-“ sign are not mathematical. The use of a minus sign helped to separate the risks of vector scenarios from the external environment, where the risk source is outside the protected zone, from other risk vector groups. Positive risk values are in the graph represented by risk vectors from the inside out, from the protected to the unprotected zone and the vectors of internal risks, i.e. risks within the protected zone. The y-axis shows the numbers of the scenarios under consideration.

Splitting the chart into two parts and coloring the groups of risk values makes the significance of the risks evaluated more transparent. The risk values groups are color-coded in accordance with the technical standard [17].

3.7 Risk treatment

In the process of risk treatment, measures are implemented with regard to risk treatment strategies selected in the Risk Assessment process. Risk treatment is carried out through one of the strategies [19]:

a) Restrictions - the use of preventive measures to minimize the probability of loss of the asset and the consequences of loss of the asset,
b) Mitigation - limiting all negative consequences of an event,
c) Transfer - sharing the cost of losses with another entity,
d) Preservation - knowingly accepting the costs of losses,
e) Avoidance - the non-possession of the asset to which the risk relates.

Each of the risk treatment strategies includes at least one of the security area. More than one strategy and more than one security area can be selected. Security areas consist of groups of measures. There are different types

[1] LFLC – Language Fuzzy Logic Controler developed in the Institute for research and Application of Fuzzy Modeling, University of Ostrava, http://irafm.osu.cz/en/c100_software/

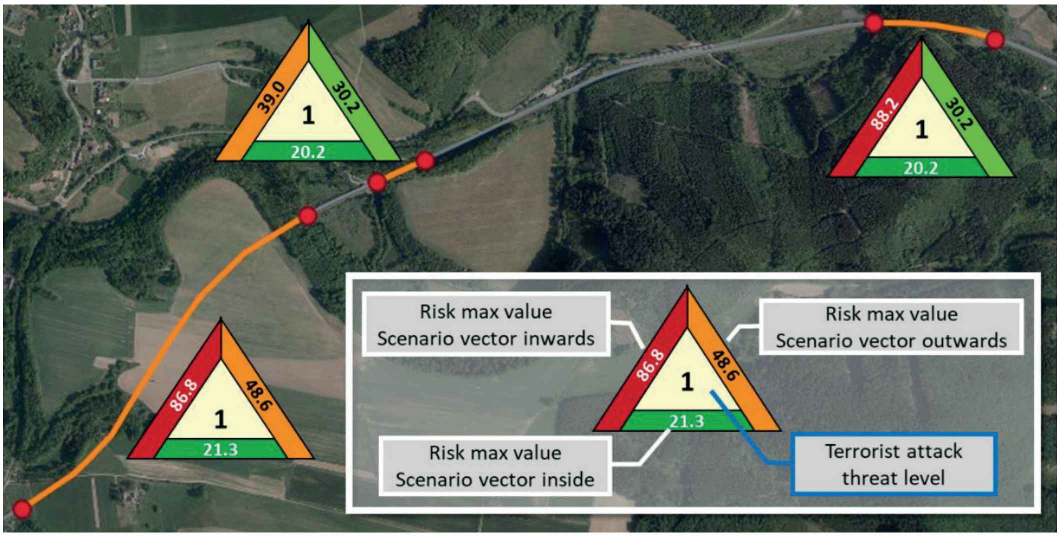

***Figure 7** Interpretation of the risk assessment results in the map*

of measures in the group of measures. Security features marked with an exact security feature specification are assigned to the type of measure. Each type of measure has a specific purpose in the physical protection system. A summary of the concept links is given in Table 6.

For example, physical protection is a security area from a „limitation" strategy. The groups of measures include technical measures, routine security precautions, and physical security. The technical measures group includes the types of measures, mechanical barriers, detection systems, camera systems and others. Types of measures in the group of mechanical barriers include fences, gates, barriers, doors, locks and others. A door is considered as a security feature when it meets the requirements of EN 1627 RC 3. Using the security features of the different types of measures of the measure groups, a physical protection system is created.

New measures can be added to the protection system. The current measure may be replaced or removed. To record details of the measure proposal in the software, the same fields as described in Subchapter 3.3 are filled in, supplemented by the following fields:

a) Duration - the time needed to implement the measures,
b) Feature description - a more detailed description of the measure, the item is not indexed,
c) Cost of measure installation - costs of installing measures,
d) Cost of measure operation for one year - cost of measure operation in 1 year.

The selected procedure was used to maintain consistency between two processes in the software application. Appropriate costs of installing measures are the costs which cover the approved organization's risk management scenario.

3.8 Interpretation of results of the security risk assessment

The results of security risk assessment are interpreted in the form of text, tables, charts, drawings in the map. Here, all the data put in and created in the assessment processes and subprocesses are applied. The interpretation method depends on the purpose and the recipients of the data. It is necessary to consider whether this is the interim information needed for the experts or the final report to the evaluator.

A possible interpretation of the risk assessment results in the map is shown in Figure 7. For the assessment, three tunnels were selected. The scenarios under consideration were divided into three vector groups. For the assessed asset, the maximum risk values for each attack vector and the information on the threat level of terrorist attack by the Ministry of the Interior of the Czech Republic are clearly outlined. The resulting risk values and degree of threat by a terrorist attack are demonstrative and can not be considered realistic.

4 Conclusion

The text summarizes the basic theoretical knowledge necessary to determine the risk value by the fuzzy logical deduction method. The example of railway transport infrastructure objects was used to demonstrate the procedure for the creation of the structure of fuzzy regulators for the determination of the risk value in the field of physical protection.

The described procedure is applicable by the security management to determine the security risk values without detailed knowledge of the fuzzy logic deduction theory and software ownership. It is relatively easy to apply it in railway transport conditions.

The proposed risk assessment method, using a fuzzy logical deduction, enables the risk criteria and the content of the auxiliary databases to be tailored to specific user conditions. The maximum range of risk values and risk assessment criteria are set with respect to the asset holder's security documentation. The selected risk assessment process increases the number of potential users of the software application.

Acknowledgements

This article was prepared under the support of the project „Analyza ohrozeni vysokorychlostni zeleznicni dopravni cesty teroristickymi utoky a extrenmismem, navrh na doplnkova bezpecnostni opatreni fyzicke ochrany/ Analysis of threats of high-speed railway infrastructure by terrorist attacks and extremism, proposal for additional security measures of physical protection", code number VH20172019016. A specific grant given by the Ministry of Interior of the Czech Republic within the program of VH - Program bezpecnostniho vyzkumu pro potreby statu 2016 - 2021 (BV III/2 VZ) (2016 - 2021).

This article was prepared under the support of the project VEGA 1/0628/18 Minimizing the level of experts' estimations subjectivity in safety practice using quantitative and qualitative methods.

References

[1] ZAGORECKI, A. T., RISTVEJ, J., KLUPA, K. Analytics for protecting critical infrastructure. *Communications - Scientific Letters of the University of Zilina* [online]. 2015, **17**(1), p. 111-115. ISSN 1335-4205, eISSN 2585-7878. Available from: http://komunikacie.uniza.sk/index.php/communications/article/view/402

[2] LOVECEK, T. 2008, Present and future ways of physical property protection. *Communications - Scientific Letters of the University of Zilina* [online]. 2008, **10**(1), p. 35-39. ISSN 1335-4205, eISSN 2585-7878. Available from: http://komunikacie.uniza.sk/index.php/communications/article/view/1028

[3] RISTVEJ, J., ZAGORECKI, A., HOLLA, K., SIMAK, L., TITKO, M. Modelling, simulation and information systems as a tool to support decision-making process in crisis management. In: Modelling and Simulation 2013 - European Simulation and Modelling Conference ESM 2013 - EUROSIS 2013: proceedings. 2013, p. 71-76.

[4] ZAGORECKI, A. T., JOHNSON, D. E. A., RISTVEJ, J. Data mining and machine learning in the context of disaster and crisis management. *International Journal of Emergency Management* [online]. 2013, **9**(4), p. 351-365. ISSN 1471-4825. Available from: https://doi.org/10.1504/IJEM.2013.059879

[5] LOVECEK, T., VELAS, A., KAMPOVA, K., MARIS, L., MOZER, V. Cumulative probability of detecting an intruder by alarm systems. In: 47th International Carnahan Conference on Security Technology ICCST 2013: proceedings [online]. IEEE, 2013. eISBN 978-1-4799-0889-9. Available from: https://doi.org/10.1109/CCST.2013.6922037

[6] NOVAK, V. Towards formalized integrated theory of fuzzy logic. In: *Fuzzy logic and its applications to engineering, information sciences, and intelligent systems. Theory and Decision Library (Series D: System Theory, Knowledge Engineering and Problem Solving)*. BIEN, Z., MIN, K. C. (eds.) [online]. Vol. 16. Dordrecht: Springer, 1995, p. 353-363. ISBN 978-94-010-6543-6, eISBN 978-94-009-0125-4. Available from: https://doi.org/10.1007/978-94-009-0125-4_35

[7] NOVAK,V., KNYBEL, J. Fuzzy modelovani / Fuzzy modeling (in Czech). Ostrava: Ostravska univerzita, 2005.

[8] NOVAK, V., PERFILIEVA, I. On the semantics of perception - based fuzzy logic deduction. *International Journal of Intelligent Systems* [online]. 2004, **19**(11), p. 1007-1031. eISSN 1098-111X. Available from: https://doi.org/10.1002/int.20034

[9] CSN EN 60812. Techniky analyzy bezporuchovosti systemu. Postup analyzy zpusobu a dusledku poruch (FMEA) / Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA) (in Czech).

[10] CSN EN 14383-1. Prevence kriminality. Planovani mestske vystavby a navrhovani budov. Cast 1: Definice specifickych terminu / Prevention of crime. Urban planning and building design. Part 1: Definition of specific terms (in Czech).

[11] CSN ISO 31000. Management rizik. Principy a smernice / Risk management. Guidelines (in Czech).

[12] HOFRIEITER, L., BOC, J., JANGL, S., LOVECEK, T., MACH, V., SEIDL, M., SELINGER, P., VELAS, A. *Ochrana objektu kriticke dopravni infrastruktury / Critical transport infrastructure protection* (in Czech). 1 ed. Zilina: EDIS - Publishing House of the University of Zilina, 2013. ISBN 978-80-554-0803-3.

[13] CSN ISO/IEC 27001. Informacni technologie. Bezpecnostni techniky. Systemy managementu bezpecnosti informaci. Pozadavky / Information technology. Security techniques. Information security management systems. Requirements (in Czech).

[14] MOZER, V., OSVALD, A., LOVECEK, T., FANFAROVA, A., VRABLOVA, L. Fire safety in tunnels forming part of critical infrastructure. In: 47th International Carnahan Conference on Security Technology ICCST 2013: proceedings [online]. IEEE, 2013. eISBN 978-1-4799-0889-9. Available from: https://doi.org/10.1109/CCST.2013.6922042

[15] SOUSEK, R. *Krizovy management a doprava/ Crisis management and transport* (in Czech). Pardubice: IJP, 2010. ISBN 9788086530642.

[16] CSN EN 15602. Poskytovatele bezpecnostnich sluzeb. Terminologie / Security service providers. Terminology (in Czech).

[17] ISO 22324. Societal security. Emergency management. Guidelines for colourcoded alerts.

[18] HADACEK, L. *Vyuziti fuzzy logiky pro studii bezpecnostnich hrozeb a rizik fyzicke ochrany / Using fuzzy logic to study security threats and physical protection risks* (in Czech). Ph.D. thesis. Ostrava: VSB - Technicka univerzita Ostrava, 2015.

[19] CNI Pokyn ISO/IEC 73. Management rizika. Slovnik. Smernice pro pouzivani v normach / Risk management. Vocabulary. Guidelines for use in standards (in Czech).