KOMUNIKÁCIE
COMMUNICATIONS

Linda Makovicka Osvaldova - Miroslav Gasparik - Javier Ramon Sotomayor Castellanos - Frank Markert
Patricia Kadlicova - Hana Cekovska*

EFFECT OF THERMAL TREATMENT ON SELECTED FIRE SAFETY FEATURES OF TROPICAL WOOD

The subject matter of the article is thermally modified tropical wood (Meranti and Merbau) and its reaction on fire. Thermal treatment of wood (thermal wood) is a new technology of wood treatment improving its physical and biological properties and increasing its resistance to biological wood destroying processes and atmospheric effects. The fire and technical properties of thermal wood, especially its reaction to fire, have not been studied sufficiently. The latter is the subject matter of this article. A comparison is made to describe the influence of process temperatures of the thermal modification of selected tropical woody plants. Experimental equipment was non-standardized laboratory equipment using a flame source of higher intensity (flame burner - propane-butane) affecting the test sample in an open environment. This is a simulation of an actual fire. The performance of the thermally treated wood (20 °C, 160 °C, 180 °C) is evaluated by measuring the weight loss and the burning rate. The results are presented in tables and diagrams and are statistically evaluated. This study investigated the effects of the thermal treatment of Merbau and Meranti wood on selected burning characteristics. The results obtained from raw (untreated) wood test specimens were compared to results obtained from the test specimens subjected to thermal treatment at 160 °C, 180 °C and 210 °C. The monitored characteristics were weight loss and the burn rate. The results showed that the thermal treatment of Merbau and Meranti wood significantly increased its flammability and accelerated its combustion. In addition, its burn rate was higher than in untreated wood, reflecting that it is necessary to add fire retardants to thermally treated Merbau and Meranti wood.

Keywords: *tropical woody plants, thermal modification, fire-resistant coating, weight loss, burning rate*

1. Introduction

Wood is used in many areas, e.g. as a construction and cladding material. It has the good weight-to-load capacity ratio and therefore it is possible to carry out wooden constructions in different areas. The material is used in exteriors, as well as interiors, of wooden buildings. The main disadvantage of wood is its ability to catch fire and burn, so lots of attention has been given to this issue for many years. There is the possibility to modify wood to increase the fire performance as well as other technical proprieties [1], [2].

The interest in thermally modified wood has significantly increased lately. This interest has arisen due to reduced production of wood as durable material, increased interest in durable construction material and legislative changes, which restrict the use of toxic substances. The large commercial importance is shown, as currently thermal wood is produced by five different modifications in Finland (Termowood), in the Netherlands (Plato Wood), in Germany (OHT - Oil Heat Treatment Wood) and two methods in France (Bois Perdure and Rectification). The process temperatures range between 160 and 260 °C and the differences between various modifications are represented by using the gas environment (nitrogen, steam), oils, different humidity levels and so on. Wood treated in such a way has better properties when used in exteriors, as well as interiors, e.g. dimensional stability, durability, color change and so on [3], [4].

The impact of thermal modification on anatomical, mechanical, physical, biological and chemical properties of wood has been the subject of many studies. In the scientific literature, however, no knowledge about fire characteristics of this thermal treated material is available. Fire characteristics are of main importance within wooden constructions. Even though there are studies dealing with thermally modified wood and its combustion [5], [6] the information on the reaction to fire performance for the modifications of thermally modified wood and the impact of these modifications on its properties is missing.

* **[1]Linda Makovicka Osvaldova, [2]Miroslav Gasparik, [3]Javier Ramon Sotomayor Castellanos, [4]Frank Markert, [1]Patricia Kadlicova, [2]Hana Cekovska**
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Faculty of Foresty and Wood Science, Czech University of Life Sciences Prague, Czech Republic
[3]Faculty of Engineering in Wood Technology, Universidad Michoacana de San Nicolas de HidalgoMorelia, Mexico
[4]Department of Civil Engineering, Technical University of Denmark, Denmark
E-mail: Linda.Makovicka@fbi.uniza.sk

The objective of this article is to assess properties of thermally modified wood, which characterize its ability to achieve flameless burning. A standard method is applied simulating real fires.

2. Thermal modification

In special furnaces, thermal modifications of wood are conducted using water, steam and high temperatures. The thermal modification device (special furnace) must be made of stainless steel and equipped with non-standardized fans and coolers. Biofuel, fuel oil, gas or electric heater are used as a propulsion agent. The whole process is conducted in three phases as described below in more details [7], [8].

2.1 Drying

Drying, i.e. the high-temperature drying, is the most time consuming phase of the process. During this stage, the moisture content of wood decreases almost to zero. Time of drying therefore depends on the initial moisture content of wood, specifications of the given type of wood and its thickness. Drying at high temperatures brings about greater elasticity and thus better resistance to deformations [1].

2.2 Heat treatment

This phase of thermal modification of wood begins immediately after drying. The heat treatment is carried out in an enclosed chamber at temperatures ranging from 185 to 215 °C. During the process, are used both steam-serving as the so-called protecting steam - and the protective gas preventing the wood from igniting and burning, which, however, influences the chemical changes inside the wood. The whole process takes up 2 to 3 hours [7].

2.3 Conditioning

The last phase of thermal wood treatment consists of cooling. During this stage, it is important to bear in mind that great differences in temperatures between wood and the outside environment may cause cracking. For its final use, wood must be re-damped to the appropriate level, since the final moisture content of wood has a significant impact on its operating characteristics. Once the phase has been completed, the modified wood should have a moisture content of approximately 5 to 7 %. The whole process takes 5 to 15 hours [7], [9].

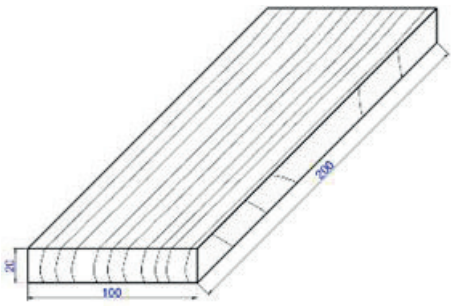


Figure 1 *Size of test samples (mm) to verify thermal modification for ignition and burning of this type of modified wood*

3. Experiment

3.1 Test samples of tropical woody plants

The test samples were made and modified in a thermal chamber (S400/03, LAC Ltd., Rajhrad, Czech Republic). Three final temperatures, 160, 180, and 210 °C, were chosen for the wood modification. The thermal modification used the ThermoWood principle developed by VTT (Finland), which takes place in a protective atmosphere (dispersed water in the air, to prevent overheating and burning), on the two tropical woody plants - Meranti and Merbau. Dimensions of samples were 200x100x20 mm (Figure 1) and they did not have any anatomical or production defects.

Five samples, made from both types of tropical woody plants, have been tested for each of the 4 temperatures of thermal modification, i.e. 20, 160, 180 and 210 °C.

The Meranti is a woody plant growing in Malaysia, Indonesia, Thailand and the Philippines. It has very hard wood with high resistance against pests, molds and weather conditions. The wood is of dark/light red color or of yellowish to white color and is very popular with buyers. Lighter wood is, however, more prone to breakage than the darker one [3], [10].

The Merbau is a type of woody plant growing in South East Asia, Indonesia, Vietnam, Thailand, Malaysia and the Philippines. At present, it is a very popular type of woody plant thanks to its hardness, firmness and brown coloring with golden stripes. In addition, it is characterized by the high durability and resistance against termites. From the point of view of its structure, it falls into the category of scattered porous woody plants [3], [10].

The structure of the given woody plants is shown in Figure 2.

3.2 Test apparatus

From the large number of test methods available a test method simulating conditions of real fire has been selected. Naked flame - of a constant value in an open space, not in an

Figure 2 *Structure of Meranti (on the left) and Merbau (on the right) [3]*

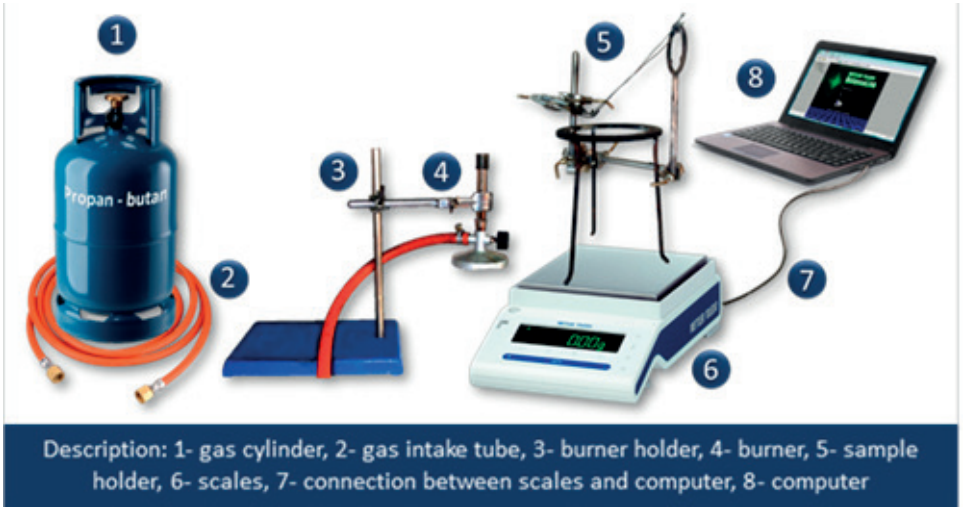


Figure 3 *Test apparatus scheme [12]*

enclosed laboratory environment - serves as a heat source. The method in question is a non-standardized EU method; however, it is traditionally used in material evaluations and their fire-retarding modifications [2], [11].

Each test sample was directly exposed to the flame of propane gas burner for 10 minutes. The test sample was placed at the angle of 45° to the horizontal plane. The flame had a length of 100 mm and the center of sample was 90 mm from the mouth of the burner. Basic measurements were carried out for 10 minutes, auxiliary measurements took additional 5 minutes (without using any heat source).

The apparatus, which was relatively simple, consisted of USBEC 1011/1 propane gas burner, which served as a regulated flame source (DIN-DVGW reg. Pan NG-2211AN0133) 1.7kW. Weight was measured using the Mettler Toledo scales with an accuracy of 0.01 g (MS 1602S / MO1, Mettler Toledo, Geneva, Switzerland). Weight changes of samples (evaluation criteria) have been recorded and the test has been carried out using the BalanceLink 4.2.0.1 (Mettler Toledo, Switzerland). During the experiment, weight change interval was set to 10 seconds. Diagnostic laboratory equipment is depicted in Figure 3.

3.3. Processing of numerical values

The main assessment criterion - weight loss of test samples - was calculated according to equation:

$$\delta_{mr}(\tau) = \frac{m(\tau) - m(\tau + \Delta\tau)}{m(\tau)} \cdot 100 \qquad (1)$$

where:

$\delta_{mr}(\tau)$ – relative weight loss at time (τ) [%],

$m(\tau)$ – weight of the sample at time (τ) [g],

$m(\tau + \Delta\tau)$ – weight of the sample at time $(\tau + \Delta\tau)$ [g] [4].

The relative weight loss value was used to calculatethe relative burning rate:

$$v_r = \frac{\delta_m}{\Delta\tau} \qquad (2)$$

where:

v_r – relative burning rate [%/s^1],

δ_m – relative weight loss in time (τ) [%],

$\Delta\tau$ – time interval recording weights [s] [4].

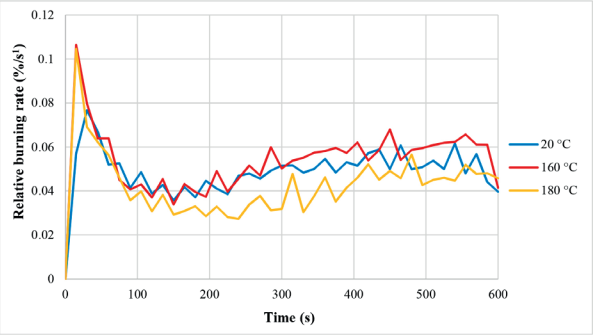


Figure 4 *Relative burning rate of the Meranti samples*

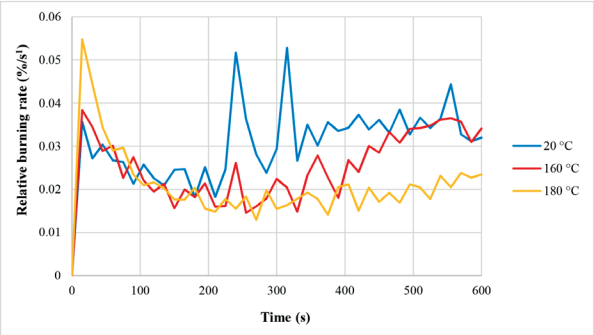


Figure 6 *Relative burning rate of the Merbau samples*

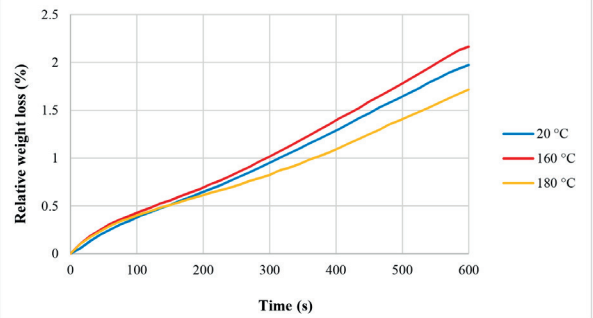


Figure 5 *Relative weight losses of the Meranti samples*

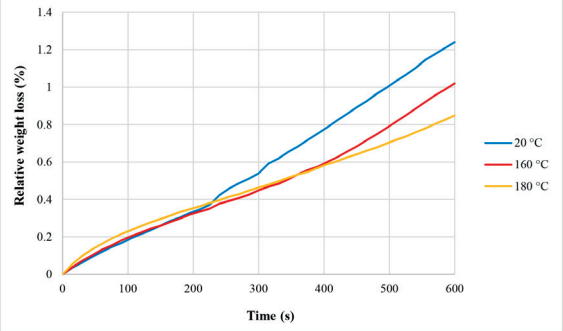


Figure 7 *Relative weight losses of the Merbau samples*

The impact of different densities of test samples on the results of the evaluation criteria was also observed. Density is calculated according to the following relation:

$$\rho = \frac{m}{V} \tag{3}$$

where:
ρ – sample density [kg/m^3],
m – total weight of the sample [kg],
V – total volume of the sample [m^3] [4].

4. The results

This section includes graphically processed results of the evaluation criteria. The first part presents average values of relative burning rate and relative weight loss of Meranti samples (Figure 4 and Figure 5, respectively) and the second one shows the summary of the same values in the same order for Merbau samples (Figure 6 and Figure 7, respectively).

Figure 4 shows rapid increase in burning rate as a result of flame exposure onto the test sample for all three thermal modifications of Meranti samples. After approximately 20 seconds, the burning rate slowed down, but a slight acceleration occurred from approximately 180 second. Samples at 20 °C and 160 °C were burning at an average speed of 0.05 %/s^1 and the sample at 180 °C by one hundredth of a second slower.

Weight losses of the samples are directly related to the above-mentioned changes in density. Figure 3 shows a detailed illustration of the process for some of the samples calculated based on relation (1).

The more significant course of relative burning rate was recorded for the Merbau samples, which is also demonstrated in the charts in Figure 6.

With both relative weight loss and relative burning rates, the rapid growth in burning rate can be observed within the very first seconds. Slowdown of burning rate occurs after approximately 20 seconds. Re-acceleration, however, differed for each sample. The sample at 180 °C was burning at an average speed of 0.02 %/s but the process was similar as with Meranti samples. Sample at 160 °C showed some slight extremes from approximately 220 second up to approximately 380 second and burning rate subsequently rapidly accelerated. The biggest variations have been recorded for the sample at 20 °C. The two peak values have been recorded and the subsequent burning proceeded more rapidly than with the other samples of different heat treatment but rather evenly.

Since the weight losses are directly related to changes in density, Figure 5 shows significant dominance samples at 20 °C over the other samples, making a difference between the flammability level of Merbau and Meranti samples. The results show that the Merbau samples resist the effect of flame a little more than the Meranti samples, since of those samples shows average values ranging from 0.02 to 0.03 %/s, whereas it is 0.04 to 0.05 %/s for the Merbau samples.

However, when comparing relative weight losses of the woody plants (separately), one can see that the Merbau samples at 20 °C surpass, on average, the weight losses of the samples at 160 °C. With the same criteria for the Meranti samples, the result is quite the opposite. Variations, that are represented by the maximum deviations in Figure 4 with the sample at 20 °C, are likely to be caused by the so-called random errors.

5. Conclusions

Thermally modified Meranti and Merbau woods have greater weight losses in open flame burning than woods that were untreated. Thermally modified Meranti and Merbau woods have a greater ability to ignite and burn more intensely than untreated Meranti and Merbau woods. It is clear from those results that thermally treated Meranti and Merbau woods, at all temperatures, have higher burn rates than untreated Meranti and Merbau woods. The Meranti and Merbau woods begin to burn after 10 s of exposure to the flame, and from 100 s to 130 s flares up significantly, resulting in a high burn rate. The highest burn rates occur within the first 200 s. The burn rate is the highest in the Meranti and Merbau woods that were thermally modified at 160 °C. The thermally treated Meranti and Merbau woods showed higher burn rates throughout the test, even after they exceeded the highest burn rate of untreated samples. For this evaluation criterion, one can also determine the causes of these phenomena, as was for the weight losses. The results show that thermally treated Meranti and Merbau woods greatly increase their ability to ignite and combust, and increase their burning intensity. This was also confirmed by the selected evaluation criteria. The authors recommend the addition of fire retardants to the thermally modified woods, which is also the objective of future experiments.

References

[1] Thermowood Handbook [online]. Finnish Thermowood Association, Helsinki, 2003. Available: http://www.vanhoorebeke.com/docs/Thermowood%20handboek.pdf [accessed: 2017-10-15].
[2] Forest Products Laboratory: Wood Handbook: Wood as an Engineering Material. Forest Service, U.S. Department of Agriculture, Madison, WI: Forest Products, 2010.
[3] DINENNO, P. J.: National Fire Protection Association and Society of Fire Protection Engineers (Eds.). SFPE Handbook of Fire Protection Engineering, 4th ed. Quincy, Mass., Bethesda, Md, 2008.
[4] GASPARIK, M., BARCIK, S.: Effect of Microwave Heating on Bending Characteristics of Beech wood. BioResources, 9(3), 4808-4820, 2014. DOI: 10.15376/biores.9.3.4808-4820
[5] KUBOVSKY, I. BABIAK, M.: Color Changes Induced by CO2 Laser Irradiation of Wood Surface. Wood research, 3, 61-66, 2009.
[6] REINPRECHT, L., VIDHOLDOVA, Z.: ThermoWood – Preparing, Properties and Applications/Termodrevo – Priprava, Vlastnosti a Aplikacie (in Slovak). Monograph, Technical University in Zvolen, Slovakia, 2008.
[7] YINODOTLGOR, N., KARTAL, S. N.: Heat Modification of Wood: Chemical Properties and Resistance to Mold and Decay Fungi. Forest Products Journal 60(4), 357-361, 2010.
[8] CEKOVSKA, H., GAFF, M., MAKOVICKA OSVALDOVA, L., KACIK, F., KAPLAN, L., KUBS, J.: Tectona Grandis linn. and Its Fire Characteristics Affected by the Thermal Modification of Wood. BioResources, 12(2), 2805-2817, 2017.
[9] CABALOVA, I., KACIK, F., KACIKOVA, D., ORAVEC., M.: The Influence of Radiant Heating on Chemical Changes of Spruce Wood. Acta Facultatis Xylologiae, 56(2), 59-66, 2013.
[10] MARTINKA, J., MARTINKA, F., BALOG, K., RANTUCH, P. HRUŠOVSKÝ, I., BLINOVÁ, L.: Calorific Value and Fire Risk of Selected Fast-Growing Wood Species. Journal of Thermal Analysis and Calorimetry, An International Forum for Thermal Studies, Springer, 2017. In: The influence of density of test specimens on the quality assessment of retarding effects of fire retardants, 2017.
[11] FANFAROVA, A., MARIS, L., OSVALD, A., MIKKOLA, E.: The Reaction to Fire Tests for Natural Thermal Insulation of Hemp Material Modified by Fire Retardant Ohnostop Special. Communications - Scientific Letters of the University of Zilina, 17(1), 15-21, 2015.
[12] MITRENGA, P.: Influence of wood density on weight loss during fire retardant tests. CD-ROM. Proceedings of the 8th International Scientific Conference Wood and fire safety, Slovakia, 213-220, 2016.

kaMUNikácie
COMMUNICATIONS

Veronika Brabcova - Simona Slivkova - David Rehak - Fulvio Toseroni - Jan Havko*

ASSESSING THE CASCADING EFFECT OF ENERGY AND TRANSPORT CRITICAL INFRASTRUCTURE ELEMENTS: CASE STUDY

This article focuses on the issue of assessing the cascading effects of critical energy and transport infrastructure elements at the fundamental level. The introductory part deals with the typology of failures and their impacts, which spread through the critical infrastructure system. At this stage, the paper presents current approaches to assessing the cascading effects and, in particular, addresses a newly developed assessment methodology. The following part defines the initial conditions of assessment and describes selected elements from the areas of energy and rail transport to which the methodology will be subsequently applied. The main part of the article is a case study of the proposed methodology, assessing the cascading effects by calculating the value of their risks, depending on the resilience and correlation of the rated elements.

Keywords: *critical infrastructure, cascading effect, assessing, resilience, correlation*

1. Introduction

Infrastructure failures brought about by system malfunction or disruption due to a terrorist attack or natural or technical causes are likely to increase significantly the extent of impacts on the failure of other dependent infrastructure. This is due to interdependencies existing between infrastructure segments which can exert a direct influence on these effects. In their paper, Zimmerman and Restrepo [1] presented the two steps aimed at facilitating the understanding of interdependencies. First, the likelihood of interdependencies between infrastructures is determined. Any identified interdependencies are subsequently categorized according to their location. A basic overview of the approaches to perceiving correlations constitutes the primary aspect affecting the identification and understanding of interdependencies. Rinaldi et al. [2] also identified the environment in which, and the degree to which, infrastructures are connected or interconnected. The authors argue that the types of interdependencies are of considerable relevance.

With respect to critical infrastructure, one should not fail to appreciate the basic difference between dependency and interdependency [3]. The critical infrastructure dependency refers to the link between two infrastructures where the condition of one affects the condition of the other. Interdependency, as opposed to dependency, implies a mutual relationship between two or more infrastructures. Those dependencies may be classified into several types. Buhne et al. [4], for example, divides dependencies into Requires-dependency, Exclusive-dependency, Hints-dependency and Hinders dependency. Hromada et al. [5] emphasize the need to make a clear distinction between positive and negative linkages. According to Rinaldi et al. [2], interdependency can be further classified as: physical, cyber, geographic and logical.

Infrastructure dependencies determine individual types of failures or effects [2]. Basic failures include a cascading failure, which occurs when a disruption in one infrastructure causes the failure of a component in the second infrastructure, which in turn leads to a disruption in the second infrastructure [6]. An escalating failure occurs when an existing disruption in one infrastructure exacerbates an independent disruption in the second infrastructure. A common-cause failure occurs when two or more infrastructure networks are disrupted at the same time.

2. Approaches to assessing cascading effects

There is currently a multitude of approaches to assessing cascading effects in critical infrastructures. The majority of these go hand in hand with the issue of evaluating the resilience

* [1]Veronika Brabcova, [1]Simona Slivkova, [1]David Rehak, [2]Fulvio Toseroni, [3]Jan Havko
[1]Faculty of Safety Engineering, VSB – Technical University of Ostrava, Czech Republic
[2]Department of Life and Environmental Sciences, Universita Politecnica delle Marche, Italy
[3]Faculty of Security Engineering, University of Zilina, Slovakia
E-mail: david.rehak@vsb.cz

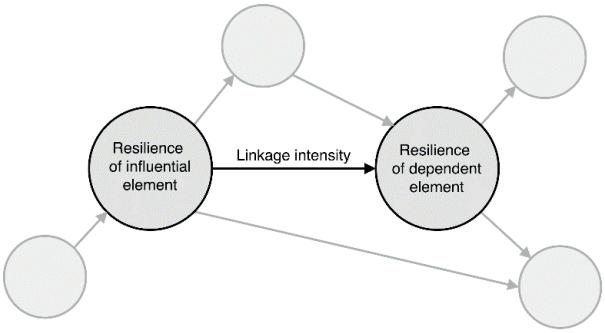


Figure 1 *Relationship between variables for calculating the risk of cascading effect propagation*

of a given system. Omer et al. [7] looked into a methodology, which proposes the application of network analysis. Via graph theory, they were able to identify the critical passage and thus establish the critical nodes with the most severe impacts on a selected network. This is well complemented by Hromada et al. [5], who developed a maths-based methodology and, in doing so, formalized a general approach to evaluating the resilience of selected critical infrastructure elements and networks. By contrast, Muller [8] advocated an approach to evaluating the resilience of an entire system via the fuzzy logic.

Aung and Watanabe [9], Dudenhoeffer et al. [10], Markuci and Rehak [11] and Rehak et al. [12] were among those to explore in greater detail the issue of modelling the interdependencies between individual infrastructures. All models can essentially be said to deal with the establishment of resilience indicators, which may vary slightly in individual publications. They are all aimed at evaluating critical infrastructure resilience or the linkages between individual critical infrastructure sectors.

A new approach to assessing the cascading effects in critical infrastructure systems was put forward in research projects Nos. VI20152019049 '"RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" and SP2017/87 "Assessing the Correlation of Selected Sectors in a Critical Infrastructure System." The completed research led to establishment of a procedure for assessment of the cascading impacts, involving assessment of the level of risk of impacts spreading between critical infrastructure elements. That approach hinges on the ability to evaluate the resilience of influential and dependent elements (the degree of the transferred impacts is assessed based on these variables) and the intensity of the linkage between those elements (the linkage intensity determines the likelihood of impact transfer). See Figure 1 for the relationship between variables for calculating the risk of cascading effect propagation.

Based on the above, the risk of cascading impact propagation can be calculated using the following Equation:

$$R = I \cdot P = V_{IE} \cdot V_{DE} \cdot LI = (1 - RE_{IE}) \cdot (1 - RE_{DE}) \cdot L \qquad (1)$$

where R is the risk level of a cascading effect spreading from an influential element (IE) onto a dependent element (DE) [%]; I is the degree of transferred impacts [%]; P is the probability of impact transfer [%]; V_{IE} is influential element vulnerability [%]; V_{DE} is dependent element vulnerability [%]; LI is the linkage intensity between influential and dependent elements [%]; RE_{IE} is the resilience of influential element [%]; RE_{DE} is resilience of dependent element [%].

Element resilience is established based on the following Equation:

$$RE = \frac{\Sigma_i^n C_{RE}}{n} = \frac{\Sigma_i^n \left(\frac{\Sigma_i^m P_C}{m} \cdot \frac{100}{P_{C_{\max}}} \right)}{n} \qquad (2)$$

where RE is the resilience level of a critical infrastructure element [%]; C_{RE} is the evaluated level of components determining the resilience of a critical infrastructure element [%]; n is the number of evaluated components of element resilience; P_C is the evaluated level of parameters determining the components of element resilience [a numerical value on a scale of 1 (i.e. the worst possible rating) to 5 (i.e. the best possible rating)]; m is the number of evaluated parameters [13].

The intensity of linkages between elements is determined based on the weighted average using the following Equation:

$$LI = \frac{\Sigma_i^p P_{LI} \cdot w}{\Sigma_i^p w} \cdot \frac{100}{P_{LI_{\max}}} \qquad (3)$$

where LI is the linkage intensity between influential and dependent elements [%]; P_{LI} is the evaluated level of parameters determining the element linkage intensity [a numerical value on a scale of 1 (i.e. the worst possible rating) to 3 (i.e. the best possible rating)]; w is the weights of parameters determining the element linkage intensity.

3. Initial conditions of the case study

A case study assessing the risk of cascading impact propagation between the critical infrastructure elements was carried out with a view to presenting the newly developed methodology. Two elements were selected for practical demonstration purposes: a transformer station (i.e. an influential energy sector element) and a level-crossing warning system (i.e. a dependent railway-transport sector element).

Power stations are located at power system nodes and are designed to transform, distribute, convert or offset electrical energy. For the purposes of the present study, the transformer station designed for the conversion of electrical energy to the required voltage and its subsequent distribution was selected. It employs power transformers interconnecting two or more networks with various voltages. Its layout is determined by the design of individual distribution facilities or substations and the placement of power transformers [14]. Pursuant to the Energy

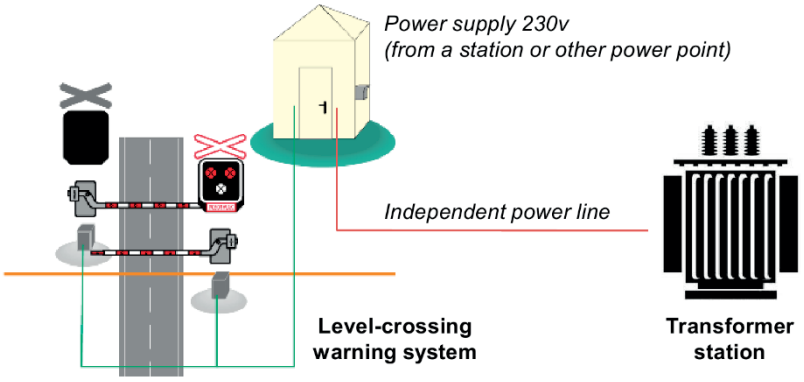


Figure 2 *Practical link diagram of the influential and dependent elements*

Act [15], the operator of the distribution system is obliged to ensure its reliable operation, modernization and development – the failure to provide electricity may be contractually penalized.

A level-crossing warning system is designed to improve safety at intersections where single or multiple railway lines cross a road at the same level. Level-crossing warning systems must have a guaranteed power supply conforming to Category 1, as stipulated in CSN 37 6605 [16]. This category includes systems whose failure due to power outage might pose an immediate threat to human life or lead to major property damage. Evidence of such impacts may be provided by an assessment of the risks in critical railway infrastructure [17]. The linkage between the two elements is illustrated in Figure 2.

In order to effectively evaluate cascading impacts in a critical infrastructure system, the scenarios of emergency impacts on the elements being evaluated must be viewed within the context of specific threats, which can be classified in five basic groups [18]:

- climatological (i.e. natural disasters such as floods, hurricanes, heavy snowfall);
- geological (e.g. earthquakes, volcanic activity, landslides);
- biological (i.e. epidemics, pandemics, epiphytic or epizootic diseases);
- technological (i.e. technological emergencies such as radiation emergencies, hazardous chemical spills, flooding caused by damage to hydraulic structures, widespread disruptions to engineering networks or public water supply emergencies);
- social (i.e. terrorism, criminal activity).

This particular case study involves a blackout caused by a terrorist attack, which is statistically one of the most common criminal threats [19].

4. Evaluating resilience of selected elements

Resilience is one of the key factors contributing to the preservation of critical infrastructure element functionality. It represents the ability of elements to mitigate the intensity of impacts caused by an emergency event and reduce the duration of their failure or disruption. The required level of resilience can be achieved via continuous enhancement of the five basic areas: preparedness, absorption, responsiveness, recoverability and adaptability. These areas and their criteria (Figure 3) determine the level of resilience of critical infrastructure elements and thereby markedly decrease their vulnerability [20].

The following evaluation of the resilience of both elements is carried out in the context of the selected emergency, i.e. a blackout caused by an act of terrorism.

4.1 Preparedness

Preparedness of critical infrastructure elements revolves around activities which help to oppose the effects of emergencies; this entails planning and having the required measures, forces and means in place to successfully manage any emergency and recover from its impacts [20]. Preparedness is determined by three parameters: risk analysis (1-5), planning (1-5) and implementation of measures (1-5).

The distribution system operator relies on preparedness in planning to cope with emergencies. At the same time, the organization adopts, as part of its continuous improvement policy, new measures aimed at enhancing its effectiveness in responding to emergencies. In consideration of this, the level of preparedness of the transformer station with regard to the aforementioned parameters was rated as “4”.

The risk analysis of the railway system element operator focused on risks associated with the warning system in relation to emergencies that are common in the railway transport sector. Based on this analysis, the operator proceeded to draw up individual safety/security plans. Some plans necessitated the adoption of mitigating measures designed to alleviate the impacts of emergencies on the railway transport system. Having analysed this information, all of the three parameters were rated as “3”.

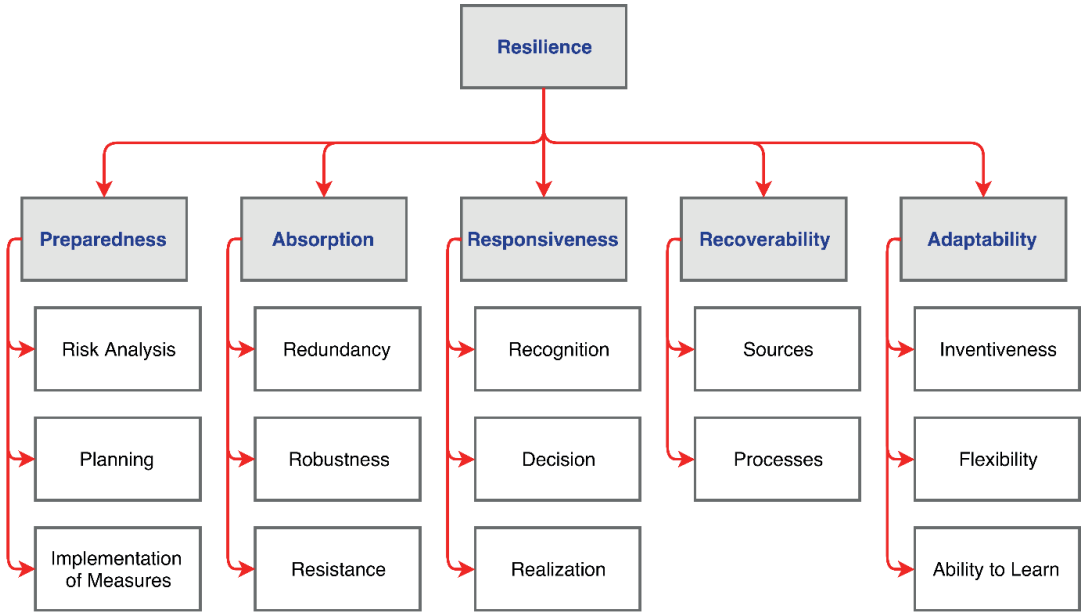


Figure 3 *Areas and their criteria determining the resilience of critical infrastructure elements*

4.2 Absorption

Absorption is the internal property of an element, which expresses its ability to automatically absorb the impacts of system failures and thereby to minimize their consequences [20]. It is one of the basic properties of an element prior to an emergency, which further determines to what extent the element will have to be recovered. Absorption enables the element to withstand negative events without any substantial deviation from the required function. Absorption is determined by three parameters: redundancy (1-5), robustness (1-5) and resistance (1-5).

With regard to redundancy, the transformer station was rated as "3", because despite it being a branched network where different loops can be activated during a failure, this option is not always available. The robustness of the transformer station was rated as "1". However, its resistance, i.e. its capacity to learn from previous events, was rated as "3".

The level-crossing warning system has a significant redundant source (i.e. a backup power source for up to 8 hours), which makes it possible to rate the redundancy of the dependent element as "4". However, neither the robustness nor the resistance of this element are considered as substantial. As this particular element is not supported or protected in any specific manner, both parameters were rated as "3".

4.3 Responsiveness

Responsiveness can be understood as the ability of an element to react to an emergency promptly and efficiently in order to minimize its impacts on the function or existence of the element [20]. Responsiveness is determined by three parameters: the time it takes to recognize an emergency (1-5), the time it takes to adopt a solution (1-5) and the time it takes to respond (1-5).

The technical design of the control room and the considerable knowledge of its operators substantially contribute to the prompt recognition of failures and facilitate the effective response of the distribution system operator. In the case of the transformer station, all three parameters were thus rated as "5".

With respect to the level-crossing warning system, the time it takes to recognize an emergency was rated as "4" due to its linkage to other systems (e.g. a control room). As the adoption and response parameters may to a considerable extent vary from one control room operator to another, they were rated as "3".

4.4 Recoverability

Recoverability expresses the time period of recovery, i.e. the time necessary for the recovery of function of the element to the required level after its disturbance by an emergency [20]. Recoverability is determined by the two parameters: allocated sources of recovery, i.e. human, material, financial and informational (1-5) and recovery processes (1-5).

Considering the penalties stipulated by the Energy Act [15] for failing to ensure the reliable operation, modernization and development of the distribution system, and considering the substantial losses resulting from the failure to provide contractual services, the allocated sources were rated as "4". The recovery processes parameter was rated as "5" due to the legal obligation of the distribution system operator to ensure its function.

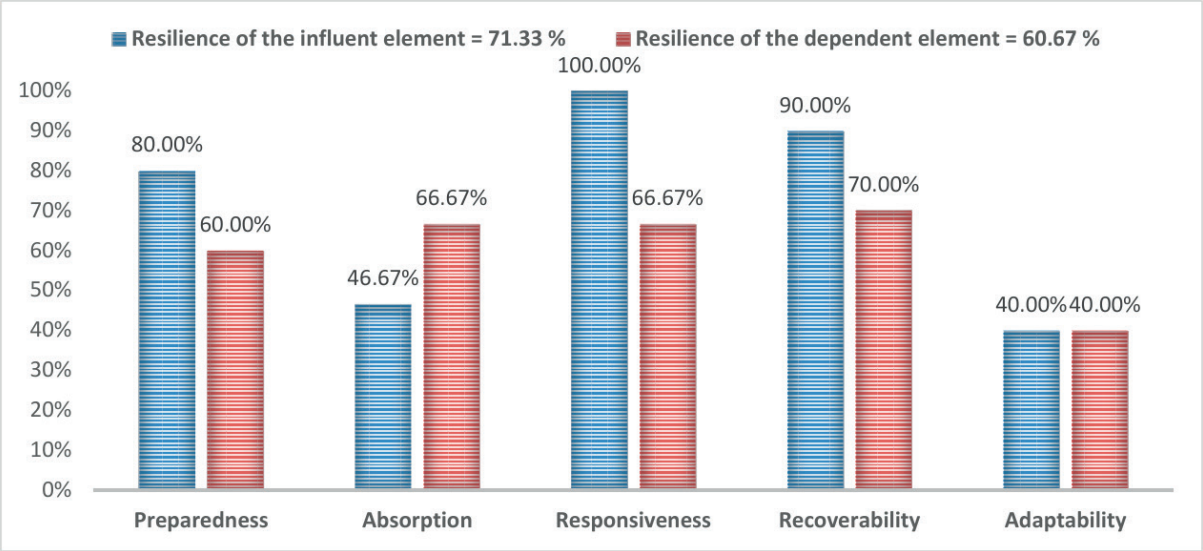


Figure 4 *The level of influential and dependent element resilience*

The allocated sources parameter related to the level-crossing warning system was rated as "2" due to the limited availability of some of the required sources. With respect to the dependent element recovery process following the complete recovery of the influential element, an immediate recovery of function may be expected; that is why this parameter was given the full rating of "5".

4.5 Adaptability

Adaptability is the ability of an organization to adapt its element to the effects of an emergency. It represents the dynamic (long-term) ability of an organization to adapt to changes in circumstances [20]. Adaptability is determined by three parameters: the level of inventiveness (1-5), the level of flexibility (1-5) and the ability to learn (1-5).

The distribution system operator is fairly limited in its ability to adapt the actual transformer station to new conditions. However, the operator may adaptively support its overall activity through research, modernization and other development activities, and thereby apply any new findings to the end elements of its system, as well. Accordingly, the parameters of the level of inventiveness and flexibility and the ability to learn were all rated as "2".

The structural and technological design of the level-crossing does not allow for much adaptability. The operator of the element may partially address these aspects through its activity, especially in cases where new options are explored with a view to managing emergencies that have previously affected its area of operation. With respect to the level-crossing warning system, all of the three parameters defined above were given the rating of "2".

4.6 Resilience

After the above-mentioned values of individual parameters have been entered into Equation (2), the level of resilience of the two elements being evaluated can be determined (see Figure 4).

5. Evaluating correlation of selected elements

An important factor affecting the correlation between the critical infrastructure elements, is the linkage intensity, which determines the speed and manner in which impacts can spread between individual elements [21]. If the intensity is low, even less resilient elements can be protected. The linkage intensity between influential and dependent critical infrastructure elements is determined by six basic parameters: the type of linkage (1-3), the condition of linkage (1-3), the level of linkage (1-3), the time characteristics of linkage (1-3), the substitution of linkage (1-3) and the structure of linkage (1-3). Due to their varying levels of significance, the parameters were assigned the following weighting coefficients: the type of linkage (0.23), the condition of linkage (0.23), the level of linkage (0.17), the time characteristics of linkage (0.15), the substitution of linkage (0.12) and the structure of linkage (0.10). The weighting coefficients for linkage intensity were determined in terms of grant project SP2017/87 "Assessing the Correlation of Selected Sectors in a Critical Infrastructure System".

In evaluating the type of linkage between the transformer station and the level-crossing warning system, physical interconnectedness was found to exist between the two elements and the parameter was accordingly rated as "3".

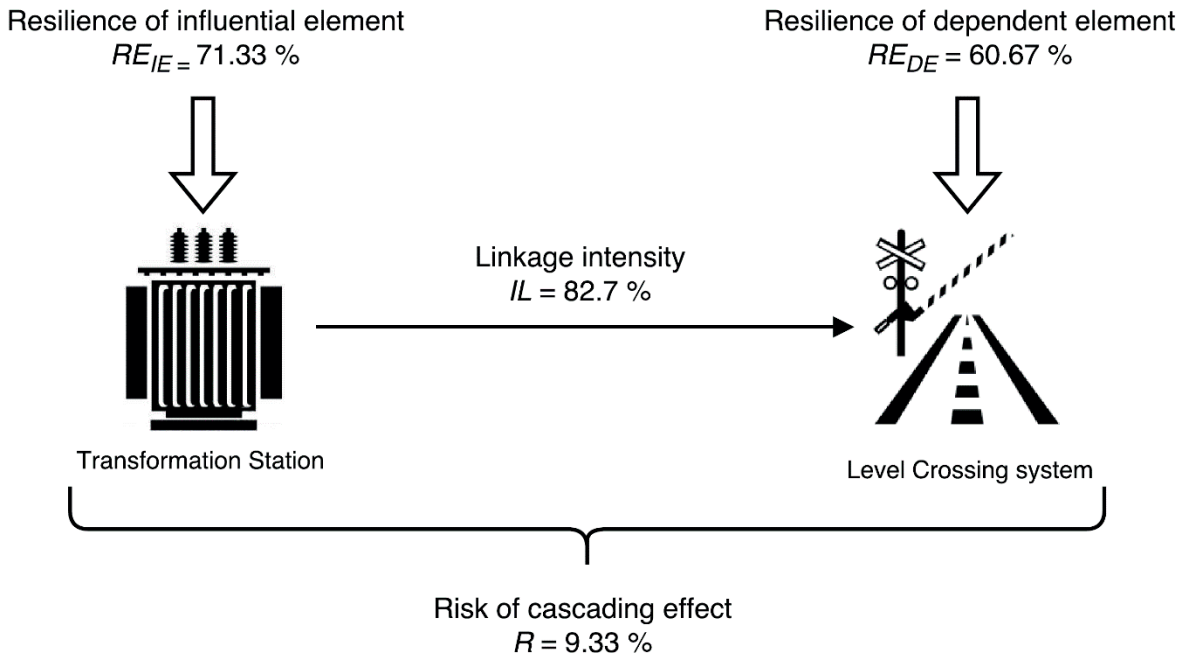


Figure 5 *The risk of impact propagation between influential and dependent critical infrastructure elements*

The function of the level-crossing warning system is dependent on the power supply, and even though it has a backup power source to rely on in the event of a blackout, its capacity is limited to 8 hours of operation only. For this reason, the dependency option was factored into evaluating the condition of the linkage and the parameter was given the rating of "2".

Operation of the level-crossing warning system is completely dependent on the power supply, thus constituting an intra-sectoral linkage. Consequently, the level of linkage was rated as "2".

Since the serviceability of the level-crossing warning system hinges on the continuous supply of electricity, the linkage was rated as "3" in terms of its time characteristics.

In the event of disruptions in the power supply, it is possible to activate different network loops in order to maintain the power supply to the equipment for the duration of the repair work. For this reason, the existence of one substitution linkage with a rating value of "2" was selected to evaluate linkage substitution between individual elements.

As the linkage between the transformer station and the level-crossing warning system is direct and does not penetrate any node, the linkage structure was given the rating of "3".

After the above-mentioned values of individual parameters have been entered into Equation (3), the determined linkage intensity between the influential and dependent elements was found to have an 82.7 % probability of impact transfer.

6. Evaluating the risk of impact propagation between selected elements

The evaluation of cascading effects in a critical infrastructure system consists of determining the level of risk of impact propagation between individual critical infrastructure elements. This essentially involves evaluation of the level of resilience of influential and dependent elements (determining the magnitude of impacts) and the linkage intensity between these elements (determining the likelihood of impact propagation).

After the above-mentioned values, relating to the resilience of the influential and dependent elements and the intensity of their linkage, have been entered into Equation (1), the level of risk of impact propagation between these elements can be determined. The resulting value assigned to the risk of impact propagation between the selected elements was 9.33 % (see Figure 5).

7. Conclusion

The continuous progress in scientific and technical knowledge inevitably leads to ever-increasing demands placed on critical infrastructure. Its structure makes it a composite system containing a vast array of elements and linkages. The disruption or failure of some elements may result in the transfer of impacts to other elements and, eventually, in fatal consequences for society, i.e. the loss of human life. That is why the ability to predict the propagation of impacts or cascading effects in a critical

infrastructure system is an important preventive tool, ensuring timely prediction of weak/vulnerable areas and implementation of adequate safety/security measures.

Based on this, the authors of the article developed a methodology for the correlations assessment in the critical infrastructure system. This methodology is based on evaluating the level of interest elements resilience and the link intensity between them. The result of the assessment is to determine the risk level percentage of the cascade effect spreading from the influent element to the dependent element. The methodology is applicable to all technical sectors of critical infrastructure, i.e. energy, communications and information technologies, transport and water management.

Acknowledgement

This research was supported by the Ministry of the Interior of the Czech Republic under Project VI20152019049 "'RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems"and by the VSB – Technical university of Ostrava under Project SP2017/87 "Assessing the Correlation of Selected Sectors in a Critical Infrastructure System".

References

[1] ZIMMERMAN, R., RESTREPO, C. E.: Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction. Proceedings of IEEE Conference on Technologies for Homeland Security (HST'09), USA, 165-170, 2009. DOI: 10.1109/THS.2009.5168029

[2] RINALDI, S. M., PEERENBOOM, J. P., KELLY, T. K.: Identifying, Understanding and Analyzing Critical Infrastructure Dependencies. IEEE Control Systems Magazine, 21(6), 11-25, 2001. DOI: 10.1109/37.969131

[3] REHAK, D., NOVOTNY, P.: Bases for Modelling the Impacts of the Critical Infrastructure Failure. Chemical Engineering Transaction, 53, 91-96, 2016.

[4] BUHNE, S., HALMANS, G., POHL, K.: Modelling Dependencies between Variation Points in Use Case Diagrams. International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03), Germany, 59-69, 2003.

[5] HROMADA, M., LUKAS, L., MATEJDES, M., VALOUCH, J., NECESAL, L., RICHTER, R., KOVARIK, F.: System and Method of Assessing Critical Infrastructure Resilience. Association of Fire and Safety Engineering, Ostrava, p. 177, 2013.

[6] KROCOVA, S., REZAC, M.: Infrastructure Operation Reliability in Built-Up Areas. Communications – Scientific Letters of the University of Zilina, 1(18), 75-78, 2016.

[7] OMER, M., MOSTASHARI, A., LINDEMANN, U.: Resilience Analysis of Soft Infrastructure Systems. Procedia Computer Science, 28, 873-882, 2014. DOI: 10.1016/j.procs.2014.03.104

[8] MULLER, G.: Fuzzy Architecture Assessment for Critical Infrastructure Resilience. Procedia Computer Science, 12, 367-372, 2012. DOI: 10.1016/j.procs.2012.09.086

[9] AUNG, Z. Z., WATANABE, K.: A Framework for Modeling Interdependencies in Japan's Critical Infrastructures. Palmer, CH., Shenoi, S. (Eds.): Critical Infrastructure Protection III, Springer, Hanover, 243-257, 2009.

[10] DUDENHOEFFER, D. D., PERMANN, M. R., MANIC, M.: CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. IEEE Winter Simulation Conference (WSC'06), USA, 478-485, 2006. DOI: 10.1109/WSC.2006.323119

[11] MARKUCI, J., REHAK, D.: Interdependencies of the Critical Infrastructure. Proceedings of International Conference on Fire Protection, Czech Republic, 207-210, 2014.

[12] REHAK, D., HROMADA, M., RISTVEJ, J.: Indication of Critical Infrastructure Resilience Failure. Cepin, M., Bris, R. (Eds.): Safety and Reliability – Theory and Application (ESREL), CRC Press, London, 963-970, 2017.

[13] LOVECEK, T., SVENTEKOVA, E., MARIS, L., REHAK, D.: Determining the Resilience of Transport Critical Infrastructure Element: Use Case. Proceedings of International Scientific Conference Transport Means, Lithuania, 824-828, 2017.

[14] Transformation Station. Electrotechnical Magazine, [online], 2008. Available: http://www.etm.cz/index.php/etm/starsi/38-energetika/139-transformacni-stanice.

[15] *Act No. 458/2000 Coll., On the Conditions of Business and the Performance of State Administration in the Energy Sectors and on the Amendment of Some Laws (Energy Act).*

[16] SSN 37 6605 ED.2. Connections of Electrical Equipments of Railway on Electric Power. Czech Office for Standards, Metrology and Testing, Prague, p. 20, 2012.

[17] TITKO, M., BYRTUSOVÁ, A.: The Risk Assessment of Critical Rail Infrastructure. Proceedings of International Scientific Conference on Transport Means, Lithuania, 99-102, 2015.
[18] REHAK, D., MARTINEK, B., RUZICKOVA, P.: Population Protection in the Context of Current Security Threats. Association of Fire and Safety Engineering, Ostrava, p. 131, 2015.
[19] SEDLACIK, M., ODEHNAL, J., FOLTIN, P.: Classification of Terrorism Risk by Multidimensional Statistical Methods. Proceedings of International Conference on Numerical Analysis and Applied Mathematics (ICNAAM'14), Greece, 1648(1), article no. 720011, 2015. DOI: 10.1063/1.4912948
[20] REHAK, D., SLIVKOVA, S., BRABCOVA, V.: Indication of Critical Infrastructure Resilience Failure. Cepin, M., Bris, R. (Eds.): Safety and Reliability – Theory and Application (ESREL), CRC Press, London, 955-962, 2017.
[21] REHAK, D., SENOVSKY, P., HROMADA, M., LOVECEK, T., DVORAK, Z., RISTVEJ, J., SVENTEKOVA, E., SLIVKOVA, S., NESPOROVA, V., BRABCOVA, V.: Bases for Assessing the Correlation of Critical Infrastructure Subsystems. VSB – Technical University of Ostrava, Ostrava, p. 22, 2016.

kaMUNikácie
COMMUNICATIONS

Maria Hudakova - Jan Dvorsky - Katarina Buganova - Ludmila Kozubikova*

ANALYSIS AND EVALUATION OF MARKET AND FINANCIAL RISKS IN SMALL AND MEDIUM-SIZED ENTERPRISES

The essence of the article is based on the collected and processed data from the survey to analyze, assess and evaluate the impact of the factor, which is the number of employees, on the market and financial risks, identified by managers of the SMEs in the Zilina region of Slovakia. The analysis of market and financial risks is carried out through the analysis of the selected statistical characteristics, using the point and interval estimates and methods of mathematical statistics. Interval estimation enables to determine not only the best estimate, but the entire interval with a certain probability of possible estimates of the mean value of the market and financial risks of a basic file, since the managers of an enterprise are more interested in intervals than in a point value. Results of the survey showed that the number of employees has an impact on the mean value of the market and financial risks of the SMEs in the Zilina region and therefore it is not possible to underestimate it.

Keywords: *risk, management, analysis, assessment, evaluation, small and medium-sized enterprise*

1. Introduction

The enterprise is facing constant changes in the business environment and the way to deal with these changes also depends on the ability of the enterprise to adapt and accept the variability of everyday life [1], [2]. In the interests of each management of the enterprise, whether it is small or medium-sized, risk management and the assessment of the current market and financial situation in relation to the potential risks should be commonplace [3]. Small and medium-sized enterprises (SMEs) in Slovakia do not pay sufficient attention to risks, whether market or financial, they do not form the prerequisites, or preventive measures of the risks assessed, which would prevent the problem or the financial crisis in the enterprise.

The economic performance of small and medium-sized enterprises has a major share of the production capacity and employment, and as Kozubikova, Homolka and Kristalas document, the presence of a thriving SMEs sector is one of the characteristic features of the developed economies [4]. Small and medium-sized business is no longer perceived as a social good to be maintained despite its economic costs, but on the contrary, a significant contribution to economic development. In today's world, small and medium-sized enterprises are increasingly perceived as the primary tools for the development of entrepreneurship, while they are not contributing to job creation and socio-political stability, but to the innovation and the competitiveness of the national economy, as well [5]. According to a [6], big companies are the driving force behind the globalization, which cooperate in a horizontal position with the competitors and in a vertical position with the key suppliers and customers. For this reason, the large enterprises work with the growing number of specialised small and medium-sized enterprises, helping them to ensure sufficient flexibility.

The Slovak economy is greatly dependent on the small and medium-sized enterprises, because they create 72 % of job positions and 67 % of the added value that extends well beyond the EU averages (67 % and 58 %). The majority of enterprises operate in the field of services and retail trade sectors, but production also represents an important sector, although it does not include a very high number of SMEs, accounting for 25 % of the jobs and 22 % of the added value creating the SMEs within the corporate economy [7].

Considering the Slovak Republic, regional disparities constitute a particularly important problem. The Slovak Republic has shown the highest level of regional disparities among the countries of the OECD in the five-year average for the period 1996 - 2000. On the contrary, as documented by the Habanik, Hostak and Kutik, the degree of regional disparities was even more developed in the years of 2002 - 2010 [8]. Although the economic performance across the country converges to the European level, the economic growth is, however, concentrated in the Bratislava region and the economic performance of the predominantly rural

* [1]Maria Hudakova, [2]Jan Dvorsky, [1]Katarina Buganova, [2]Ludmila Kozubikova
[1]Department of Crisis Management, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Enterprise Economics, Faculty of Management and Economics, Tomas Bata University in Zlin, Czech Republic
E-mail: maria.hudakova@fbi.uniza.sk

Table 1 Classification of the frequency of SMEs according to the number of employees [10], [11]

Risk	SME		
	Microenterprise (up to 10 employees)	Small enterprise (10 - 50 employees)	Medium-sized enterprise (up to 499 employees)
Financial	66	16	15
Market	92	27	12

regions still lag behind. In this context, there is a particularly important need to examine the economic phenomena of the Slovak Republic, not only at the national but at the regional level, as well.

2. Data, methodology and methods

The aim of article is to analyze, assess, and evaluate the impact of the factor, which is the number of employees, on the market and financial risks, identified by the managers of the SMEs in the Zilina region of the Slovak Republic, based on obtained and processed data from the survey. The analysis of market and financial risk is carried out through the analysis of the selected statistical characteristics, using the point and interval estimate and methods of mathematical statistics (analysis of variance). The number of employees in the enterprise is an important factor, which may or may not affect the assessment of the market and the financial risks and their control method. Result of the analysis of the market and financial risks' selected statistical characteristics is a point estimate of the mean value and variance of risks, when evaluating managers of the SMEs. Then, using the statistical testing, the conditions for the implementation of interval estimates (two-sided confidence interval) were determined. Determination of the impact of market and financial risks from the perspective of the number of employees in the SMEs, using the point estimate is a place of a particular point estimate of a mean value of market and financial risks, where the value of risks will lie on with a probability of 0.95, whereas the managers of enterprise are more interested in interval as the point value. This is a more accurate representation of the value of market and financial risks and its variance not only from the sample, i.e., a random set of SMEs, but the broader interval representation of the sample, i.e. the basic set of risks for the SMEs. Results obtained from the survey are based on the business experience of the SMEs' owners and managers and their attitude to risk, as well as their ability to manage the risk.

In order to meet the stated objective, empirical methods of examination (questionnaire, interview with the competent persons of SMEs), statistical induction of applying statistical methods were used, that is, the analysis of variance using the quantitative tools of statistics (percentage, average values, heteroscedasticity, Cochran's test, Bartlett's test, Kolmogorov-Smirnov test, F-test, Kruskal-Wallis test, point and interval estimate, graph of the mean values) and statistical software SPSS Statistics [9].

In 2013 - 2015, a statistical survey of business risks of small and medium-sized enterprises in the Zilina region was realized, within the framework of the project FaME/13/MSPRISK: „The recent trends in the area of business risks faced by the small and medium-sized enterprises in the selected regions of the Czech Republic and Slovakia". In the Zilina region, 164 small and medium-sized enterprises were polled, in the form of empirical research (questionnaires and interviews with the competent persons from SMEs).

The structure of the enterprises was as follows: 17 % in the production, 21 % in trade activities, 17 % in construction business, 6 % in transport, 1 % in agriculture, and the largest share of 38 % formed enterprises doing business in other sectors (consulting, distribution, etc.). In the Zilina region, 80.49 % of business owners stated the market risk as the biggest risk of the business at the moment and 58.54 % mentioned financial risk as the second key risk of business [10].

The survey shows that 67.68 % of enterprises can largely manage financial risks, 23.17 % claims they can properly manage financial risks. Only 1.83 % thinks that they cannot manage the financial risks. This is admittedly a subjective assessment of their own abilities; it is nevertheless possible to say that this capability may be partially supported even by fairly decent educational structure of the entrepreneurs. Point estimates have been calculated on the basis of selected statistical characteristics (SSC), listed in Table 1 and Table 2, which are necessary for the processing of mathematical statistics method, i.e. analysis of variance: μ - average value of the risk to the enterprise, σ - standard deviation of the value of the risk to the enterprise, σ^2 - variance of the values of the risk to the enterprise.

According to the stated purpose in the introduction of the article and with use of statistical methods and tools, it was examined whether or not the factor such as the number of employees in the enterprise in the Zilina region has an impact on mean (average) values of the market and financial risks. To meet the objective, the statistical induction has been used, which consists of a wide range of statistical methods and its findings, obtained from the sample extends the base file. Results of statistical induction have been processed using the point estimate. Thus it was possible to find an estimate of the mean value of the market and the financial risks of the base file using a single value or point.

Table 2 *Point estimates of statistical characteristics of the financial and market risks [10], [11]*

Risk	SSC	SME		
		Micro-enterprise (up to 10 employees)	Small enterprise (10 - 50 employees)	Medium-sized enterprise (up to 499 employees)
Financial	μ	31.74	40.33	34.36
	σ	13.48	13.95	14.74
	σ^2	181.92	194.52	217.45
Market	μ	52.29	51.22	55.67
	σ	19.53	16.17	20.73
	σ^2	381.43	261.47	429.73

Table 3 *Analysis of variance of market risk values*

	Number of enterprises	The average in group
Micro-enterprise	66	42.77
Small enterprise	16	61.57
Medium-sized enterprise	15	48.36
	P- value = 0.042	

Then, the quantitative method of "analysis of variance" was used. The analysis of variance was set using either a parametric or non-parametric test. Two essential conditions had to be met for calculation of the parametric tests and it was chosen that the resulting p-value of the market and financial risks of the homoscedasticity test (i.e. identity of variance) and the test to verify the normality of groups of SMEs, must be higher than the level of significance of 0.05. Evaluation of differences in mean values of the market and financial risks among the groups of the SMEs was the result of the analysis of variance. Using the interval estimate only a single best estimate was identified. However, the whole interval of potential estimates of the mean value of the market and the financial risks is of a base file with a probability of 0.95.

2.1 Analysis and assessment of selected statistical characteristics of the market risk

The parametric test of mean values of the risk could not be used for the analysis of variance of the market risk. The non-parametric test of market risk medians was realised in the three groups of SMEs according to the number of employees in the Zilina region, whereas the conditions have been met. The condition of homoscedasticity - the identity of variances of different groups has been verified using the following tests: Bartlett´s test: p-value = 0.649.

From results of the individual tests can be concluded that the resulting p-value was higher than the level of significance that was chosen, in all the tests. The condition of the normal distribution of market risk in enterprises, according to the number of employees using the Kolmogorov-Smirnov test included: p-value of enterprises with the number of employees up to 9 is 0.01; p-value of enterprises with the number of employees up to 50 is 0.571; p-value of enterprises with the number of employees up to 499 is 0.555.

Regarding the level of significance, an assumption that microenterprise risk assessment comes from the normal distribution was refused.

In relation to the fact that the calculated p-value of the Kruskal-Wallis non-parametric test of the analysis of variance is smaller than 0.05 (Table 3), one can say that there are statistically significant differences among medians of the values of the market risk, according to the number of employees of small and medium-sized enterprises in the region of Zilina.

Graphic analysis of the market risk, Figure 1, confirmed the test results using the methods of mathematical statistics "Analysis of variance". It was confirmed that the number of employees has an impact on the mean value of the market risk designated by managers of SMEs.

2.2 Analysis and assessment of selected statistical characteristics of the financial risk

The parametric test of mean values of the risk for the analysis of variance of the financial risk could not be used. The non-parametric test of financial risk medians was realised in three groups of SMEs, according to the number of employees in the Zilina region, whereas the conditions have been met. The condition of homoscedasticity -the identity of variances

Table 4 *Analysis of variance of financial risk values*

	Number of enterprises	The average in group
Micro-enterprise	92	66.05
Small enterprise	27	62.50
Medium-sized enterprise	112	73.54
	P- value = 0.009	

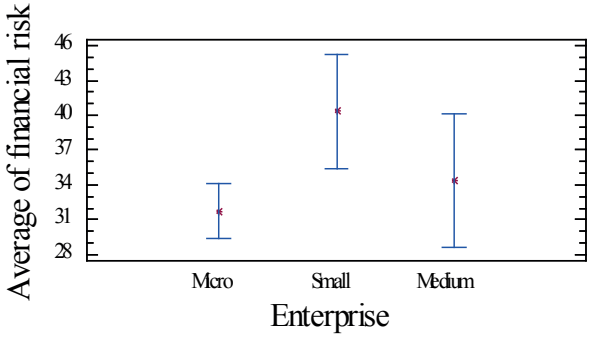


Figure 1 *Graph of the average values of market risk in groups of SMEs*

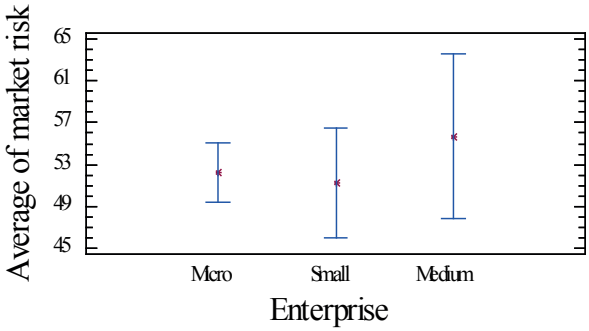


Figure 2 *Graph of the average values of financial risk in groups of SMEs*

of different groups has been verified using the following tests: Cochran test: p-value = 0.934.

From results of the individual tests can be concluded that the resulting p-value was higher in all tests than the level of significance that was chosen. The condition of the normal distribution of financial risk in enterprises, according to the number of employees using the Kolmogorov - Smirnov test included: p-value of enterprises with the number of employees up to 9 is 0.003; p-value of enterprises with the number of employees up to 50 is 0.701; p-value of enterprises with the number of employees up to 499 is 0.433.

On the surface the significance, an assumption that microenterprise risk assessment with the number of employees up to 9 come from the normal distribution was refused.

In relation to the fact that the calculated p-value of the Kruskal-Wallis non-parametric test of the analysis of variance is smaller than 0.05, one can say that there are statistically significant differences among medians of the values of financial risk, according to the number of employees of small and medium-sized enterprises in the region of Zilina, with the reliability of 0.95. Table 4 shows that the median assessment of the small enterprises in relation to financial risks is on average about a third higher than the risk of micro and medium-sized enterprises in the Zilina region in Slovakia.

Graphic analysis of financial risk, Figure 2 confirmed the test results using the methods of mathematical statistics "Analysis of variance". It was confirmed that the number of employees has impact on the mean value of the financial risk designated by managers of SMEs.

2.3 Interval estimates of the statistical characteristics of financial and market risks

Based on the knowledge of the selected statistical characteristics of the assessment of market and financial risks by managers of the SME from the Zilina region (Tab. 2), the probability model of normal distribution of mean value of market and financial risks was found. Subsequently, the generalised conclusions on the assessment and evaluation of the market and financial risks, by the managers of the SME in the Zilina region in the Slovak Republic were drawn and a base file was created. An important factor in statistical induction was development of the calculation of interval estimates with a specified reliability of 0.95 (estimate reliability). Since it was a sample of managers and owners of SMEs in the Zilina region, expressing general conclusions on the assessment of market and financial risks, it was counted on the potential uncertainty with probability of 0.05. Point estimates of the sample file of the selected statistical characteristics, such as the mean value, variance and standard deviation of financial and market risks, calculated in Table 2 represent point estimates of the base file, which are the basis for determining of the interval estimates.

Interval estimates of the base file, such as the mean value and standard deviation of financial and market risks of the assessment of the SME managers, with the probability of 0.95, are calculated in Tables 5 and Table 6: μ_d - the lower limit of the interval estimate of the mean value with reliability 95 %; μ_h - the upper limit of the interval estimate of the mean value with reliability 95 %; σ_d - the lower limit of the interval estimate of standard deviation; σ_h - the upper limit of the interval estimate of standard deviation.

Table 5 *Interval estimates of the mean value of financial and market risk*

Risk	SME					
	Micro-enterprise (up to 10 employees)		Small enterprise (10 - 50 employees)		Medium-sized enterprise (up to 499 employees)	
	μ_d	μ_h	μ_d	μ_h	μ_d	μ_h
Financial	28.42*	35.05*	32.60	48.05	24.45	44.27
Market	48.24*	56.33*	43.02	59.42	45.39	65.94

**Condition of normal distribution of data in the group has not been met.*

Table 6 *Interval estimates of the standard deviation of financial and market risk*

Risk	SME					
	Micro-enterprise (up to 10 employees)		Small enterprise (10 - 50 employees)		Medium-sized enterprise (up to 499 employees)	
	σ_d	σ_h	σ_d	σ_h	σ_d	σ_h
Financial	11.51*	16.2*	10.21	21.99	10.30	25.87
Market	17.06*	22.8*	16.32	28.40	11.45	27.45

**Condition of normal distribution of data in the group has not been met.*

Based on the results of the Kolmogorov-Smirnov test of the mean value of the financial and market risks, analyzed and evaluated in subsections 2.1 and 2.2, one cannot take into account the interval estimates of the selected statistical characteristics (the mean value and standard deviation) with a probability of 0.95. The reason is that the assessment of the market and financial risks by managers in microenterprises does not follow the condition of probability model of normal distribution. Interval estimates of the mean value and standard deviation of market and financial risk by managers of SMEs in the Zilina region were determined using the method of mathematical statistics with the probability of 0.95. Based on this fact one can conclude that there is a high degree of significance of results analyzed and assessed in the processed survey.

3. Evaluation of the results

Based on the results of the survey analysis of market and financial risks of the SMEs, through the analysis of the basic statistical characteristics of point and interval estimates and methods of mathematical statistics, one can conclude that the number of employees has an impact on the mean values of the market and financial risks identified by managers of the SMEs in the Zilina region. Therefore, their impact cannot be underestimated. Defining the point and interval estimation the interval of market and financial risks impact for managers from the perspective of the number of employees in SMEs in Slovakia was set.

Based on calculations, an interesting finding was obtained that the greatest impact of financial risk, in view of the number of employees in SMEs in Zilina region, has been identified in small enterprises. The reason may be the growing number of fraud cases in the fields of accounting, operations or customer service. If a small enterprise management is not sufficiently informed of all the processes of the enterprise and the lack of funds is forcing it to restrict the costs of the high-quality external services in the fields of accounting, or safety, it may affect the conduct of employees in a negative way. An unclear distribution of responsibilities, competence and powers is a frequent source of disagreement at the workplace, as well as of possible financial losses as a result of failure to comply with the stated objectives.

The impact of the number of employees on the occurrence of market risk in the SMEs in the Zilina region is the highest in the medium-sized enterprises, and the lowest among small enterprises. In view of the volume of production and the operation of the market, the medium-sized enterprises are more sensitive than the small ones. Their operation is often very little flexible, or there is too much dependence on the customer, or supplier, which may affect their pricing policy, low load from the perspective of the production capacity and last but not the least, their profits. Those aspects have impact on wage and tax policy of the enterprise. The rising costs are the major source of risk for the SMEs in this area.

Financial risks in the form of operational risks, which are usually caused by a failure of the human factor or technological failure, may lead to financial losses. Those are the risks that are mostly short-term in duration, but the possible negative effects of the crisis situation arising as a result may have extensive or disastrous consequences (risks to health, life, property). One of the most common causes of the ending of an enterprise includes incorrect calculation of minimum capital and very often underestimated calculation of unit costs, incorrectly calculated prices of goods and services, errors in accounting (tax, levy),

high input investment and insufficiently or improperly secured funding sources (own, foreign). From the point of view of the financial burden, the largest source of risks is the high tax load, which acts negatively on the amount of the total costs of work and is administratively challenging, as confirmed by the results of the survey.

The SMEs can manage risks in several ways. One of the options, which, however, a lot of SMEs do not use, is to create financial reserves of the enterprise for the period of the recession. This is due to limited financial resources. Therefore, it is recommended in the field of SMEs to move risk to the business partners. In terms of functioning of the financial markets and the insurance market, which provides a range of products and credits, one of the most viable ways is to reduce risk by providing security or insurance. A higher level of planning requires reducing the risk by diversifying into different commercial activities. Diversifying risks into the various activities requires combining the financial resources. Securing funding through loan products, or from other available sources to support SMEs, requires the processing of a detailed financial and cash-flow plan, taking into account the potential risks of the business.

4. Conclusions

Most of the enterprises abroad integrate risk management into their planning and decision-making process s, i.e. systematically consider the potential risks when taking decisions in the area such as cash-flow management, investment, pricing. They see the implementation of enterprise risk management as the greatest potential for increasing efficiency in risk management. Even in Slovakia, medium-sized enterprises, in an effort to improve risk prevention, should have integrated risk management, i.e. centralize the risk management into one department and create teams composed of different departments to control individual types of risks. The biggest barriers that prevent enterprises in Slovakia from effective control of market and financial risks, are related to problems with the availability of information, whether internal or external data necessary to the evaluation and management of risks, or their integration into the decision-making process. They identify the financial risks only on the basis of the data in the accounts and according to the degree of profitability, after their implementation (establishment). Based on the present experience, many managers are based on the knowledge of the past. However, evaluating the risk only based on own experience and feelings is currently insufficient. Analysis and assessment of the researched factor, such as the number of employees, revealed the impact on the level of market and financial risks cannot be underestimated. Therefore, owners of the SMEs in Slovakia and responsible managers must rethink their approach to the assessment and management of market and financial risks and consider the level of the action of risk resources for the purpose of managing risks arising from them.

Acknowledgment

Publication of this paper was supported by the Scientific Grant Agency - project VEGA No. 1/0560/16. Risk Management of Small and Medium Sized Enterprises in Slovakia as Prevention of Company Crises.

References:

[1] AGARWAL, R., ANSELL, J.: Strategic Change in Enterprise Risk Management. Strategic Change-Briefings in Entrepreneurial Finance, 25(4), 427-439, 2016.
[2] BOGODISTOV, Y., WOHLGEMUTH, V.: Enterprise Risk Management: A Capability-Based Perspective. Journal of Risk Finance, 18(3), 234-251, 2017.
[3] FRASER, J. R. S., SIMKINS, B. J.: The Challenges of and Solutions for Implementing Enterprise Risk Management. Business horizons, 59(6(SI)), 689-698, 2016.
[4] KOZUBIKOVA, L., HOMOLKA, L., KRISTALAS, D.: The Effect of Business Environment and Entrepreneurs´ Gender on Perception of Financial Risk in the Smes Sector. Journal of Competitiveness, 9(1), 36-50, 2017.
[5] BROLL, U. A., MUKHERJEE, S. B.: International Trade and Firms' Attitude towards Risk. Economic Modelling, 64, 69-73, 2017.
[6] LUSKOVA, M., TITKO, M.: Current Trends in Work Motivation and Perceived Risks. Proceedings of the 3rd International Multidisciplinary Scientific Conference on Social Sciences and Arts (SGEM 2016), Bulgaria, 157-164, 2016.
[7] URBANCOVA, H., HUDAKOVA, M.: Employee Development in Small and Medium Enterprise in the Light of Demographic Evolution. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 63(3), 1043-1050, 2015.
[8] HABANIK, J., HOSTAK, P., KUTIK, J.: Economic and Social Disparity Development within Regional Development of the Slovak Republic. Economics and Management, 18(3), 457-464, 2013.
[9] HAIR, J. F.: Multivariate Data Analysis. Upper Saddle River, Prentice-Hall, 2010.

[10] HUDAKOVA, M., BUGANOVA, K., DVORSKY, J., BELAS, J., DANA, L. P.: Analysis of the Risks of Small and Medium-Sized Enterprises in the Zilina Region. Communications - Scientific Letters of the University of Zilina, 17(1), 34-39, 2015.
[11] BELAS, J., BUGANOVA, K., HOSTAK, P., HUDAKOVA, M., LUSKOVA, M., MACHACEK, J., SOBEKOVA-MAJKOVA, M.: The Business Environment for Small and Medium-Sized Enterprise in the Czech and Slovak Republic. Georg, Zilina, p. 153, 2014.

Lucia Figuli - Vladimir Kavicky - Stefan Jangl - Zuzana Zvakova*

COMPARISON OF THE EFFICACY OF HOMEMADE AND INDUSTRIALLY MADE ANFO EXPLOSIVES AS AN IMPROVISED EXPLOSIVE DEVICE CHARGE

More than 95% of all the terrorist attacks are carried out using the ANFO explosives. The ANFO explosives are explosives made from ammonium nitrate and fuel oil. They can be in three different variants (ammonium nitrate with oil, ammonium nitrate with oil and aluminium powder or ammonium nitrate with oil and TNT). This paper describes analysis of the field test results of ANFO explosives of different types. The efficacy of industrially made and the homemade ANFO explosives is compared and their possible usage in terrorist attacks for the treatment or the damage of critical infrastructure elements is described.

Keywords: *ANFO explosives, field tests, homemade explosives, industrially made explosives, explosive device charge, critical infrastructure element*

1. Introduction

The global threat of terrorism presents a grave security problem in the 21st century. Combating this threat in the coming decades will require constant adjustment of forces, concepts, as well as capacities. Those changes will also affect the issues of protection of persons and property in the civilian environment. Improvised explosive devices (IED) as means of asymmetric threat in the present, as well as in the future, pose significant threat for the democratic states. IEDs are insidious and effective weapons being used by terrorists, alien militants and criminals, primarily for the purpose of crippling or killing people, destroying country's economy or for instilling fear among the civilians. Their aim is to challenge the legitimacy of governments and their ability to give their citizens freedom and security. Where the democratic processes end, the radical solution begins [1].

More than 95% of all the terrorist attacks are carried out using the ANFO explosives or other type of agents [2] and [3]. After the human targets, elements of the critical infrastructure are the second most important target. The critical infrastructure element can be from one of critical element sectors (government buildings, embassies, traffic nodes - airports, railways and bus stations, banks, hospitals, dams, pipe infrastructure, power or information centers and others). As is obvious from the [4] those elements have greater safety risks and are the objects, the security breach of which can cause extensive damage, not only in terms of protection of human life and health, but also to the economy and to the performance of state functions.

2. ANFO explosives

The ANFO explosive is a widely used explosive mixture. It can be prepared industrially or it can also be made at home very easily.

From the chemical-technological point of view it is possible to differentiate three different versions of the ANFO explosives:

- ammonium nitrate + fuel,
- ammonium nitrate + fuel + powder metal (usually aluminium or magnesium) and
- ammonium nitrate + fuel + wooden powder - delaborated TNT.

Optimal content of diesel or oil in ANFO is about 5.5-6%, in porous AN about 10-11%. Mixture where the fuel content is less than the optimum decreases the energy of the explosion while simultaneously significantly increases the content of nitrogen oxides in products of the explosion. On the contrary, the higher content of fuel leads to an increase in the content of carbon

* [1]Lucia Figuli, [2]Vladimir Kavicky, [1]Stefan Jangl, [1]Zuzana Zvakova
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Ministry of Defence of the Slovakia
E-mail: lucia.figuli@fbi.uniza.sk

Figure 1 *Industrially made explosives DAP - E (left) and DAP - 2 (right) in the prilled form*

monoxide in the products of the explosion and again to a decrease in the energy of the explosion.

ANFO under the most conditions is considered as highly explosive; it decomposes through detonation rather than deflagration and with a high velocity. It is a tertiary explosive consisting of distinct fuel and oxidizer phases and requires confinement for efficient detonation and brisance. Its sensitivity is relatively low; it generally requires a booster (e.g., one or two sticks of dynamite, as historically used, or in more recent times, Tovex or cast boosters of TNT/PETN or similar compositions) to ensure reliable detonation [5].

This type of explosive is used in coal mining, quarrying, metal mining where its good characteristics as low cost and easiness of use matter more than the benefits offered by conventional industrial explosives, such as water resistance, oxygen balance, high detonation velocity and performance in small diameters is taken advantage.

The ANFO explosives are very popular among the terrorists due to their simplicity of preparation. They were the main explosives used by organizations such as IRA, PIRA, Al-Quaeda. The ANFO explosives were used for the terrorist attacks in New York, in Oklahoma City and Oslo. They are used by semi armed units in Afghanistan, Iraq, Syria and North Caucasus.

The ANFO explosives are present in improvised explosive devices, where they are also known as fertilizer bombs.

3. Industrially made ANFO explosives

The basic components of the first ANFO explosives were based on fertilizer ammonium nitrate and charcoal. The improvement of explosives began when the charcoal was substituted for hydrocarbon as fuel oil and fertilizer ammonium nitrate for technical one. Later, the crystalline ammonium nitrate was substituted for porous prilled one. This type of ammonium nitrate is produced so that the prills in a size of 0.5-3.0 mm are created. Blasting grade AN prills are made by spraying molten AN into a prilling tower (see Figure 1). Droplets fall under carefully controlled cooling conditions. The AN solidifies while falling, taking on an approximately spherical shape of relatively uniform size. Prilling tower conditions must enable production of a "porous" prill that will absorb the proper amount of fuel oil (6 percent by weight). High density prills will not properly absorb the fuel oil and blasting performance will suffer [6]. Prilled ammonium nitrate is capable to absorb 11 percent of fuel oil weight. The final explosive characteristics of prepared ANFO depend on the sizes and porosity of prills (on the density). Generally, ANFO with small porous prills has a higher detonation velocity and the higher detonation sensibility [7]. Dense prills are often not detonable, or if initiated, perform at very low rate of detonation [6].

For this research the products DAP - 2, DAP - E (see Figure 2) and POLONIT, manufactured by a of the Slovak company called Istrochem Explosives a.s. Bratislava, were chosen. Their characteristics and the represented type of explosive are given in Table 1. It should be pointed out that all used explosives were fabricated industrially, meeting the standards of the production technology.

DAP - 2

The explosive is a mixture of ammonium nitrate, kerosene and dye. The explosive is of loose consistency, red in colour and is used for blasting on the surface, as well as is in the underground, without the danger of gas, vapour and dust explosions as a rock mining explosive.

DAP - E

The explosive is a mixture of ammonium nitrate, methyl esters of higher fatty acids, vegetable oil and red dye. The explosive is of loose consistency, red-grey in colour and it can be used in blasting operations on the surface, as well as in the underground, in an environment without the danger of gas, vapour and dust explosions as a rock mining explosive.

POLONIT - V

The explosive is a mixture of ammonium nitrate, kerosene, charcoal, ground TNT with water-resistant additives. The explosive is of loose consistency, white to yellowish in colour and it can be used in blasting works on the surface, as well as in

Table 1 Characteristics of industrially made ANFO explosives

Explosive	Type of represented ANFO explosive	Explosive velocity [m/s]	Heat of combustion [kJ/kg]	Density [g/cm^3]	Explosive pressure [GPa]
DAP - 2	AN+oil	2650	3830	0.65	2.95
DAP - E	AN+oil+Al	3100	4200	0.65	4.58
Polonit - V	AN+oil+TNT	4000	5138	0.9	6.93
TNT	Reference	6800	4200	1.58	18.4

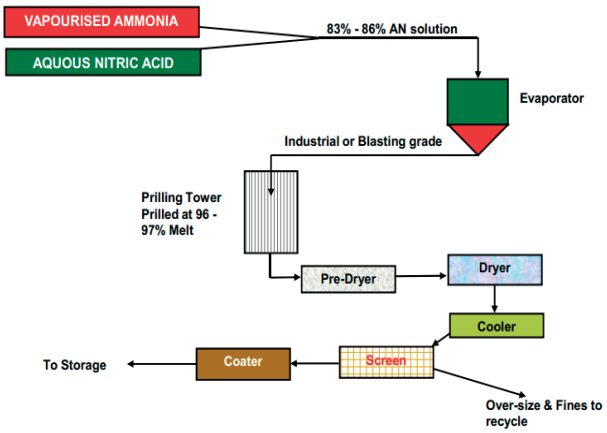


***Figure 2** Ammonium nitrate prill manufacturing [6]*

a) *b)*

***Figure 3** Ammonium nitrate used in the field tests a) sack b) prills*

the underground, in an environment without the danger of gas, vapour and dust explosions.

4. Homemade ANFO explosives

These types of explosives are very dangerous for the society. Prices of needed components are very low; the preparation does not require specialised knowledge and components for the preparation are freely available. Described explosives can be made by fertilizer based on ammonium nitrate used for agricultural purposes. Availability of fertilizers and oils (oil, fuel oil, kerosene) is not controlled. A malaxer for the production of chocolate or a concrete mixer can be used as mixing machines.

It is thought that the homemade explosives are not mixed well, made from low quality raw material (nitrogen content), they contain chemical impurities, possibly water and thus one can suppose that their efficiency is 70-90 % of standardly fabricated explosives.

Blasting prill, considered a porous prill, better distributes the fuel oil (fuel oil distribution for fertilizer prill is on surface only and for blasting prill goes throughout prill) and results in much better performance on blasting job (velocity of detonation of fertilizer prill is 1829 m/s and of blasting prill is 3353 m/s) [6].

5. Field tests

The field tests were focused on the measurement of the overpressure differences in the homemade and industrially made ANFO explosives. The set of field tests took place at the development and testing set of the Ministry of Defence of the Slovak Republic called Military Technical and Testing Institute Zahorie. They took place in the period from 2011 to 2014. Methodology of the measurement is based on [8]. Maximum overpressure was measured using the blast pressure sensors type 137A23 and 137A24 PCB Piezotroics. The explosive charge was positioned at a wooden base at the height of 1.6 m over the ground, i.e. in the height of human chest. Sensors were placed at the distances of 2, 5, 10 and 20 meters from the source (see Figure 5). Besides the maximum overpressure, the velocity of blast wave and the noise level were also measured.

The GPN HD Ammonitrate 33.5 (composed of 33.5 % of ammonium nitrate - 16.7 % of nitric nitrogen and 16.8 % of ammoniacal nitrogen) and fuel oil Extra M2T (5 % of charge weight) (see Figure 3) were used for the preparation of ANFO explosives for the blast tests. The shape of explosives was cylindrical and the explosive material was wrapped in a cardboard cover not to influence the resultant value of overpressure.

The two types of homemade ANFO explosives and three types of industrially made ANFO explosives were used in the field tests. One was Ammonium nitrate with the fuel oil and the second type was a pure Ammonium nitrate. The explosives were used together with 20 g of ignition explosive PLNp10 and the weight

Figure 4 *Explosive DAP - E weight 1000 g for field test*

Figure 5 *Preparation of measuring sensors for field tests*

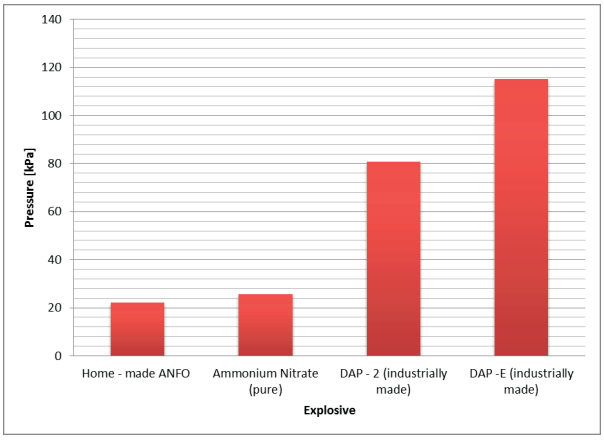


Figure 6 *Maximum pressure of homemade and industrially made ANFO explosives*

Table 2 *Comparison of industrially made and homemade ANFO explosives*

Explosive	Type of represented ANFO explosive	Pressure [kPa]	Difference [kPa]	Difference [%]
Industrially made ANFO	AN + oil	80.9	60.7	75.03
Homemade ANFO	AN + oil	20.2		

of charges was 1000 g (see Figure 4). From industrially made ANFO explosives the products DAP - 2, DAP - E (see Figure 2) and POLONIT were chosen. In the case of pure ammonium nitrate there was an uncompleted detonation of the explosive and the portion of ammonium nitrate prills was spread into the environment in the radius of 3.5 m from the explosive source.

The measured data of the ANFO explosives were chosen for the comparison at the distance of 2 m from the explosive source. The maximum over pressure of the homemade and industrially made ANFO explosives, used in the field tests, are shown in Figure 6. From the comparison it is obvious that the homemade ANFO explosives feature the lower efficacy than the industrially made ones. There is a big difference between the different types of industrially made ANFO explosives, which presents three different types of possible ANFO explosives.

Table 2 shows the comparison of average overpressure of industrially and homemade explosives of the same explosives type from the field tests.

6. Conclusion

The results of the presented field tests as from the field tests conducted by J. Stoller [9], [10] demonstrated the difference between the homemade and industrially made ANFO explosives. The homemade explosives have by 75 % lower efficacy than the industrially made ones. It was confirmed that the differences of preparation between explosives (homemade explosives are not mixed well, made from the low quality raw material (nitrogen content), they contain chemical impurities and water, and blasting

prills are porous prills, which better distribute the fuel oil) influences the efficacy of the explosive.

When the safety of persons and property is being considered, safety treatment measures are based on the values of industrially made explosives. More than 95 % of all the terrorist attacks are carried out using the homemade ANFO explosives and therefore the treatment measures employed for the protection are sufficient and even overcharged.

References

[1] KAVICKY, V., FIGULI, L., JANGL, S., LIGASOVA, Z.: Analysis of the Field Test Results of Ammonium Nitrate Fuel Oil Explosives as Improvised Device Charges. WIT Transactions on the Building Environment, 141, 297-309, 2014.
[2] VANDLICKOVA, M.: Terrorism and the Possibility of CBRN Agents Misuse: Security Management and Society, electronic source (in Slovak). Proceedings of International Conference on University of Defence in Brno, Czech Republic, CD-ROM, 537-541, 2013.
[3] ORINCAK, M.: Hazardous Industrial Accidents of LPG Gasses. Proceedings of 11th International Scientific Conference Science 2003, Education and Society, Slovakia, section No. 6, 97-100, 2003.
[4] MANAS, P., KROUPA, L., URBAN, R., COUFAL, D.: Blast Threat to Critical and Military Infrastructure. Security and Defence Quarterly, 1, 32-53, 2013.
[5] COOK, M. A.: The Science of Industrial Explosives. IRECO Chemicals, 1974.
[6] SHARMA, P. D.: Presentation [online]. Available: http://www.slideshare.net/ sharmapd1/an-anfo-hanfo [accessed 2014-09-19].
[7] ZEMAN, S.: Technology of Basic Explosives - Lectures (in Czech). Fakulta Chemicko technologicka, Univerzita Pardubice, 2004.
[8] ITOP 4-2-822: Electronic Measurement of Airblast Overpressure and Impulse Noise, 2000.
[9] STOLLER, J., MANAS, P., ZEZULOVA, E.: Blast Testing and Simulation Methods. CVUT, Praha, p. 35-100, 2015.
[10] STOLLER, J., DVORAK, P.: Field Tests of Cementitious Composites Suitable for Protective Structures and Critical Infrastructure. Key Engineering Materials 722 KEM, 3-11, 2017.

kaMUNikácie
COMMUNICATIONS

Jiri Pokorny - Vladimir Mozer - Lenka Malerova - Dagmar Dlouha - Peter Wilkinson*

A SIMPLIFIED METHOD FOR ESTABLISHING SAFE AVAILABLE EVACUATION TIME BASED ON A DESCENDING SMOKE LAYER

Keeping the smoke layer at a safe height is one of the most important tenability criteria in assessment of evacuation from buildings. The basis of this approach is an accurate approximation of the fire and smoke plume, which is formed above the fire source. The major variables affecting smoke filling are the fire growth rate and enclosure geometry, i.e. the floor area and height. This paper deals with the implementation of a new method for establishing safe available evacuation time based on the fundamental principles of smoke generation and flow into the national fire safety design standards in the Czech and Slovak Republic. Some of these calculation methods have also been included in fire safety engineering ISO standards. The devised method is based on the t-squared fire growth model and correlations for smoke production and air entrainment into the rising plume of smoke. Subsequently, the proposed method is validated against a wide range of benchmark scenarios in the two-zone fire model CFAST. The paper compares the differences, comments on their causes and evaluates the applicability of the new method in both countries. The proposed method is not only compatible with the national fire safety design standards, but also allows for a more precise assessment of life safety without the need for overly complicated calculations.

Keywords: *available safe evacuation time (ASET), t^2-fire, CFAST, smoke layer*

1. Introduction

One of the most important requirements of buildings, from a fire safety point of view, is to ensure safe evacuation of occupants. Safe evacuation is usually established by the comparison of the required safe evacuation time (RSET) and the available safe evacuation time (ASET) [1], [2], [3], [4], [5]. Safe evacuation conditions and sufficient evacuation time are particularly important in cases with challenging conditions such as high-rise buildings, assembly spaces, occupants with impairments, etc. [6].

The primary factor affecting the ASET is the threat resulting from the descending layer of smoke in an enclosure or the availability of a smoke-free clear layer at low level. The clear layer in an enclosure is considered safe until the smoke layer descends to 2.5 m above the floor, i.e. the smoke-free layer is 2.5 m high and smoke is above the heads of the occupants. The clear layer height criterion depends on the type of occupancy within the building; for example, in public buildings it is 3 m above the floor and in car parks 80 % of their total clear height. Given the average construction and clear height of a storey, 2.5 m may be considered as a representative value for typical situations [7].

A number of methods have been derived for the determination of smoke filling and layer descent in an enclosure (e.g. [7], [8], [9]). The methods derived by foreign authors employ variables, which the standardised design calculation in the Czech Republic and Slovak Republic usually do not utilize (e.g. fire growth coefficient). This limits the applicability of the smoke calculation methods in the national fire safety design frameworks.

The aim of this paper is to present a set of modified equations from ISO 16735 [8] for the descending smoke layer, which have been derived so that they utilize the variables contained in the fire safety design standards in the Czech Republic and Slovak Republic. A comparison with the CFAST zone computer fire model was carried out to evaluate the validity and applicability of the derived equations.

2. Smoke spread in an enclosure

Fire growth is usually represented by a localised fire, which is a fire on a limited area, resulting in burning of a limited amount of fuel (fire load) [10]. One of the characteristic accompanying phenomenon is the formation of a vertical plume of combustion

* [1]Jiri Pokorny, [2]Vladimir Mozer, [1]Lenka Malerova, [3]Dagmar Dlouha, [4]Peter Wilkinson
[1]Department of Civil Protection, Faculty of Safety Engineeing, VSB – Technical University of Ostrava, Czech Republic
[2]Department of Fire Engineering, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Department of Mathematics and Descriptive Geometry, VSB – Technical University of Ostrava, Czech Republic
[4]Pyrology Limited, Harborough Innovation Centre, Market Harborough, Leicestershire, United Kingdom
Email: jiri.pokorny@vsb.cz

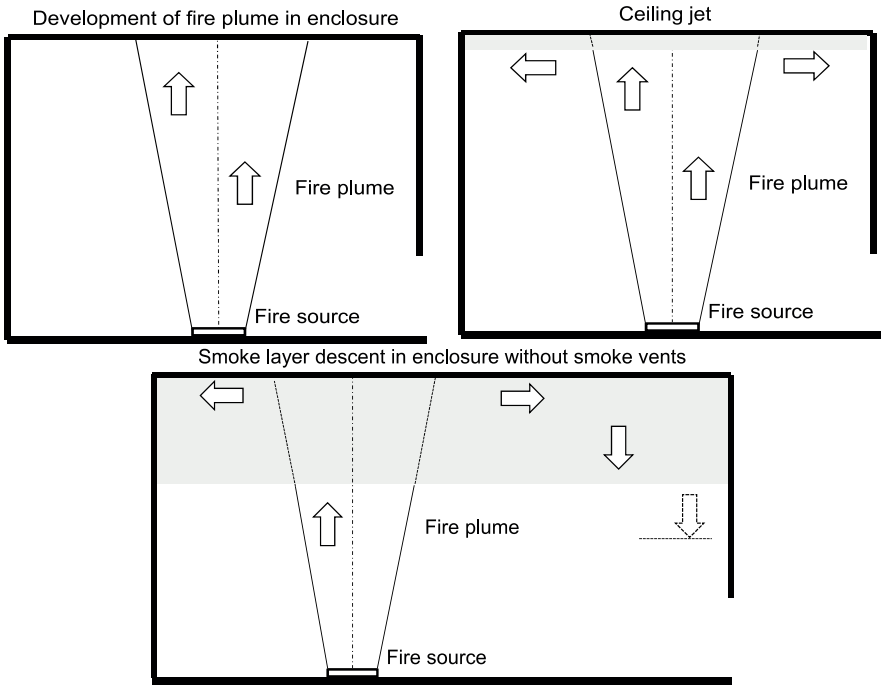


Figure 1 *Schematic depiction of enclosure smoke filling (adapted from [13])*

products (fire plume). The fire plume is a representation of mass and energy transport from the fire into the enclosure.

With the progressing fire growth, the temperature of smoky gases (combustion products) raises, resulting in increased buoyancy. When the temperature difference is sufficient the fire plume reaches the ceiling of the enclosure and a ceiling jet (radial smoke spread) is formed.

Smoky gases spread radially under the ceiling in a relatively thin layer from the plume centreline until they reach the enclosure bounding constructions. Once the radially spreading thin smoke layer reaches the enclosure boundaries the layer starts descending. This is known as smoke filling, when more hot smoky gases enter the layer through the plume, thereby increasing its volume and temperature. Due to the decrease of the smoke layer height, the distance between the fire source and the bottom of the layer is reduced, resulting in less ambient air entraining into the plume and a further increase in smoke layer temperature [1], [11], [12]. The layer descends until it fills the enclosure completely or reaches an opening with sufficient discharge capacity.

The process of smoke filling in an enclosure is shown in Figure 1.

3. Methodology

National and international technical standards play an important role in building quality and fire safety design [14]. One of the possibilities for the determination of smoke filling in enclosures without smoke management measures, is described in the fire safety engineering standards from International Organization for Standardization (ISO) [8]:

$$z = \left(\frac{0.076}{\rho_s} \frac{(1-\chi)^{1/3} \cdot \alpha^{1/3}}{A} \frac{2}{n+3} t^{\left(1+\frac{n}{3}\right)} + \frac{1}{H^{2/3}} \right)^{-3/2} \qquad (1)$$

where

- z Interface height above the base of fire source (m)
- χ Fraction of heat released that is emitted as thermal radiation (-)
- α Fire growth rate (kW.s^{-2})
- ρ_s Smoke density (kg.m^{-3})
- A Floor area of enclosure (m^2)
- n *n-th* power (-)
- H Height of enclosure (m).

Equation (1) provides valid results only in case that the distance between the fire and the bottom of the smoke layer is greater than the average flame height [7].

Fire dynamics in Equation (1) is taken into account through the fire growth rate α, i.e. the equation describes a fire that grows with time. The fire growth rate α, however, does not have a direct connection to the national fire safety design standards in the Czech Republic and Slovak Republic.

Analytical work, analysing the localised fire was, undertaken during 2016 and 2017. Possible connections between the fire growth rate α and selected design values describing fire growth in national standards were analysed. As a result the following equation was derived to calculate the fire growth rate α, using the national design parameters [13]:

Table 1 *Input variables for model cases*

Type of use	CSN 730802 Annex A	Variable fire load p_n (kg.m^{-2})	Fixed fire load p_s (kg.m^{-2})	Coefficient a_n (-)	Coefficient a_s (-)
Sport hall	item 5.1	15	6.2	0.8	0.9
Shopping centre	item 6.2.5	90	6.2	1.1	0.9

$$\alpha = \frac{a^2 \cdot p}{2560} \tag{2}$$

where

a fire growth rate coefficient (-)

p fire load (kg.m^{-2}).

Equations for the determination of the time for smoke layer descent to 2.5 m above floor level in non-industrial and industrial occupancies were derived by substituting Equation (2) into Equation (1) and subsequent mathematical adjustments.

The time for smoke layer descent to 2.5 m above the floor level in non-industrial occupancies can be determined by the following equation:

$$t = \left(114 \cdot 10^6 \frac{A^3}{a^2 \cdot p} \cdot (0.543 - H^{-\frac{2}{3}})^3 \right)^{\frac{1}{5}} \tag{3}$$

where

t time for smoke layer descent to 2.5 m above floor level (s).

The time for smoke layer descent to 2.5 m above floor level in industrial occupancies can be determined by the following equation:

$$t = \left(114 \cdot 10^6 \frac{A^3}{\bar{p}} \cdot (0.543 - H^{-\frac{2}{3}})^3 \right)^{\frac{1}{5}} \tag{4}$$

where

$\bar{p}$ average fuel load (kg.m^{-2}).

Further details regarding the determination of fuel load p, fire growth rate coefficient a, and average fuel load $\bar{p}$ may be found in [15], [16].

4. Model description

A set of rectangular-geometry compartments of varying area and height was modelled in CFAST, a zone computer model.

4.1 Consolidated Model of Fire and Smoke Transport (CFAST)

CFAST is a two-zone fire model used to calculate the evolving distribution of smoke, fire gases and temperature throughout compartments of a building during a fire. These can range from very small containment vessels, of the order of 1 m^3 to large spaces of the order of 1000 m^3, [17], [18].

The modelling equations used in CFAST take the mathematical form of an initial value problem for a system of ordinary differential equations (ODEs). These equations are derived using the conservation of mass, the conservation of energy (equivalent to the first law of thermodynamics), the ideal gas law and relations for density and internal energy. These equations predict as functions of time quantities such as pressure, layer height and temperatures given the accumulation of mass and enthalpy in the two layers. The CFAST model then consists of a set of ODEs to compute the environment in each compartment and a collection of algorithms to compute the mass and enthalpy source terms required by the ODEs, [17], [18].

The zone fire model is considered as an adequate tool for the assessment of accuracy of the derived equations in relation to the spatial descent of smoke layer, since local deviations are not significant in general ASET determination. In addition, CFAST was used within the limits stated in the accompanying documentation [17], [18] and the cases modelled were simple smoke-filling scenarios without complex flows and geometry. It is therefore reasonable to accept the results as generally valid for the purposes of this research.

4.2 Compartment geometry and ventilation

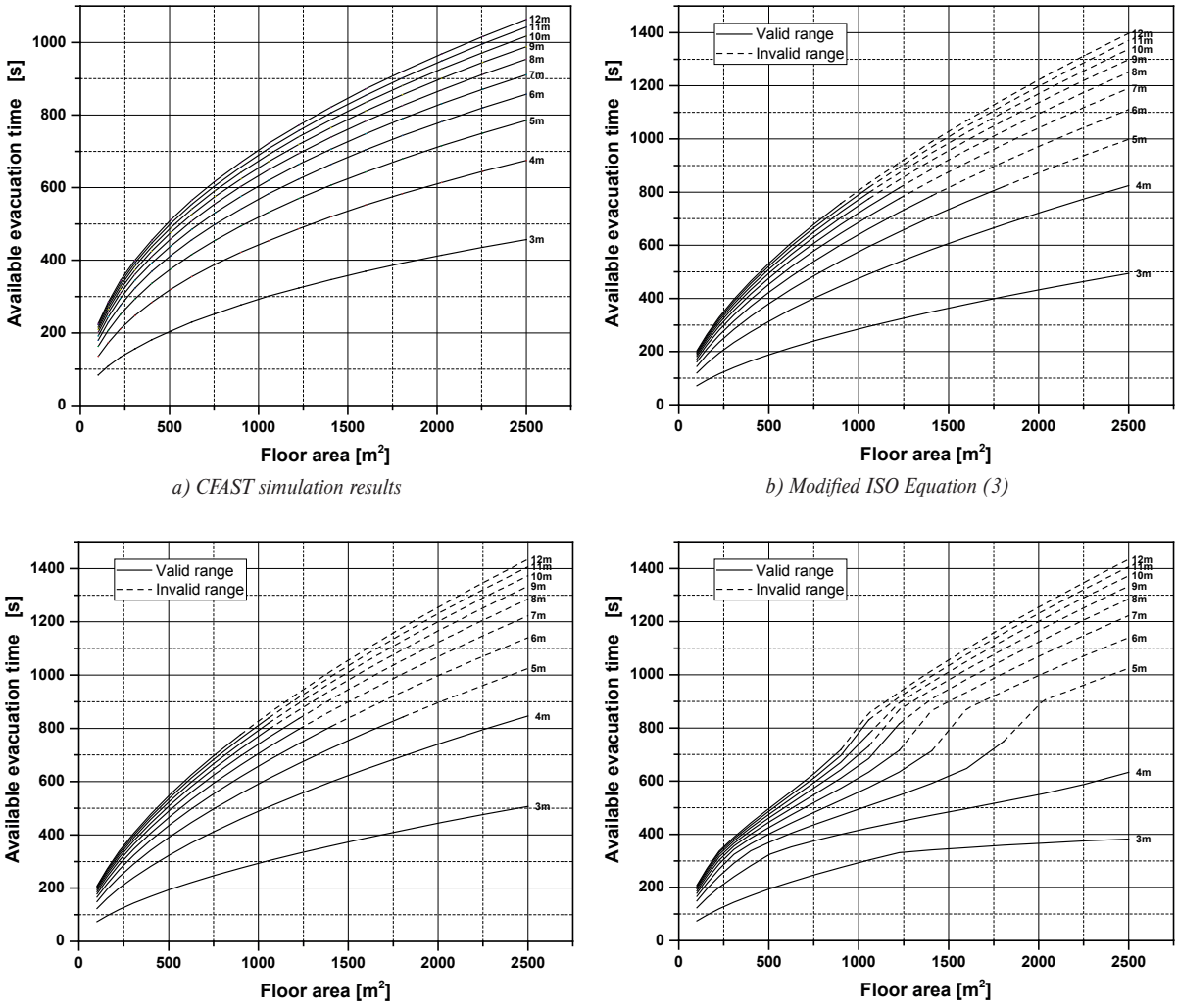
The derived equations were evaluated against the results from the CFAST zone computer fire model in two model cases. The first one was a sports hall with a low variable fire load and slow fire growth rate coefficient (lower a_n) and the second one was a shopping centre with a significantly greater variable fire load and fire growth rate coefficient (greater a_n). The base input parameters are listed in Table 1.

In both model cases the floor area was varied from 100 up to 2500 m^2 and the clear height from 3 up to 12 m.

There were no ventilation openings assumed in the enclosure apart from an opening (1 m wide and 2 m high) at the floor level to allow free air circulation and avoid pressure build-up in the enclosure. This opening had no effect on the smoke layer itself as its soffit was below the critical smoke layer height of 2.5 m.

4.3 Fire scenarios and fuel properties

Fires are usually described by a time-temperature relation or heat release rate. The basic assumption employed in this study



a) CFAST simulation results

b) Modified ISO Equation (3)

c) ISO Equation (1) - no flame height criterion

d) ISO Equation (1) - with flame height criterion

***Figure 2** Available safe evacuation time for the sports hall model (each curve represents a different enclosure height)*

is that only the growth phase of a fire is considered relevant to evacuation. The tenability limits are far exceeded by the time the fire reaches flashover, therefore, it is not necessary to consider the phase of fully developed fire when evaluating the safe available evacuation time in the room of fire origin.

During the growth phase, the fire is fuel-bed controlled (well ventilated) and its heat output grows with time. For this purpose the t^2 – fire model was used in this paper to prescribe the development of the heat release rate (HRR) with time. This model is well established widely used in the fire safety engineering field, see e.g. [19], [20]. Based on the previous work [13] and in relation to the standards [15], [16], a modified version of this equation was employed:

$$Q = \frac{p \cdot a^2 \cdot t^2}{2560} \qquad (5)$$

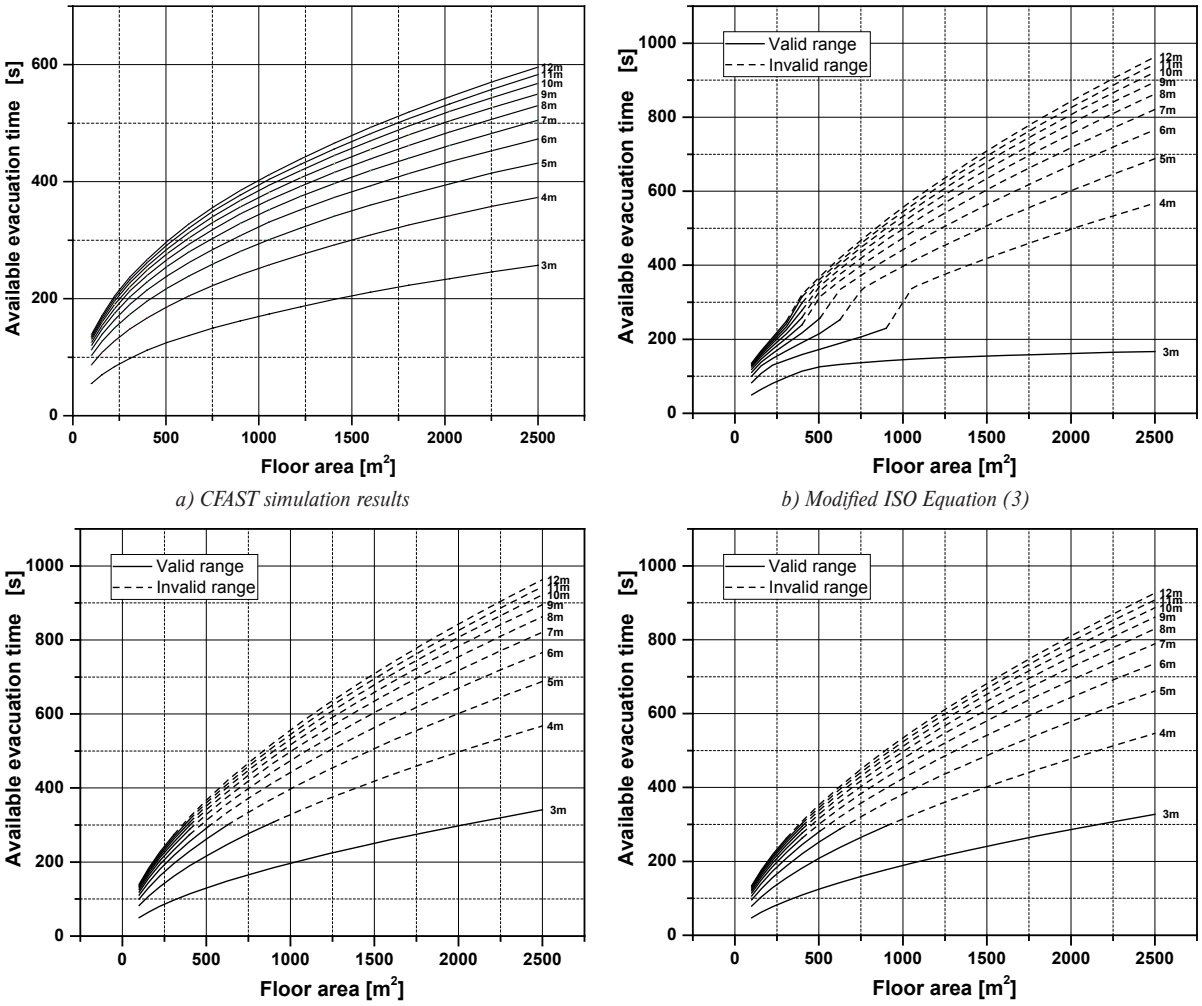
where

Q Heat release rate (kW).

Since the incubation time – the period from ignition to sustained growth – is rather variable, ranging from 0 to 100's of seconds, it was not included in the simulation. The HRR grows from t = 0 s without any delay. Once again, this errs on the side of safety and allows for a wide application of the obtained results.

It is not necessary to consider the detailed fuel composition and combustion chemistry, see for example [21], since the cut-off criterion (the smoke layer 2.5 m above floor level) is set such that no occupant exposure is expected. This allows for a more general application of results, which are primarily dependent on the geometry of the enclosure and the heat output of the fire.

The fire burning duration in all simulated cases was set to 600 s.



a) CFAST simulation results

b) Modified ISO Equation (3)

c) ISO Equation (1) - no flame height criterion

d) ISO Equation (1) - with flame height criterion

***Figure** 3 Available safe evacuation time for the shopping centre model (each curve represents a different enclosure height)*

4.4 Tenability criteria

The decrease of the smoke layer height to 2.5 m above the floor was considered as the tenability cut-off criterion. The time of smoke layer descent to this height was considered as the available safe evacuation time.

5. Results

For each of the evaluated building use types, i.e. a sports hall (Figure 2) and a shopping centre (Figure 3), a series of graphs were produced, showing the dependency of the ASET on the enclosure floor area and height, in relation to the calculation approach employed. The CFAST simulation results were considered as benchmark to which the other calculation approaches were compared.

The x-axes of the graphs represent the variable floor area and y-axes the available safe evacuation time, i.e. the time in which the smoke layer descended to 2.5 m above the floor level and each curve in the series represents a different clear height of the enclosure.

The curves resulting from the application of Equation (1) and Equation (3) are shown partially in solid and partially in dashed line. The continuous line indicates the range in which the average flame height is lower than the smoke layer height, i.e. the range in which the equations are valid. The dashed line indicates the range in which the average flame height exceeds the smoke layer height, i.e. the range in which the equations are invalid.

The differences between the results from equations described above and the benchmark CFAST simulations were summarised in Table 2. The differences within the valid and invalid ranges are indicated for comparison.

Table 2 *Differences between simulation and calculation results*

Type of use	Average difference from simulation results (%)			
	Equation (1)		Equation (3)	
	Valid range	Invalid range	Valid range	Invalid range
Sports hall	9	22.6	8.1	19.9
Shopping centre	11.6	38.7	8.7	33.8

It is expected that similar differences in results would be obtained when using Equation (4) for industrial buildings due to the significance of the flame height.

6. Discussion

The developed method (derived Equation (3) and Equation (4)) for determination of the available safe evacuation time (ASET) was based on the descending smoke layer in an enclosure without smoke ventilation openings. It was validated against two model cases: a sports hall and a shopping centre. These building use types represent two ends of the spectrum from the variable fire load (p) and the burning rate coefficient (a) points of view (high and low values characterising the fire dynamics). These variables also represent important input for the application of the devised method.

The selected geometry parameters of the model cases, the floor areas 100 – 2500 m^2 and heights 3 – 12 m, cover a significant range of the enclosures in real buildings of these types. The maximal floor area of the evaluated enclosures also corresponds with the standard spatial limits of smoke sections used in smoke management system design [7].

Equation (5) was used to establish the heat output of the design fires, which creates a connection to the input values used in building fire safety design in the Czech Republic and Slovak Republic.

The results of the modelled cases are shown in Figure 2 and Figure 3 and the average differences (in %), resulting from the comparison of the application of Equation (1) and Equation (3) and the zone fire model CFAST, are listed in Table 2. The differences were established for the range in which the average flame height is lower than the smoke layer height, i.e. the range in which the equations are valid, as well as the range in which the average flame height exceeds the smoke layer height, i.e. the range in which the equations are invalid.

As expected there is a strong dependence of the equation validity range on the fire growth rate expressed through Equation (2). Since the height of the flame is proportional to the heat output of the fire, the slower the fire growth is the greater the range in which Equations (3) and (4) remain valid. Overall, for the valid range for Equation (3) are as follows:

- sports hall (lower fire growth rate) – equation is valid for ASET values below 800 seconds;
- shopping centre (greater fire growth rate) – equation is valid for ASET values below 300 seconds.

The above validity limits are relevant for the entire range of enclosure floor areas and heights evaluated. This may appear contradictory with regard to the enclosure height. However, a greater height results in a greater air entrainment, resulting in a greater volume of smoky gases filling the smoke reservoir.

The above is also confirmed by the results from Table 2, which states differences for the modified ISO Equation (3) of 8.1 % and 8.7 %, for the sports hall and shopping centre respectively. Based on these values, the application of the modified ISO Equation (3) yields relevant results within the stated validity limits and is acceptable.

However, outside the valid range the difference of the modified ISO equation results and simulation results increase significantly, to almost 40 % for the shopping centre, and its use is not recommended. Above the validity limits, it is necessary to employ a more detailed evaluation method which takes into account the effect of flames projecting into the smoke layer.

Figure 2 and Figure 3 also confirm that the differences between results from Equation (1) and Equation (3) (subfigures b) and c) are negligible, less than 3 %, which confirms that Equation (3) was derived correctly.

Due to the to the fact that Equation (3) and Equation (4) are practically identical, it is expected that the above results and limitations established for the application of Equation (3) would be the same for Equation (4), as well.

7. Conclusions

The paper describes a newly developed method for determining the available safe evacuation time (ASET). The calculation method was derived by modifying the ISO 16735 calculation procedure for enclosure smoke filling and implementation of the latest research results. To assess the validity of the proposed calculation method, a comparison was made with the CFAST zone model for a wide range of enclosure geometries and two types of building occupancy – sports hall (low fire load and fire growth) and shopping centre (high fire load and fire growth).

The proposed calculation method has been shown to produce results correlating well with the zone fire model simulation results. Within the identified ranges of validity, the results are of a comparable accuracy when compared to simulation results,

meaning that the proposed simple calculation method may be used when establishing ASET from the national fire safety design parameters for the given occupancy types.

It may be concluded that this initial investigation into the utility of the proposed calculation methods yielded positive results, established the range of their validity, and identified areas for their further refinement.

Acknowledgements

This work was supported by the Ministry of the Interior of the Czech Republic, project no VI20162019034 "Research and development of established models of fire and evacuation of persons and their practical application to assessment of fire safety of buildings".

References

[1] HOSSER, D.: Manual of Fire Protection Engineering Methods [online]. Braunschweig: Technisch-Wissenschaftlicher Beirat (TWB) der Vereinigung zur Forderung des Deutschen Brandschutzes e.V. (vfdb), Technical Report TB 04/01., 3. revised and completed edition, p. 419, 2013. Available: http://www.kd-brandschutz.de/files/downloads/Leitfaden2013.pdf.

[2] TOMASKOVA, M.: Evacuation of Persons Using Fire Lifts in the Case of Fire. Svetrada, 13(6), 550-558, 2016.

[3] MRACKOVA, E.: Complex Services in the Area of Safety Systems for Persons and Property Protection. Delta, 5, p. 32, 2009.

[4] MOZER, V., POKORNY, J., KUCERA, P., VRABLOVA, L., WILKINSON, P.: Evacuation of Persons from Selected Departments in High-Rise Buildings of Healthcare Facilities. Communications - Scientific Letters of the University of Zilina, 17(4), 67-72, 2015.

[5] BS 7974:2001 Application of Fire Safety Engineering Principles to the Design of Buildings. Code of Practice. British Standards Institution, London, 2001.

[6] BENESOVA, S., BRADACOVA, I., JAGER, T.: Utility of Computer Modelling in Determination of Safe Available Evacuation Time. Communications - Scientific Letters of the University of Zilina, 18(1), 117-122, 2016.

[7] CSN P CEN/TR 12101-5 Smoke and Heat Control Systems - Part 5: Guidelines on Functional Recommendations and Calculation Methods for Smoke and Heat Exhaust Ventilation Systems. Office for Technical Standardisation, Metrology and State Testing, Prague, 2008.

[8] ISO16735 Fire safety engineering - Requirements Governing Algebraic Equations - Smoke Layers. International Organization for Standardization, Geneva, p. 55, 2006.

[9] NFPA 92 B Standard for Smoke Management Systems in Malls, Atria and Large Spaces. National Fire Protection Association, Maryland, p. 57, 2009.

[10] CSN EN 1991-1-2 Eurocode. Czech standardisation institute, Prague, p. 56, 2004.

[11] HESKESTAD, G.: Fire Plumes, Flame Height, and Air Entrainment. SFPE handbook of fire protection engineering, 4th ed., Section two, Fire Dynamic, Chapter 2-1. Society of Fire Protection Engineers, Bethesda, Md., 2008.

[12] KARLSSON, B., QUINTIERE, G. J.: Enclosure Fire Dynamics. CRC Press, Boca Raton, FL, p. 315, 2000.

[13] POKORNY, J.: Fire Plume Characteristics in the Context of Czech National Standards for Building Fire Safety Assessment. Habilitation thesis, Faculty of Safety Engineering, VSB - Technical University of Ostrava, Ostrava, p. 170, 2017.

[14] BLECHARZ, P., STVERKOVA, H.: Assessing the Service Quality in Small and Medium-Sized Companies. Actual Problems of Economics, 154(4), 206-217, 2014.

[15] CSN 73 0802 Fire Protection of Buildings - Non-Industrial Buildings. Office for Technical Standardisation, Metrology and State Testing, Prague, p. 122, 2009.

[16] CSN 73 0804 Fire Protection of Buildings – Industrial Buildings. Office for Technical Standardisation, Metrology and State Testing, Prague, p. 155, 2010.

[17] PEACOCK, R. D., RENEKE, P. A., FORNEY, G. P.: CFAST – Consolidated Model of Fire Growth and Smoke Transport (Version 7) Volume 1: Technical Reference Guide [online]. National Institute of Standards and Technology, Gaithersburg, 2017. Available: http://dx.doi.org/10.6028/NIST.TN.1889v1 [accessed 2017-02-25].

[18] PEACOCK, R. D., RENEKE, P. A., FORNEY, G. P.: CFAST, Fire Growth and Smoke Transport Modelling [online]. Available: https://www.nist.gov/el/fire-research-division-73300/product-services/consolidated-fire-and-smoke-transport-model-cfast [accessed 2017-08-18].

[19] MAYFIELD, C., HOPKIN, D.: Design Fires for Use in Fire Safety Engineering. IHS BRE Press, BRE Trust, Bracknell, 2011.

[20] SFPE Handbook of Fire Protection Engineering. 4th ed., DINENNO, P. J. (Ed.). Society of Fire Protection Engineers, National Fire Protection Association, Bethesda, Md, Mass., 2008.

[21] MARTINKA, J., HRONCOVA, E., CHREBET, T., BALOG, K.: The Influence of Spruce Wood Heat Treatment on Its Thermal Stability and Burning Process. European Journal of Wood and Wood Products, 72(4), 477-486, 2014.

Stanislav Lichorobiec - Lucia Figuli*

DEVELOPMENT AND TESTING OF RESCUE DESTRUCTION CHARGES FOR THE DEMOLITION OF STATICALLY UNSTABLE BUILDINGS

Due to the industrial accidents (the effects of explosion of improvised explosive devices or gas) or other unexpected events, heavily damaged buildings represent threat to environment. Generally, their damage is so serious that their reconstruction is not considered and the only solution is a demolition. Advantageously emergency shaped explosive charges can be used in these risk situations of buildings that are beyond repair. With such shaped charges is possible to execute a fast and effective implosion of an unstable building without the posing any threathening effects on surrounding, mainly in urban areas. This papers is focused on the design and development of mentioned shaped explosive charges, their testing in the field test and practical applications.

Keywords: *rescue destruction charge, statically unstable building, shock wave, Semtex*

1. Introduction

One of the possible approaches for the demolition of the building without threat to persons is using the cumulative shaped charges. Strength of used construction materials and elements can be decreased for about 30-60 % due to the buildings disruption. Such values can be obtained only by professional estimation and practical skills of structural engineers. Using of explosives charges in the weakened part of building is related to the knowledge of explosion effects, structural system of a building and the resistance of used materials. The development of shaped charges is an aim of the project "Development of rescue destructive charges for liquidation of static disrupted buildings". During the realisation of the mentioned project specialised departments of Fire Rescue Service of the Czech Republic will have a possibility to demonstrate a demolition of dangerous buildings using direct, effective and quick method of rescue destructive charge (RDC).

2. Shaped charges

The medium, using the explosive cumulated into the high pressure flow, is in the front part of the straight section. In the back part of a charge e is placed an imitated volume of water in the so-called "plug area", enabling the higher effect of the working beam and creating the water fog in the back space of the charge. Such a fog eliminates inflammation of easily flammable objects and dampens the blast wave in the zone. With such an approach, damage to surrounding objects and buildings is eliminated [1], [2], [3].

2.1 Mass accelerating with explosion

When a brisant explosive explodes, created gases would propagate in all the directions, specifically influenced by the shape of the charge. The higher detonation velocity is, the directional effects are more prominent. The created gases have a tendency to propagate more quickly from the places with the higher concentration of explosives. By creating the adequate cavity in a brisant explosive charge, the flows of gases can be directed in such a way that they are unified in a compact flow and so it would be possible to obtain flow with high speed response to immense accumulation of energy (see Figure 1) [4], [5], [6].

2.2 System of sequentially time shaped charges

System of sequentially time shaped charges is an alternative method developed for ice breaking in the rivers and which could

* [1]Stanislav Lichorobiec, [2]Lucia Figuli
[1]Department of Security Services, Faculty of Safety Engineering, VSB -Technical University of Ostrava, Czech Republic
[2]Department of Technical Sciences and Informatics, Faculty of Security Engineering, University of Zilina, Slovakia
E-mail: lucia.figuli@fbi.uniza.sk

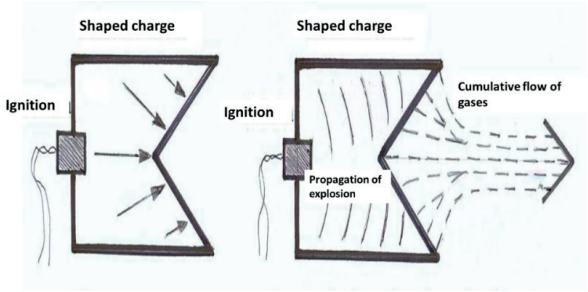


Figure 1 *Creating of cumulating flow of gases generated by explosion [5]*

Figure 2 *Detasheet explosive Semtex Pl SE*

Figure 3 *Industrial Perunit E - Ø28 mm*

be even optimally used for demolition of damaged buildings. Design of technical solution arises from the use of exactly timed charges placed on the ice surface. For the arising of explosive effect of ice surface, the charges are plugged in the upper part by textile water bags. Such a method is not as effective as using of explosive under the ice, but the effect of such modified charges is remarkably higher than that of the freely placed explosive charges. The main advantage of the proposed procedure is that the water bag absorbs the explosive energy from the back part, under the charge and minimise the fragmentation of ice. With the exact timing and optimal placing of such determined charges, it is possible to obtain effect of ice layers breaking and to regulate the weight of the freed ice. The system was developed in the security research N°VG20132015117. Described system is composed from three components:

Explosive - for the ice barriers replacement, various industrial or special explosives can be used. The higher brisance helps to smaller fragmentation of ice, the higher work capacity increases

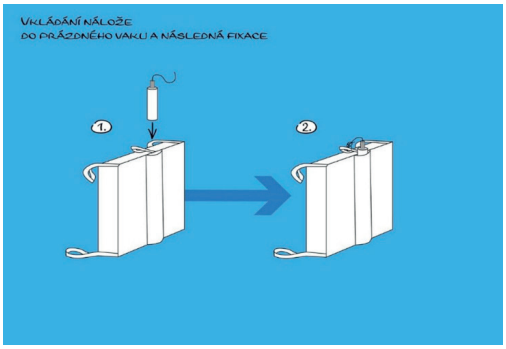


Figure 4 *Bag placement and fixing of explosive*

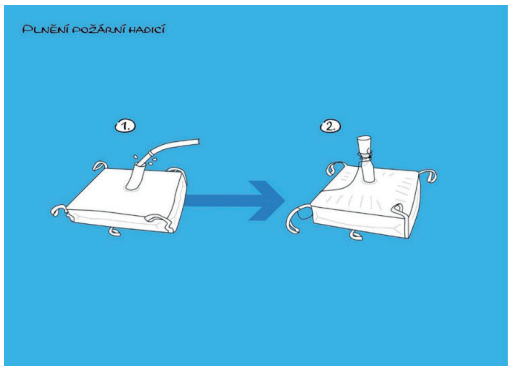


Figure *5 Bag filling with water*

the total volume of freed ice mass. The explosive has to be impermeable, capable of initiation and detonation in the diameters to 30-35 mm. From generally used explosives, such conditions fulfil dynamites of small diameter. Another alternative is a special detasheet explosive as Semtex 10-SE, prepared in the form of thin slices.

Two types of explosives (produced by company Explosia Pardubice a.s.) were selected: detasheet explosive Semtex 10-SE with detonation velocity of 7000 m/s and industrial explosive Perunit E with detonation velocity of 5500 m/s, see Figure 2 and Figure 3.

Textile plug bags - construction of textile plug bags was designed with regard to the sufficient resistance for manipulation, filling with water and blast resistance. Their construction allowed: to insert adjusted charge with the ignition into the pocket on the external part of bag, to fixate the ignition system using loop against it losing from the explosive charge when bags are placed or filled with water, Figure 4 and Figure 5.

All parts of bags are made from the soft textile. So, no rigid and sharp debris from bags are present after the explosions. Thanks to the loops at the bag corners, bags can be joined. Such loops are even used for their fixations on the flexible ropes for removing from freed ice mass. The filling sleeve, placed in the centre of the upper side of a bag, can be tied after filling. Bags are produced with the standard volume of 250 litres (Figure 6), square base with the area of 1 m^2.

Figure 6 *Photo of textile bags with the volume of 250 litres of water*

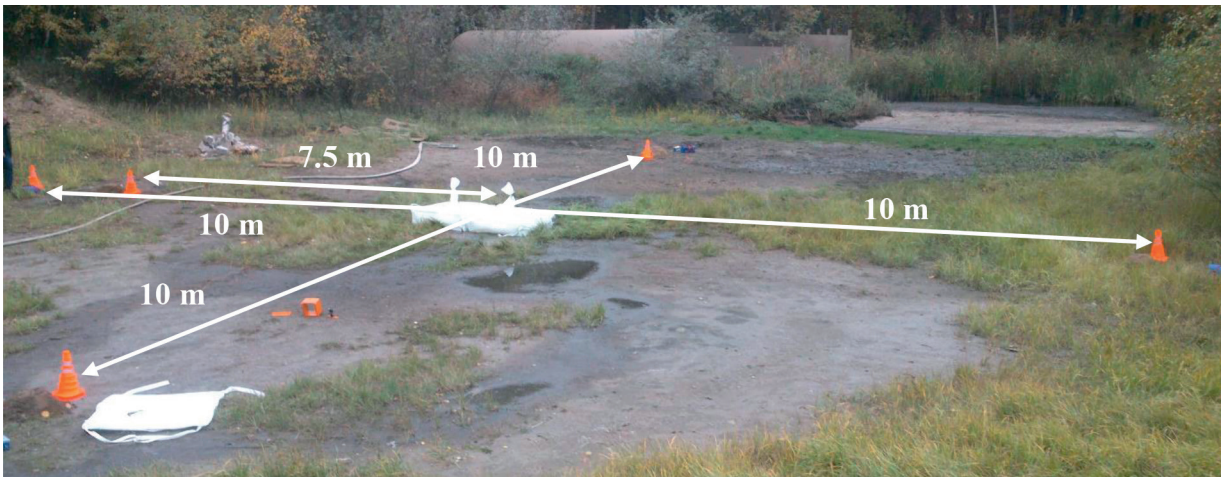


Figure 7 *Disposition of sensors in seismic tests*

Initiation system - as an initiation system, an electrical or nonelectrical ignition can be used or even a timed electronical initiation system. From the point of view of the possibility to programme any initial time sequence, in practical cases is advantageous to use system of variable electronic timing. For longer times, with the smaller precisions of timing in the interval from 25 ms to 75 ms, electronical ignition was used. Initial times were chosen with regard to the maximal seismic effect by using of charges at determined distances.

3. Seismic measurements of the system effectiveness

Seismic measurements of the system effectiveness were conducted by companies_Austin Detonator s.r.o. and Geodyn, spol. s.r.o., with the system of seismographs type Instantel MiniMate plus, BE 7901, 9146 and 13846. Four perpendicular directions were measured with first charge in the centre (see Figure 7). Acoustic pressure was measured by a linear microphone with weighting filter. Sensors were placed at a distance of 10 m from the first charge and in the direction of timing sequence a complementary sensor at a distance of 7.5 m was placed. Two shaped charges were always set off with the determined timing sequence.

Total energetic effectiveness is displayed in Figure 8.

The total effective energy of explosion was obtained with the value of 19.17 $(mm/s)^2$ and in the second case of 8.38 $(mm/s)^2$. With the increase in the distances from charges and with the higher timing, resulting value of energy is more shattering than summing (see Figure 8).

4. Practical use of developed system

Use of the presented system of sequential charges is variable in practice. The fundamental advantage is that it can be prepared on the river bank, transferred to the ice surface and filled with water. Possible placement and timing sequence of initial system is shown in Figure 9, where*, czech word "*řada*" means row, positions of bags*.

Time sequence of charge explosion (Figure 10) shows a minimal secure space for practical use.

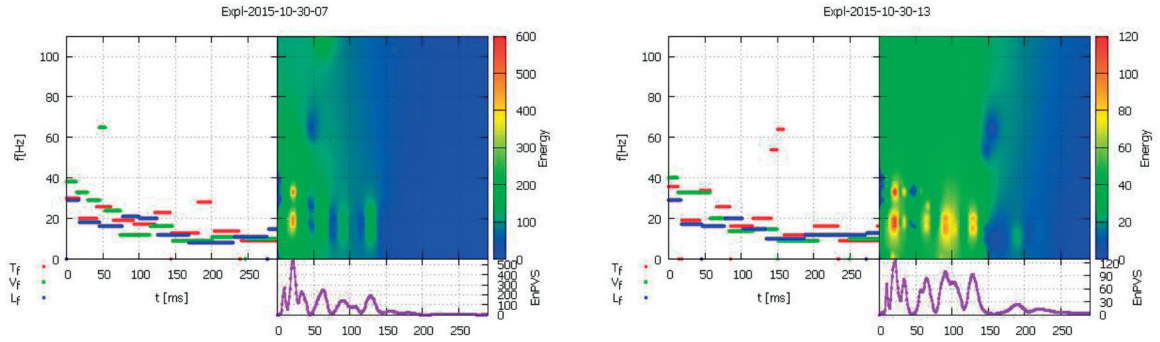


Figure 8 *Energetic effectiveness of measurements dependent on the time and frequency of seismic waves vibration*

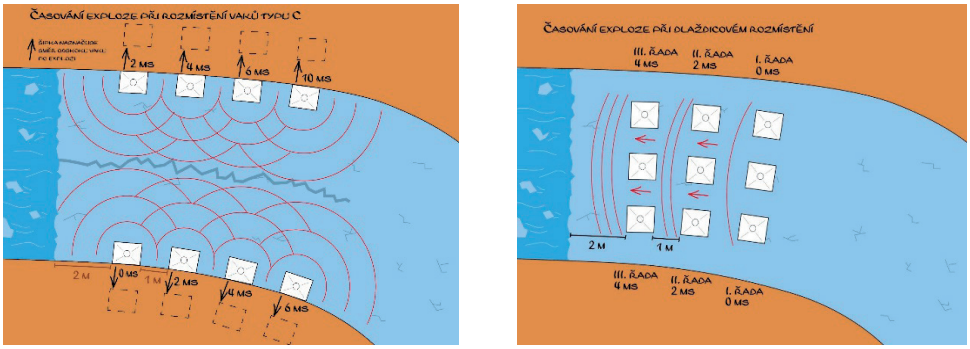


Figure 9 *Placement of charges for freeing of ice mass - along the river bank (left) and in the river bed (right)*

Figure 10 *Time sequence of charge explosion - 3 water bag placed*

a) *b)* *c)*

Figure 11 *Field tests a) position of charges b) cracks on concrete slabs c) destruction of samples*

Other practical test realisation was made in simulated conditions in the block of flats. Charges where placed at the concrete floors (see Figure 11). Similar test were conducted by Stoller [7], [8].

The force of accumulated energy is demonstrated in the Figure 12, where a cut of steel floor bars is registered.

Figure 12 *Detail of cut steel bars in the floor slab*

Figure 13 *Test of the explosion regularity of Semtex 10-SE, t = 5.236 ms*

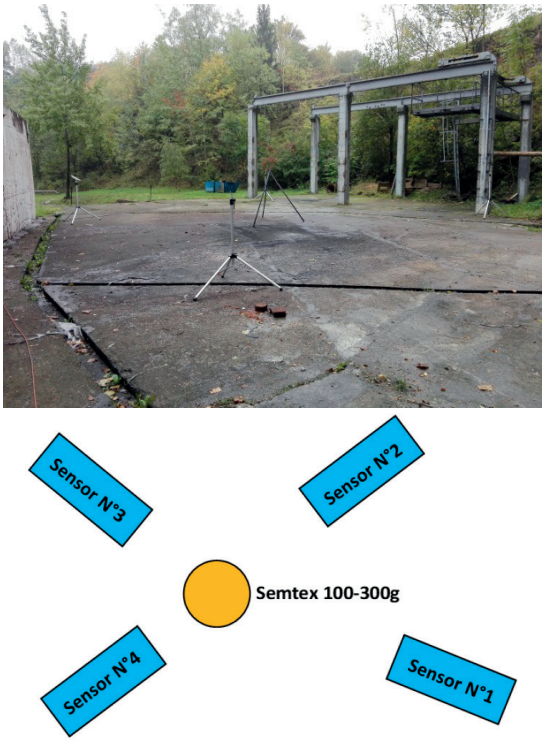


Figure 14 *Disposition of blast sensors used in field test*

Table 1 *Stand-off distances (from the source to blast sensors)*

Sensor N°	1	2	3	4
Distance (m)	5	4	3	2

Described method of shaped charges is possible to use for demolition of buildings. Problem of the fixation of huge water bags in perpendicular direction has arisen. Due to this difficulty, security research project was initiated, where charges with smaller dimensions were taken into account.

5. Development of rescue destructive charges

The rescue destructive charge (RDC) are based on the method described above. The plastic explosive Semtex 10-SE is convenient to use it for experiments, since it is easy to work with. It is produced as detasheet explosive with the thickness of 2 mm, width of 300 mm and length of 10 metres. It is in a sticky form and can be easily placed on any shaped cavity. Its detonation capacity is stable and regular in all directions (see photo in Figure 13).

6. Experimental test results

The propagation of blast wave was measured in the preliminary tests. Maximal pressures, created by plastic explosive Semtex 10-SE in the form of a sphere, with the weight of 100, 200 and 300, were measured. Disposition of blast sensors are shown in Figure 14; dimensions are listed in Table 1.

For practical realisation of the field test a prototype of cumulative shaped charge was realised. The test had to confirm if the water beam was adequate for demolition of selected building elements. Test had to confirm the effectiveness of water mass for elimination of blast wave in the back area of the charge. As a charge, the following wrapping was used (see Figure 15):1 is an area for cumulative cavity for water mass, 2 an explosive Semtex fixed on cumulative cavity and 3 the back area of the charge with the plug function.

Two different sizes of cumulative shaped charge were constructed - with the volume of 5 and 10 litres of water. Figure 16 is documenting the creation of pressure water beam in the front part of the charge with the velocity of 620 m/s.

7. Conclusions

Based on the above facts, one can conclude that the development of special rescue destruction charges and their

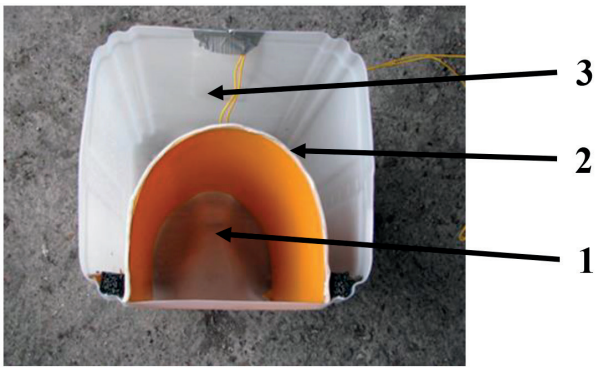


Figure 15 *Body of cumulative shaped explosive*

practical implementation are substantially complemented by a range of means for the safe disposal of statically degraded buildings. The benefits are:

- Simple construction - one solid element, consisting of two separate parts, is equipped with an initiator explosive and is filled with water,
- The charge is placed on walls of the building very quickly as a load, without drilling holes in its skeleton,
- The transport time, composition and activation on site are very short,
- The production of segmented canisters is not complicated,
- It does not contain metallic elements and therefore there is no risk of fragmentation with metal fragments,
- Fragmentation of plastic debris using improvised IEDs occurs within a maximum of 5-8 meters,
- The back plug canister has adequate volume of water to create sufficient water mist to suppress the fire and heat effects of an explosion, thereby avoiding secondary fires and at the same time suppressing the impact of the blast wave spreading to the back part of IEDs, which would not endanger the surrounding objects.

a)

b)

Figure 16 *Test of improvised water charge: a) volume of 5l in t = 0.6 ms b) volume of 10l in t = 1.5 ms*

Acknowledgement

This research was supported by the project "Programme of Security research MVCR - BV III/1-VS, with the title „Development of rescue destructive charges for liquidation of static disrupted buildings" with the number VI 20152019047.

References

[1] VAVRA, P., VAGENKNECHT, J.: Explosion Theory (in Czech). Univerzita Pardubice, Pardubice, 2002.
[2] DOJCAR, O., HORKY, J., KORINEK, R.: Explosive Techniques (in Slovak). Montanex, a. s., Ostrava, 1996.
[3] ZUKAS, A. J., WALTERS, W. P.: Explosive Effects and Applications. Springer-Verlag, New York, 1998.
[4] COOPER, P. W., KUROVSKI, S. R.: Introduction to the Technology of Explosives. VCHPubl., USA, 1996.
[5] LICHOROBIEC, S., BARCOVA, K.: Verification of the Efficacy of the Special Water Shaped Charge Prototype. Defence Science Journal, 65(5), 363-366, 2015. DOI: 10.14429/dsj.65.8850
[6] LICHOROBIEC, S.: Alternative Development of Projectiles to Deactivate the Explosive Means Explosive Systems - Pipe Bombs. Communications – Scientific Letters of the University of Zilina, 13(2), 20-25, 2011.
[7] STOLLER, J., ZEZULOVA, E.: Use of Ultrasound - The Ultrasonic Pulse Velocity Method for the Diagnosis of Protective Structures after the Load of TNT Explosion. 6th International Conference on Military Technologies (ICMT 2017), Czech Republic, 230-235, 2017
[8] STOLLER, J., DVORAK, P.: Experimental Ballistic Loading of Steel Fiber Reinforced Concrete Slabs and Unreinforced Concrete Slabs by Plastic Explosives. Lecture Notes in Mechanical Engineering, 110-119, 2017.

Bohus Leitner - David Rehak - Robertas Kersys*

THE NEW PROCEDURE FOR IDENTIFICATION OF INFRASTRUCTURE ELEMENTS SIGNIFICANCE IN SUB-SECTOR RAILWAY TRANSPORT

The paper focuses on the problem of importance/significance elements evaluation in the railway transport infrastructure sub-systems. It contains main features of the proposed theoretical approach to the significance assessment of the key typological elements of railways infrastructure. The research also attempted to design an effective methodology, which allows assessing the significance of infrastructure objects. The purpose of the multi-criteria assessment of selected sections and typological objects is to select the most significant/important ones from the point of view of maintaining the railway operability. The selection is conducted using the assessment of a section or an object, following the pre-defined criteria. The developed methodology should help to set a group of potential elements of critical infrastructure in the railway sub-sector.

Keywords: *transportation, railway infrastructure objects, risk assessment, criterion, multi-criterial decision, critical elements*

1. Introduction

The problem of Critical Infrastructure (CI) and its security, especially the resilience assessment of the most important elements and services of infrastructure systems and their efficient protection is a topical problem nowadays. Despite the numerous publications [1], [2], [3] and proposed approaches [4], [5], one cannot apply any universally accepted approach to understand the relations between individual infrastructures. The crucial problem here is how to identify the potential CI elements, based on their parameters and properties or mutual relations. Several influential papers [1], [2], [3], [6], [7] focus on identification methodology of critical sections and elements of the transport infrastructure. The Slovak methodology of the national and the European CI elements determination [8] is regulated by the Act 45/2011 Coll. on Critical Infrastructure [9]. The Government of the Slovak Republic (hereinafter SR), based on the proposal of the Slovak Ministry of Interior, according to § 4 letter c) of the Act No. 45 /2011 Collection of Laws on critical infrastructure, determined the so-called sector criteria, European sector criteria, cross-sectional criteria and European cross-sectional criteria that are at present classified. Due to this reason, the proposal of procedures for objective determination of the set of the so-called "potential CI elements" is an important objective not only of field experts, but in academic environment, as well. The paper focuses on the problem of identification of important infrastructure elements in the transportation sector - railway sub-sector. It contains characteristics and main features of the proposed theoretical approach to identification of importance of defined typological elements of the transport infrastructure. By applying the original developed procedure, it is possible to decide objectively about the structure of the subset of potential CI elements in the railway sub-sector. At present, a respective software support for its practical application is being developed.

2. The current state of the railway infrastructure elements significance valuation

The main objectives of all participating countries of the EPCIP *(European Program for Critical Infrastructure Protection*) [10], in the transportation sector are to identify the most important elements of transport infrastructure, to reveal and assess their risks that can possibly negatively affect the transportation system functioning and also to prepare efficient protection measures. However, the EPCIP countries often apply different procedures for selection of significant infrastructure elements and their risk and resilience assessment. Nowadays,

* **[1]Bohus Leitner, [2]David Rehak, [3]Robertas Kersys**
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Faculty of Safety Engineering, VSB - Technical University of Ostrava, Czech Republic
[3]Faculty of Mechanical Engineering and Design, Kaunas University of Technology, Lithuania
E-mail: Bohus.Leitner@fbi.uniza.sk

Table 1 *An example of the hazardous events*

Methodical / procedure	Slovakia - Risk analysis in sector Transport	Czech rep. - CritInfo	Germany -SECMAN	USA -RAMCAP	Denmark - RVA	Germany - SeRoN
Sector / sub-sector of Critical infrastructure	Road and railway transport subsector	Transport – all subsectors	Road transport	Transport - all sub-sectors	Transport - all sub-sectors	Road transport
Approach to determine	Sections, objects	Sections, objects	Sections, objects	Particular element	Particular element	Sections, objects
Determination of criteria	Yes	Yes	Partially	No	No	Partially
Evaluation of criteria	Threshold limits	Point scale	Qualitative	Not defined	Not defined	Qualitative
Risk assessment	Yes	Yes	Partially	Yes	Yes	Yes

it is possible to use a wide variety of different methods for risk assessment or comprehensive parametric assessment of infrastructure element resilience. The CI experts are continuously creating or modifying approaches that enable them to conduct more specific assessment of system parameters of selected groups of elements, the so-called typological objects. They have been frequently involved in designing procedures for selecting potential CI elements, identifying the active factors, assessing the risk level and proposing measures for protection of the most significant/important CI systems and services [11].

The European cross-sectional criteria are identical in all the participating countries, but they are not defined clearly, e.g. by determining the limit values of observed parameters. The cross-sectional criteria mostly focus on failure impact of a significant infrastructure element only. On the contrary, the sector criteria in the railway sub-sector (but also in other transport sub-sectors) do not primarily focus on the assessment of an element failure impact, but they represent specific technical parameters for infrastructure element assessment. The sector criteria, except for the Czech Republic, are classified in all the EU countries and that is why it is only possible to assume and not clearly state which criteria were applied for identification and selection of the set of CI elements [4], [5], [7], [12], [13].

The approaches and methodology for identification of the CI set elements generally depend on the country as each country uses a specific methodology. Table 1 shows a basic comparison of approaches used in various countries.

3. Procedure for identification of potential CI elements in the railway sub-sector

Suitable model methodologies mainly include the German methodology SECMAN [13], the Czech methodology CritInfo [5], but also other mostly road transport-related methodologies. The criteria generally focus on assessment of transport infrastructure performance and at the same time on its possible failure impact.

The general methodology SECMAN mostly deals with road infrastructure with the aim to define the precise criteria for assessment of structural properties of the most important infrastructure elements (tunnels and bridges). For the mentioned types of objects, qualitative criteria were defined as a basis for creation of typological objects of bridges and tunnels. A specific vulnerability value was calculated for each typological object. Based on the above mentioned approaches, a universal procedure for defining the set of potential CI elements in the railway sub-sector was designed and verified.

The proposed procedure consists of subsequent steps:

1. defining and assessment of basic characteristics of line elements - sections - in the area of infrastructure,
2. identification of important sections and determination of the "**Index of Section Importance I_U**" - it means selection of the most important sections,
3. defining and assessment of basic typological objects in a section (tunnels, bridges, stations, centralized traffic control and other important technological elements of railway infrastructure,
4. identification of important elements and determination of the "**Index of Object Importance I_O**", based on the calculated values of "**General Index of Object Importance I_V**" and "**Specific Object Index I_S**" - it means selection of the most important objects,
5. quantification and interpretation of "**Overall Index of Criticality I_K**".

The procedure is based on the assessment according to [14], [15] and applies multi-criteria assessment. The purpose of the multi-criteria assessment of selected sections and objects is to select the most significant ones from the point of view of maintaining the railway operability [16]. The selection is conducted using the assessment of a section or an object following

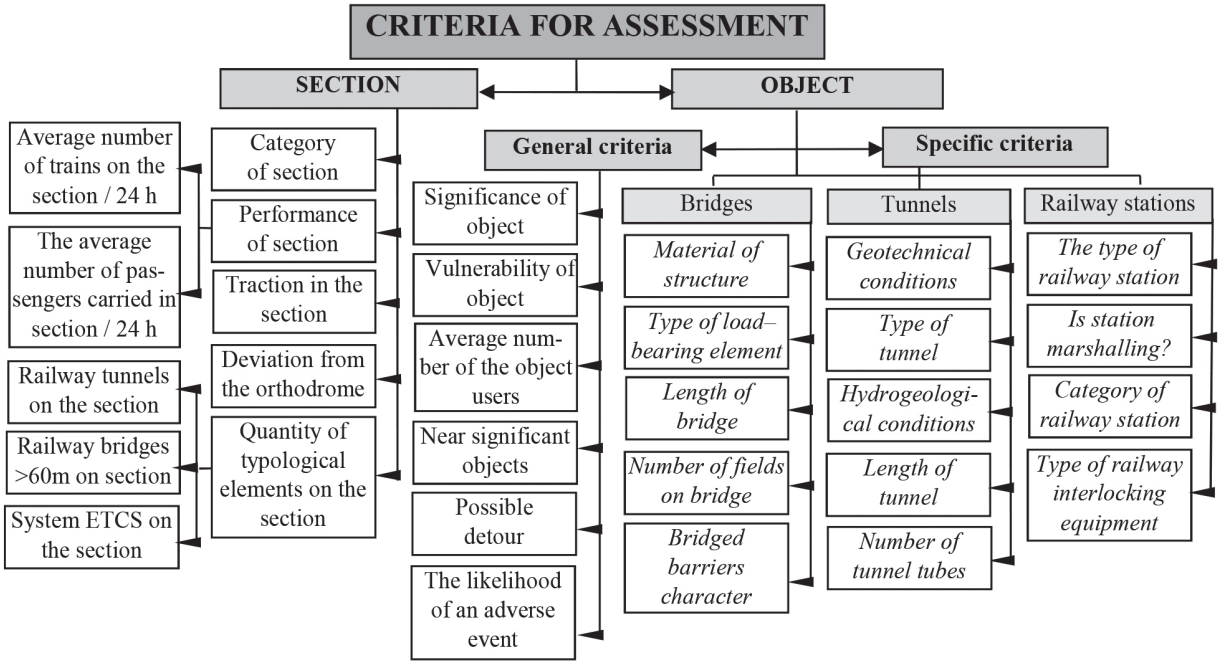


Figure1 *Structure of assessment criteria used in the proposed procedure*

pre-defined criteria. For importance assessment of sections and objects, different criteria are defined. On the level – objects - the assessment criteria according to their significance can be divided into general and specific criteria. The structure of proposed criteria is demonstrated by Figure 1.

The basic structure of the proposed procedure of the potential CI element identification and assessment in the field of railway infrastructure is shown in Figure 2.

The above mentioned activities help to identify the important sections of the railway infrastructure on the network level and on the object level. The output of the assessment process is a set of important sections and objects located on them – as the potential CI elements in the railway sub-sector.

For more objective assessment of sections applying individual criteria, it is necessary to determine **weight coefficients** of particular criteria. This is conducted based on their (pair-wise) comparison following the Saaty method [17], [18] of analytic hierarchies. Based on weight coefficients of criteria w and the attributes of the assessed sections / objects expressed by the point value, it is then possible to acquire the ***Index of section importance*** I_U and ***Index of object importance*** I_O. Their calculation is based on the relation formed by the sum of products of the point value for section / object and the weights of their individual criteria w_i. Before identifying the most important elements of the railway infrastructure, it is necessary to conduct several preparatory activities:

- to define the selected area of interest,
- to divide the railway track in the area of interest into discrete sections,
- to select parameters and criteria of assessment [15].

PHASE 1: Assessment on the section level - line infrastructure elements

The aim of the first phase of the assessment procedure is to identify the most important sections of railway track in the area of interest and to determine the Index of Section Importance I_U.

In the proposed procedure, the selected sections are assessed according to five criteria (K1 – K5) that are assigned points following the scale designed by authors. The pairwise comparison makes possible to state the order of importance of the assessment criteria for sections. The following order of importance of the section criteria is used: **K1 = section performance, K2 = section category, K4 = occurrence of important typological elements, K5 = deviation from the orthodrome** and the least important criterion **K3 = traction on section.**

Naturally, the individual assessment criteria could become a subject of discussion. For example, the section performance does not have to be the most important criterion. From the point of view of maintaining primary functions of the state, it is important what is being transported in a given section. The load of 50 000 t of cars would not be of the same importance for the state as 50 000 t of coal for a power plant. The outcome of the first phase is the list of all sections of the railway infrastructure in the area of interest and the corresponding value of the Index of section importance I_U which can be expressed as follows

$$I_U = \sum_{i=1}^{5} \frac{(K_i \times w_i)}{5} \qquad (1)$$

where K_i is point value of the i-th criterion for a given section, w_i is weight coefficient of the i-th criterion. The theoretical - *benchmark*

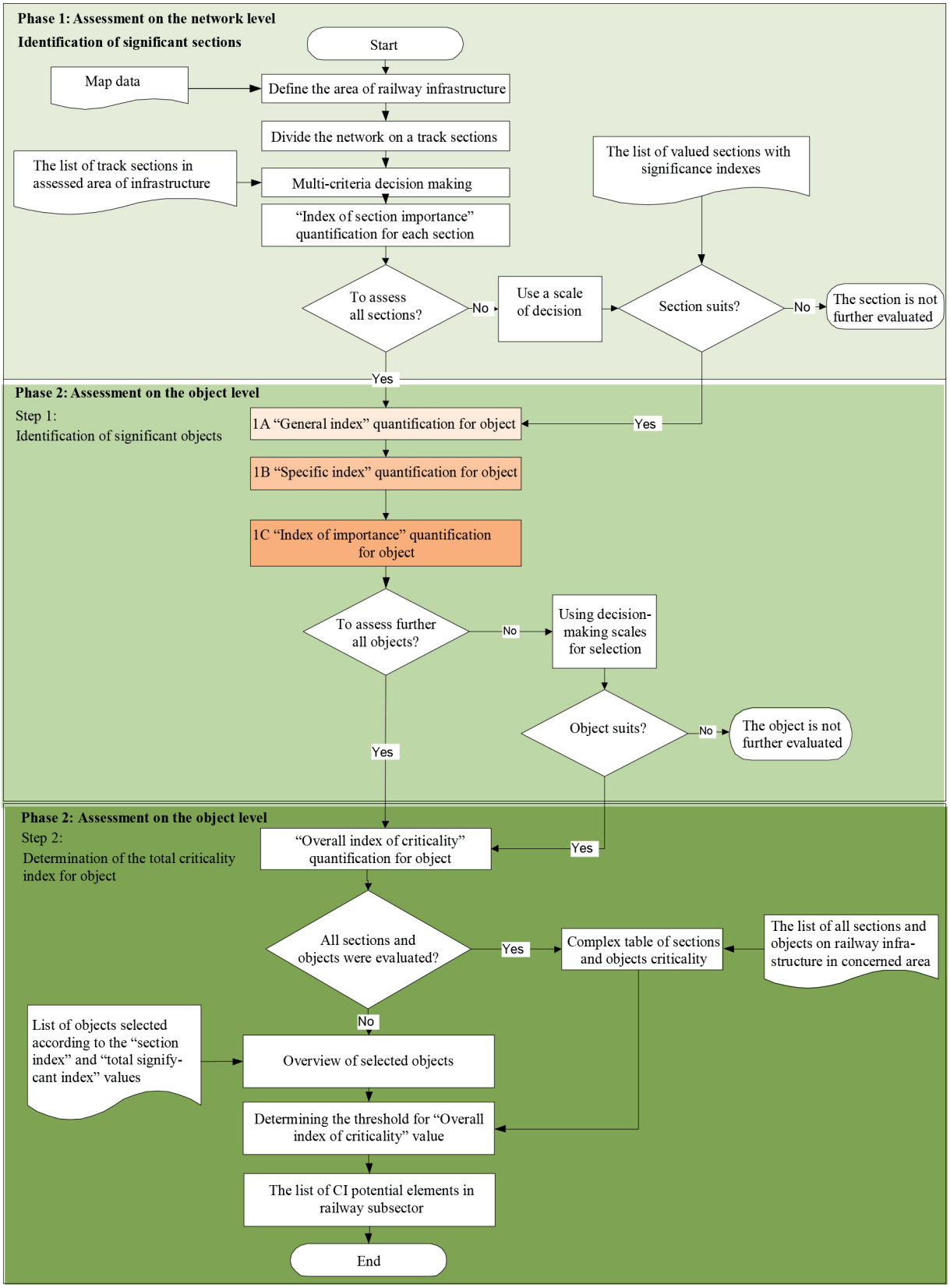


Figure 2 *Procedure for CI elements identification in railway sub-sector*

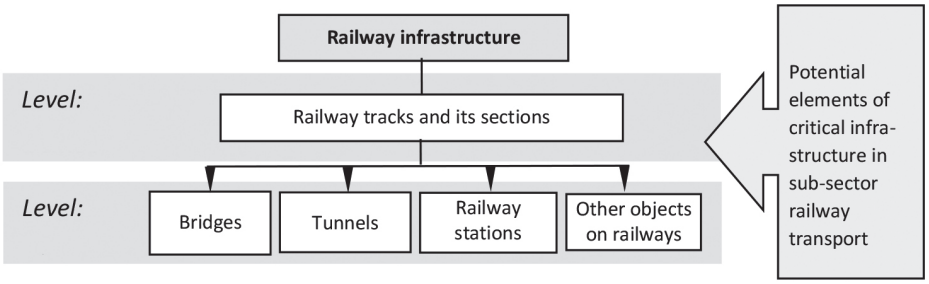


Figure 3 *Typological objects*

- section (maximum possible value) reached the value I_U =12.6 and the following relation is valid:

$$I_U = \frac{K_1 \times w_1 + K_2 \times w_2 + K_3 \times w_3 + K_4 \times w_4 + K_5 \times w_6}{5} = \\ = \frac{5 \times 5 + 5 \times 4 + 2 \times 1 + 2 \times 3 + 5 \times 2}{5} = \frac{63}{5} = 12.6$$

PHASE 2: Assessment on the object level - point infrastructure elements

The aim of the second phase is to identify the most important objects in the sections, selected in the first phase - i.e. in the most important railway sections in the area of interest, as well as to determine the **Index of object criticality** I_O. The most important elements of railway infrastructure will be understood as typological objects. It is possible to assume that the primary typological objects - ***railway bridges, railway tunnels, railway stations, dispatching centers for remote-controlled tracks*** etc. – will probably form a set of potential CI elements in the railway sub-sector. The phase of assessment on the object level consists of two steps:

PHASE 2 - Step 1: Determination of the Index of object importance I_v.

An expected outcome is a list of all objects in the most important sections (selected in the 1st phase). Each object is assigned a respective value of Index of object importance I_O and for its quantitative expression it is necessary to determine:

A. **General index of object importance** I_V: detailed section analysis in order to create a list of section objects and define their operational and security attributes. The objects are assigned points according to defined scales for individual criteria (VK1 – VK6). The order was determined by pair wise comparison of criteria. The most important criterion is VK6 – probability of occurrence of an undesirable event. The other criteria, respectively, are: VK3 – number of object users, VK4 – object environment, VK2 – object vulnerability, VK5 – possible detour and VK1 – object importance.

For the sake of further clarification, e.g. in criterion VK5, it is possible to consider replacing railway transport by road transport (which is besides detour the most frequent method how to provide transport in case of distortion or destruction, etc. of an important element of transport infrastructure. Based on the assigned points VK and the weight coefficient of the criterion *w*, for the General index of object importance the following relation is valid:

$$I_V = \sum_{i=1}^{5} \frac{(VK_i \times w_i)}{5} \qquad (2)$$

where VK_i is value of the *i*-th criterion for the given object, w_i is weight coefficient of the *i*-th criterion.

B. **Specific index of object importance** I_S: detailed analysis of an object for the purpose of defining its typology and attributes. Based on assessment of specific parameters of typological objects – *bridges, tunnels, stations, terminals or other objects*, it is possible to determine the value of the Index I_S, following the predefined matrices of individual groups of typological groups (Figure 3).

For each typological group, the Specific Index of Object Importance I_s is determined as:

$$I_S = \sum_{i=1}^{5} \frac{(SK_i \times w_i)}{5} \qquad (3)$$

where SK_i is value of the *i*-th specific criterion for the given object, and *n* is number of relevant specific criteria selected for the object. Based on the set of specific criteria SK_i [14], their combinations and object types, 12 types of bridge structures, 6 types of tunnels and 8 types of railway stations were defined. Each object was clearly assigned a specific value of the index I_S, specifying its vulnerability (or resilience) level. The determined value was based on specific object properties and parameters.

C. **Summary value of the object importance**: it's called ***Index of object importance*** I_O. Here, the following relation is valid:

$$I_O = \frac{I_V + I_S}{2} \qquad (4)$$

where I_v is the value of the General index of object importance, I_s is the value of the Specific index of object importance. The Index of object importance I_O must be determined separately for each typological group, because the specific criteria of each typological group are different, featuring different point values and different maximum value each typological object can reach. The maximum possible (reference) values of the Index of object importance I_O for each typological group are stated in Table 2.

Table 2 *Maximum values of the Object importance index*

Typological group	Maximal value of General index of object importance Iv	Maximal value of Specific index of object importance I_S	Maximal value of Total index of object importance I_O
Bridges	$I_{V\,max} = 15$	8.4	11.7
Tunnels		7.4	11.2
Railway stations		7.5	11.25

Table 3 *Scale for assessing - Overall criticality index of object*

Level	Scale for assessing	Index I_K
1	Very important / Very critical	0.90 – 1.00
2	Important / Critical	0.75 – 0.90
3	Moderately important / Moderately critical	0.65 – 0.75
4	Low important / Low critical	0.50 – 0.65
5	Insignificant / not critical	0.00 – 0.50

PHASE 2 - Step 2: Calculation of the Overall Criticality Index I_K

The Overall Criticality Index I_K is determined based on the above mentioned data and is determined by the following relation:

$$I_K = \frac{I_{U_i} + I_{O_i}}{\max(I_{U_i} + I_{O_i})} \qquad (5)$$

where I_{Ui} is a resulting value of Index of Importance for section *i*, I_{Oi} is a resulting value of the Index of Importance for object *i*, $\max(I_{U_i} + I_{O_i})$ is the maximum possible value of the sum of values of indices I_U and I_O for a particular object *i*. The Overall Criticality Index I_K always acquires values from the interval <0; 1>. The principle of identification or determination of the object importance lies in comparing the acquired number of points of the assessed object with the maximum number of points a given typological object is able to reach. To determine the level of criticality, a scale with value range of IK was defined according to Table 3.

In a conducted case study, the authors decided that the objects reaching values over 0.75 can be considered as objects that compose a set of potential CI elements. Why the value 0.75? Interestingly, the users can define the limit values according to their needs and according to the desired size of the set of important elements.

It is obvious that if the set of important elements of transport infrastructure is too large, the costs for securing prevention or subsequent protection measures will be higher. If the criterion limit for including the object to the list is set arbitrarily, (e.g. value 0.5 or 0.95), and the group of potential CI elements includes arbitrarily high number of transport infrastructure elements, the final range of carried out measures will always depend on financing possibilities of their protection. For example, in compliance with § 9, para. 4 of the Act [9], the operator of a CI element is entitled to a financial support (from the respective Ministry) to meet the duties related to performing security measures for a CI element protection. It is thus possible to select hundreds of elements and label them as "vitally important". If financial support for security measures is not available, the fact whether the object is on the CI element list or not will not protect it against any potential threat. It also means that the value 0.75 - benchmark selected by methodology authors, cannot be understood dogmatically. A set of railway infrastructure objects acquired in the stated way needs to be further assessed applying objective risk assessment methods [19]. Based on results of the risk assessment and the resilience level assessment of the CI systems and services, it is possible to decide objectively about the size and structure of CI system in a specific sector/sub-sector on national and European level.

4. Conclusions

The procedure was designed in the way to provide an assessment of railway infrastructure on the network and object levels. The aim of this methodology is to identify important railway sections and determine values of section importance. Subsequently, it is necessary to define and assess typological objects in the section and set the values of object importance. This enables us to focus attention on prevention checks, maintenance and organizational measures for securing the desired protection level. The authors are aware of the fact that the designed procedure is only one of possible steps applicable in a comprehensive process of the CI element selection, specifically in railway infrastructure (bridges, tunnels and railway stations). It is necessary to realize here that the proposed procedure does not include all the important attributes of conducted transport services, e.g. characteristics or commodity mix transported in individual track sections, redirecting the flow of goods or people to another track section.

In the moment of redirecting the flow, the importance of element value changes (the criterion values for selected elements of railway infrastructure change) and the original element that seemed to be critical loses its importance. There are also problems of possible impact of replacement of the railway transport by the road transport and assessment of railway infrastructure elements in terms of their uniqueness. For example, the only 100-m-long bridge on a 100-km-long section will be of different importance than a 100-m-long bridge on a 20-km-long section with 5 other bridges, even if the tracks were loaded identically.

The most significant deficiency of the CI element determination and protection is the fact that no EU document states exhaustively the required level of the CI element protection in the transport sector, either on the European or national level. The need is even more obvious if we realize that it was the EU that started discussion on this problem. From this point of view, it is not clear what final state of element protection should be reached. There is space for more extensive research (e.g. scientific project, study, final thesis, etc.). For example, it should be possible to quantify that a railway station with more than 30 000 passengers per day must have a CCTV and a security guard service and a different station with more than 15 000 passengers per day at least a CCTV, etc. A similar system can be adopted as a protection measure for other typological elements, e.g. bridges, tunnels, etc. Our research has revealed other areas that need to be focused on in terms of functionality and versatility:

- adding more typological objects to typological groups and determination of their specific parameters and criteria (e.g. energy supplying systems, controlling systems, etc.),
- detailed definition of main criteria and vulnerability analysis for each object type in each typological group,
- completing the next process step: comparison of objects based on another index that would consider some risk factors of objects,
- creation of software tool enabling automated assessment of object criticality that would be based on developed procedure and current railway infrastructure databases,
- cooperation with GIS systems in presentation of object location in the area of interest and criticality parameters of the analyzed sections / objects on a map.

Systematic solution of the above mentioned areas of problems and partial activities in the processes of identification and importance assessment and object resilience in infrastructure networks can contribute to more efficient processes of security management and protection of important sections and elements of transport infrastructure.

Acknowledgements

This work was supported by project 1/0240/15 “Process model of critical infrastructure safety and protection in the transport sector” and by the project VI20152019049, “Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems”.

References

[1] BAKER, J.: A Vulnerability Assessment Methodology for Critical Infrastructure Facilities [online]. James Madison University, 2005. Available: pphttp://www.jmu.edu/iiia/wm_library/Vulnerability_ Facility_ Assessment_05-07.pdf.

[2] KAUNDINYA, I., MAYER, M., KRIEGER, J., ROTHENPIELER, S.: Security of Road Transport Networks – Identifying and Assessing Critical Road Infrastructure [online]. Transport research area, Paris, 2014. Available: http://tra2014.traconference.eu/papers/pdfs/TRA 2014_Fpaper_17827.pdf.

[3] LOVECEK, T., REHAK, D., SISER, A., HROMADA, M.: Resistance of Passive Security Elements as a Quantitative Parameter Influencing the Overall Resistance and Resilience of a Critical Infrastructure Element. The tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), France, 200-205, 2016.

[4] ONDREJKA, R.: Risk Analysis of Transport Sector – Subsectors Road Transport and Rail Transport (in Slovak). Final report. Research Institute of Transport, Zilina, p. 844, 2014.

[5] FUCHS, P., SOUSEK, R., ZAJICEK, J., HAVLICEK, J.: Transport Infrastructure as Element of the State Critical Infrastructure: Assessment of Criticality in Czech Republic (in Czech). VSBM Kosice, p. 85, 2011.

[6] SVENTEKOVA, E., LUSKOVA, M., DVORAK, Z.: Use of Network Analysis in Conditions of Critical Infrastructure Risk Management. The 20th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2016), USA, II., 247-250, 2016.

[7] NOVOTNY, P., MARKUCI, J., TITKO, M., SLIVKOVA,S., REHAK, D.: Practical Application of a Model for Assessing the Criticality of Railway Infrastructure Elements. Proceedings of scientific works, VSB – Technical university Ostrava, 26-32, 2015.

[8] Council of the EU, 2008. Non-Binding Guidelines for the Application of the Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection [online]. Available: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015616%202008%20INIT [accessed: 2017-05-18].

[9] Act 45/2011 Collection of Laws on Critical Infrastructure (in Slovak) [online]. Bratislava, 2011. Available: http://www.zakonypreludi.sk/zz/2011-45.
[10] European Programme for Critical Infrastructure Protection [online]. Available: http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=URISERV%3Al 33260.
[11] Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection [online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114.
[12] RAMCAP Framework. ASME Innovative Technologies Institute [online]. 2006. Available: http://www.personal.psu.edu/jsd222/SRA311/RAMCAPframework_Risk_Analysis_and_Manage.pdf.
[13] SECMAN Project [online]. Available: http://www.secman-project.eu/.
[14] JANUSOVA, L.: Increasing the Objectivity of Identification Critical Infrastructure Elements in Transportation Sector (in Slovak). Dissertation work, University of Zilina, p. 149, 2015.
[15] JANUSOVA, L., LEITNER, B.: Procedure to Identification of Critical Infrastructure Potential Elements in Railway Sub-Sector (in Slovak). Crisis Management, 2, 5-13, 2015.
[16] BREZNICKA, A., CHOVANEC, A., STODOLA, J.: Discrete Simulation with a Variable Time Step in Assessing Costs to Mission. International Conference on Military Technologies (ICMT 2015), Czech Republic, 103-106, 2015.
[17] DVORAK, Z., LUSKOVA, M., HRUZA, P., SOUSEK, R.: Complex Automated Information System for Remote Management of Crisis Situations in Rail Transport. Communications: Scientific Letters of the University of Zilina, 15(3), 83-88, 2013.
[18] SAATY, T. L: Analytic Hierarchy Process. McGraw-Hill, New York, USA, 1980.
[19] SAATY, T. L.: Decision-Making with the AHP: Why is the Principal Eigenvector Necessary. European Journal of Operational Research, 145(1), 85–91, 2003.

Ladislav Janosik - Ivana Janosikova - Pavel Polednak*

THEORETICAL CALCULATIONS OF ECONOMIC LIFE OF FIREFIGHTING APPLIANCES BASED ON CHASSIS TATRA IN THE SOUTH MORAVIAN REGION

This paper is focused on the evaluation of economic data obtained from operational records of firefighting equipment with a focus on firefighting and rescue appliances, especially on exit vehicles based on the chassis CAS 20 – TATRA T815-231R55 18 325 4x4.2. These vehicles have been operated by professional units of the Fire and Rescue Service in the South Moravian Region since September 2013. The producer of firefighting superstructures WISS GROUP, Bielsko-Biala, Poland, was a supplier of all these vehicles. The paper's aim is to specify the optimum lifetime of the firefighting vehicles by the analysis of firefighting vehicles' economical operation. Theoretical calculations of the optimum lifetime have been processed with implementing both the method of exponential trends and the Brown method. The residual value of vehicles has been calculated both according to the current Czech tax law, and to the Expert Standard Valuation of motor vehicles in force in the Czech Republic.

Keywords: *acquisition value, costs, depreciation, residual value, economic life*

1. Introduction

This paper follows on previous authors' publications focused on the assessment of economic data of firefighting appliances based on the chassis Renault Midlum and Mercedes-Benz Atego [1], [2]. These vehicles were deployed at professional units of the Fire and Rescue Service of the Zlin and Moravian-Silesian Region during the reporting period. This paper shows results of alternative calculations of theoretical economic lifetime of observed appliances. The comparison of results for all the assessed vehicles is performed in the conclusion.

2. Characteristics of observed firefighting and rescue appliances

Essential tactical-technical characteristics of the assessed appliances TATRA can be traced in the literature, e.g. [3], [4]. Key operational and economic characteristics of the monitored equipment for the period October 2013 to November 2016 are shown in the Table 1. All three vehicles were bought at the same time, with the purchase price CZK 5,626,467 (221,427.28 €). Those appliances started to operate on October 17, 2013. The primary operational data from the information system IKIS II were exported into Excel file and then used for the assessment of operation and maintenance costs of those vehicles [5].

3. Methods

Economic life of the vehicle can be generally characterized as reaching the limit state when further operation is economically unsustainable [6]. The *economic efficiency of the investment* is calculated to assess the economic life of the technical system in the business environment. This procedure would be relatively difficult to apply for the evaluation of firefighting appliances. The methodology of these calculations is based on the input data extremely difficult to define in the sphere of public service [7], [8]. One of the reasons for the impossibility of using this calculation method is the requirement of the initial setting of the technical system's lifetime. The approximate lifetime can be only theoretically estimated or assumed from the Machinery Service Order [9] in which approximate lifetimes of firefighting appliances are set. The 10 years long standard lifetime of the rescue firefighting vehicle is prolonged for next 6 years after technical improvement.

* [1]Ladislav Janosik, [2]Ivana Janosikova, [1]Pavel Polednak
[1]Faculty of Safety Engineering, VSB - Technical University of Ostrava, Czech Republic
[2]Faculty of Economics, VSB - Technical University of Ostrava, Czech Republic
Email: ladislav.janosik@vsb.cz

Table 1 *Basic characteristics of referred vehicles during years 2013-2016*

Vehicle location	Registration mark	Year		Mileage	Amount of fuel	Maintenance and repair costs		Cumulative costs	
				[km]	[l]	[CZK]	[EUR]	[CZK]	[EUR]
Vyskov	5B4 3485	2013	0	3,218	1,722	0	0	0	0
		2014	1	5,269	3,061	7,074	278.39	7,074	278.39
		2015	2	10,149	4,756	23,414	921.45	30,488	1,199.84
		2016	3	7,721	4,438	43,343	1,705.75	73,831	2,905.59
Pozorice	5B4 3487	2013	0	2,800	1,614	0	0.00	0	0.00
		2014	1	4,050	2,846	0	0.00	0	0.00
		2015	2	8,526	6,231	45,898	1,806.28	45,898	1,806.28
		2016	3	5,819	4,259	24,019	945.24	69,916	2,751.52
Tisnov	5B4 3486	2013	0	3,198	1,493	0	0.00	0	0.00
		2014	1	8,508	4,827	17,721	697.39	17,721	697.39
		2015	2	9,716	5,347	41,965	1,651.51	59,686	2,348.90
		2016	3	8,153	4,731	24,019	945.24	83,704	3,294.14

Therefore, the calculation of the monitored vehicles' economic life was performed by use of the two simple and generally known methods, the *exponential trends method* and the *Brown method* [10], [11]. Calculations according to both methods were performed for a 4-year operation time period. The *residual value* of appliances, which is one of data used for calculations, was variously calculated according to the Act No. 586/1992 Coll. on Income Taxes [12], and according to the Expert Standard No. I/2005 - Valuation of motor vehicles [13].

3.1 The Exponential trend method

Theoretical foundations of the method were published in 1963 [14]. The principle is displayed graphically in Figure 1.

This method is based on the theoretical assumption that the value of firefighting appliances in time $N_p(t)$ has the shape of downward sloping exponential curve [10]. The curve is defined by the equation:

$$N_p(t) = C \cdot e^{-\alpha \cdot t}. \quad (1)$$

Similarly, one can define the trend of costs for maintenance and repairs $N_u(t)$ by using an upward sloping exponential curve according to the equation:

$$N_u(t) = A \cdot e^{\beta \cdot t}. \quad (2)$$

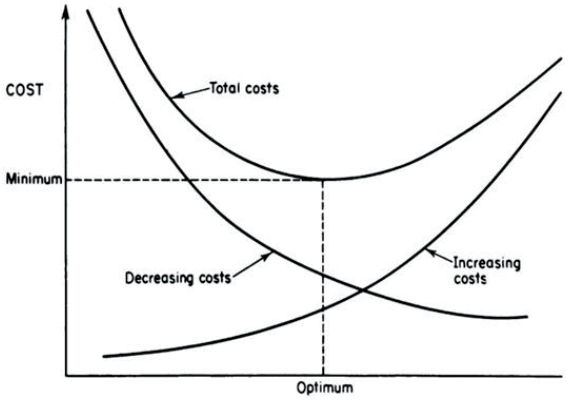


Figure *1 Fundamentals of operation research [14]*

The total value of firefighting appliances $N_c(t)$ is a sum of Equation (1) and Equation (2):

$$N_c(t) = C \cdot e^{-\alpha \cdot t} + A \cdot e^{\beta \cdot t}. \quad (3)$$

Then, one calculates the local extreme of this function by modification of Equation (3). The local extreme ($N_c(t)$ minimum in this case) represents the optimal time T_{opt} for replacing the appliance:

$$T_{opt} = \frac{1}{\alpha + \beta} \cdot \ln\left(\frac{\alpha \cdot C}{\beta \cdot A}\right). \quad (4)$$

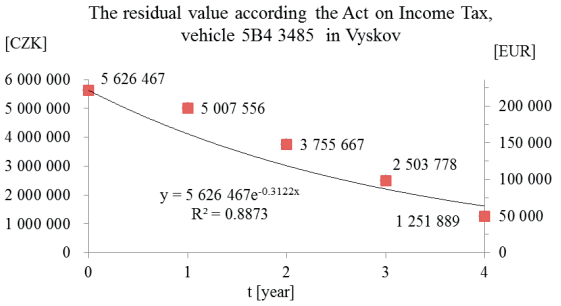


Figure 2 *The residual value according to the Act on Income Tax*

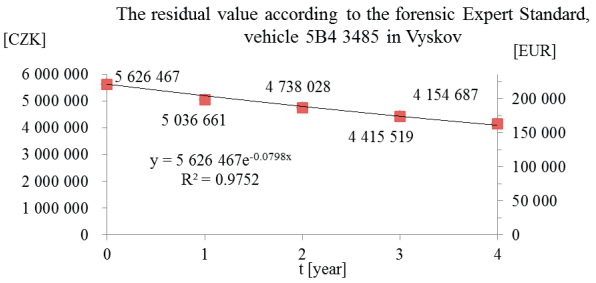


Figure 3 *The residual value according to the forensic Expert Standard*

After reaching the minimum point, the function $N_c(t)$ rises, due to declining price of the firefighting vehicle $N_p(t)$ and increasing maintenance and repair costs $N_u(t)$. After processing the input economic data and building charts of the exponential curve (by using appropriate software, e.g. MS Excel), constants *A, C* and exponent coefficients **α, β**, were obtained.

3.2 The Brown method

This method was published first over 55 years ago in the journal Railway Age, in Brown's paper "What's the Life of a Diesel?" Theoretical foundations then were summarized and published in 1963 [14]. The method was used for the preliminary determination lifetime of rail vehicles [11]. The optimum lifetime T_{opt} is given by:

$$T_{opt} = \sqrt{\frac{2 \cdot H_0}{B}}. \tag{5}$$

Here, H_0 is the vehicles' acquisition value given as a percentage=100 % and B is the linear incremental trend coefficient of the maintenance and repair costs. This coefficient was obtained likewise from the charts using linear regression of data. Application of this method is connected with some weaknesses, as discussed below in the results.

3.3 Vehicle's residual value calculations

Calculations of the vehicle's residual value, according to the Act on Income Tax [12], consider the depreciation period of 5 years in Article 30 within motor vehicles for special purposes, according to the classification in Appendix No. 1 of the Act. Depreciation percentages are fixed for the first year at the level of 11 % and they are changed to 22.25 % for the next four years. Calculating the relative technical value of the vehicle *PTHS* in any year of operation is carried out in percentages of the purchase price, in accordance with the Expert Standard [13], by equation:

$$PTHS = \frac{THSN \cdot (100 - ZA) \cdot (100 \pm TS) \cdot PDS}{10^6}. \tag{6}$$

The initial technical value of the group *THSN* = 100 %, technical condition changes *TS* = 0.0 % and the relative group proportion value *PDS* = 100 % were applied in the equation, in the case of maintained and operational firefighting appliances. Basic amortization *ZA* [%] which is calculated as the arithmetic average of the following equation was the only variable in the Equation (6):

$$ZA = \frac{ZAD + ZAP}{2}. \tag{7}$$

The ZAD parameter is the basic percent reduction during the operation defined in Annex No. 1.4 of the Expert Standard [13] and ranges from 20 % in the first year of operation to 90 % in the tenth and following year of operation. The *ZAP* parameter [%] determines the percentage of the basic reduction for the mileage (see ibid.).

4. Results

Overall results of calculations are stated in the following tables and graph exemplifications of which are evident constants and coefficients exponents values used for the calculations in Equation (4) and Equation (5).

A significant decrease in the residual value of all the observed vehicles was elicited by calculating according to the Act on Income Tax [12], as shown in Figure 2 on the case of the vehicle registration number 5B4 3485 from the fire station Vyskov. The difference in results of the residual value calculations according to the Expert Standard [13] is shown in Figure 3. It is evident that the Expert Standard is more suitable under consideration the mileage of the firefighting appliance. This can significantly affect the vehicle wearing. Finally, the Expert Standard gives the higher residual value of the particular vehicle at the end of the year 2016, which is closer to its market value.

Results of the repair cost functions calculations according to both the exponential trend method and the Brown method, can be seen in Figure 4 and Figure 5. Those results for all three vehicles are distorted by the fact that the vehicles are under warranty. Each vehicle has travelled an average of 3000 km in less than

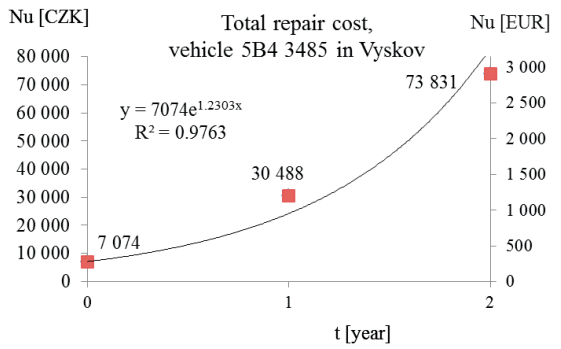


Figure 4 *Total repair costs according to the exponential trends method*

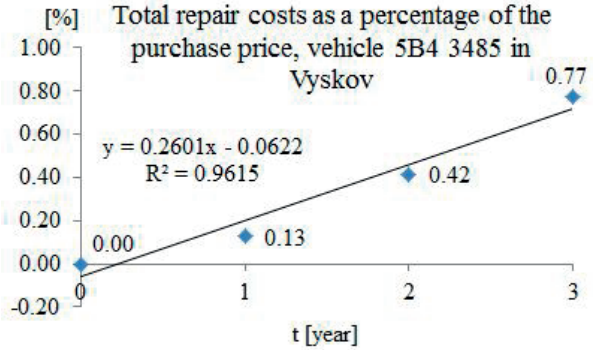


Figure 5 *Repair costs according to the Brown method*

Table 2 *Economic lifetime in accordance with the Act on Income Tax*

		Maintenance and repairs cost ratio $N_u(t)$			Residual value of firefighting appliances in time $N_p(t)$ coefficients			T_{opt} [year]
Vehicle location	Registration mark	A [CZK]	β [-]	Correlation coefficient R	C [CZK]	α [-]	Correlation coefficient R	
Vyskov	5B4 3485	7,074	1.2303	0.99	5,626,467	0.3122	0.94	3.4
Pozorice	5B4 3487	45,898	0.4209	1.00	5,626,467	0.3122	0.94	6.2
Tisnov	5B4 3486	17,721	0.8639	0.94	5,626,467	0.3122	0.94	4.0

three months of use during the year 2013 and underwent the first servicing under warranty conditions, i.e. free of charge. In terms of the traffic load, an average number of the rescue exits per vehicle was only 16, but there were 38 condition rides when the vehicle was not overloaded (in 2013). Hence, there was not much opportunity for the occurrence of a failure. From a mathematical point of view, this additionally means that the exponential curve, describing the development of maintenance and repair costs, begins since 2014, when these costs were non-zero.

Further distortions in the trend of maintenance and repair costs might be caused by vehicle accidents. The vehicle 5B4 3485 from Vyskov Station had two traffic accidents in 2014 and afterwards it was out of service for almost six months - from February 3 to May 22, when repair costs reached approximately CZK 268,000 (10,547.03 €), and then from August 9 to October 14, when repair cost amount was approximately CZK 220,000 (8,658.01 €). The operating load of that vehicle was about 5300 km in 2014. The vehicle 5B4 3487 from Pozorice Station had one traffic accident in the year 2014, and was out of operation from February 2 to May 5 (the repair cost increased to CZK 746,000, that was 29,358.52 €). The operating load of that vehicle was about 4000 km in 2014. The recorded maintenance and repair costs are zero for this vehicle in 2014.

Depreciation results, according to the Act on Income Tax [12], are presented in Table 2. Table 3 displays variant calculations results while using depreciation according to the Expert Standard [13]. Both results were obtained by applying the exponential trend method. Compared to the previous calculations published in [1], [2], the impact of the residual value method had not such a significant effect on the resulting economic lifetime in the case of vehicles deployed at stations Vyskov and Pozorice.

Total maintenance and repair costs in particular years and B-coefficient values for the theoretic recovery time calculating are summarized in Table 4. Figure 5 shows the linear trend of the cumulative cost. Both the curve, and its mathematical expression with the B-coefficient used for the calculation according to Equation (5) were automatically generated by the MS Excel.

Results acquired by the Brown method with using the linear trends are shown in Table 5. Calculations confirmed again that the Brown method application is not optimal for firefighting appliances. The use of this method has its shortcomings. The method was formulated for rail vehicles, which have high initial costs and the expected technical life is considerably longer than 10 years. For example, the rail kit RegioSprinter BR 654 costs CZK 47 million (1.85 million Euros) within the technical lifetime of 25 years. Application of this method assumes steady repair costs, as well as costs increasing with time. To evaluate the lifetime of less costly firefighting vehicles then the results are not those we expected.

Table 3 *Economic lifetime in accordance with the Expert Standard*

		Maintenance and repairs cost ratio $N_u(t)$			Residual value of firefighting appliances in time $N_p(t)$ coefficients			T_{opt} [year]
Vehicle location	Registration mark	A [CZK]	β [-]	Correlation coefficient R	C [CZK]	α [-]	Correlation coefficient R	
Vyskov	5B4 3485	7,074	1.2303	0.99	5,626,467	0.0798	0.99	3.0
Pozorice	5B4 3487	45,898	0.4209	1.00	5,626,467	0.0788	0.99	6.3
Tisnov	5B4 3486	17,721	0.8639	0.94	5,626,467	0.0891	1.00	3.7

Table 4 *Input values for calculating the B-coefficient according to the Brown method*

Vehicle location	Registration mark	Year		Maintenance and repair costs [CZK]	Vehicle purchase price [CZK]	Maintenance and repair costs in [%] of the purchase price	coefficient B	R^2	R
Vyskov	5B4 3485				5,626,467		0.2601	0.9615	0.98
		2013	0	0		0.00			
		2014	1	7,074		0.13			
		2015	2	23,414		0.42			
		2016	3	43,343		0.77			
Pozorice	5B4 3487				5,626,467		0.2096	0.4760	0.69
		2013	0	0		0.00			
		2014	1	0		0.00			
		2015	2	45,898		0.82			
		2016	3	24,019		0.43			
Tisnov	5B4 3486				5,626,467		0.1712	0.5150	0.72
		2013	0	0		0.00			
		2014	1	17,721		0.31			
		2015	2	41,965		0.75			
		2016	3	24,019		0.43			

Table 5 *Economic lifetime in accordance with the Brown method*

Vehicle location	Registration mark	B [-]	Correlation coefficient R	T_{opt} [year]
Vyskov	5B4 3485	0.2601	0.98	27.7
Pozorice	5B4 3487	0.2096	0.69	30.9
Tisnov	5B4 3486	0.1712	0.72	34.2

Correlation coefficients of each interleaved curve for the two vehicles are very low. However, the calculated theoretical lifetime of the monitored equipment is closer to the real technical lifetime, from the economic life point of view. For example, the conception of the Czech Ministry of the Interior of 2007 [15] refers that the average age of firefighting appliance at units of the

Fire Rescue Service of the Czech Republic exceeds 15 years and at units of the Voluntary Fire Brigades of the Czech Republic more than 29 years. However, such old vehicles have already been technologically obsolete.

5. Conclusion

The clear outcome resulted from the presented calculations, that the calculated optimal economic lifetime of the monitored firefighting appliances is only theoretical. The average value 4.4 years for exponential trends is out of reality. On the contrary, in accordance with the Brown method, the minimum economic lifetime of almost 28 years in the case of a vehicle deployed at the Vyskov fire station is beyond the expected technical life, which reaches maximum of 25 years for the rebuilt vehicles [15].

Compared to previous calculations for firefighting appliances based on chassis Renault Midlum [1], the average theoretical economic lifetime for exponential trend method was 6.5 years. Calculations for firefighting vehicles, based on Mercedes-Benz Atego chassis [2], showed the average theoretical economic lifetime of up to 8.0 years. Both vehicle groups were assessed for a 5-year period of operation. The longer time series resulted in the better regression functions of recorded maintenance and repair costs. For example, Brown recommends at least 8 years period for rail vehicles [10].

The next paper on the same topic, was published in the conference proceedings of the International Scientific Conference on Fire Protection, Safety and Security 2017 [16]. The firefighting appliances, based on the MAN TGM chassis, deployed at Fire Brigades of the Czech Republic in South Moravian Region were assessed in that paper. For those vehicles, the assessed period of operation was 6 years. The average theoretical lifetime from an economic point of view was 6.4 years, with using the exponential trends method. Those examples confirmed that a longer time series for evaluating maintenance and repair costs increase the economic lifetime.

Acknowledgements

This paper was supported by an internal grant of specific research *"SP2014/44 - Determining aspects of operational and functional reliability of firefighting equipment."*

References

[1] JANOSIK, L., JANOSIKOVA, I., POLEDNAK, P.: Assessment of Economic Life of Firefighting and Rescue Appliances Based on Chassis Renault Midlum in the Zlin Region. Communications – Scientific Letters of the University of Zilina, 18(4), 112-116, 2016.

[2] JANOSIK, L., JANOSIKOVA, I.: Determining the Lifetime Parameter of Firefighting Appliances (in Czech). 21st International Scientific Conference Solving of Critical Situations in Specific Environment, Slovakia, 239-246, 2016.

[3] JANOSIK, L.: Functional Reliability of Operation of Selected Firefighting Vehicles (in Czech). Ph.D. thesis, VSB - Technical University of Ostrava, Ostrava, p. 142, 2015.

[4] MONOSI, M., SLOBODA, A., PALUCH, B., HAJDUOVA, Z.: Fire Equipment (in Slovak). EDIS - Publishing Institution of the University of Zilina, Zilina, p. 402, 2013.

[5] JEZEK, B.: Personal Consultation and Operational Data Export from IKIS II (in Czech). Fire Rescue Service of South Moravian Region, Regional Directorate Brno, November 2016.

[6] STODOLA, J.: Operational Reliability and Diagnostics (in Slovak). University of Defence, Brno, p. 88, 2002.

[7] SPACILOVA, L., JANOSIKOVA, I., HON, M.: Microeconomics B (in Czech). Workbook, 1st ed. Faculty of Economics, VSB-Technical University of Ostrava, Ostrava, 19, p.121, 2014.

[8] JURECKA, V., JANOSIKOVA, I.: Microeconomics (in Czech). Textbook for bachelor studies, 1st ed. Faculty of Economics, VSB-Technical University of Ostrava, Ostrava, p. 315, 2005.

[9] Instruction of the Director General of the Fire and Rescue Service and the Deputy Minister of the Interior of 13. 3. 2006 issued Machinery Order of Fire Rescue Services of the Czech Republic (in Czech). The Collection of Internal Management Director General of Fire Rescue Service of the Czech Republic and the Deputy Minister of the Interior, Prague, 9, p. 28, 2006.

[10] DANEK, A., SIROKY, J.: Theory of Replacement of Conveying Vehicles (in Czech). VSB-Technical University of Ostrava, Ostrava, p. 156, 1999.

[11] HOLUB, R., VINTR, Z.: Fundamentals of Reliability (in Czech). University of Defence, Brno, p. 174, 2002.

[12] Czech National Council Act No. 586/1992, Collection of laws, on Income Tax, as mended (in Czech). Collection of Acts, part 117, p. 48, 1992.

[13] KREJCIR, P., BRADAC, A.: Expert Standard No. I / 2005 - Valuation of Motor Vehicles (in Czech). Academic publishing CERM Ltd., Brno, p. 103, 2005.

[14] BROWN, R. G.: Smoothing Forecasting and Prediction of Discrete Time Series. Englewood Cliffs, NJ, Prentice-Hall Inc., p. 464, 1963.
[15] Concept of Replacement of Basic Firefighting Equipment for Fire Protection Units Included to the Coverage of the Territory of the Czech Republic (in Czech). Ministry of the Interior, Directorate General of Fire Rescue Service of the Czech Republic, Prague, No.: PO –1089/IZS-2007, p. 10, 2007.
[16] JANOSIK, L., JANOSIKOVA, I., MONOSI, M.: Assessment of Economic Life of Firefighting and Rescue Appliances Based on Chassis MAN TGM in the South Moravian region. Proceedings of Fire Protection, Safety and Security 2017, Slovakia, 285-292, 2017.

komunikácie
COMMUNICATIONS

Lenka Sivakova - Anna Zubkova - Witalis Piellowski*

APPLICATION OF A PRIORI AND A POSTERIORI ESTIMATE ON RISK ASSESSMENT

The problem of setting the values and interconnections between elements of the models in the safety, protection and security field, appears as the biggest obstacle in taking crisis management decisions. The article attempts to represent a mathematical approach to modify the expected values and interconnections that can occur in the models describing the protected system in order to minimize errors caused by subjectivity. Here presented procedures are described in the examples of their potential use. The main idea is to focus on improving estimates for better response to reality, then to find new estimates, since those would still be weighed down by the subjectivity caused errors. Based on this premise this article attempts to characterize application of mathematical methods on minimizing the subjectivity caused errors in the models in risk assessment.

Keywords: *expert estimates, safety, security, mathematical approach*

1. Introduction

In Safety and Security Engineering as in many areas of modern science and technology we can see the shift to testing hypothesis on models rather than in real environment. It is obvious, how dangerous could it be to apply any new measure or process to for example crisis management without any previous testing or estimation of consequences. Very effective approach is to create a model of object, area, state, etc. and to simulate different scenarios [1], [2]. This can be done by various methods for particular results. It must be taken into account that every model is only approximated abstraction and therefore inaccuracies can appear. Those mistakes affect adequacy of results obtained with application of such a model. In other words it means that input errors are often mistaken for errors of model itself even that model in general can be good. Consequently, the models are considered as useless or just tools for theoretical science and so they are used at 100% of their potential. On the other hand, if there would be uncritically made decisions based on false results of model, the taken measures might be incomplete but harmful as well. Hence, it is important to keep in mind that even the best model gives only as good outputs as there are the data that comes into it. It is more than understandable why safety and security engineers distrust such tools and avoid their use. In the following article we attempt to illustrate the most often errors and how to avoid them. In article will be presented mathematical approach to modify the expected values and interconnections that can occur in the models. In summary, this article attempts to characterize application of mathematical methods on minimizing the subjectivity.

2. Modern modelling

In a model there are usually some parameters that describe a modelled system. The particular parameter values are determined by the two different types of methods. Those methods are designed to either measure or estimate either qualitative or quantitative characteristics of the given system. Both types of methods can be used in one estimation of the system and in that way create the mixed method research. The most commonly used methods are listed in the Table 1:

- **Qualitative methods** - deal with understanding of given behaviour of system or quantity with non-controlled observation, process oriented, and are characterized by the high level of subjectivity [3].
- **Quantitative methods** - search for facts or causalities, is invasive, they are result oriented and measurement controlled and objective [3]. Those methods are based on measurement and use of statistics as case studies. These methods are

* [1]Lenka Sivakova, [2]Anna Zubkova, [3]Witalis Piellowski
[1]Department of Security and Safety Research, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Institute of Mathematics and Scientific Computing, University of Graz, Austria
[3]Faculty of Security Studies, General Tadeusz Kosciuszko Military University of Land Forces Wroclaw, Poland
E-mail: lenka.sivakova@fbi.uniza.sk

Table 1 Selected qualitative and quantitative methods

Qualitative method	Quantitative method
Individual interviews	Confirmatory Statistics
Observations	Interval Estimates
Questionnaire	Hypothesis Tests
Active approach	Uncertainty Estimates
Estimation by experts	Theories

exact, look like experiment (physical measurement) and are commonly well known from their application in physics or biology.

In application of these methods there are errors that have a major impact on the accuracy of the values obtained. The most frequent are:

- **Measurement errors** - are the physical measurement type of errors. Those errors are natural type of errors and there is a question of optimization between refinement of measurements and necessary precision.
- **Insufficient total number of experiments or measurement repetitions**. The lack of repetition gives data that cannot be statistically analysed. There is a well-known that less than 50 repetitions is statistically insignificant. On the other hand, it is not economically effective to make 50 same measurements or same experiments.
- **Replacing experiments with expert estimates** without subsequent analysis of these estimates. In the case when even one experiment or measurement would be too expensive, or time and material demanding, it is typical to use estimates made by experts. This can be very fast and effective way how to obtain required values but they can also be misleading if any post estimate analysis of obtained data is missing.
- **Insufficient number of estimates made by experts (estimation).** This case is very similar to insufficient total number of experiments or measurement repetitions. Despite the tendency to create a good estimates made by experts, it is uncertain if there is not enough of them.
- **Inherent subjectivity of experts** can cause unequal estimation of values and is a big problem if it is not sufficiently reduced.

In modern Safety and Security engineering, common practice is to replace measurements and experiments with estimations made by experts. Strong argumentation pro this approach is that usually it is not acceptable to make any experiment that could potentially harm health and lives of population, or they are have heavy financial burden, and expert estimates are, indeed, less time consuming [4].

Expert's estimation is a special type of finding approximation of uncertain effects, phenomenon or events. Thence, fundamental condition of forming expert's estimations is to have experts. The necessary condition of forming respectable estimations is to have enough experts. However, in the normal practice, the above conditions cannot be met and therefore the principles of proper expert's estimates are often neglected. The most common mistake is the insufficient number of expert estimates obtained as a result of insufficient number of experts to deal with the issue under consideration. Clearly, the biggest challenge is to provide enough experts. Usually, there are not more than 5 experts in reachable distance. Furthermore, all obtained expert estimates need to be further evaluated. It is necessary to remove the factors reducing the noticeable value of the expert estimates thus obtained.

The actual work with expert's estimates and their evaluation reduces calculating the mean value or meridian without any deeper analysis or justification. Consequently, all irregularities are mistaken for the "vagueness" of social, psychological, economic sciences, although it is known for long time that even such parameters can be measured.

Potential gap in proper application of estimations made by experts is the lack of literature on this topic. For instance, there is not one monography; in Czech language there is only one [5]. Only a few articles can be found with direct application of particular method [6] for specific problem, but methods are used *ad hock* without taking into account appropriateness of the used method. This can be another source of vague results. And for more, every estimation made by any expert is, lastly, is burdened by a subjectivity, and thus error.

3. Understanding of estimations

Estimation usually involves data and their statistics. They are used either to approximate one single value or a small range (interval) in which value most likely appear. Likewise, a function can be found that describes behaviour of unknown parameter based on measurable parameters, what is the matter of this article's interest. Although it is assumed that values of unknown parameters are random, they mostly have some distribution of probability of occurrence of such values. The probability of occurrence is called probability distribution and it is described by those parameters that are measureable [7], [8].

This approach can apparently be used in combination with estimations made by experts if expert's estimations are considered as measurable parameters $x = (x_1, \ldots, x_n)$ while the unknown values are corresponding parameters $\theta = (\theta_1, \ldots, \theta_m)$. The unknown values have some probability density function $p(x|\theta)$ and probability distribution of unknown parameters $\pi(\theta)$.

Probability distribution of a random variable y is defined by probability density function $f(y)$, such that:

- For continuous variable

$$F(y) = P[y_1 \leq P(y) \leq y_2] = \int_{y_1}^{y_2} f(y)dy \quad (1)$$

- For discrete variable

$$F(y) = P[y_1 \leq P(y) \leq y_2] = \Sigma_{i=1}^{2} f(y_i) \quad (2)$$

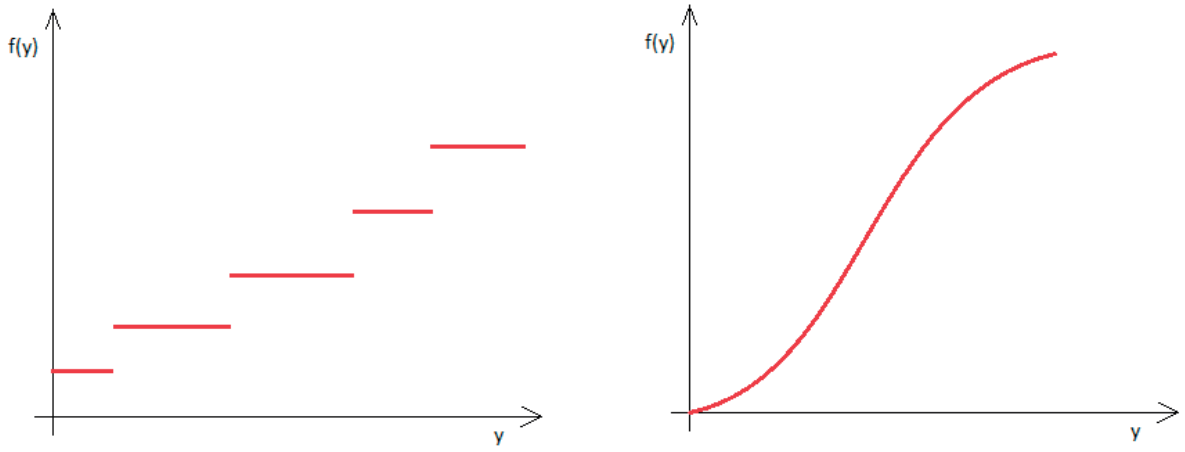


Figure 1 *Probability density function (discrete on the left-hand side, continuous on the right-hand side)*

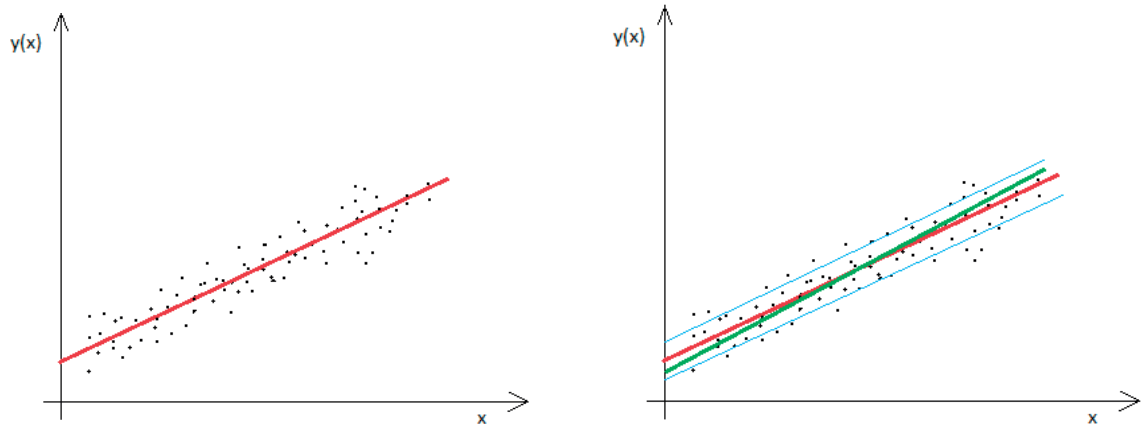


Figure 2 *Linear regression (linear regression on the left-hand and representation of the errors on the right-hand side)*

In both cases the probability that expected value is in interval $\langle y_1, y_2 \rangle$ [9]. Distribution probability function $F(x)$ is the area under the curve as it is obvious from the Figure 1.

In other words, for search values $\theta = (\theta_1, \ldots, \theta_m)$ with some probability distribution $\pi(\theta)$, for example a normal distribution of breaking barriers time there is known a set of expert's estimates $x = (x_1, \ldots, x_n)$ and the probability density function $p(x|\theta)$, which explains what is the likelihood of observing (or good guess of expert) x if the real value is θ.

The nature of estimation depends from case to case. Every situation requires a certain method of finding the estimation function.

Well known estimation functions (estimators) are:

- Maximum likelihood estimators are used for cases where the type of probability distribution is known but mean value and variance need to be estimated.
- Bayesian estimators are used when there are known values from observations of similar parameters or different observations of the particular parameter.
- Minimum mean squared error is the best known method that starts with prior estimation of probability density function and can be tested with posterior data.
- Maximum a posteriori is similar to maximum likelihood method enriched with the optimization of posterior distribution.
- Best linear unbiased estimator can be understood as a linear regression which is its most basic case.

Methods above are used in Safety and Security Research only as the statistical data processing tools, if ever. The possibility how to use those methods in combination with estimations made by experts, can be found in the following text.

The estimation will enter into those methods as a priori estimation, meaning the estimation before measuring. Those methods differ according to what they approximate. That can be the valuation of particular parameter (e.g. the barriers break time), probability density function (e.g. the density of particular risk), dependence of some parameter on others (e.g. probability of threat manifestation), numerical calculation of complex system

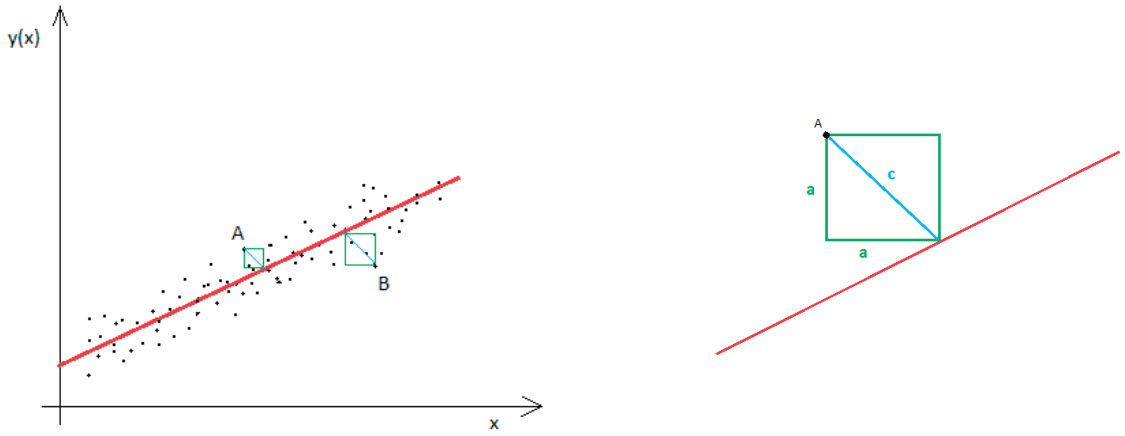


Figure 3 *Minimum mean square value*

(e.g. obtaining values in risk assessment). Detailed explanation of those methods is believed to be helpful in creation of functional and accessible models in the future. Application of corresponding mathematical techniques into already existing custom of using expert's estimations instead of measuring parameters will lead to objectification of conclusions made in all areas of Safety and Security Research.

Linear regression is a conventional technique how to estimate some dependent parameter if there are some observed independent variables and there is an assumption that the relation between observed and estimated parameters is a linear dependence. In that case, the expectation of errors is uncorrelated. This technique is successfully used in cases where the forecast of the next value is expected and there is enough data available.

Linear regression can be written in a vector form:

$$y = \beta x + \varepsilon \tag{3}$$

where:

y is the dependent measured (observed) parameter,
x is the independent parameter (e.g. time),
β is the regression coefficient which define the effect of estimation,
ε is the error term.

On the left-hand side graph in Figure 2 is shown the solution of linear regression (red line) on data presented as dots. This linear regression is defined by the regression coefficient , which determines the slope of the red line and has some tolerance (errors) , represented by the two blue lines on the right-hand side graph in Figure 2. Depending on the mass of data that falls between these two lines, the model is accurate. Of course, for good match of linear regression with the real dependence, represented by the green line, it is fundamental to define small enough. Under those conditions, the linear regression can be found for example with the least square method or the by the minimum mean squared error described in the following paragraph.

In other words, in the case where enough data is available (at least 50 estimations made by experts or at least 50 measurements), this method can find the estimation of linear behaviour if it exist. This method has a greater predictive value than the forecasting based on arithmetic mean, median and similar one dimensional statistical characteristics. The observed data are an *a priori* estimation and the prediction is an *a posteriori* estimation since it will decide if the constructed approximation (linear regression) describes the behaviour good enough. For example, it can find application in the future behaviour prediction of aggressors at football matches and to help design effective countermeasures or for avoiding repeated theft in supermarkets.

For improvement of already existing estimations **minimum mean square error** can serve very well. From the text above, error is the difference between the estimated value and real value.

Observed data are values of random variable and therefore their difference from estimated linear regression is also a random variable and has given mean value. To calculate the mean value of differences between estimation and the real data, it is necessary to understand that the difference is the (perpendicular) distance between for example point A and the red line, as it is clear from Figure 3. According to the Pythagorean Theorem, the square of the distance equals the area of the biggest square that can be in between A and the red line. Calculation with the second power of difference is furthermore good way of penalization errors. The mean value of errors penalization is good estimation of fitting the estimation on data 10].

For example, there be a threat, the probability of performance has a uniform prior distribution with the mean value $\bar{x} = 0.5$ and variance $\sigma_x^2 = \frac{1}{12}$. Two experts were asked to estimate the probability of threat performance. The first one said y_1, the second y_2. From previous experiences, the first expert is inaccurate with an error ε_1 with (unknown distribution) mean zero and variance $\sigma_{\varepsilon_1}^2$ and the second expert is inaccurate with an error ε_2 with (unknown distribution) mean zero and variance $\sigma_{\varepsilon_2}^2$. How to

Table 2 *Parameters of Maximum likelihood estimations*

parameter	description
θ	unobserved parameter that need to be estimated
$x = (x_1,...,x_n)$	observations
f	sampling distribution
$f(x\|\theta)$	probability that is observed if θ is significant
$\mathcal{L}(\theta;x_1,...,x_n)$	likelihood function
$\arg\max_\theta f(x\|\theta)$	Maximum likelihood estimate of θ

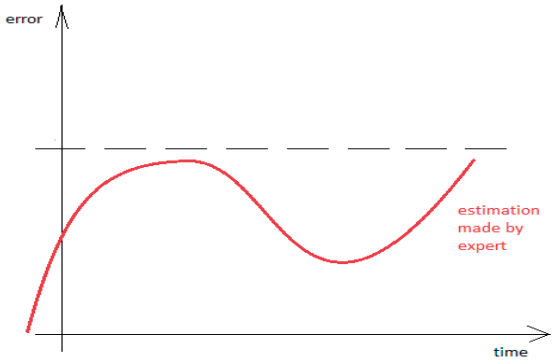


Figure 4 *Maximum likelihood estimation*

obtain the probability of threat preformation from these experts' estimations?

Both estimations have some error (difference) from the real probability x, therefore:

$$y_1 = x + \varepsilon_1$$
$$y_2 = x + \varepsilon_2 \quad (4)$$

The mean values of estimations are the same as the mean value of the given distribution $\bar{x}$. Thus, the linear combination of both estimations gives us the linear minimum mean square error estimator:

$$\hat{x} = v_1(y_1 - \bar{x}) + v_2(y_2 - \bar{x}) + \bar{x} \quad (5)$$

where v_1, v_2 are experts' estimation weights. Those weights give the higher weight to the expert with the lower error and, likewise, the lower weight to the expert with the higher error. Weights are given by equations:

$$v_1 = \frac{\frac{1}{\sigma_{\varepsilon_1}^2}}{\frac{1}{\sigma_{\varepsilon_1}^2} + \frac{1}{\sigma_{\varepsilon_2}^2} + \frac{1}{\sigma_X^2}} \qquad v_2 = \frac{\frac{1}{\sigma_{\varepsilon_2}^2}}{\frac{1}{\sigma_{\varepsilon_1}^2} + \frac{1}{\sigma_{\varepsilon_2}^2} + \frac{1}{\sigma_X^2}} \quad (6)$$

The variance of prediction is given by formula:

$$\sigma_{\hat{X}}^2 = \frac{\frac{1}{\sigma_{\varepsilon_1}^2} + \frac{1}{\sigma_{\varepsilon_2}^2}}{\frac{1}{\sigma_{\varepsilon_1}^2} + \frac{1}{\sigma_{\varepsilon_2}^2} + \frac{1}{\sigma_X^2}} \sigma_X^2 \quad (7)$$

giving the reader the good information about the behaviour of predicted probability. The similar process can be done with generally estimations [10].

Sometimes can models used in Safety and Security Research seem as the non-transparent composition of plenty parameters. Work with corresponding model can lead to misunderstanding of studied system, to cumulative mistakes, etc.

A number of times the model can be reduced to simpler one that would sufficiently describe the considered system. In that situation is convenient to use the **Maximum likelihood estimation**, which maximizes agreement between the fixed set of data $\{x_1,\ldots,x_n\}$ and the selected model. Its application in Safety and Security Research is promising since it works very well for data with normal (and uniform prior) distribution.

Let now be assumed that the observations are independent, with unknown probability density function $f(\cdot|\hat{\theta})$ of a certain type of distribution. The task is to find the estimator $\hat{\theta}$ with the highest agreement with the real parameter θ. Now, fix the observed data and let vary the parameter in joint density function $f(x_1,\ldots,x_n|\theta)$, then the likelihood function is defined as:

$$\mathcal{L}(\theta;x_1,\ldots,x_n) = f(x_1,\ldots,x_n|\theta) = f(x_1|\theta)\times\ldots\times f(x_1|\theta) \quad (8)$$

Or

$$\ln\mathcal{L}(\theta;x_1,\ldots,x_n) = \Sigma_{i=1}^{n}\ln f(x_1|\theta) \quad (9)$$

which is more practical.

The method produces estimation $\tilde{\theta}$, while minimizes the average likelihood $\frac{\ln\mathcal{L}(\theta;x_1,\ldots,x_n)}{n}$.

For a uniform prior estimation it forms two special cases **Maximum a posterior probability estimate** and **Bayesian estimator.**

The point estimation of unobserved parameter θ can be done by **Maximum a posterior probability estimate** that estimates the mode (most often value) of posterior distribution.

The **Bayesian estimator** for the given prior distribution for parameter θ, called $P(\theta)$ and probability of selected data from all the data available $P(x_1,...,x_n)$ is the maximum a posteriori estimate of θ is given by the Bayes' theorem:

$$P(\theta|x_1,\ldots,x_n) = \frac{f(\theta|x_1,\ldots,x_n)P(\theta)}{P(x_1,\ldots,x_n)} \quad (10)$$

and calculated with maximizing of numerator. The maximum likelihood function $\ln\mathcal{L}(\theta;x_1,\ldots,x_n) = f(x_1,\ldots,x_n|\theta)$ and the Bayesian estimator $P(\theta|x_1,\ldots,x_n)$ are the same as for the uniform prior estimation.

The **Maximum a posterior probability estimate** has the same starting assumptions as both cases above. For completeness they are shown in Table 2.

By assumption of existence of a prior distribution $P(\theta)$, the posterior distribution can be calculated from the Bayes' theorem. Then, from the maximum likelihoodestimate $\arg\max_{\theta} f(x \mid \theta)$ the Bayesian estimator of will be estimated [11].

For example, estimation of expert's error can be calculated from maximum likelihood function. Unobserved parameter θ is this time the expert's error, observations x can be some testing examples. At first, expert has to estimate some already for researcher known values. Then from the maximum likelihood estimation $\arg\max_{\theta} f(x \mid \theta)$ his error parameter can be calculated. This calculation can change after every new estimation made by an expert giving the information about change of experts judgement. Taking testing time as continuous, the curve in Figure 4 can be observed.

The prior and posterior probability distributions are tools used in Bayesian probability and statistics. The prior probability distribution allows to make assumption about how values of parameter will be distributed before the parameter is measured. And then can this guess be improved after every observed value giving the posterior probability distribution. The best agreement between assumption and reality is delivered from the maximizing likelihood function.

4. Conclusion

The distrust of Safety and Security Engineers into models is understandable and it is seen as major cause of their misprision. The mathematical modelling in terms of suitable methods for finding values of parameters with its' two distinctive approaches, namely the quantitative and qualitative methods can be the proper way of dealing with problematic of modelling in Safety and Security Research. The proper usage of methods mentioned in this article can lead to better finding of unknown values if the most common mistakes (measurement errors, insufficient total number of experiments or measurement repetitions, replacing experiments with expert estimates, insufficient number of estimates made by experts, inherent subjectivity of experts) will be avoided.

The objectification of estimations made by experts as an important part of the modern modelling can be seen as the future of the Safety and Security Engineering. Among the benefits of the experts' estimations are: first of all, little time consumption accompanied with little financial consumption; secondly, possibility to estimate such parameters, which cannot be measured or are difficult to measure; and lastly, the possibility of their constant repetition. On the other hand, limitations are in their tricky interpretation and obligation of their future adjustments, which are regularly neglected.

In order to adopt the proper estimations made by experts, it is crucial to understand what estimations are, how they are made, and at least the minority of the mathematical notation such as: probability density function, linear regression and commonly used minimum squared error method, or likelihood function.

Exact processing of data used as an inputs into Safety and Security models can enhance actual results and their benefits in decision making. Safety and Security Engineers can use this article as the base line of proper qualification of estimations made by experts and also in obtaining values and their proper analysing.

References

[1] ZAGORECKI, A., RISTVEJ, J., COMFORT, L. K., LOVECEK, T.: Executive Dashboard Systems for Emergency Management. Communications - Scientific Letters of the University of Zilina, 14(2), 82-89, 2012.
[2] LOVECEK, T., VELAS, A., KAMPOVA, K., MARIS, L., MOZER, V.: Cumulative Probability of Detecting an Intruder by Alarm Systems. Proceedings of 47th International Carnahan Conference on Security Technology, Colombia, 2013.
[3] SILVERMAN, D.: Qualitative/Quantitative. Core Sociological Dichotomies. Thousand Oaks (CA), SAGE, 78-95, 1998.
[4] BANDER, E. A.: An Introduction to Mathematical Modelling. Dover Publications, New York, 1978.
[5] KROVAK J., ZAMRAZILOVA E.: Expert's estimation/Expertni Odhady (in Czech). SNTL, Praha, 1989.
[6] NOVOTNY, P., MARKUCI, J., REHAK, D., ALMARZOUQI, I., JANUSOVA, L.: Critical Infrastructure Designation in European Union Countries: Systems Approach Implementation. Communications – Scientific Letters of the University of Zilina, 18(2), 163-169, 2016.
[7] DEGROOT, M.: Optimal Statistical Decisions. McGraw-Hill, 1970.
[8] HALD, A.: A History of Parametric Statistical Inference from Bernoulli to Fisher, 1713-1935, Chapter: Gauss's Derivation of the Normal Distribution and the Method of Least Squares, 1809. Springer, New York, 55-61, 2007.
[9] KAILATH, T., SAYED, A. H., HASSIBI B.: Linear Estimation. Prentice-Hall, NJ, 2000.
[10] RIECAN, B.: Probability and Statistics/Pravdepodobnost a Statistika (in Czech). SPN, Bratislava, 1986.
[11] JAYNES, E. T.: Probability Theory: The Logic of Science. Cambridge University Press, 2003.

komunikácie
COMMUNICATIONS

Maria Luskova - Michal Titko - Alan O'Connor*

SOCIETAL VULNERABILITY TO IMPACTS OF EXTREME WEATHER EVENTS ON LAND TRANSPORT INFRASTRUCTURE

The paper is focused on understanding how failure of land transport infrastructure leads to societal vulnerability. It presents the multi-level approach to societal vulnerability measuring. The level of the societal vulnerability is expressed through the Vulnerability Index, which is calculated based on the vulnerability indicators. Identification and selection of those indicators are based on definition of vulnerability as a function of exposure, susceptibility to change and capacity to adapt to that change.

Keywords: *societal vulnerability, transportation, critical infrastructure*

1. Introduction

Transport infrastructure and services provided in transport are integral parts of everyday life of the population. Transport provides comprehensive service to the state territory and the functioning of the economy in the country [1]. It has a significant impact on socio-economic development and increases the standard of living and prosperity of society, increases the competitiveness of the country and its individual regions, contributes to elimination of unemployment and helps to reduce disparities between regions and states. It is also a key factor for the inflow of foreign investment and the development of tourism [2].

Enhancing safety and security in transport infrastructure is a key objective of the European Commission [3]. At present, one of the biggest threats facing the transport sector are extreme weather events and their impact on transport infrastructure [4], [5]. Over the past years, a variety of extreme weather events have threatened and disrupted transport infrastructure across many European countries and worldwide. The frequency of those events is expected to increase [6]. In this regard several projects, that addressed the sensitivity of transport system to extreme weather, were funded by the European Commission within the 7th Framework Programme for Research and Technological Development.The Project Risk Analysis of Infrastructure Networks in response to extreme weather (RAIN), solved within the call of FP7-SEC-2013-1, topic SEC-2013.2.1-2: Impact of extreme weather on critical infrastructure is one of them. It was focused on research of transport and energy/telecommunication infrastructures exposed to the impact of extreme weather hazards. The principal objective of the RAIN project was to provide an operational analysis framework to minimize the impact of major weather events on land based transportation and energy and telecommunications critical infrastructure in the EU. A holistic risk-based decision making framework was developed to establish the key components of those infrastructure networks and to assess their sensitivity to extreme weather events, as well as to facilitate identification of the impact of alternative mitigation measures [7].

University of Zilina, Faculty of Security Engineering participated in the RAIN project as a leader of the work package entitled "Land Transport Vulnerability". This work package was focused on the identification of critical land transport infrastructure, a review of failures as a result of extreme weather events, the current means of critical land transport infrastructure protection and development of an understanding how failure of this infrastructure leads to societal vulnerability.The aim of this paper is to present the scientific and technical results related to the work performed on assessing the Effects on Societal Vulnerability represented by the definition of Indicators of Societal Vulnerability and in the developed approach to measure vulnerability and specifically societal vulnerability due to the failure of critical land transport infrastructure elements.

* [1]Maria Luskova, [2]Michal Titko, [3]Alan O'Connor
[1]Department of Technical Sciences and Informatics, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Crisis Management, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Department of Civil, Structural & Environmental Engineering, Trinity College Dublin, Ireland
E-mail: Maria.Luskova@fbi.uniza.sk

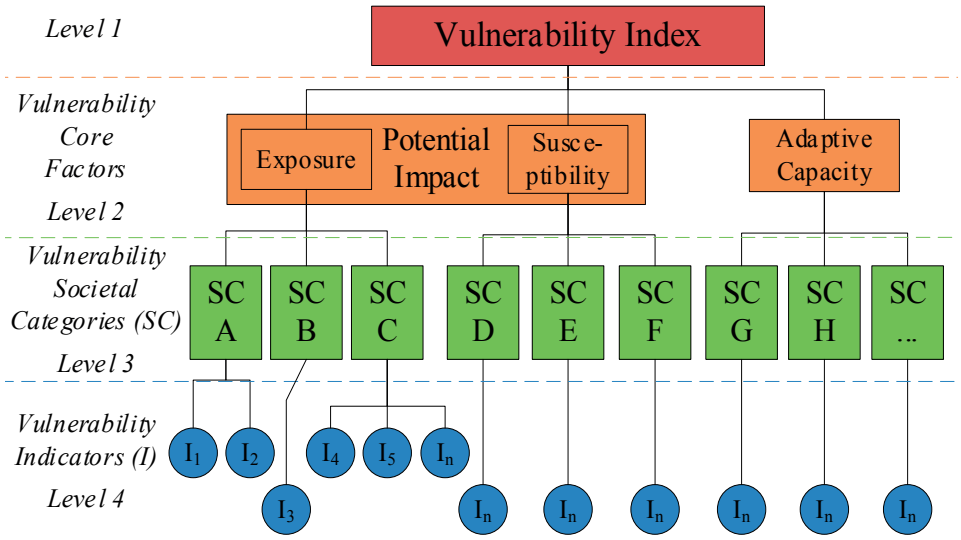


Figure 1 *Multilevel Approach to the Vulnerability Index Identification*

2. Background

The concept of vulnerability has emerged, discussed and continuously developed over almost past five decades, especially in the fields of geographic development and poverty research and hazard and disaster risk research. In the 1970s, research focused on disasters and crises associated with droughts in Africa, significantly contributed to development of social and societal vulnerability concept in geographic development and poverty research. Hazard and disaster risk research, associated with the disaster risk reduction, started in the 1980s. In the last two decades vulnerability has become also a key topic in the climate change science, as well [8].

The term "vulnerability" is used very loosely in dependence on an individual's background and the applied context [7], [8]. In the context of the transport network in connection with effects on society one can define societal vulnerability as an extent to which society is likely to be susceptible resulting from a lack of reliability of critical infrastructure [8], [9], [10], [11]). In this approach to development of understanding how a failure of the land-based critical infrastructure leads to societal vulnerability, that idea was followed. Moreover, for measuring the societal vulnerability, the structural approach was used, based on understanding of the vulnerability as a function of three core factors [8]:

- exposure to extreme weather events,
- susceptibility to change,
- capacity to adapt to that change.

Components of society, which can be in danger (Exposure), components, which are more sensitive to effects of extreme weather events (Susceptibility), as well as capacities (Adaptive Capacity), which assessed region is in disposal of, in order to manage the impacts of extreme weather events, were taken into consideration [12].

Therefore, it is proposed that the Societal Vulnerability should be expressed as a function of the mentioned core factors:

$$\textit{Societal Vulnerability} = f(\textit{Exposure, Susceptibility, Adaptive Capacity}) \quad (1)$$

3. Multilevel approach to societal vulnerability measuring

The content of the individual core factors was questionable. This problem was solved within the RAIN by a structural, multilevel, big data approach (Figure 1). The approach was formulated by gradual splitting of Societal Vulnerability (represented by Vulnerability Index) into lower levels and, at the same time, the requirement for performing the vulnerability assessment by definition of relevant vulnerability indicators was fulfilled (Figure 2):

- Vulnerability Core Factors (3 factors).
- Vulnerability Societal Categories (9 categories).
- Vulnerability Indicators (31 indicators).

Within the proposed approach each Vulnerability Core Factor stands for one component of vulnerability which describes the actual state in a target region. According to assessment of the actual state, it is possible to subsequently determine the level of vulnerability in given region (exposure, susceptibility, adaptive capacity).

For each Vulnerability Core Factor it was necessary to define categories [13]; in this case Societal Categories. Societal

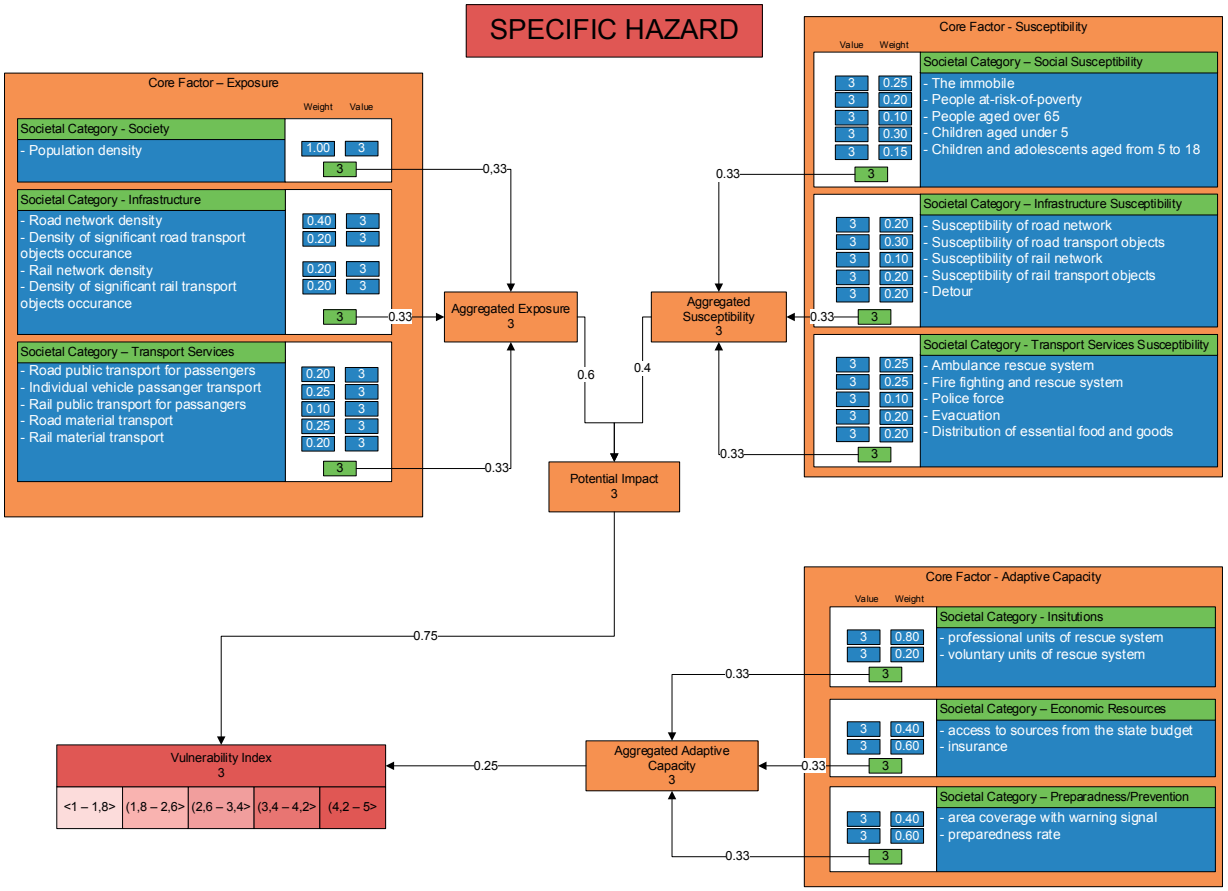


Figure 2 *Multilevel approach to the Vulnerability Index calculation (example of given values)[4], [15], [16], [17], [18], [19], [20], [21]*

Categories stand for those parts of society which form the main interest/centre of this research. They concern mainly transport critical infrastructure and society, hence, performing the functions of transport infrastructure operation for society.

Individual Societal Categories are formed by Vulnerability Indicators. Those Indicators describe concrete specific characteristics of each society, which are significant considering their vulnerability to extreme weather impacts.

As the selection of relevant indicators was the very important part of the research, the selection based on the following three sources was conducted:

- the indicators were selected based on the previous projects and investigations (ESPON CLIMATE [14]; ATEAM),
- related articles,
- indicators were also discussed with the subject matter experts in vulnerability task-related workshops (in the Netherlands, Spain, Slovakia). Experts were from the Dutch USAR-team (Urban Search and Rescue), Dutch police academy, United Kingdom Network Rail asset management, expert involved in EC and UN-assessments and other researchers.

All selected indictors and societal categories within each core factor are shown in Figure 1.

4. Vulnerability index calculation

The Vulnerability Index (VI) is calculated by assessment of the mentioned levels (upwards). By assessment of the Vulnerability Indicators and integration of the Vulnerability Societal Categories and henceforth, within the Vulnerability Core Factors, one obtains the resulting value of VI. The Vulnerability Index represents unlimited value (values from 1 to 5 were proposed). Increasing values indicate increasing vulnerability. VI values have no strict interpretation, but if the given approach is applied on more sectors (areas) simultaneously, it is possible to compare them and it allows the identification of more vulnerable areas.

The Societal Vulnerability is so complicated to define in regard to society and transport that it was necessary to consider many factors and relations, which affect this vulnerability. It was found out that Vulnerability Indicators are so different that it was not possible to find a unifying unit to express the societal vulnerability (e.g. determination through money or other). Therefore, it was suggested to use the point's assessment for each Vulnerability Indicator. Each Indicator was given a value from 1 to 5. As the relevance of indicators does not need to be the same, the indicators were given also weights of importance (w_I).

Table 1 *Vulnerability Index values*

VI value	Description
<1;1.8>	The level of societal vulnerability is minimal. Indicators of societal vulnerability indicate that the examined region (area) is minimally vulnerable in comparison to the average vulnerability in the country. It can be said that the examined region shows a negligible rate of possible impacts caused by specific extreme weather event. Preparedness in terms of material resources and personnel capacities is at a high level. In the long-term planning tasks aimed at maintaining the preparedness level of the society and monitoring the risk factors, changes that could increase the vulnerability level should be included.
(1.8;2.6>	The level of societal vulnerability is low. Indicators of societal vulnerability indicate that the examined region (area) is less vulnerable in comparison to the average vulnerability in the country. It can be said that the examined region shows an acceptable rate of possible impacts caused by specific extreme weather event. Preparedness in terms of material resources and personnel capacities is at a sufficient level. In the long-term planning tasks, aimed at reducing the risk factors that could endanger the examined region and maintaining a required level of capacities for solving possible crisis, events should be included.
(2.6;3.4>	The level of societal vulnerability is medium. Indicators of societal vulnerability indicate that the vulnerability of examined region (area) is comparable to the average vulnerability in the country. It can be said that the examined region shows a moderate rate of possible impacts caused by specific extreme weather event. Preparedness in terms of material resources and personnel capacities is at a tolerable level, but in the case of large-scale disasters could be insufficient. Within the crisis planning, in the medium-term aspect, tasks aimed at reducing the societal vulnerability level and increasing the level of preparedness for coping with extreme weather, events should be included.
(3.4;4.2>	The level of societal vulnerability is high. The society contains several parts which are very sensitive to extreme weather event. Transport network and society are poorly prepared to cope with the potential extreme event and very sensitive towards the impacts of that event almost in every aspect. The transport network can be so disturbed that it is not possible to provide essential services for society. It is necessary to adopt measures to reduce the society susceptibility and to ensure the higher level of resources and personnel capacities to cope with an extreme weather event.
(4.2;5>	The level of societal vulnerability is very high. The transport network and society contain many critical parts, which make them more vulnerable. In addition, the transport network and society are minimally prepared to cope with respective crisis event and they are also very sensitive towards the effects of the crisis event almost in every respect. Transport networks can be so disturbed that it is not possible to provide essential services for society. It is necessary to make measures to reduce vulnerability as soon as possible because in the case of crisis event, extensive impacts on society can occur.

To set the resulting value of Vulnerability Index, it is necessary to assess the weight of all the Core Factors, Societal Categories, as well as of all indicators (w_I, w_{SC}, w_{CF}).

By summing the values of Vulnerability Indicators and considering indicator weights, values of Vulnerability Societal Category will be calculated according to relation:

$$SC_x = \Sigma_{n=1}^{i} w_{In} I_n \quad (2)$$

where:
SC = Societal Category,
x = designation of Societal Categories,
i = number of indicators within Societal Category (from 1 to n_x),
w_I = weight of Indicators,
I_n = value of Indicators.

Similarly, values of Societal Categories were added to the value of the Core factor. As in the case of other indicators, even all the Societal Categories needed their weight (w_{SC}) to be assessed. The aggregated value of the Core Factor is calculated according to relation:

$$CF_y = \Sigma_{n=1}^{i} w_{SC_n} SC_n \quad (3)$$

where:
CF = Core Factor,
y = designation of Core Factors,
j = number of Societal Categories within Core Factor (from 1 to n_y),
w_{sc} = weight of Societal Category,
SC_n = value of Societal Category.

The resulting value of the VI is obtained in a similar way as it was done in previous steps. The final calculation of the VI is preceded by an extra step, which lies in the calculation of Potential Impact (PI). Potential Impact represents possible level of impacts on society after considering all the aspects which can be in danger (Exposure) and after considering all the societal groups, which are more sensitive to extreme weather impacts (Susceptibility). The weights of Exposure and Susceptibility (w_E, w_S) are counted as well. Sum of weight factors should be equal to 1. The Potential Impact is calculated according to relation:

$$PI = w_E E + w_S S \quad (4)$$

where:
PI =Potential Impact,
E= Exposure,
S = Susceptibility,
w_E = weight of Exposure,
w_S = weight of Susceptibility.

The resulting value for the VI is the sum of the PI weight value and the weight value of Adaptive Capacity:

$$VI = w_{PI} PI + w_{AC} AC \quad (5)$$

where:
VI = vulnerability index,
AC = Adaptive Capacity,
w_{PI} = weight of PI,
w_{AC} = weight of Adaptive Capacity.

The proposed Vulnerability Index can obtain value from 1 to 5. The higher VI value indicates the higher societal vulnerability. The index and related interpretations (Table 1) serve for evaluation of the current state in specific region, as well as for decision making purposes. In describing VI values, some recommendations for vulnerability reduction in terms of crisis planning, risk management and preparedness enhancing are provided. With increasing values of the VI, the time pressure for immediate reaction (vulnerability reduction), as well as the necessity of a higher level of resources and personnel capacities to cope with extreme weather events, is rising. If the given approach was applied to more sectors simultaneously, it is possible to compare them and it allows the identification of more vulnerable areas.

Authors [22], [23] argue that a system might be vulnerable to certain events, but be resilient to others; therefore it is important that while defining vulnerability one must consider hazardous events characteristic to the area under consideration. There could be significant differences between vulnerabilities of the same area to the same hazard with different intensity, e.g. windstorm with speed of 70km/hour or 140km/hour; flood with probability of occurrence 1 in 10 years, and flood with probability of occurrence 1 in 1000 years. Therefore, it is necessary to evaluate vulnerability for each threat or danger separately as it is illustrated in Figure 2.

Other methods for vulnerability analysis based on network modelling are suggested by authors of [24], [25].

5. Conclusions

Measuring and assessing vulnerability is a prerequisite for effective risk analysis and risk reduction, which was also confirmed within the RAIN project execution. If one is able to measure the societal vulnerability, one can adopt adequate measures for a target region and define disaster-risk management and disaster-relief priorities. Moreover, objective information to decision-makers (policy makers and public authorities - at all levels) and for all the relevant stakeholders (community as well) are provided. If the given approach is applied to more areas (regions) simultaneously, it is possible to compare them and it allows identification of the more vulnerable areas or communities. Exploring and understanding of societal vulnerability can addresses social, economic, security and environmental changes within the society, which can help to protect the most vulnerable parts of the society.

Acknowledgements

Publication of this paper was supported by the European Union within the FP7 project No. 608166 “Risk Analysis of Infrastructure Networks in response to extreme weather” and by VEGA grant No. 1/0240/15 “Process model of critical infrastructure safety and protection in the transport sector”.

References

[1] Research Institute of Transport: Risk Analysis of the Transport Sector, Subsectors of Road Transport and Rail Transport (in Slovak). Zilina, 2014.
[2] Ministry of Transport and Construction of the Slovak Republic: Strategic Transport Development Plan of Slovakia by 2030 - Phase II. (in Slovak). Bratislava, 2016.
[3] European Commission: Transport Safety and Security [online]. 2016. Available: https://ec.europa.eu/jrc/en/research-topic/transport-safety-and-security.
[4] SVENTEKOVA, E., DVORAK, Z., LEITNER, B.: Transport Critical Infrastructure in Slovak Republic.: Proceedings of the 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC´17), USA, 212-215, 2017.
[5] ZAGORECKI, A., RISTVEJ, J., KLUPA, K.: Analytics for Protecting Critical Infrastructure. Communications - Scientific Letters of the University of Zilina, 17(1), 111-115, 2015.
[6] O’CONNOR, A.: RAIN Project. Annex I, Description of Work, 2013.
[7] O’CONNOR, A.: RAIN Project. Final Report, Part A, 2017.

[8] BIRKMANN, J.: Measuring Vulnerability to Natural Hazards: Towards Disaster Resilient Societies. United Nations University Press, Tokyo, Japan, 2013.
[9] TAYLOR, M. A. P., D'ESTE, G. M.: Concepts of Network Vulnerability and Applications to the Identification of Critical Elements of Transport Infrastructure. Proceedings of 26th Australasian Transport Research Forum, New Zeland, 2003.
[10] BERDICA, K.: An Introduction to Road Vulnerability: What Has Been Done, Is Done and Should Be Done. Transport Policy, 9(2), 117-127, 2002.
[11] JENELIUS, E., PETEMEN, T., MATTSSON, L. G.: Importance and Exposure in Road Network Vulnerability Analysis. Transportation Research Part A: Policy and Practice, 40(7), 537-560, 2006.
[12] FIELD C. B., BARROS V., STOCKER T. F., DAHE Q., DOKKEN D. J., ELBI K. L., MASTRANDREA M. D., MACH K. J.: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation. Special Report of the Intergovernmental Panel on Climate Change, IPCC, Cambridge University, 2012.
[13] CUTTER, S., BURTON, C., EMRICH, C.: Disaster Resilience Indicators for Benchmarking Baseline Conditions. Journal of Homeland Security and Emergency Management, 7(1), 2010.
[14] GREIVING, S., FLEISCHHUAER, M., LINDNER, C., LUCKENKOTTER, J., PELTONEN, L., JUHOLA, S., VEHMAS, J., DAVOUDI, S., ACHINO, E., LANGELAND, O., LANGSET, B., MEDBY, P., SAURI, D., MARTIN-VIDE, J., OLCINA, J., PADILLA, E., VERA, F., HOLSTEN, A., BACKMAN, B., SCHMIDT-THOME, P., JARVA, J., TARVAINEN, T., KRUSE, S., SCHNELLER, K., CSETE, M., CHICOS, A., TESLIAR, J.: Espon Climate - Climate Change and Territorial Effects on Regions and Local Economies. Applied Research Project 2013/2014, Final Report, IRPUD, Dortmund, 2014.
[15] BURTON, G. CH., KHAZAI, B.: Social Vulnerability and Disaster Resilience in GEM [online]. Proceedings of the 15th World Conference on Earthquake Engineering: Global Earthquake Model Objectives and Activities, Portugal, 2012. Available: http://www.globalquakemodel.org/media/cms_page_media/2012/11/14/SS1_GEM_3_SocialVulnerability.pdf.
[16] CARDONA, O. D., ORDAZ, M. G., MARULANDA, M. C., BARBAT, A. H.: Use of the Disaster Deficit Index in the Evaluation of the Fiscal Impact of Future Earthquakes [online]. Intersections, 6(2), article No. 1, 2009. Available: http://intersections.ro/archive/2009/No02/Intersections_V06_No02_01.pdf.
[17] CUTTER, S. L., BORUFF, B. J., SHIRLEY, W. L.: Social Science Quarterly. Social Vulnerability to Environmental Hazards, 84(2), 242-261, 2003.
[18] NEDELIAKOVA, E., HUDAKOVA, M., STEFANCOVA. V.: Application of risk Management Methods in Transport Companies. Proceedings of 21th International Scientific Conference Transport Means 2017, Lithuania, 237-241, 2017.
[19] ISOARD, J., GROTHMANN, T., ZEBSICH, M.: Climate Change and Adaptation: Theory and Concepts. The Workshop: Climate Change Impacts and Adaptation in the European Alps: Focus Water, 2008.
[20] SCHNEIDERBAUER, S., PEDOTH, L., ZHANG, D., ZEBISCH, M.: Assessing Adaptive Capacity within Regional Climate Change Vulnerability Studies - An Alpine Example. Adaptation to Natural Hazards, 2011.
[21] SMIT, B., WANDEL, J.: Adaptation, Adaptive Capacity and Vulnerability. Global Environmental Change, 16(3), 282-292, 2006.
[22] DILLEY, M., BOUDREAU, T. E.: Coming to Terms with Vulnerability: a Critique of the Food Security Definition. Food Policy, 26, 229-247, 2001.
[23] WISNER, B., BLAIKIE, P., CANNON, T., DAVIS, I.: At risk: Natural Hazards, People's Vulnerability and Disasters, 2nd ed. Routledge, London, 2004.
[24] KHAKZAD, N., VAN GELDER, P.: Vulnerability of Industrial Plants to Flood-Induced Natechs: A Bayesian Network Approach. Reliability Engineering System Safety 169, 403-411, 2018. DOI:10.1016/j.ress.2017.09.016
[25] LI, H., HU, X., GUE, X., XU, Z., VAN GELDER, P. A.: New Quantitative Method for Studying the Vulnerability of Civil Aviation Network System to Spatially Localized Hazards. International Journal of Disaster Risk Science, 7(3), 2016. DOI: 10.1007/s13753-016-0098-1

kamUNikácie
COMMUNICATIONS

Andrej Velas - Tomas Lovecek - Jan Valouch - Jacek Dworzecki - Eva Vnencakova*

TESTING RADIO SIGNAL RANGE OF SELECTED COMPONENTS

The radio signals range of selected wireless components of security systems is defined by the area within which components can communicate properly. In practice, the range of communication between components is often insufficiently taken into account, which results in the system malfunction. There are cases where the radio signal range of wireless components was inadequate due to use in an environment constructed from non-transmitting materials.

The installation of wireless systems requires the implementation of a testing methodology of radio-communication range and its continuous improvement. Currently, the procedures within EN 50 131-5-3 and EN 300 220-1 standards can be used to test the wireless components, but they do not target the range between wireless components.

Dependability and functionality are the main attributes of electrical security systems and need to be verified by testing the range of wireless components.

Keywords: *alarm systems, signal range, wireless, communication, motion detector*

1. Introduction

Security systems are nowadays a common inseparable standard of operations, facilities, family houses and other utilities. As technology evolves, the classic Intruder alarm systems (IAS) wired components are no longer adequate and need to be complemented by the wireless ones. Those have become synonymous with low cost, time saving, easy implementation, easy maintenance and flexibility. They are suitable for spaces where classic cabling (already occupied premises, historical buildings, etc.) cannot be conducted.

However, wireless communication between components also has its limits. Those are the specific limits of the signal range, which affect the dependability of the entire security system. It is thus important to define the problem of the signal range of selected wireless components of the security systems; to find out to what extent the range of the communication signal is influenced by the environment; to examine whether the range can be determined in general by using a specific parameter. This issue is important for effectively managing the selection and placement of selected wireless components when designing and implementing wireless IAS [1].

The 433 MHz and 868 MHz bands have different range, functionality and dependability parameters that can be affected by compliance with the wireless component assembly recommendations. The range is also affected by the attenuation properties of materials that are different for each frequency and can be measured by the spectral analyzer. For the range calculation, a component parameter can also be used: the radiated signal strength that can be obtained by measuring in a non-impact chamber [1], [2]. This work describes testing for which Jablotron wireless components were used. The testing took place at the premises of dormitories of the University of Zilina's and at the CEBIA-Tech center in Zlin.

1.1 Wireless radio communication of security system components

Wireless communication works on the principle of telegraph, that is, the components communicate with each other through short messages at a certain time on frequencies belonging to ultra-short waves [2]. The messages are encoded with the information about the state of the monitored object.

In practice, the electromagnetic field intensity (E_x) parameter is used to calculate the range. Its value is determined by measuring, in a remote field where the capacitance and inductive coupling is not applied, the energy transmitted by electromagnetic

* [1]Andrej Velas, [1]Tomas Lovecek, [2]Jan Valouch, [3]Jacek Dworzecki, [1]Eva Vnencakova
[1]Department of Security Management, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Security Engineering, Faculty of Applied Informatics Tomas Bata, University in Zlin, Czech Republic
[3]Police Academy in Szczytno, Poland
Email: andrej.velas@fbi.uniza.sk

Table 1 *Technical Parameters of the JA-60 Series Components, [5], [6]*

Technical Parameters - UC- 260 Annunciator	
Working frequency	433.9 MHz
Way of communication	One-way communication
Technical Parameters - JA- 60P Detector	
Range	100 m to direct visibility
Working frequency	433.9 MHz
Way of communication	One-way communication
Technical Parameters - JA- RC11 Remote Control	
Range	30 m to direct visibility
Working frequency	433.9 MHz
Way of communication	One-way communication

Table 2 *Technical Parameters of the JA- 100 Series Components, [5], [6]*

Technical Parameters - Module JA- 110R	
Working frequency	868.1 MHz
Way of communication	Two-way communication
Technical Parameters - Detector JA- 160PC	
Range	300 m to direct visibility
Working frequency	868.1 MHz
Way of communication	Two-way communication
Technical Parameters - Detector JA- 151M	
Range	200 m to direct visibility
Working frequency	868.1 MHz
Way of communication	Two-way communication
Technical Parameters - Detector JA- 180B	
Range	100 m to direct visibility
Working frequency	868.1 MHz
Way of communication	One-way communication
Technical Parameters - Remote Control JA- 154J	
Range	30 m to direct visibility
Working frequency	868.1 MHz
Way of communication	Two-way communication

waves, and the ratio between the components of the E - electric field strength and the H - magnetic field strength is given by the impedance of the wave saturated environment.

For the electric field strength, the following applies:

$$E_x \approx \sqrt{(30*P)/r} \quad [V/m; kW,km] \qquad (1)$$

where P is the power of the tested device and r is the distance of the tested device from the measuring device. Measurement takes place either in the open space or in the non-impact chamber, the properties of which are defined in the relevant standards. The uncertainty of electromagnetic radiation intensity measurement can be ± 4 dB [3].

As soon as we know the effective radiated power, we can already calculate the intensity of the electric component of the electromagnetic field at a particular distance from the transmitting antenna [4].

2. Testing methods

Components of the Jablotron company operating at 433 MHz and 868 MHz with declared ranges of 30, 100 and 300 meters were tested.

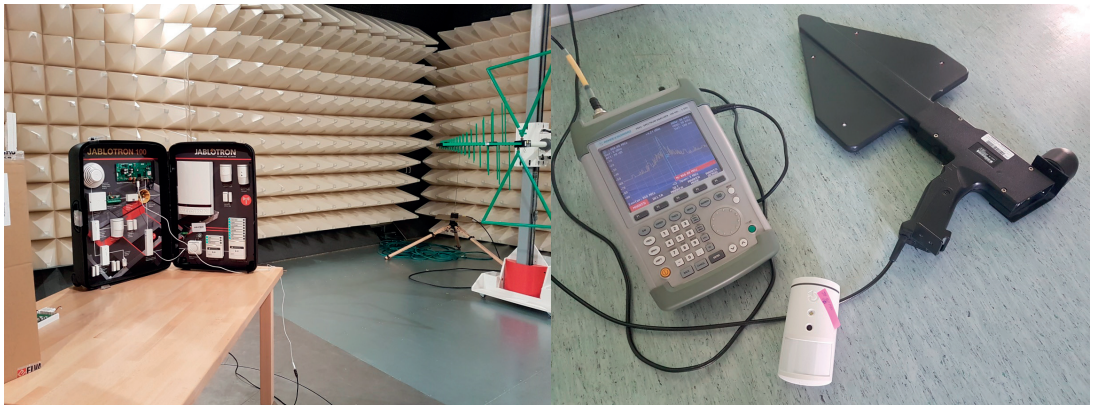


Figure 1 *The Franconia non-reflecting chamber and the spectrum analyzer and the antenna during testing*

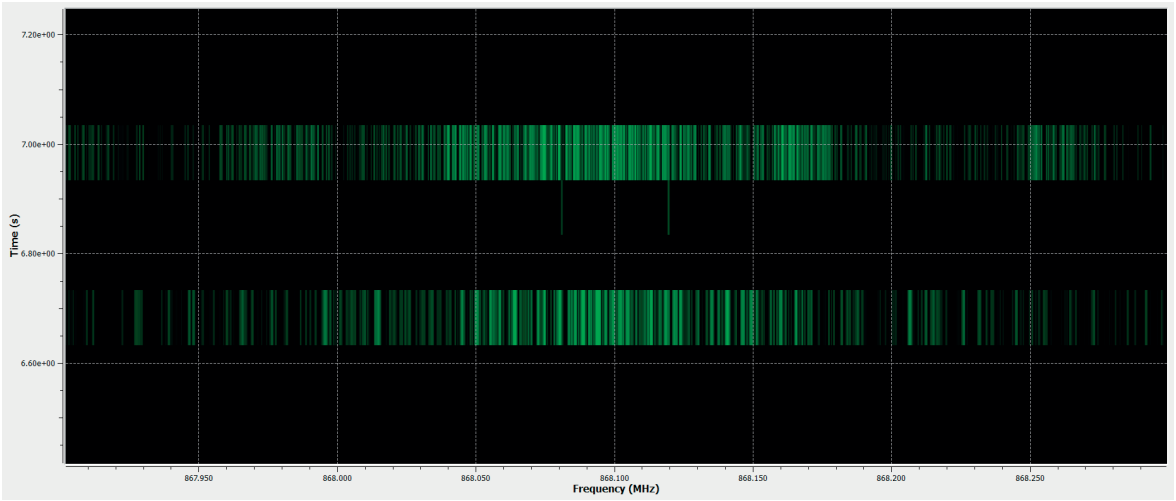


Figure 2 *Frequency spectrum detail when transmitting an alarm message from the periphery*

- JA- 60 series (UC-260 Wireless Acoustic Annunciator, JA-60P Wireless PIR Detector, JA- RC11 Remote Control), see Table 1.
- JA- 100 series (JA- 160PC wireless PIR video camera motion detector, mini JA- 151M wireless magnetic door opener, JA- 180B wireless glass-break detector and JA- 154J two-way remote control, see Table 2.

Besides the tested components, the following devices for testing were used, as well:

- **The Franconia non-reflecting chamber** - simulates test conditions in the open space, where the signal is not reflected but absorbed. Together with the R&S EMC 32 measuring system it is used for measuring antennas and EMC, Figure 1.
- **FSH3 spectrum analyzer with antenna** – used to measure signal strength in terrain.
- **EMC32 software** ensures complete control and remote control of instrumentation in a non-impact chamber.
- **USRP N210** - used to collect and analyze wireless signals [7].

The sequential steps of testing selected components of the 60 and 100 series were as follows:

- Radio communication observation,
- Measurement of radio signal strength,
- Measurement of attenuation size,
- Practical range testing.

2.1 Radio communication observation

The measurement was performed in a non-impact chamber. At 4 meters distance from the component, the measuring antenna was located at the same height as the tested component. During the measurement, the antenna was polarized and triggered an alarm. Through the USRP N210, the communication of peripherals with the control panel was monitored. With this observation, images of the monitoring and alarm message were received as well as information about the way of communication. Figure 2 shows an example of the PIR JA- 60.

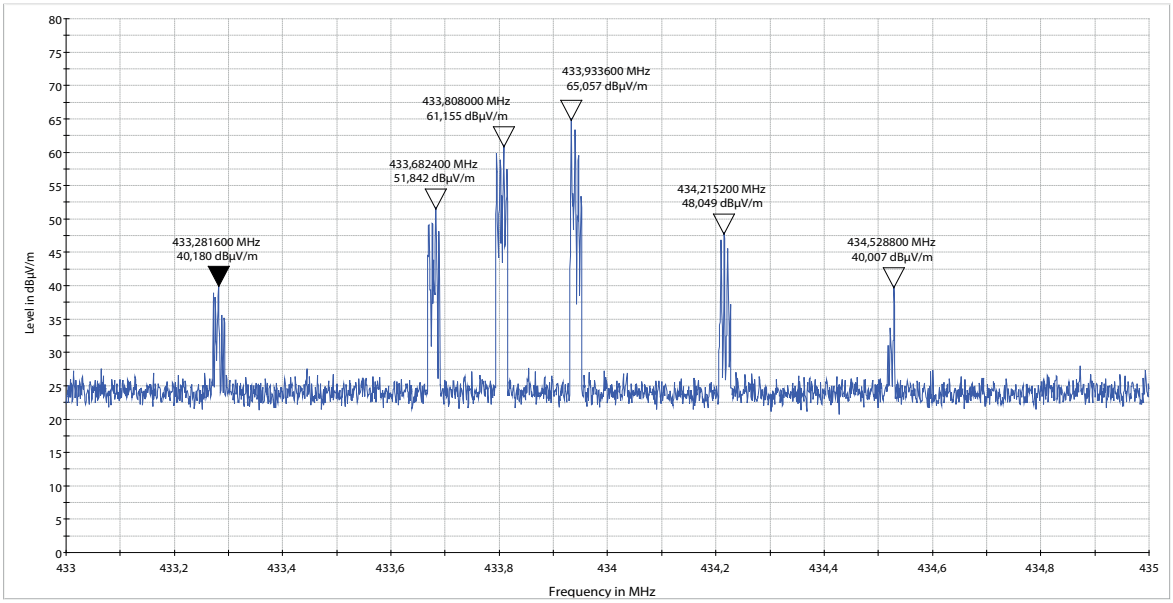


Figure 3 *JA- 60P signal emission spectrum in the EMC32 program*

Table 3 *Table of parameters for calculating effective radiated power*

Component	Electromagnetic intensity (dBµV/m)		Frequency (MHz)	Distance (MZ-TZ (m)	Intensity (dBµV/m)→(V/m)	Component power (mW)
	Horizontally rotated antenna	Vertically rotated antenna				
JA- 60P	45.851	65.057	433.8	4	0.00179	0.00170883
JA- RC11	51.606	77.74	433.94	4	0.007709	0.03169558
JA- 160PC	80.497	101.226	868.09	4	0.1151596	7.07291971
JA- 151M	94.756	99.657	868.129	4	0.0963274	4.94878661
JA- 180B	84.574	100.465	868.089	4	0.1054994	5.93606609
JA- 154J	81.951	90.163	868.112	4	0.0322218	0.55373086

2.2 Measurement of radio signal strength

The following intensity measurement was completely controlled by the EMC32 program according to the normative procedure for measuring the radiated signal in the non-impact chamber [8], [9]. The program, using a measuring antenna with 4 m distance from the test component, scanned the RF bands according to the set parameters and displayed the resulting spectrum of radiated signals on the screen, see Table 3. The resultant spectrum with the values was used to calculate additional parameters. Figure 3 shows the signal emission spectrum from the JA- 60P PIR detector.

2.3 Attenuation measurement

Measurements of the environment attenuation were carried out, as well. There were either a door or a window, a ceiling, or a wall between the spectral analyzer antenna and the component. The measurement was performed at the height of 1.5 m by directing the antenna directly to the wireless component transmitting alarm messages. One of the above-mentioned environments was between the antenna and the component. After setting the parameters, the spectral analyzer shows the frequency spectrum with the measured values, Figure 4 and Table 4.

2.4 Practical Range Testing

After the previous measurements, the practical testing was performed. In that measurement, the two methods were used, namely the walk-through tests and a simple function test. The component was placed at a height of 2 m on a non-conductive stand and in a position that most closely matches normal use. Then, the distance to the PBX, using a laser meter, was measured at the border points.

In Figure 5 are presented the measured ranges of components with an operating frequency of 433 MHz. The control panel

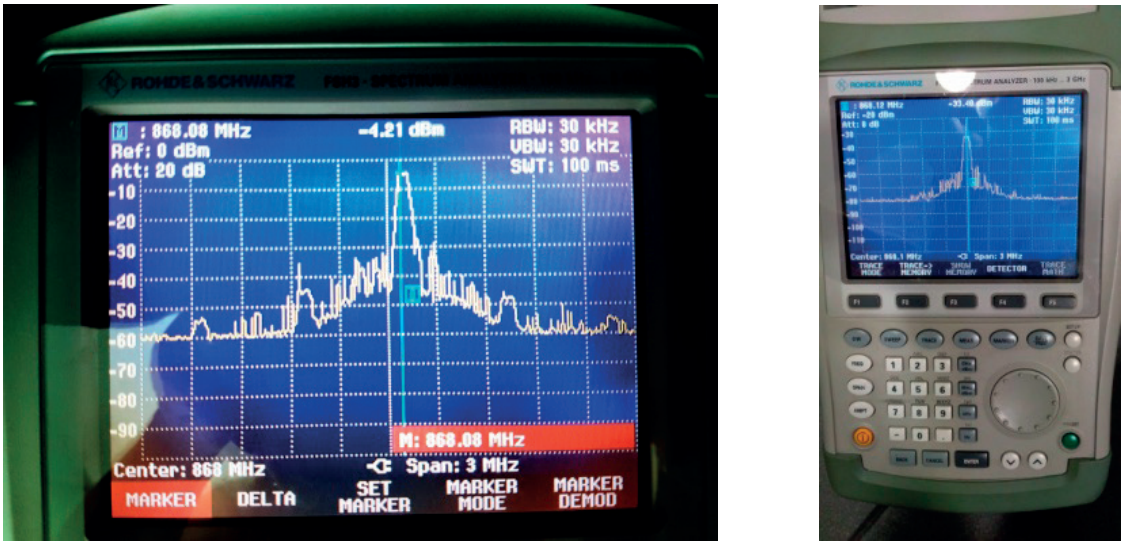


Figure 4 *Demonstration of the measured value of the environment attenuation*

Table 4 *The magnitude of the signal attenuation in the environment at 868.1 MHz*

Environment	Attenuation (dB)
Direct visibility (1 m),	4
Window	4
Door (wood - 0.035 m)	11
One wall (non-load bearing - 0.1 m)	19
Two walls (load bearing - 0.2 m and non-load bearing 0.1 m)	28
Ceiling (reinforced concrete slab - 0.25 m)	34

Table 5 *Comparing parameters of selected components*

	JA- 60P	JA- RC11	JA- 160PC	JA- 151M	JA- 180B	JA- 154J
Declared range (m)	100	30	300	200	100	30
Signal intensity (dBμV/m)	65.1	77.7	101.2	99.7	100.5	90.1
Power (mW)	0.0017	0.0317	7.0729	4.9488	5.9361	0.5537
Measured range (m)	30	19	54	43	46	37

was located in the center of the building. The range of the communication signal did not exceed the boundary of the building.

Diagram in Figure 6 shows the reach of components with a working frequency of 868 MHz. The control panel was also placed in the center of the building. The ranges have significantly exceeded the boundaries of the building and are only approximate.

3. Results

The results of the measurement and testing are shown in the following tables and charts. First, in Table 5 are compared all the tested components with respect to the parameters that were looked at. The declared range with the measured one was compared. The actual measured values were, in almost all the cases, clearly lower than the declared range.

Another chart (Figure 7) compares the frequencies of 433 MHz (JA- RC11) and 868 MHz (JA- 154J). The given frequencies represent remote controls with the same declared range. Components at 868 MHz have a larger range [10], [11]. The magnitude of the range in this case could have been influenced by the fact that the 868 MHz band is less disturbed and thus the signal quality is better [12].

When comparing the results, a case was discovered when the JA- 180B component with a smaller declared range had a higher measuring range than the JA- 151M, Figure 8. Since components work at the same operating frequency, have the same antennas and have the same test conditions during the testing, the conclusion was reached that power has a significant impact

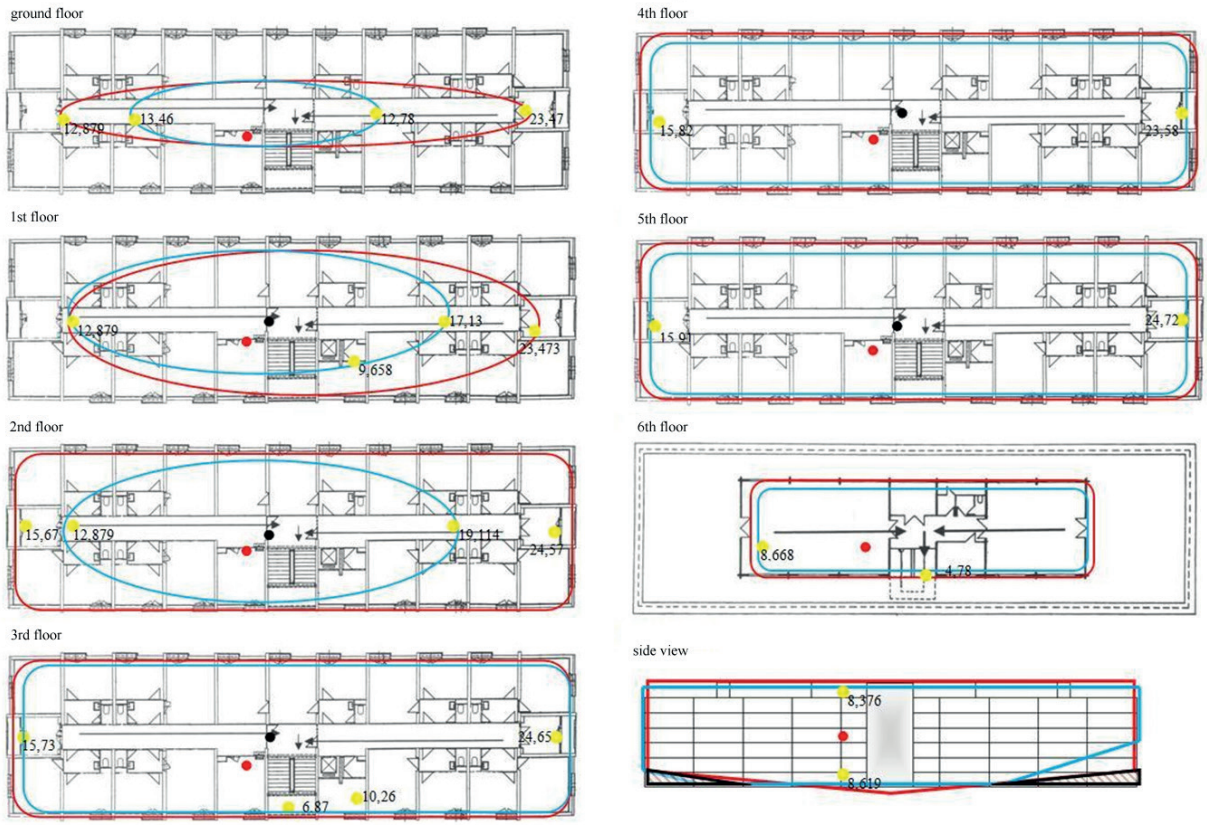


Figure 5 *Sketches of the signal range for JA- 60P (marked by the black dot) and JA- RC11 (marked by the red dot). They were located in the center of the building on the 3rd floor*

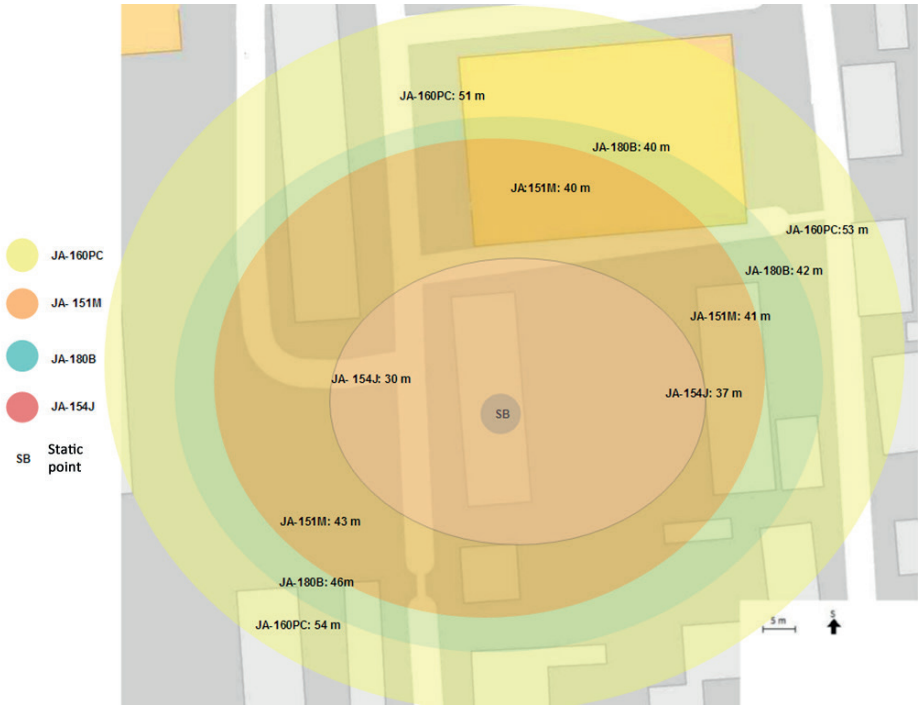


Figure 6 *Sketches of the signal range of JA- 160PC, JA- 51M, JA- 180B and JA- 154J*

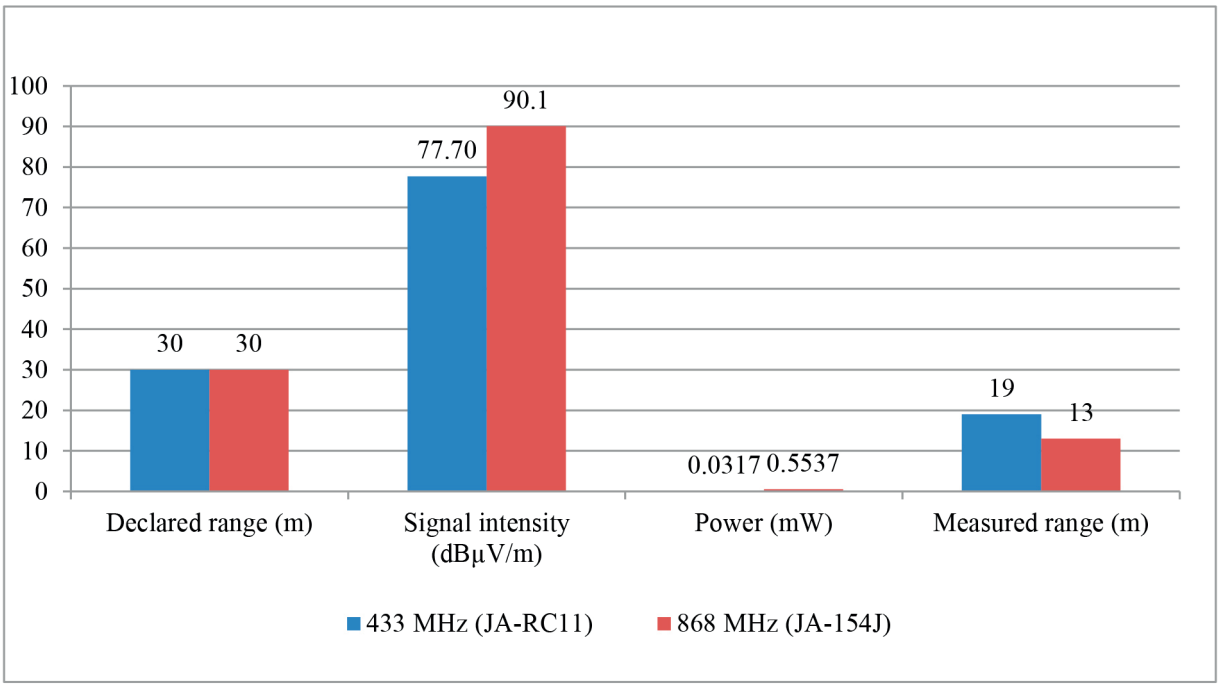


Figure 7 Comparison chart for JA- 60 and JA- 100 series components

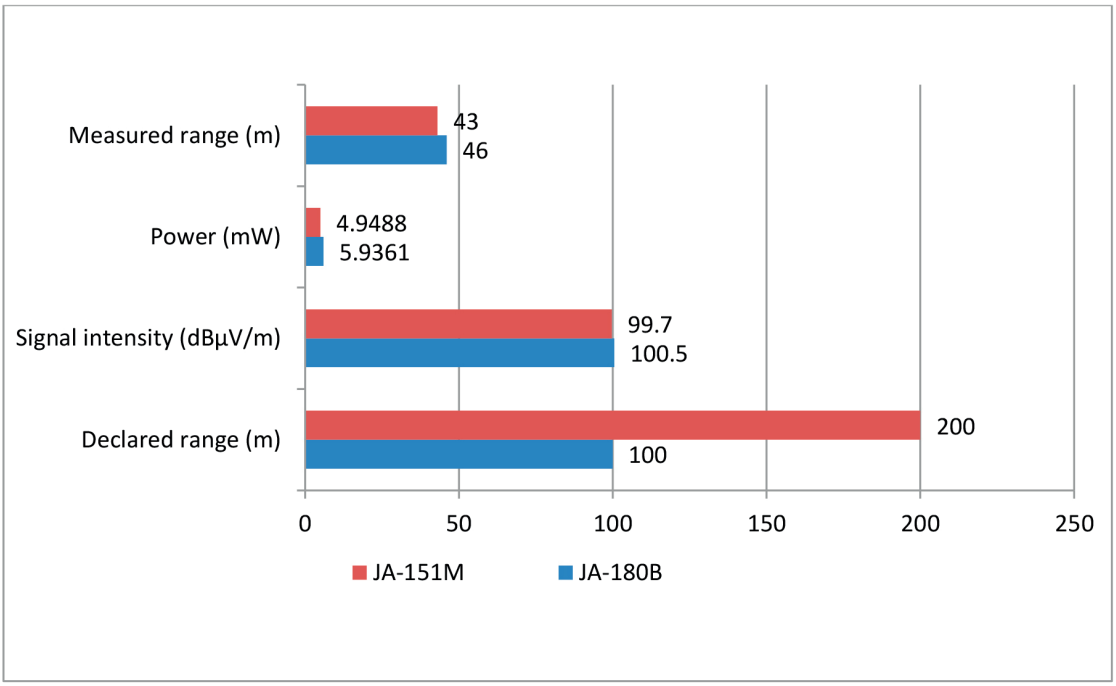


Figure 8 Graph showing power impact on range

on range. From this finding, it can be stated that the determined declared range may be incorrectly determined because there is no normative way of measuring the range.

The magnitude of the environment attenuation impact was impossible to predict or calculate in advance. The intensity of the signal was affected by the environment so much that a difference of up to 27 m occurred between the different lengths of the JA-160PC component transmission paths. At 868 MHz, the signal has a low permeability through the materials, so it is assumed that it was reflected back to space and spread out of the window. While

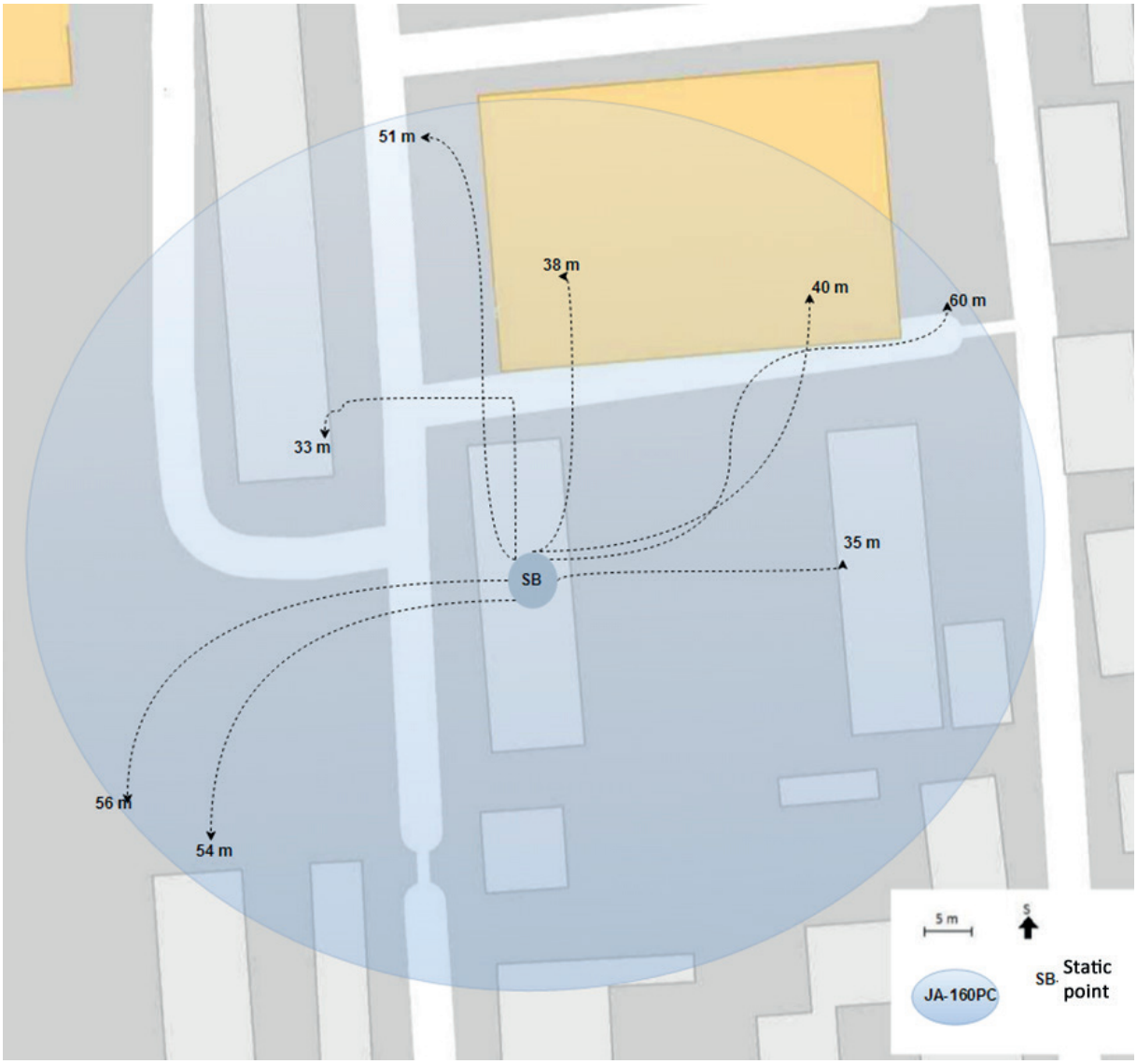


Figure 9 *Outline of JA- 160PC signal transmission routes from periphery*

there was a range of 60 meters in the open space, it was only 33 meters inside buildings, Figure 9.

4. Discussion

- The problem of radio communication range cannot be calculated precisely and should therefore be verified at the installation site. In addition, the attenuation of typical environments, such as the corridor, the door and the walls, cannot be estimated beforehand either. The attenuation of the environment cannot be generalized, calculated or solidly considered.
- The 433 MHz frequency range is much smaller, which was confirmed during the 6-storey building test.
- The 868 MHz frequency is less disturbed and more convenient as a working environment for security systems. The range of the 868 MHz frequency band is much larger, with a range of 33 to 60 meters outside the building when placed in the center of the 6-storey building. It was, however, very influenced by reflections from objects and the environment.

4.1 Options for use

In the case of a larger object or an object of less penetrable material without windows, it is advisable to use the JA- 150R

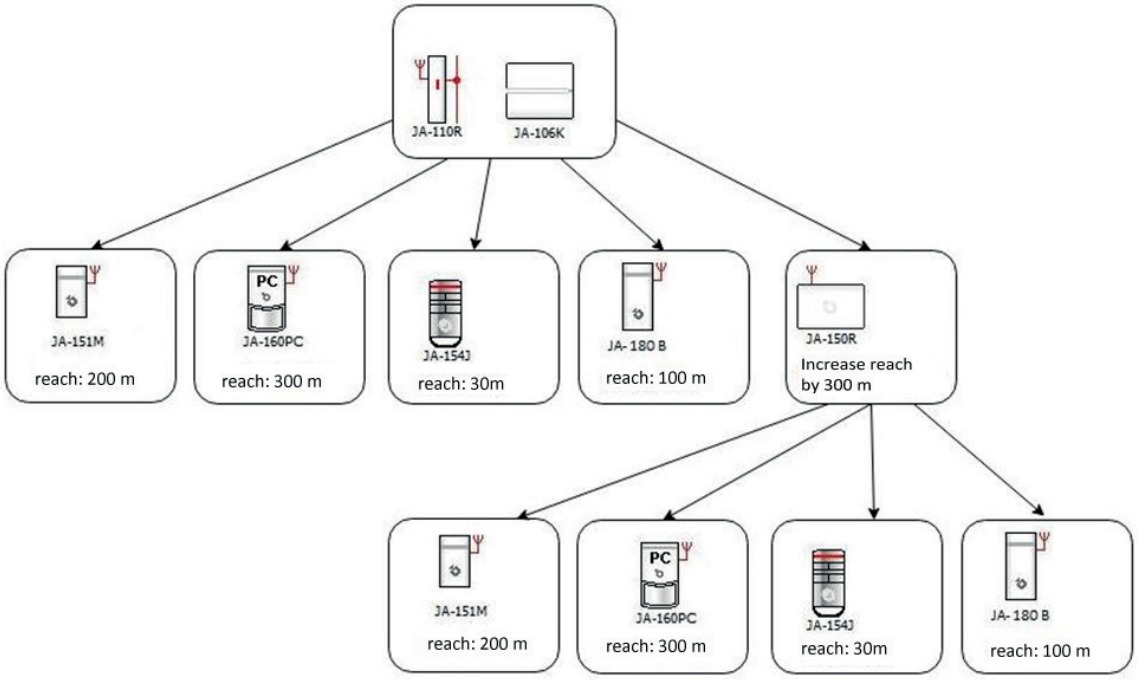


Figure 10 *Typology of a wireless system to increase reach*

signal repeater, which extends the range up to an additional 300 m, Figure 10.

4.2 Conclusions

In this area, it is necessary to introduce the normative conditions and layout of the test facility and the testing procedure of the declared range in order to avoid errors as for instance the JA- 151M and JA- 180B components.

On-site testing should be performed in the way that the tested component is not attenuated and should therefore be placed on a stand that does not have attenuating properties. It was found that even the declared impacts are not determined correctly due to which this testing is not subject to any norm. Different test site spacing and test conditions can cause enormous differences in the calculated range under these conditions.

The range tests should always be carried out on the same site (same conditions and arrangement) and under comparable weather conditions. The real range within the limits of direct visibility in the open space should be measured on the x samples. From the measured values it is necessary to calculate the average values and then declare them. At the same time, it is necessary to state, in the technical parameters, that the actual range is lower in the built-up conditions [13], [14].

The found pros and cons of wireless IASs have been evaluated in the following points:

- The IAS range, installation flexibility, installation speed and great variety of wireless components to choose from, are considered as its benefits.
- As a downsides of such a system, are seen a high degree of environmental impact, the necessity to verify suitability of the component location on site, the inconsistency of the declared range with the real one, and insufficient protection against the loss of signal with the wireless periphery.

References

[1] LOVECEK, T., VELAS, A., KAMPOVA, K., MARIS, L., MOZER, V.: Cumulative Probability of Detecting an Intruder by Alarm Systems. Proceedings of the 47th IEEE Annual International Carnahan Conference on Security Technology (ICCST 2013), Colombia, 1-5, 2013.

[2] VELAS, A.: Intruder Alarm Systems. University of Zilina, Zilina, p.104, 2010.

[3] HOFREITER, L., MARIS, L., LUKAC, L., KISTER, L., GRZYWNA, Z.: New Approaches to the Analysis of the Security Environment and Their Importance for Security Management. Communications – Scientific Letters of the University of Zilina, 17(1), 99-104, 2015.

[4] POSPISILIK, M.: Measurement of Disturbing Signals (EMI) Pre-Certification. UTB, Zlin, p. 62, 2015.
[5] SVACINA, J.: Electromagnetic Compatibility: Principles and Notes. 1. Technical University, Brno, p. 156, 2001.
[6] Electronic Control and Automation Technology [online]. Jablotron Slovakia, 2008. Available: http://www.jablotron.sk.
[7] System JABLOTRON 100 [online]. Jablotron Slovakia, 2014. Available: http://www.jablotron.sk.
[8] Electromagnetic Compatibility Measuring Instruments at Tomas Bata University in Zlin [online]. UTB, Zlin, 2015. Available: http://www.utb.cz/fai/struktura/pristroje-pro-mereni-elektromagneticke-kompatibility.
[9] General Authorization no. VPR-10/2014 for the Use of Frequencies for the Operation of Non-Specified SRD Broadcast Radio Transmitters.
[10] General Authorization no. VPR-11/2014 for the Use of Frequencies in the Frequency Band 868.6 MHz - 869.700 MHz for the Operation of Short-Range Radio Equipment in the Category of High-Reliability Low Duty Cycle Equipment.
[11] NAGY, P.: Security Systems: Control and Indicating Equipment of IAS. Faculty of Electrical Engineering, University of Zilina, Zilina, p. 26, 2005.
[12] Signal Distribution and Radio Systems Installation [online]. Eldes, 2014. Available: http://bezpecnadomacnost.sk/files/Instalacia_bezdrotovych_systemov.pdf.
[13] SLANAR, V.: Wireless Component Communication, 2017. E-mail from viktor.slanar@jablotron.cz to vnencakova.e@gmail.com.
[14] 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, 9(4), 351-365, 2013. DOI: 10.1504/IJEM.2013.059879

Zuzana Kurillova - Lukas Fischer - Thomas Hoch*

BEHAVER - BEHAVIOURAL PATTERNS VERIFICATION FOR PREVENTION OF PHYSICAL PENETRATION USING IDENTITY THEFT

Nowadays every provider of critical infrastructure is obliged to use alarm systems - mainly simple surveillance CCTV cameras - to increase security and safety of those objects. Yet such systems have proven ineffectual in preventing security disrupting situations, such as identity theft, as the most they can do is offer evidence to identify perpetrators of criminal acts once they have occurred. To use them for crime prevention, specially trained personnel need to monitor all screens constantly on the look-out for potentially dangerous activity - which is financially and time-consuming and prone to mistakes.

This study aims at developing semi-automatic video surveillance technologies, which are able to detect events of changed behaviour of employees in relation to their standard behaviour - this means for example cases of identity theft, possible blackmail of a person, or safety disrupting cases - an employee might be sick or under influence of drugs what may lead to potentially dangerous acts.

Keywords: *behavioural patterns, CCTV surveillance cameras, crime prevention, identity theft*

1. Introduction

Nowadays, protected premises are mandatorily equipped with closed-circuit television (CCTV) infrastructure, which proves to be ineffectual for the prevention of identity theft. Resource constraints often make it impossible to have human monitoring of all the CCTV screens all of the time in order to recognize any inappropriate access in protected premises of soft targets. Criminals, using stolen proofs of identification such as cards, documents or passwords can freely enter, unrecognized by the CCTV monitoring operatives. Biometrics controls are not always applicable due to technical, economical and ethical reasons.

Use of identity theft is one of the most probable scenarios in targeting of the protected premises. To emphasize the importance of the BehaVer project, the following quote is used from Mr Alan Gooden, former (to 2017) National Identity Crime Operational Lead UK Policing & Identity Security Adviser to Home Office UK Government Dept.: *" In my experience it is extremely difficult to quantify with any confidence the full extent of any form of Identity Theft / Impersonation owing to the way that crimes are recorded. This is because the Identity Theft is an enabler to the resultant offending / crime and as a consequence is not recorded as the crime in and of itself.*

It is however clear that Identity Theft and Impersonation is an increasing threat to society within multiple forms of criminality most notably theft and fraud and it follows that acting as an enabler to corruption and insider threats within high value / risk institutions the threat is equally and proportionately increased and will continue to be so for the foreseeable future. Identity related crime is responsible for losses within all sectors of the economy including business, charity, government, as well as enabling terrorist threats. The targeting of staff members by organised crime groups, coercing them into providing sensitive information or to help the criminals facilitate criminal activity is a very real concern. Law enforcement requires enhanced tools to address this burgeoning threat as a matter of urgency" [1].

The principal aim of this project is to put in place robust, real time identity verification measures and intervention strategies to stop an attacker with the stolen identity of an authorized person before the attack.

Currently three levels of identity control are identified:

- virtual (specified by logins and passwords, PINs, certificates or digital signatures [2], [3], [4]),
- document-based (defined by documents or identification cards like a passport, badge, drivers licence and similar [5]), and

* [1]Zuzana Kurillova, [2]Lukas Fischer, [2]Thomas Hoch
[1]Department of Security and Safety Research, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Software Competence Center Hagenberg GMBH, Austria
E-mail: Zuzana.Kurillova@fbi.uniza.sk

- human-biometrics-based (e.g. via fingerprint [6], [7] or retina).

The strongest protection can be reached when there is a combination of multiple identity controls. For example - a combination of a password (something to know), an identity card (something to have) and a biometrics check (something to be) [8] should decrease the possibility of identity theft to the lowest possible measure.

However - both virtual, document-based identification and even some biometrics controls can be duped or they are not applicable due to technical, economic or ethical reasons. For example, face recognition can be easily circumvented [9], while duping of behaviour needs intensive observation of the person, which makes these kind of attacks time consuming.

2. BehaVer framework

The proposed solution described in this paper, the BehaVer framework, will offer an easy to implement solution for identity control of authorized persons in the protected premises that can be tailored for the adaptation within existing CCTV infrastructure. The proposed software based solution uses deep learning of big data extracted from the cameras and intelligent video surveillance to recognize changes of the actual behaviour of the authorized persons in comparison to their standard behavioural patterns.

The BehaVer framework is technically easy to implement in the protected premises (and therefore a robust yet economically viable solution). Video surveillance by the CCTV cameras for example is already wide spread and is installed for the daily use inside the protected premises. As such, only the software needs to be installed and some slight changes in the working environment are recommended in order for the benefits of the BehaVer system to be realised. This software, together with a standard for prevention of physical penetration using identity theft and an e-learning platform, will offer an effective, financially viable and technically accessible solution for protected premises EU-wide [10].

Moreover, the proposed software also offers the effective use of already installed CCTV infrastructure in the protected premises to increase security and safety of those facilities. So far, such systems have proven ineffectual in preventing security disrupting situations, such as identity theft. Rather, they have been utilised only as means of evidence gathering to identify perpetrators of criminal acts - once they have occurred. The use of behavioural detection systems for the crime prevention, such as identity theft, requires specially trained personnel to monitor all screens constantly on the look-out for potentially dangerous activity - which is financially untenable, time-consuming, as well as being prone to mistakes. Security personnel would, for example, need to monitor all authorized persons and their privileges in the protected premises all the time at all the locations.

The primary goal of this project is to develop the **BehaVer software** to prevent identity theft based on video surveillance of physical behavioural patterns (i.e. how the person usually behaves), especially when other identity control mechanisms are outmanoeuvred or are not deemed applicable or sufficiently robust. The project will propose a novel technology that can be used to check physical identity of authorized persons based on analysis of usual behavioural patterns of authorized persons - how do they park a car in the parking lot - how do they show their badge or - which door they normally use etc. In the case of a stolen identity of an authorized person in the protected premise, the proposed BehaVer software could recognize that the person's actions were inconsistent with usual patterns of behaviour and thus detect and raise awareness of a potential threat in real time. Based on big data analysis of video surveillance of the authorized persons' daily behavioural patterns, the BehaVer project will develop novel technologies that are very difficult to overcome or manipulate. With the amount of data collected, the technology will become more and more accurate, due to constant learning of behavioural patterns of the authorized persons. Furthermore, the technology will be cost-effective and easy to implement in protected premises, as it uses already existing infrastructure of surveillance cameras that are mandatorily installed in the protected premises, but so far ineffectively used.

The secondary goal of the project is to develop a **standard for prevention of the physical penetration using identity theft**. It will present the knowledge and implementation of selected methods and useable approaches. The application of this standard in protected premises will support the prevention of identity theft.

The tertiary goal of the project is to develop an **e-learning platform for prevention of the physical penetration using identity theft** based on the above mentioned standard and software. In a user friendly way, the BehaVer e-learning platform will present the knowledge collected in the project to be used for further education of stakeholders. It will also be used as a training repository and toolkit for the education of practitioners before the field demonstration of the BehaVer software (Figure 1).

3. Technology for prevention of the physical penetration using identity theft

In the following section the technology for prevention of identity theft of an authorized person will be described, to explain the proposed solution. The technology is based on:

- Surveillance from the CCTV cameras that are already mandatorily installed in protected premises,
- Token, in the form of a mobile phone, is carried by the authorized person - this helps re-identification of a person at each checkpoint. (At this stage of development, the token is still necessary. One of the aims of the project will be to eliminate this token from the technical infrastructure - so that

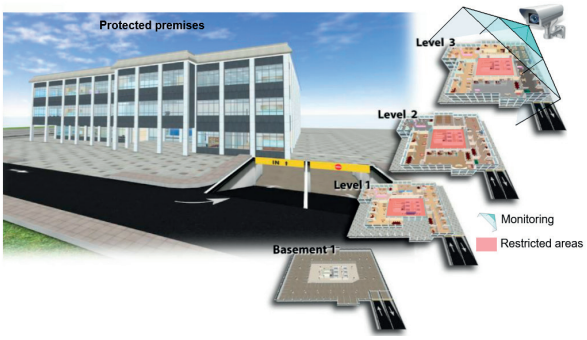


Figure 1 *Premises containing monitored restricted areas protected and/or operated by practitioners and other strategic operators*

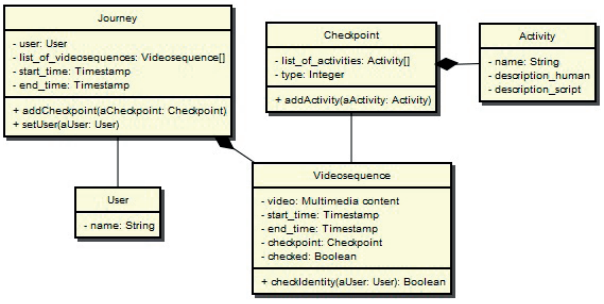


Figure 2 *Object-oriented diagram of the information system. Each journey contains video sequences of the user's presence near a checkpoint*

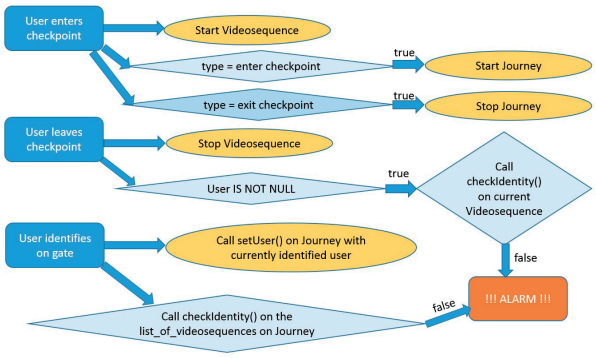


Figure 3 *Event-driven diagram to describe the system*

the person can be re-identified on different cameras without the token.)

- Prototype software that will process the real-time data from the cameras and the token and analyse them accordingly to the techniques developed in the project. It will compare previous behavioural patterns with the actual one of the authorized person. The output of the prototype software will be determination if the behaviour of the authorized person is consistent or inconstant with established behavioural patterns. Finally, in the event of a change, a notification will be sent to authorised security personnel in order to initiate further checks and validation.

The protected premises contain various "checkpoints" - these are places where CCTV cameras are installed. Each time an authorized person enters the area under control, it means he or she will approach an entering checkpoint with a CCTV camera, the "journey" will be created and started in the system. This journey will contain all the video sequences of the authorized person until he or she leaves the controlled area at the exit checkpoint (Figure 2).

Each checkpoint contains a list of "activities", selected from the Key Behavioural Pattern (KBP) list which are analysed (parking the car, entering the doors, showing the badge). These activities are described in a human language to be understandable for the technical staff and in the script language (Motion Description Language - MDL), to be understandable for the computer (see Activity in Figure 2).

Event-driven architecture [11] will be used for implementation of the system, as it really suits the nature of the mechanism - where the activity is triggered by the events that occur in the surveillance area. As detailed in Figure 3, a user (authorized person) either:

- Enters the checkpoint area,
- Exits the checkpoint area, or
- Identifies himself/herself at the gate (for example with a card, password and/or biometrics)

When an authorized person enters a checkpoint, the video sequence will start. When he or she leaves the checkpoint, the recording will stop. In the spots before identification of the authorized person at the gate, those video sequences are only recorded. When the authorized person identifies at the gate (by an object, like a card, knowledge, like a password and/or a biometrics), the Journey will be matched with the User and the *checkIdentity* process can start - on all the previous activities of the user (in the parking lot, entering the area).

The *checkIdentity* process will be based on comparison of the behavioural patterns of the examined authorized person with the current activity. The behavioural patterns will be the result of the big data analyses of the previous daily behaviour of the user and deep learning processes will give the sensitivity of the differences of the behaviour.

With every other checkpoint after the gate, the *checkIdentity* process will be performed for each activity defined in the checkpoint. Authorised security personnel will be notified immediately, if the patterns do not match with the pre-recorded behaviour (in the limits of the sensitivity). The process of constant deep learning will be optimized to prevent false cases, but to identify the real emergency cases.

4. Methodology

The essence of this project is firstly the creation of a software tool to prevent identity theft of an authorized person, based on intelligent video surveillance of daily behavioural patterns recorded on surveillance CCTV cameras. If the actual behaviour

of the authorized person changes in comparison to the behavioural patterns - there is a potential of identity theft and appropriate security authorities will be notified. Secondly, it aims to create a standard for the prevention of physical penetration using identity theft. The third goal is to create an e-learning platform that presents the knowledge accumulated by the project in a user-friendly way. These three outputs will provide a strong prevention foundation against the physical penetration to protected premises using identity theft.

The following steps need to be taken to create the software:

- Data Collection and Requirements Analysis - Firstly, all the relevant data is collected from practitioners to describe the current state, such as daily activities of the authorized persons in protected premises and requirements of the practitioners that can be provided by the better tools in prevention of identity theft.
- Key Behavioural Patterns (KBP) - In this step behavioural patterns of authorized persons in various types of daily activities are defined. This step focuses on the psychological analysis and listing of subconscious behavioural patterns that can uniquely define a concrete authorized person. Then, a machine-readable language (Motion Description Language - MDL) for the KBP description is defined and the KBP are described in this language.
- Specifications of the Software Prototype - This is a preparatory phase for implementation of the prototype. The two technologies will be created as the background for implementation of the software prototype. The first technology is developed for optimal recognition of the KBPs from the video sequences in the surveillance cameras. The second technology is based on deep learning that follows the daily KBP of individual authorized persons and learns the specificities of each of them so that he or she is uniquely defined in the system. Afterwards, models of the future software prototype will be created based on the analysis of practitioners' requirements and the above-mentioned technologies in order to be implemented.
- Software prototype implementation - In this step the software prototype is implemented based on the specifications and the user manual is created.
- Software Prototype Testing - Laboratory tests and real-environment tests of the software prototype are performed. Test results are repeatedly reported back. The technical parameter recommendations are noted to be included into the user manual.
- Field Demonstrations - An e-learning platform will be implemented to present the BehaVer software and the standard at the sites of the practitioners and validate if the final product meets their needs.

The following steps need to be taken to create the standard:

- Analysis of identity theft tools - Analysis of possible security incidents in the protected premises will be performed based on physical penetration using identity theft, with help of the practitioners' experience.
- Risk assessment - The likelihood and consequences of the specified scenarios and strategies for the treatment will be evaluated. This will include the description of used cases when the newly developed software can be used.
- Identity theft prevention measures - The newly developed software will be described here as an effective solution.
- ©EN standardization - A framework for prevention of the physical penetration using identity theft will be created and the standardization process will be initiated.

5. Conclusion

In this paper a solution for prevention of the physical penetration using identity theft - the BehaVer framework was introduced, consisting of a software tool, a standard and an e-learning platform that will be implemented in the future BehaVer project.

The BehaVer project proposal was submitted as a H2020 RIA project under the call Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism. In the case of support, it is believed that the project has potential to solve the above mentioned problem of prevention of the physical penetration using the identity theft. Ideally, the BehaVer software and standard would be adopted by the practitioners, such as operators of critical infrastructure [12] and operators of any monitored restricted areas with certain level of anonymity and limited number of authorized persons. Thus, the prevention of such crimes, using the software and the recommendations from the standard, would reduce possible investigative costs and costs caused by the harm of the attacker [13], as well as reduce societal distress and the impact on victims and their relatives. Furthermore, it is believed that the standard for prevention of the physical penetration using the identity theft would be accepted by the scientific community and research organizations and thus it would cultivate and advance technological innovations for prevention of more terrorist endeavours that include identity theft.

References

[1] GOODEN, A.: National Identity Crime Operational Lead UK Policing & Identity Security Adviser to Home Office UK Government Department. "Quote to BehaVer". E-mail to prof. HARAN, M., 2017-08-14.

[2] CUIJPERS, C., SCHROERS, J.: eIDAS as Guideline for the Development of a Pan European eID Framework in FutureID. Proceedings of Open Identity Summit 2014, Germany, 237, 23-38, 2014.
[3] TRABELSI, S., SENDOR, J., REINICKE, S.: PPL: PrimeLife Privacy Policy Engine. Proceedings of IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY 2011), Italy, 184-185, 2011.
[4] SABOURI, A., RANNENBERG, K.: ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life. Proceedings of International Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation, Greece, 2014.
[5] LIU-JIMENEZ, J., SANCHEZ-REILLO, R., BLANCO-GONZALO, R., FERNANDEZ-SAAVEDRA, B.: Making Stronger Identity for EU Citizens. Proceedings of 49th Annual IEEE International Carnahan Conference on Security Technology (ICCST 2015), Taiwan, 333-339, 2015.
[6] GAWANDE, U., GOLHAR, Y., HAJARI, K.: Biometric-Based Security System: Issues and Challenges. Studies in Computational Intelligence, 660, 151-176, 2017.
[7] RAJESWARI, P., VISWANADHA RAJU, S., ASHOUR, A. S., DEY, N.: Multi-Fingerprint Unimodel-Based Biometric Authentication Supporting Cloud Computing. Studies in Computational Intelligence, 660, 469-485, 2017.
[8] LOVECEK, T., VELAS, A.:Security systems, Alarm systems (in Slovak). EDIS, Zilina, 2015.
[9] Dupe Facial Recognition Software Using Bespoke Glasses. Available: http://www.prodigitalweb.com/ dupe-facial-recognition-software-using-bespoke-glasses/.
[10] Maris, L. Fanfarova, A.: Modern Training Process in Safety and Security Engineering, Key Engineering Materials, 755, 202-211, 2017.
[11] Souleiman, H., O'Riain, S., Curry, E.: Approximate Semantic Matching of Heterogeneous Events. Proceedings of 6th ACM International Conference on Distributed Event-Based Systems (DEBS 2012), Germany, 252-263, 2012.
[12] Zagorecki, A., Ristvej, J., Klupa, K.: Analytics for Protecting Critical Infrastrusture. Communications - Scientific Letters of the University of Zilina, 17(1), 111-115, 2015.
[13] STRELCOVA, S., REHAK, D., JOHNSON, E. A. D.: Influence of Critical Infrastructure on Enterprise Economic Security. Communications - Scientific Letters of the University of Zilina, 17(1), 105-110, 2015.

kamUNikácie
COMMUNICATIONS

Zoran Cekerevac - Zdenek Dvorak - Ludmila Prigoda - Petar Cekerevac*

HACKING, PROTECTION AND THE CONSEQUENCES OF HACKING

Understanding the term hacking as any unconventional way of interacting with some system it is easy to conclude that there are enormous number of people who hacked or tried to hack someone or something. The article, as result of author research, analyses hacking from different points of view, including hacker's point of view as well as the defender's point of view. Here are discussed questions like: Who are the hackers? Why do people hack? Law aspects of hacking, as well as some economic issues connected with hacking. At the end, some questions about victim protection are discussed together with the weakness that hackers can use for their own protection. The aim of the article is to make readers familiar with the possible risks of hacker's attacks on the mobile phones and on possible attacks in the announced flood of the internet of things (next IoT) devices.

Keywords: *hacking, hacker, information technology, internet of things, protection, economics*

1. Introduction

Under a term, the hacking one can include any unconventional way of interacting with systems, i.e. interaction in the way that was not foreseen as a standard by the designer, [1].This term is mainly connected with the modern technologies hacking, computers and computerized devices. So, the computer hacking is broadly defined as intentionally accessesing a computer without authorization or with exceeding of authorized access. More detailed about the legal aspect of hacking is given in [2], [3], [4], [5]. In any case, and above all, the hacker is responsible for the legal consequences of his actions.

What is considered by unconventional interaction with the system? The document in MS Windows can be opened in various conventional ways, one of which is double-click on the icon of the document, or, the second, double click on MS Word or Excel, and then the opening of one of the memorized files, etc. There are also other ways of opening documents using MS Office, or Open office, but they are considered as conventional. The same document can be accessed in any other way, for example, from another operating system, completely bypassing Windows and office software, and reaching the document in the text format. Such a method is considered as unconventional. And whoever accessed the document in this way can be called a hacker.

2. Who are the hackers?

The hacker can be anyone if he/she has a basic knowledge, desire, motivation, and (sometimes) some money. In addition to these characteristics, the successful hacker must have a large dose of patience and planning workability. However, neither all hackers are all the same, nor all hackers have the same goals. They are usually categorized into three main groups:

1. Black-hat hackers
2. White-hat hackers and
3. Gray-hat hackers.

Per relevant information sources, "a black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons" [6]. So, the Black-hat hackers are bad guys. Per the same source, "a white-hat hacker is a computer security specialist who breaks into protected systems and networks to test and assess their security. The White-hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them." But, the world of hackers is not black and white. There is also the third big group, the Gray-hat hackers. "A gray-hat hacker is someone who may violate ethical standards or principles, but without the

* **[1]Zoran Cekerevac, [2]Zdenek Dvorak, [3]Ludmila Prigoda, [4]Petar Cekerevac**
[1]Faculty of Business and Industrial Management, "Union - Nikola Tesla" University in Belgrade, Serbia
[2]Faculty of Security Engineering, University of Zilina, Slovakia
[3]Faculty of Economics and Service, Maykop State Technological University, Maykop, Russia
[4]Hilltop Strategic Services, Belgrade, Serbia
E-mail: zoran@cekerevac.eu

malicious intent ascribed to black hat hackers" [6]. The Gray hat hackers are often operating for the common good.

In practice, in communications, a term: "Ethical hacker" can also be heard, but discussion about ethics can be a wide and slippery terrain. Is it ethical to spy own children "for their good"? So, we'll stay in the named group. It is interesting that all of them use the same tools and methods, and the main difference is in their aims and results. On the other hand, hackers can be divided into several groups according to their knowledge and skills. The highest level consists of hackers who know exactly what they do, that are very familiar with the system and are able to create the appropriate software, including viruses and another malware. The middle level consists of the so-called "technicians" who are able to use tools that can be purchased in the market of software and hardware. The third, the lowest level of hackers, consists of the so-called "script kiddies". A script kiddie is a derogative term for the more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. They exploit weaknesses in the Internet computers often randomly and with little regard or perhaps even understanding of the potentially harmful consequences [7].

3. Why do people hack?

Hacking can be done for different reasons. However, the following four groups can be distinguished:

- One of the first reasons is collecting data. In doing so, the data can be very varied, from business data to the private data, practically anything and everything, from important to useless.
- Another group could be the impersonalization of persons or clients. Thereby, there can be collected numbers of bank accounts, e-mails, and the like. One of the reasons for the impersonalization can be preparing for a distributed denial of service (next DDoS) attack.
- The third reason can be of destructive nature. The targets of destruction may be websites, databases and the like. The main objective, in this case, is to make damage.
- The last, but very often reason for hacking is hacking for fun. Many find a pleasure in burglary into other people's systems, walk through them and come out unnoticed. Will they, in fact, have some benefit, (if they even have) is the less important for them. Any significant inroads into the specific network, like Pentagon, Central Intelligence Agency (next CIA), etc. increase their dose of adrenaline.

4. Hacking and the law

The Internet, as a rather modern technology, brings new challenges. It is very difficult to define what is right and what is wrong. If some user publishes his email address, and the other involve this address in its database and sends a bulk of emails to this address, is it legally or not? Privacy and the information privacy are a great issue. The person or institution, who owns the computer, or the computer system is not necessarily the owner of the data on that system. Internet service providers that host Web sites are not the owners of the contents of the hosted websites. The doctor who owns a database on their patients is not the owner of those data and if he publishes them he can found himself in a big trouble.

5. Methods of hacking

Data can be stolen in a variety of ways, from the brutal theft of the entire computer, over the copying of contents of hard drives, to sophisticated methods by remote access.

The easiest way is to steal data from the inside. It can do permanent employees dissatisfied with working conditions, temporary or part-time employees, or even an employee in charge of security and maintenance of the system. Access can be provided through the so-called backdoor. If he provides a constant external connection and on cable glues a label "Security - Do not unplug" it is likely that no one will with interfere this connection until the new reconfiguration of the system. In all these actions a direct physical contact with the device is necessary.

The attacks carried out on the network are more sophisticated and usually include searching for an open access port, email addresses and passwords, DDoS, access to file servers, holes in the firewall, etc. One possibility is the use of backdoors that many manufacturers left open for the purposes of control of the products.

The development of software and hardware can be a quite boring job. These activities require frequent testing, resetting, connecting different contacts and/or parts of programs, troubleshooting and the like. If any change would require re-authentication, this would significantly reduce the work efficiency. Therefore, developers initially leave open the possibility of applying various, only to them known, commands that skip certain phases of work. They are called "Easter eggs". As a rule, those controls should be deleted from the program code as work is completed. However, very often, the Easter eggs remain permanently in the software. By testing different key combinations, or by user error, or accidentally, users can find and use them. As an example, keyboard shortcuts for Microsoft Word on Windows can be used [8].

For realization of the hacking, it is unavoidable to use the social engineering. There is a variety of diverse and imaginative solutions, but one of the stupidest and the most frequently applied, is that by an e-mail, the attacker from their victim requests to provide personal information, including the password for the specified e-mail address, so as not to be ruled out in the next few

days. It is needless to say about the possibilities that attacker gains using these data. This hack is based on sending mass e-mails. One of the frequently used is the variant in which some person is aimed to be a victim. E.g. an attacker, using a disposable cell phone, calls on the victim posing as a representative of the Internet service provider or bank in which the victim has an account. The attacker explains to the victim that there is some problem with a victim's account that the operator cannot solve without the help of the victim and that he needed a password for that purpose. Surprised victim usually tells their password. Fraud can continue by the offering of providing help for payment of outstanding bill if the victim provides the credit card information, etc.

In addition, phishing, fake emails and fake websites are used in hacking, but they will not be discussed here.

6. Planning of attacks

Hacking is the real threat of today's virtual world. There is no attack that can be realized by pressing a single button with just passing by the computer or mobile phone. Even when a hacker has access to a victim's computer within a reasonable time (which is never the case) and when "only" needs to find a password for email or logging in, it might be mission impossible. Such attempts were unsuccessful and quickly point to the perpetrator.

From the aspect of an attacker, as well as from the aspect of a defender, there are several things that need to be considered:

- What does an attacker want to achieve using the attack?
- What can be profitable to an attacker? Stealing of banking credentials might not be profitable. This hack can be solved in a few minutes, by only one telephone call. For an attacker, it is more favorable, and for the victim more dangerous, if the attacker takes over credentials of PayPal, E-Bay, amazon.com, a directory of users, etc. If the attacker is a parent, what he/she wants to follow?
- The next question is: How to realize the attack? Among many possibilities, there are two main approaches:
  - a mass attack that demands long and careful planning and preparation, and adequate malware and
  - a targeted attack that demands careful analysis and collecting data about a concrete person or a company.
- The final question for an attacker and for the defender is: Which information the attacker wish to get?

From the attacker's side, there is also a question concerning the available tools.

And finally, and perhaps it is better to put it at the very beginning, there is a question about the profitability of the action: what will happen in the most favorable case, and what in the most unfavorable case?

7. Economic aspects of hacking

Quantifying losses caused by the cyber-attacks is very difficult and unprecise. Losses consist not only of the direct cost of lost money, but of the costs of cleaning up and the investigation, as well. In addition, every day improving protection costs money. And information technology staff do not work for free. The year 2011 was called "The Year of the Hack" [9]. According to that source, hackers earned 12.5 billion USD that year. A lot of companies did not publish their financial losses, but among the companies that did it there are:

- Sony, with 171 million USD;
- Citigroup, with 2.7 million USD;
- Stratfor and AT&T, with 2 million USD each; and
- Fidelity Investments, Scottrade, E*Trade, Charles Schwab, with 1 million USD.

Per Richard Power, from the Computer Security Institute, "single instances of hacking may cost as much as $600,000 to $7 m a day for online businesses in 2011, depending upon the revenue of the operation" [10]

Author of [11] stated that the hackers cost U.S. economy up to 500,000 jobs each year. In his study, he blames the Chinese hackers for espionage. This analysis was based on similar reports of McAfee and the Center for strategic and international studies [12]. The authors of the study said that each time when an information is stolen, some company went into the risk of bankruptcy. They estimate that hacking costs the US economy up to USD 100 billion a year.

Hacking reached enormous sizes, and each year it getting bigger and bigger. The Chinese side is constantly accused for espionage and eavesdropping. Such an analysis is given in [13]. On the other hand, a book was written about the computer virus Stuxnet that was designed by the USA and Israeli computer experts to sabotage the Iranian nuclear program [14]. This was the first known cyber weapons used in the war with the aim of destroying the infrastructure of a country. Finding of the Stuxnet malware successors Duqu and Duqu 2.0 suggests that the arms race was never interrupted and that in parallel with conventional forms cyber warfare exists. Many articles were written about other examples of hacking and cyber espionage, like projects PRISM and Tempora [15], [16], [17], [18], [19], [20], so those will not be further discussed here.

8. Attacker's protection

In any case, a hacker needs to think about self-protection. All Internet activities can be, and they are, monitored and tracked via Internet service provider (next ISP), network routers, a computer system. Although this is happening 24/7, the collected data are rarely used. Only if the attackers caused serious problem he could expect legal consequences.

Each hacker intends to work remotely from a place, which is far away from his home. In addition, the attackers change their location frequently choosing locations and computers that cannot be easily connected with them. For conducting an attack the best for attackers is the use of others computers, for example, computers in public libraries, cafes, or, eventually, cheap computers that can be destroyed immediately after use. One possibility is the use of operating systems and software written on CDs on computers from which the HD was previously removed.

That hacking is risky tell the fact that all financial transactions a hacker needs to make with money in cash. The alternative can be using pre-paid credit cards and telephone numbers.

9. Victim's protection

On the other hand, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use. An organization can suffer a lot from a hacker attacks. When the organization survives an attack, it needs to make deep changes it its protection, must apply a new philosophy, very often with the new staff. Some organizations outsource their protection. So, many new independent companies can benefit from specializing in hacking prevention. Outsourcing can be a good solution for small and medium companies because of their limited staff and money capabilities, [21], [22], [23].

10. Conclusions

To protect a computer and/or a computer system from hacker attacks, a defender needs to know the way of an attacker thinking and methodology, as well as about the tools, which attacker can use.

All attackers use similar methods and tools. Their intentions can determine whether they will be the Black-hat, Gray-hat or White-hat hackers. A hacker attack needs time, and cannot be realized without a lot of work.

According to the latest research, majority of users do not recognize attacks at all, some of them identify attack within 200 days and only a few manage to identify and react on attack within 24 hours. If the attack on informational system does not corrupt data, the chance that system administrator will identify an attack is very low. If the data was corrupted, the chance for recognizing of an attack is rising.

The authors of this paper in no case encourage readers to engage in risky hacking especially of the Black-hat hacking type, but they want to make readers familiar with the possible risks in the announced flood of the IoT devices.

References

[1] Eli the Computer Guy. Introduction to Hacking [online]. Available: https://www.youtube.com/watch?v=yGIHjTmTFfA [accessed: 2010-12-12].
[2] JARRET, H. M., BAILIE, M. W.: Prosecuting Computer Crimes [online]. Available: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.
[3] National Assembly of the Republic of Serbia. Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime [online]. Available: http://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_ organa_za_borbu_protiv_visokotehnoloskog_kriminala.html [accessed: 2017-03-18].
[4] Ukrainian National Assembly. Law of Ukraine of 7 September 2005 ℓ 2824-IV on the Ratification of the Convention on Cybercrime (with amendments and addenda of 2010-09-21) [online]. Available: http://search.ligazakon.ua/l_doc2.nsf/link1/T052824.html.
[5] Kazakhstan. Proposed a Convention Project to Combat Cyberspace [online]. Available: http://www.zakon.kz/4808903-rf-predpolozhila-proekt-konvencii-po.html [accessed: 2016-08-01].
[6] Black Hat. Black Hat Hacker [online]. Available: http://www.blackhat.com.
[7] ROUSE, M.: Script Kiddy [online]. Available: http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy.
[8] Microsoft. Keyboard Shortcuts for Microsoft Word on Windows [online]. Available: https://support.office.com/en-us/article/Keyboard-shortcuts-for-Microsoft-Word-on-Windows-95EF89DD-7142-4B50-AFB2-F762F663CEB2.
[9] STANESCU, B.: Top 5: Corporate Losses Due to Hacking [online]. Available: https://hotforsecurity.bitdefender.com/blog/top-5-corporate-losses-due-to-hacking-1820.html.
[10] GISH, W.: The Effects of Computer Hacking on an Organization [online]. Available: http://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html.
[11] LEWIS, J. A.: Economic Impact of Cybercrime [online]. Available: https://www.csis.org/analysis/economic-impact-cybercrime.
[12] SMITH, G.: Hackers Cost U.S. Economy Up To 500,000 Jobs Each Year. Study Finds [online]. Available: http://www.huffingtonpost.com/2013/ 07/25/hackers-jobs_n_3652893.html.

[13] BARRET, D., YARDON, D., PALLETA, D.: U.S. Suspects Hackers in China Breached about 4 Million People's Records. Officials Say [online]. Available: https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

[14] SANGER, D. Obama Order Sped up Wave of Cyberattacks against Iran [online]. Available: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber attacks-against-iran.html?_r=3&adxnnl=1&pagewanted=all&adxnnlx=1338548715-2wt62+m6D3KzuVRTaa2QJQ.

[15] DERESPINA, C.: WikiLeaks Releases 'Entire Hacking Capacity of the CIA'WikiLeaks Releases 'Entire Hacking Capacity of the CIA' [online]. Available: http://www.foxnews.com/us/2017/03/07/wikileaks-releases-entire-hacking-capa city-cia.html.

[16] BACON, J.: WikiLeaks: CIA Can Hack into Phones, TVs-Everything [online]. Available: http://www.usatoday.com/story/news/nation/ 2017/03/07/wikileaks-says-has-published-cia-hacking-codes/98844256/ [accessed: 2017-03-07].

[17] SCEKIC, D., CEKEREVAC, Z.: Privacy by Design - Possible Solution in the Protection of Privacy and Personal Data. Proceedings of International Scientific-Professional conference Information Technologies, Economics and Law: state and development perspectives (ITEL-2016), USA, 260-262, 2016.

[18] JASEK, R.: SHA-1 and MD5 Cryptographic Hash Functions: Security Overwiev. Communications - Scientific Letters of the University of Zilina, 17(1), 73 – 80, 2015.

[19] CEKEREVAC, Z., DVORAK, Z., CEKEREVAC, P.: Internet Safety of SMEs and E-mail Protection in the Light of Recent Revelations about Espionage of Internet Communication System. Zbirnyk naukovykh prats Bukovynskoho universytetu, Ekonomichni nauky, 10, 25-33, 2014.

[20] KUBINA, M. & KOMAN, G.: (2016). Big Data Technology and its Importance for Decision-Making in Enterprises. Communications - Scientific Letters of the University of Zilina, 18(4), 129 – 133, 2016.

[21] PRIGODA, L., CEKEREVAC, Z., DVORAK, Z., CEKEREVAC, P.: One Look at the Modern Information Security [online]. Sustainable Development of Mountain Territories, 4(22). Available: http://www.meste.org/cekerevac.eu/biblioteka/ij_23.pdf.

[22] CEKEREVAC, Z., CEKEREVAC, P., VASILJEVIC, J.: Internet Security of SMEs is an Aspect of Security E-mail. FBIM Transactions, 2(1), 45-56, 2015. DOI:10.12709/fbim.02.02.01.05

[23] CEKEREVAC, Z., RADONJIC, S.: Some SMEs Data Safety and Security Issues in the In-House and in the Cloud Computing. Proceedings of 18th International Science Conference Solving of Crisis Situations in a Specific Environment, Slovakia, 99-106, 2013.

Marcin Paweska - Jozef Ristvej*

LOGISTICS DURING POPULATION AND ANIMALS EVACUATION IN CASE OF EXTRAORDINARY INCIDENTS AND CRISIS EVENTS

Evacuation is one of the main tasks of administration and its forces and resources in different types of extraordinary events, as well as natural and anthropogenic (non-military and military events) unusual/emergency situations. Evacuation at the level of normative acts and plans is precisely defined and categorized. Existing normative documents and regulations are described in detail and govern to carry out the evacuation of population. This is not the case for animal and property evacuation, which is often treated in general terms and considered to be organized in similar manner to evacuation of people. In the evacuation process of animals, the specific of this process must be taken into account, because badly prepared and performed evacuation may bring more harm than benefit. Hence, the aim of this article is to present, selected essential and specific issues relating to the evacuation of animals, based on theory provisions of the normative and practical experience of the authors.

Keywords: *logistics, evacuation, evacuation degrees, danger, risk, population, animals*

1. Introduction

According to the Constitution of the Republic of Poland, the source of law in Poland are laws and regulations, as well as ratified international agreements. Thus, they become the basis for planning and realizing the evacuation of people, animals and property in the event of danger to their safety. The international agreements ratified by Poland concerning evacuation include: the IV Geneva Convention, and the I and II Additional Protocols to the Geneva Conventions.

Under the national law, the basic arrangements for evacuating the population are laid down in the regulations of the Council of Ministers, where it has been stipulated that the heads of civil defence are responsible for the preparation, organization and management of evacuation. The arrangements referring to dates, to evacuation routes and evacuation locations are subject to agreement with the relevant authorities and services and all the preparations and their implementation should be in accordance with the regulations of the Chief of Civil Defence of the Country (SOCK), dated 17th of October 2008 [1], which are guidelines on the principles of evacuation of the population, animals and property in the event of a mass threat, and annex to these guidelines in the form of the Instructions on the principles of evacuation of the population, animals and property in the event of a mass threat. The subject-related guidelines cover the provisions of all the so-far-existing evacuation acts, as well as the theory and practice of planning and executing evacuation.

2. Theoretical and legal aspects of evacuation

In the theory of the tackled issue there are many definitions of evacuation, which distinguish the evacuation of people, animals, property, objects, as well as the evacuation of specific character: medical, technical, veterinary, war and military activities. However, they all have a common denominator, namely the movement of people, animals and property from the threatened to safe areas.

Evacuation (lat. *evacuatio – emptying, disappearing*) in general is one of the basic measures, which aims at protecting life and health of humans, animals and saving property, including antiques and important documentation, in the occurrence of any kind of threat. It is usually carried out in the form of relocation from a region (site) where the danger occurs, to the safe area. In practice, most frequently the evacuation is carried out for the injured or those at risk (including animals and property at risk) after the occurrence of a hazardous event (e.g. flood, fire,

* [1]Marcin Paweska, [2]Jozef Ristvej
[1]International University of Logistics and Transport in Wroclaw, Poland
[2]Department of Crisis Management, Faculty of Security Engineering, University of Zilina, Slovakia
E-mail: Jozef.Ristvej@fbi.uniza.sk

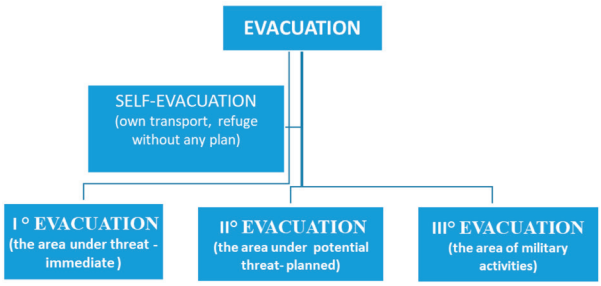


Figure 1 *The degrees of evacuation*

explosion or other local threat) in objects or areas affected by the incident, that is, the area already covered by the emergency event. Evacuation can also be of the preventive nature, i.e. it can be carried out from areas and facilities in the event of an imminent threat, e.g. due to the spread of dangerous events (flood, chemical catastrophe, etc.) or the threat of military action in the case of war risks..." [2], [3]. However, the author of this definition also only perfunctorily deals with animals in the first part of the discussion [2].

The definition which took into account all the basic aspects of evacuation has been presented by K. Przeworski, who defined it as "... organized movement (removing, taking out, moving) of the population, all kinds of material goods and farm animals from areas or facilities threatened or affected by armed forces or disasters, in order to protect them, to provide assistance, also understood as rescue and limitation of material losses..." [4].

Due to the nature and scale of the threat, the evacuation of I, II and III degree is distinguished [5] (Figure 1).

The individual degrees of evacuation consist of:

- **I degree evacuation** involves immediate relocation of the population, animals and property outside the threatened area where sudden, unforeseen direct threats occurred. It is organized at the mayor's or the city president's order. Evacuation may also be ordered by the person conducting the rescue operation in the area where rescue operations take place. The leader of the rescue operation is obliged to inform the competent self-government administration about the decision taken. The I degree evacuation can be carried out based on documentation prepared for the II degree evacuation;
- **II degree evacuation** is the planned relocation of the population, animals and property from the adjacent areas to plants, hydro-technical facilities, floodplains and areas adjacent to other facilities that pose a potential threat to the population, animals or property in the event of their destruction or failure. It is implemented in the presence of symptoms of such a threat, according to previously developed plans and procedures;
- **III degree evacuation** means the previously planned and prepared relocation of the population, animals and property, while heightening the states of defence preparedness. It is run during the threat to the state security and war. Preparation of the evacuation associated with the war time includes the following variants:
  - organizing the evacuation from the anticipated areas (sites) of the operational activities of the Armed Forces;
  - organizing the evacuation of the population, which expresses the desire to leave areas potentially threatened by military activities [6].

Table 1 *Forms of evacuation*

EVACUATION	
CRITERIA OF DIVISION	FORM
According to the form of the process	- scattering - co-location (leading out) - pulling back (moving away) - evacuation transit - anarchic (escape)
According to the occurrence of threat	- lifesaving - preventive
According to the activation mode	- alarm - successive (by stages and batches)
According to the target (destination)	- people - animals - materials - cultural resources, archives,
According to the organizational preparation	- planned - interim
According to people's motives	- natural (self-evacuation) - preordained

Each of these evacuation degrees may, depending on the circumstances, be implemented in by means of various forms, the details are presented in Table 1 [4].

As far as the population is concerned, all those who are in the area of danger are evacuated. The first and foremost, evacuation includes among others: mothers and children, pregnant women, people with disabilities, people from health centres, from orphanages, hospitals for chronic and incurable illnesses, beneficiaries of social care etc. Depending on the type of evacuation, the following people might not be subject to it: people involved in rescue organizations, civil protection and law enforcement services; people essential for ensuring the continuity of the life of the local community; people assigned to armed forces or armed formations not included in the armed forces; officers of armed formations not included in the armed forces (The Internal Security Agency, the Border Guard, the Government Protection Bureau, etc.); people who have been assigned the allocation to a unit destined for militarization or a militarized unit; individuals who have been assigned for civil defence formation; those necessary for the area due to the tasks performed by the armed forces.

Table 2 *Gradation of time and sort of the logistics services for the affected*

Time lapse	1°	2°	3°	4°	5°	6°
	in order	in order	in order	in order	in order	in order
T 6						well-being services
T 5					low-line articles	
T 4				deliveries of water and food		
T 3			EVACUATION			
T 2		transport				
T 1	medical help					

Both evacuation and **self-evacuation** should be planned within the evacuation of I, II and III degree [5]. Self-evacuation refers only to the population and consists of moving from areas where there is, or may appear, an immediate threat to life and health, to the outside of the threat area. It is mainly executed based on one's own, individual possibilities (transport, accommodation, etc.). It can take place even before the decision to evacuate, as well as while it lasts. In this context, particular attention should be paid to the following: estimation of the possible scale of self-evacuation; identification of potential directions and self-evacuation areas - including family relationships, recreational plots, accommodation (in designated housing resources - holiday homes, boarding houses, hotels, residence at families residing in the distribution area); designation of escape routes and traffic management; providing fuel and technical assistance on evacuation routes; providing supplies of water, food and medical assistance.

In order to increase the effectiveness of the evacuation authorities' operations, in the evacuation areas, on the evacuations routes and at destination points, the following are organized:

- information and registration teams;
- the evacuated gathering teams;
- loading for means of transport teams;
- medical assistance teams;
- logistical assistance teams, including technical assistance;
- unloading teams;
- distribution teams [5].

The essentials of the evacuation arrangements presented confirm the thesis that most of them refer to evacuation of the population, while evacuation of animals and property is treated ""on the fly".

Animal evacuation, the same as population evacuation, is a complex process requiring appropriate planning and organization. Both evacuations have many common and cohesive features, such as the fact that evacuation of animals can also be divided into I, II and III degrees, but it is difficult to imagine self-evacuation.

However, it is important to note here that there is a need to strictly adhere to **the principle** that **human life** is a greater value and that it should be rescued **in the first place**. At the next stage of the evacuation, depending on the development and the state of the threat, animals and material possessions are saved.

3. The needs of evacuation

In the case of extraordinary events, especially in times of floods and fires, as it results from the experience, the catalogue of needs in providing help to the affected is really broad as far as logistics needs are concerned. Ensuring safety to the affected and protection of life and health have always been the priorities. Considering all the needs according to their importance and urgency, they can be hierarchically defined as providing services in the following way [3]:

- medical help and healthcare,
- transport,
- evacuation,
- deliveries of drinking water and foods,
- delivering of the low-line articles,
- well-being services.

The order and urgency of providing the above mentioned logistics services always results from the situation, e.g.: during the 1997 flood, as the first and most urgent were deliveries of water and foods, as well as evacuation. Gradation of time and sort of the logistics services for the affected are presented in Table 2.

Ensuring safety and proper realisation of the logistics help for the affected requires advance planning, with generated risk of the extraordinary events and their primary and secondary results as the base.

4. Planning and organization of population and animal's evacuation

Planning for evacuation activities is the duty of all the authorities responsible for public safety. To ensure smooth and efficient operation and proper coordination of evacuation, in accordance with the regulations resulting from "the Instruction of evacuation of the population, animals and property in the event of a mass threat" issued by SOCK, it is necessary to

prepare the Evacuation Plan as part of the Crisis Management Plan (I and II degree Evacuation) and the Civil Defence Plan (III degree Evacuation). Such a plan should specify both the manner of evacuation, depending on the existing conditions, and the resources needed to carry out the task. The condition for the effectiveness of this plan is its validity, which must be verified by means of regular inventory-taking and updating resources, as well as verification of adopted solutions.

The II and I degree Evacuation Plan, which is the part of the Crisis Management Plan, is developed by Crisis Management Teams at specific levels of administration. It consists of a descriptive and graphic parts and should contain [5]:

- Objects and areas intended for evacuation, depending on the possible hazards,
- Criteria for the selection of people for the evacuation, including the order of evacuation, for people who, for various reasons, are not subject to evacuation (if this is the case),
- Estimation of the possible scale of self-evacuation, including directions and locations of relocation,
- Criteria for the decision to evacuate, and the people (units) authorized to announce the evacuation,
- Evacuation announcement ways (techniques),
- Routes and destination locations of evacuated people and property,
- People (groups, teams, formations etc.) responsible for evacuation (people responsible for the designation of evacuation locations for individual populations and indication of the way and routes of movement, according to schedule or in an interim way);
- Places (points) of collection of evacuees,
- Loading points for means of transport and unloading points,
- Distribution locations (points),
- Detailed lists and methods of delivering tasks performed at designated points by individual teams,
- Protection of abandoned areas,
- Lists of planned means of transport, selected places of temporary residence and source of acquisition of materials and means of logistic and mode of obtaining them,
- The return of people and property to places of permanent residence or location after the end of the threat, organization of communications and traffic management,
- other data as needed.

No separate evacuation plan is developed for evacuation of the I degree, the evacuation measures of this stage are included in the II degree evacuation plan, annexed to the Emergency Management Plan, at various levels of public administration and self-government. In the case of the development of the III Degree Evacuation Plan, the main planning effort rests with the civil defence (CD) bodies responsible for drawing up civil defence plans. The III degree evacuation plan is a subject to agreement with the armed forces, police, border guards, non-governmental organizations, Polish Railway Lines, telecommunications, neighbouring CD entities (for example the province CD plan should be agreed with the province authorities of neighbouring provinces) and the supreme head of the civil defence. It is signed by the head of the CD unit (e.g. at the province level - head of the regional security and crisis management department) and approved by the CD head of a given level (e.g. the province level).

The organ for planning evacuation of animals at the provincial level is the Provincial Veterinary Doctor and at the county level the relevant services subordinate to him/her and cooperating with them [3]. In order to accomplish this task, a relevant animal evacuation unit (team) is formed at the meeting of the Crisis Management Team (CMT), which consists of the functionaries designated by the chairman of the CMT. The created organ/ team can be extended and other employees can join (depending on needs). The principle of expanding the team is the same as in the case of the population evacuation, in particular that in the context of widely understood evacuation, projects involving the evacuation of populations and animals, in principle, are carried out in parallel. The tasks of the Animal Evacuation Team include:

- Preparation of the fiat - the relevant CD Chief - regarding evacuation (adoption) of
- animals, which specifies:
- areas being evacuated, evacuation routes and areas to which the movement of animals will take place;
- manpower and equipment necessary to accomplish the task;
- the way to provide veterinary aid for the evacuated animals, the distribution and the necessary supplies;
- the organization of cooperation with, among others, military authorities, police, Polish Railway Lines, Polish Telecommunications, Province Veterinary Inspectorate and the CD Heads of neighbouring provinces;
- the organizational elements of animal's evacuation in the communes involved in the evacuation process;
- the date of completing the evacuation;
- other factors to be considered in planning and organizing the evacuation process.
- Developing animal's evacuation (adoption) plan, which is agreed upon according to the needs of the evacuated livestock with the military authorities, the police, the Polish Railway Lines, the province management of the Polish Telecommunications, the provincial veterinary inspection, the CD heads of the neighbouring provinces and the Chief Veterinary Officer of the country.

Animal evacuation is generally carried out in parallel with evacuation of the population. In this process, organizational units, which provide veterinary care, transportation, living conditions, order and security, are involved. For evacuation, the available means of transport (short distances) are used, and only as the last resort animals are flogged [7].

Evacuation of both the population and animals or property must be recorded, depending on the degree and scale of the

evacuation. Evacuation cards should be pre-numbered forms and prepared along with the Evacuation Plan. In recording procedures, the use of record cards and evacuation cards has to be taken into consideration. The following rules should apply as far as the circulation of record documents are concerned [5]:

- Evacuation card:
- the card consists of three parts: A, B and C,
- evacuation cards are issued by the record and information teams in the municipality (district) appropriate for the place of actual stay of an evacuee,
- part B of the card remains at the disposal of the said units, the remaining two parts are given to the person being evacuated,
- after arriving at the place of temporary accommodation, the evacuated person hands in part C of the evacuation card to the record and information team in the municipality (district) appropriate for this place,
- part A of the card remains at the disposal of the person who collected it, if the evacuation card cannot be collected in the municipality (district) appropriate for the place of actual stay, the evacuee applies in order to receive the evacuation card to the team of temporary accommodation,
- Record cards of evacuated people, groups of evacuated people, evacuated animals and evacuated property:
- they are prepared by the record and information teams in municipalities (districts) appropriate for the place of actual residence of people, animals or location of property, according to the municipalities (districts) to which the person or property will be evacuated,
- copies of the relevant records are forwarded to the information and record teams in the municipality(ies) to which the person or property is evacuated, where they are compared with the actual state of the people and property, and they are completed and/or corrected as needed,
- in the case of not being able to deliver a copy of the record card, the obligation to prepare it is transferred to the records keeping teams in the municipalities (districts) appropriate for the place of temporary accommodation or movement,
- copies of the evacuation cards should also be sent to the record and information teams at higher levels of administration involved in the evacuation of given groups of people or property.

5. Executing Evacuation

In the case of evacuation of the I and II degree, the decision to conduct it, depending on the type and scale of the threat, is taken by [4]:

- mayor, president of the citymayor from areas directly threatened;
- bodies that supervise the operations to prevent the effects of a natural disaster, or to remove such a disaster's effects removal (during the state of a disaster); depending on the area covered by the disaster, these are:
- mayor, city president - if the state was introduced only in the municipality,
- mayor - if the state was introduced in the area of more than one commune constituting the county,
- duke - if the state of natural disaster was introduced in the area of more than one county constituting the province,
- minister appropriate for internal affairs, if the state of disaster was introduced in the area of more than one province
- duke in the case of radiation incidents of provincial coverage;
- minister appropriate for internal affairs, in the case of national radiation incidents;
- the person who supervises the rescue operation, by means of informing the affected area of the appropriate public authority (civil defence).
- In the last case mentioned above, the person in charge of the rescue operation is obliged to inform each time the competent civil defence authority of the decision made, stating:
- the area, region, facilities or complex of buildings for which the evacuation was ordered,
- the type of threat that has been the determining factor in evacuation,
- the estimated number of evacuees.

It is up to the local authority to provide the conditions necessary for evacuated and injured population and for evacuated animals to survive.

In the case of necessity of evacuation of the III degree, the decision to conduct it in accordance with the law in power is taken by the public administration bodies, i.e. the competent civil protection body or the military unit in the direct combat area.

6. The specificity of logistics of animal's evacuation

Animal evacuation, like population evacuation, is a complex process requiring appropriate planning. Both evacuations have many common features. Evacuation of the I, II and III degree also takes place while evacuating animals. The I degree evacuation, if it needs to be performed, does not differ from the procedure of evacuation of the population. It is the responsibility of the hosts of the facility (hosts) in which the livestock is located. Often the evacuation of animals is carried out in parallel with the evacuation of the population, hence the convergence of the rules of conduct. A properly prepared evacuation plan for animals should include information on the order of departure and on their location. Evacuation of animals in urgent cases, i.e. evacuation of the I degree, is not easy and requires proper preparation, therefore it is carried out only if it does not present a direct threat to the lives of people performing this task. The construction of buildings does not always allow capable rescue operations and evacuation. In case of evacuation from a building

on fire, flammable structural elements already covered by fire may prevent entering into the building. The low ceilings can cause dense smoke in rooms. Existing baffles can force rescuers to walk the animals individually, etc.

Evacuation of animals is a difficult and demanding task, and therefore it is important to acquire the appropriate knowledge and skills in this area and to prepare specialist equipment for rescuers and managers, because unlike humans, animals will usually follow their instinct rather than think rationally. During the evacuation, one must not ignore the fact that animals feel dread and anxiety when in danger. Moreover, they are less resistant to smoke. In the case a factor threatening and animal enters the room, an animal often lies on the ground, making it difficult to evacuate. Therefore, the evacuation of animals should begin as soon as the first signs of possible danger appear, i.e. as soon as possible. It is worth remembering to approach animals from the front, calmly, carefully and gently speak to them. They sense the frustration of the rescuer and it is easily spread. Animals walked out of an endangered area should be directed to safe places, which they cannot leave on their own will. It should also be taken into consideration that depending on the evacuated species, different activities are undertaken. For example, horses and cows shall simply be moved out of pits, but poultry shall "get out" in bags (quickly release it and provide fresh air) or in baskets. Small pets are brought out in cages.

Evacuation takes place in the land of the municipality, county and province, and if necessary to neighbouring counterparts, with whom appropriate agreements should be signed.

Evacuation should not be planned or led to:

- areas in close proximity to major industrial, transportation and military facilities;
- areas of foreseen and conducted warfare;
- areas of anticipated hazards (e.g. floods, fires, etc.).

In the process of evacuation, organizational units should provide veterinary care, transportation, living conditions, order and security. For evacuation, the available means of transport used (mainly railways - for long distances, e.g. between provinces and vehicles for shorter distances) are used. In the absence of adequate quantities, the evacuation is carried out combining allocated and own means, and flogging animals shall be done only as an ultimate solution.

Evacuation locations should be characterised by [5], [8]:

- situation on a small elevation, and in the case of planned evacuation, consideration should be given to the location of animals in other farms away from activities such as e.g. warfare;
- the possibility of providing a quick makeshift fence;
- providing conditions for watering and feeding animals;
- at least 50 m away from slaughterhouses, as well as agricultural and food processing buildings, rendering plants and feed mills;
- providing the possibility to protect against insects and rodents;
- smooth, paved and severed surface of the inside pads;
- durable and easy to maintain walls and floors of buildings, and the ability to disinfect them.

Moreover, the designated collection sites should have [5], [9]:

- equipment for loading and unloading animals;
- drinking water access;
- a sewage system capable of carrying out decontamination and waste removal;
- equipment for watering and feeding animals;
- animal testing station, equipped with a wash basin and a device for immobilization of animals at the time of the test, coops for sick or suspected of being sick animals, with a separate sewage system;
- a separate and properly located manure storage area;
- devices and equipment necessary for cleaning and disinfection of rooms as well as a warehouse for storing equipment and disinfectants;
- storage room for storage of animal feed;
- social-living rooms for keepers.

Evacuation of animals is a difficult task, requiring proper preparation, therefore it is only carried out if it does not pose a direct threat to the lives of rescuers and keepers of animals [8].

The evacuation of animals should be started by people who handle those animals on a daily basis [9]. Before the evacuation, rescuers should recognize the way animals are placed and tied. In large breeding facilities the evacuation plans should be prepared, including information on the locations of the animals and the sequence of their removal. In the case of tying animals, the chains should be released, trying to expel the group of animals from the room to prevent them from spreading around the facility. It often happens that in the herd there is the order of precedence. In this case, it should be kept during the rescue work. Evacuation methods are always defined by rescuers, with the use of the experience of the evacuated animals' keepers.

The experiences of the Authors of this publication during the floods of 1997 and 2010, the analysis of fires of farm buildings, especially of the breeding ones, and materials based on practical experience, elaborated mainly by the State Fire Service (PSP) and designed for the training of rescuers [9], allow to formulate the basic principles of dealing with animals during the evacuation:

- animals should be approached calmly from the head, no fear or anxiety should be shown, because the same behaviour can occur among them (do not approach the back of animals, especially the large ones such as horses);
- animals kept in the group or tied (chains, ropes) should be released as soon as possible;
- it must be kept in mind that animals are attached to their place of residence, so they often try to return to places where they have been evacuated from, so that the evacuation area must be protected so that they cannot leave;

- large and strong individuals should be walked out by several rescuers, often with the help of their owner, and in the case of bulls only by their caretakers, rescuers as "strangers" may be treated as "enemies";
- young animals and individual species should be evacuated separately, in case of taking the young ones from their mothers, the reaction of adult animals should be closely monitored;
- In the case of herd animals, if possible, "herd leader" (indicated by the owner/keeper) shall be evacuated first, so that the whole herd would follow.

As evacuations are generally for domestic animals, reared on home farms and specialized farms, additional remarks may be done referring to the evacuation of their basic species, i.e. horses, cows, pigs, sheep and poultry. These remarks result from own observations and the analysis presented in [8], [9].

While rescuing horses one should not approached them suddenly from behind. Young, strong horses, especially stallions, should be led by their keepers. Individuals accustomed to the harness can wear a harness and be calmly walked out. Horses led next to the stress-causing places should have their eyes covered with a sack or a cloth. In order to eliminate odours, a little manure can be applied close to the nostrils.

The evacuation of cows is similar to the evacuation of horses. However, careful attention should be paid to walking breeding bulls out of the threatened areas. If strangers approach, they can take a defensive attitude and even attack. The safest way to evacuate a bull can be with a stick attached to the nose ring.

Pigs are usually evacuated without much trouble by pushing into designated areas. The problem can be sows feeding piglets, which usually do not want to leave them. In this case, the piglets should be collected in bags or baskets, and the sow is then placed behind the piglets.

In addition, the poultry shall be rescued in sacks or baskets. When picking up from an endangered place, poultry should be released as quickly as possible from the bags so that there is no suffocation risk due to insufficient amount of air.

The evacuation of sheep can cause considerable problems, because sheep naturally fall into a circle or group in the corners of the rooms. It is important to lead the flock leader, after which the sheep usually follow.

In addition to the evacuation of animals from farm buildings and adjacent facilities, evacuation of animals endangered by flood: from quagmires, mudslides, marshes and deep excavations, trees, poles, roofs shall be also taken into consideration, [8]. Rescue of animals threatened by flood does not usually cause major problems. This is done mainly by farmers themselves. Difficulties arise mainly when they need to be rescued from rooms flooded with water or on fire. To save an animal, it is often enough to free them from closure or tether. The animal rescues itself. To rescue animals trapped in trenches, swamps the most common equipment and tools are used. They can be: cranes, pneumatic pillows, tripods with blocks, rods, ropes. During the evacuation some veterinary advice may come in priceless.

7. Conclusions

Evacuation is a very important undertaking in the event of an emergency that threatens the safety of people, animals and property. It is performed according to a plan, following previously prepared evacuation Plans or on interim bases, if necessary. The existing legal regulations in power clearly identify the responsible people and evacuation rules. The supreme principle resulting from normative documents and the practical realization of evacuation, implicitly orders to rescue in the first place the lives of people, as the highest good, and only later animals and property.

The evacuation process as a multi-stage one must be well prepared (plans, procedures) and logically secured, especially in the case of evacuation of animals, which unlike humans, need special loading and unloading and transportation facilities.

The evacuation of animals, especially farm animals, in practice is almost in parallel with the evacuation of the population. However, it is characterized by the specificity resulting from the instinctive behaviour of particular animal species in the face of threat. Therefore, rescuers of animals must take into account the specifics of their often unnatural behaviour resulting from fears and unrest in a new unnatural situation. The specificity of the evacuation of the animals is also connected with the necessity of proper preparation of rescuers, and the use of the equipment adapted accordingly, which is not always available.

Therefore, it seems appropriate to improve the rules and prepare owners of animals and rescuers, as well as equipment for the efficient conduct of the evacuation of animals. It would also be advisable to consider the evacuation of wild animals in special farms (e.g. fox or bison farms, etc.) and in zoos, where the multiplicity and diversity of species can greatly complicate their evacuation. Another question is a human factor, more references regarding [10].

Acknowledgments

This article was created as a one of project outcomes of work co-funded by the Slovak Research and Development Agency under the contract No. SK-CN-2017-0023 Enhancing Cooperation of the Ningbo University of Technology and the University of Žilina in research, innovation and cooperation within the topic of "Intelligent Transport Systems".

The views expressed, however, are solely those of the authors and not necessarily those of the institutions with which they are affiliated or of their funding sources. The authors are solely responsible for any errors or omissions.

References

[1] Guildlines of Civil Protection Force of 17 October 2008 on Rules for Evacuation of People, Animals and Property in Case of Mass Crisis Situation.
[2] NOWAK, E.: Logistics in Crisis Situations. AON, Warszawa, 2005.
[3] FICON, K.: Crisis Logistics. BELStudio, Warszawa, 2011.
[4] PRZEWORSKI, K.: Evacuation as a Mean to Protect People. AON, Warszawa, 2002.
[5] Instruction on the Rules of Evacuation of People, Animals and Property in case of Main Crisis. Warszawa, 2008.
[6] SIENKIEWICZ-MALYJUREK, K., KRYNOJEWSKI, F. R.: Crisis Management in Public Administration. Difin, Warszawa, 2010.
[7] BIELICKI, P.: Evacuation of People, Animals and Property. Training materials of State Fire Service, Ostrow Wlkp., 2016.
[8] SURALA, Z.: Training Materials for Fireman. Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej im. Jozefa Tuliszkowskiego, 2009.
[9] Exerpt from Council Regulation (EC) No 1/2005 of 22 December 2004 Related to Protection of Animals during Transport and Related Operations.
[10] ZANICKA HOLLA, K., MORICOVA, V.: Human Factor Position in Rise and Demonstration of Accidents. Communications - Scientific Letters of the University of Zilina, 13(2), 49-52, 2011.

Martin Boros - Anton Siser - Zoran Kekovic - Jan Mazal*

MECHANICAL CHARACTERISTICS OF CYLINDER PIN TUMBLER LOCKS AS THEY RELATE TO RESISTANCE TESTING

In recent years, there has been a great development of methodologies, procedures and software tools for quantitative assessment of reliability, efficiency and effectiveness of physical protection systems. Absence of some important input values, as well as missing method to obtain them, is still the most serious problem. This paper is focused on analysis of possibilities how to obtain delay time values in the case of cylinder pin tumbler locks using non-destructive methods of breaking. In the introduction of the article, a proposal of the methodology for testing the mechanical resistance of cylinder pin tumbler locks is elaborated. Consequently, the focus is set on analysis of results obtained during the pilot tests in order to verify the correctness of the proposed methodology. With the tests, it is possible to assess the resulting resistance of cylinder pin tumbler locks also in terms of classification into resistance classes. The pilot testing needs to be implemented mainly due to the lack of a technical standard that processes the issue within the established methodology.

Keywords: *cylinder pin-tumbler lock, resistance, delay time, methods, testing*

1. Introduction

The aim of this article is to find out the mechanical resistance of cylinder pin tumbler locks against the non-destructive methods. The first part deals with description and characteristics of cylinder pin tumbler locks; basic terms that are necessary for understanding this field of study; structure of cylindrical pin tumbler locks and the principles of their function. The next section is focused on methods of breaking the cylinder pin tumbler locks, specifically using bumping, picking and racking, which will also be discussed in more detail. The article also includes a proposal for a testing method, which does not have a normative basis for the selected breaking methods. The final part is focused on connecting the results from the tests performed with their implementation in practice.

2. The cylinder pin tumbler lock - characteristics

The effort to increase safety brought with it a focus on locking systems for cylinder pin tumbler locks. The principle of their function is based on controlling a latch by a cylinder pin tumbler lock. And it is the cylinder pin tumbler locks which increase the level of passive safety in terms of disallowing entry using unauthorized keys. This type of lock is wide-spread in our territory and it's used in most houses, flats and industrial objects, [1], [2]. The principle of cylinder pin tumbler lock's function is based on inserting a key into the keyhole. Every key is unique in its profile, which ensures the tumblers and driver pins, which are being pressed towards the key using springs, to line up and create a separation between the cylinder and the plug (Figure 1).

As can be seen in Figure 1 left, a common cylinder pin-tumbler lock is made of several basic parts. The main part is the shell and its shape depends on the use and type of the locking system. Its main function is to connect all parts of the cylinder pin tumbler lock into one compact unit. Plug is the rotating part which can be rotated by 360° and thus move the locking mechanism. The plug contains in itself all the openings used for inserting the key pins, usually of a cylindrical shape. Their function is to level the surface between the plug and the shell to allow rotation. The key pins can be put into this position only by inserting the correct key. Opposite to the key pins lay the driver pins, which are used to block the plug. Driver pins can be of various shapes, which influence the ability to resist breaking. In case of protecting against bumping, longer driver pins are preferred. Movement of the driver pins is governed by springs, which are placed in the pin changers inside the shell. They serve to block any movement between the shell and the plug of the lock

* [1]Martin Boros, [1]Anton Siser, [2]Zoran Kekovic, [3]Jan Mazal
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Faculty of Security studies, University of Belegrade, Serbia
[3]NATO Modelling & Simulation Centre of Excellence, University of Defence, Czech Republic
E-mail: martin.boros@fbi.uniza.sk

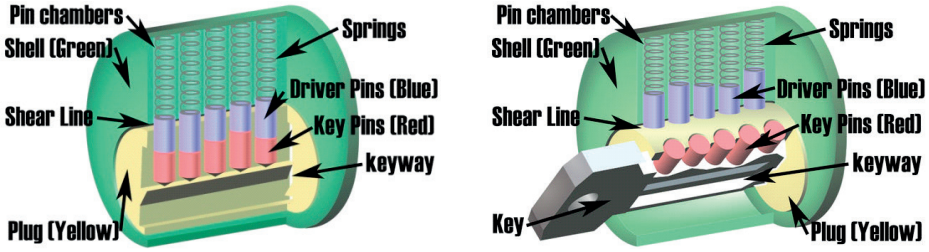


Figure 1 *left - Cylinder pin-tumbler lock design and parts, right - rotation of the plug using a key with correct paracentric profile [3]*

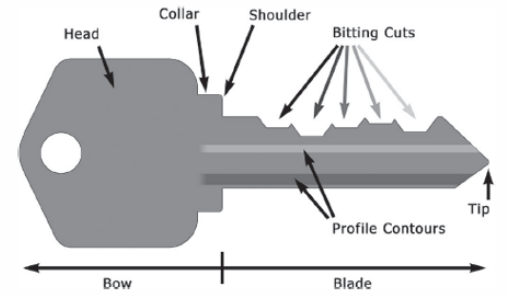


Figure 2 *The various parts and profiles of the key [4]*

when no key is inserted. A unique and important characteristic of a cylinder pin tumbler lock is the shape of the keyway inside the plug. It corresponds with the character of the key which consists of several unique edges and profiles (Figure 2). This way, it is possible to ensure opening a cylinder pin tumbler lock with the correct key only.

3. The cylinder pin-tumbler lock testing using the nondestructive methods

A common trait of all the passive protection systems is their breachability. This depends on various factors, such as length of the attack, types of tools used and abilities of the perpetrator and the structure of the unit. The breaching itself can be achieved in two ways:

- Destructive method, i.e. using tools or brute force with the aim of breaking the structure and properties of the unit, which usually leads to its destruction or permanent damage;
- Non-destructive method, which uses sophisticated tools, which allow to break a passive protection system once or repeatedly without leaving any visible marks [5].

In this article, the focus is on the latter methods for testing the resistance of cylinder pin tumbler locks. The reason for this is an increase of these methods being used in illegal activities, as well as the insufficient processing of the methodology for testing the delay time property of these elements. The technical standard STN EN 1627 through 1630 focus on resistance in static and dynamic load, as well as a manual breaking attempt. STN EN 1303:2015 only focuses on testing through destructive methods, such as breaking the lock or unscrewing the cylinder pin tumbler locks. However, there is not an existing norm, which would contain the methodology for testing the resistance of a cylinder pin tumbler locks through the non-destructive methods of entry in realistic conditions. The absence of such norm makes it impossible to evaluate the delay time of the mentioned locks without resistance class assignment. Without those values, in turn, one cannot evaluate the level of safety for secured objects where such elements are installed [2].

In relation to cylinder pin tumbler locks, we distinguish three most commonly used methods of breakthrough these locks through non-destructive means:

- Bumping,
- Picking,
- Racking [7].

3.1 The bumping method

Bumping represents a dynamic non-destructive method of overcoming a cylinder pin tumbler lock. This method requires the use of a specially modified key. By hitting this key, the energy gets transferred onto the key pins and driver pins, which then jump out of the way and release the plug. The plug can then be rotated and the locking system is deactivated. The whole process begins with preparation, selection or creating of the so-called bump key. The key is inserted into the cylinder pin tumbler lock, its profile and shape must allow for smooth insertion and pulling out of the key. The key is inserted into the keyway stopping before the final key pin. The key is held between two fingers or a specialized tool which allows for greater sensitivity. The second hand holds a screwdriver or a rubber hammer intended for bumping shown in Figure 3. The key is then hit with the rubber part of the screwdriver. When the key is hit, it is slightly rotated. It is necessary to do this at the right moment when the key pins and driver pins are moved away from the shear line – this creates a gap, which allows rotation. The hits and rotation of the key require some sensitivity, skill and training.

When performing the testing, the cylinder pin tumbler locks from security class 1, 2, and 3 underwent the bumping method. In the case of the security class 3, it was not important to establish a breakthrough time. The test should only verify the claimed resistance against this method. Representatives of the security classes 1 and 2 had the maximum breach time set for 3 minutes and 5 minutes, respectively. For the practical use of the bumping

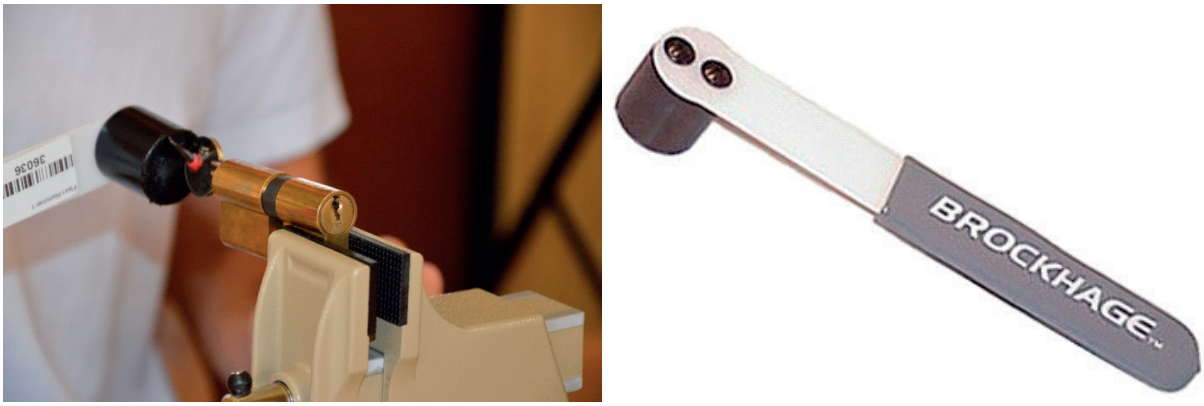


Figure 3 *left - Testing cylinder pin-tumbler locks using a bumping method and right - special bump hammer*

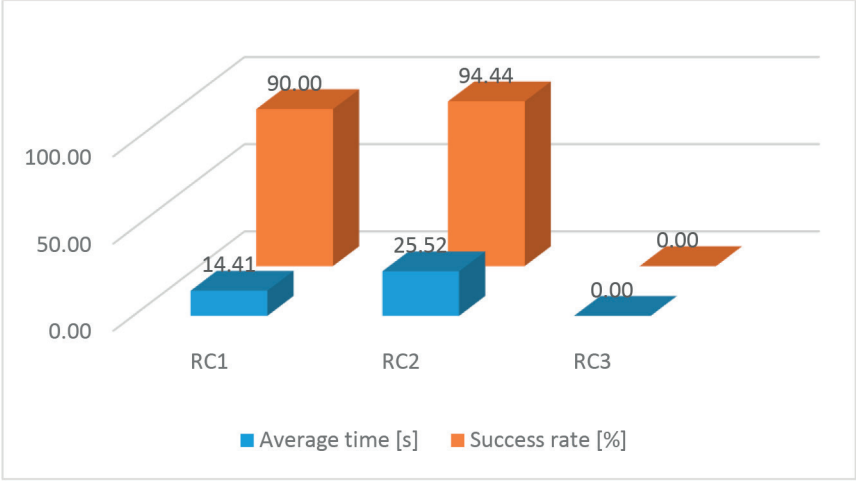


Figure 4 *Average times and success rate obtained from testing*

method, the experimental units were installed into a vice, which allowed for sufficient grip needed for performing the tests. The bumping method was applied to each unit, measuring the time necessary to break it. The idea was to statistically evaluate the success rate of students in breaking the cylinder pin tumbler lock in a non-destructive way. The testing itself was performed by 3 students, each had 30 tries. The results of the breaking test was recorded in form of numerical results.

When testing the unit that belongs to the security class 1, the average time necessary for breaking the cylinder pin tumbler lock was calculated to be 14.41 seconds. Out of the 90 tries, 81 were successful and 9 were unsuccessful. The success rate for breaking the lock was 90%. The average breakthrough time in units belonging to security class 2 was 25.52 seconds. Out of the 90 tries, 85 were successful and 5 unsuccessful. The success rate for breaking the lock was 94.44%. In the case of units belonging to security class 3, the resistance to the bumping method was verified. All acquired results are laid out in Figure 4.

3.2 The picking method

The picking method is generally considered as the most difficult way of overcoming the cylinder pin-tumbler locks. It requires a lot of skill, sensitivity and patience from the perpetrator. A potential criminal with sufficient theoretical and practical skills is, however, able to use this method to breach even the complicated security systems. Similar to other methods, the picking method uses imperfections in the factory processing, which allows slight rotation of the plug, as well as leaving it in the right position without using the correct key. Applying tension is the most important stage of the process, which determines the overall success of the operation. The amount of tension causes the driver pins to stay on the edge of the plug and not return back. The entire process has to be done using specialized tension tools shown in Figure 5 left. The second process, occurring simultaneously with continuous application of tension, is pushing individual key pins, which act on the driver pins with the aim of finding the correct unblocked position. This is done using different picks, their shape depending on the type of the cylinder

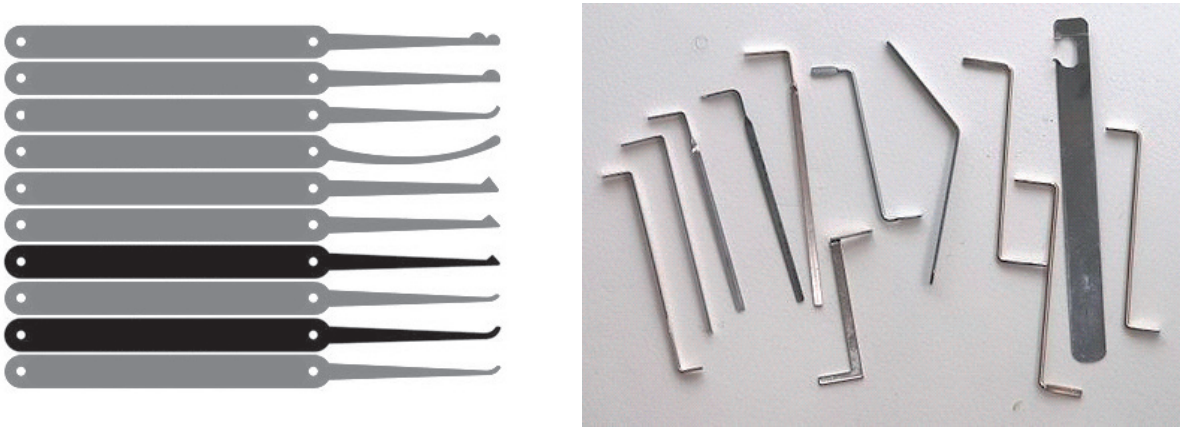


Figure 5 *left - Set of various picks and right - tension tools used in lock picking method [8]*

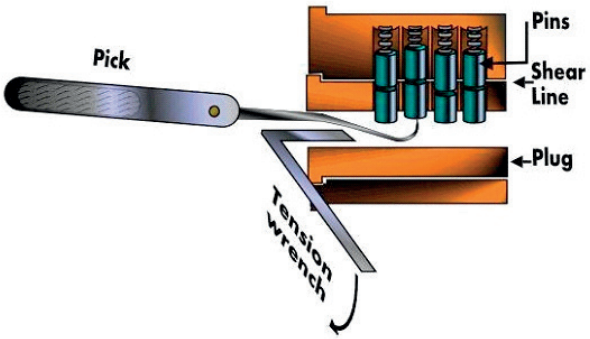


Figure 6 *Use of the picking method in practice [9]*

pin-tumbler lock. The basic pick types are shown in Figure 5 right. The process of this method is shown inn Figure 6 for easier understanding.

Testing of the picking method was performed on representatives of cylinder pin tumbler locks from resistance class RC1 through RC3 using a process described earlier. In the case of the RC1 representative, the maximum time for opening the lock was set for 5 minutes. Out of 10 tries to open the lock using the picking method, the lock was breached two times with the average breakthrough time of 4 minutes and 47 seconds. To breach an RC2 cylinder pin tumbler lock, the maximum time was set for 10 minutes. The lock was only overcome once out of 10 tries in 8 minutes and 12 seconds. All other tries were finished after the predetermined amount of time has run out. In the case of the RC3 cylinder pin tumbler lock, the maximum time for overcoming it was set for 15 minutes. Not a single try resulted in opening this lock. The reason for this is the technical solution and quality of the tested unit, which is protected against this method by a blocking driver pin. The result of the testing is shown in Figure 7.

3.3 The raking method

Raking is the fastest method of non-destructive breach of a cylinder pin-tumbler lock. The perpetrator does not need very skilled hands, but the method is less effective than the picking method. As with the picking method, there is a very important phase of raking, which is applying the correct tension on the plug. This is done in the same way, using the same tension tools. The important distinction lies in the way the driver pins are pushed by interacting with the key pins. In this method, different picks are used (Figure 8), which are generally longer and have more bends. These picks are inserted into the keyway and by repeated swift movements over the key pins, one is trying to find a position in which the plug can be rotated. The process of this method is shown in Figure 9.

Testing the resistance using the raking method was performed on identical samples as with the case of picking method. The RC1 representative was breached 18 out of 20 times, average time for opening the lock was 1 minute and 53 seconds. The second tested unit represented the RC2 category resisted only 7 times out of 20 tries. Average breakthrough time was 4 minutes and 13 seconds. Same as with the picking method, the RC3 locks were not broken. The reason for this is the aforementioned technical solution. For an easier understanding of all the results acquired from the testing, all the measured values are projected in graphs in Figure 10.

4. Conclusions

The article focused on the problem of testing the mechanical resistance of the cylinder pin tumbler locks. The first part focused on describing the testing of cylinder pin tumbler lock using the non-destructive bumping method. Then the methodology for testing the lock through this method was proposed. Based on the tests performed, one can state that breaching a cylinder pin tumbler lock requires some knowledge and skills, which can be

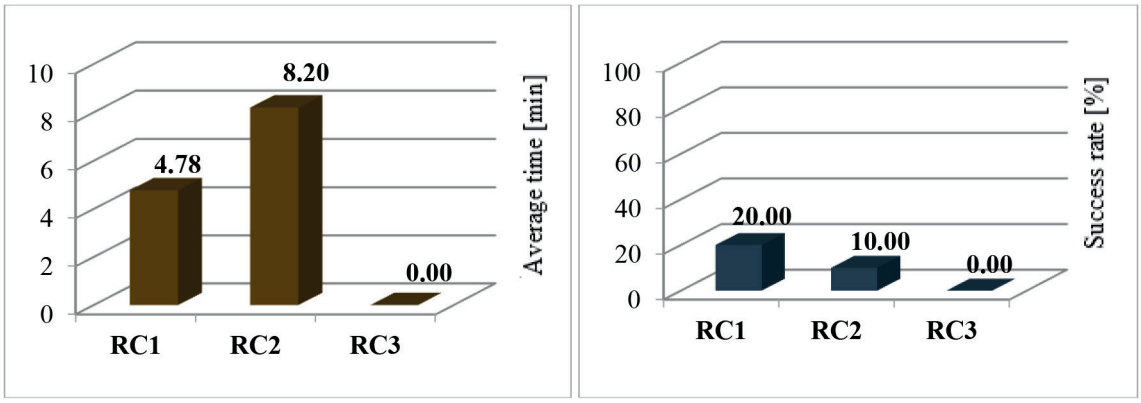


Figure 7 *left - Average breakthrough time and right - success rate using the picking method*

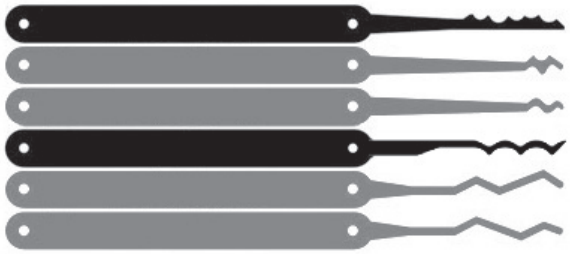


Figure 8 *Set of various picks used in the lock-raking method [8]*

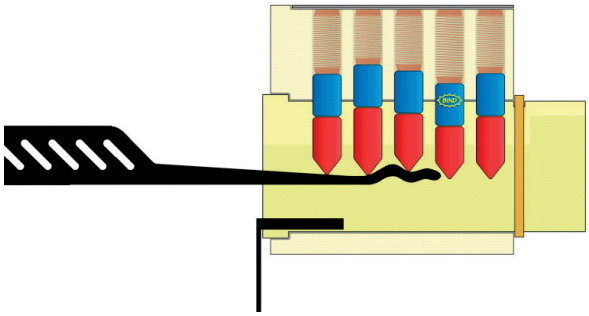


Figure 9 *Use of the raking method in practice [9]*

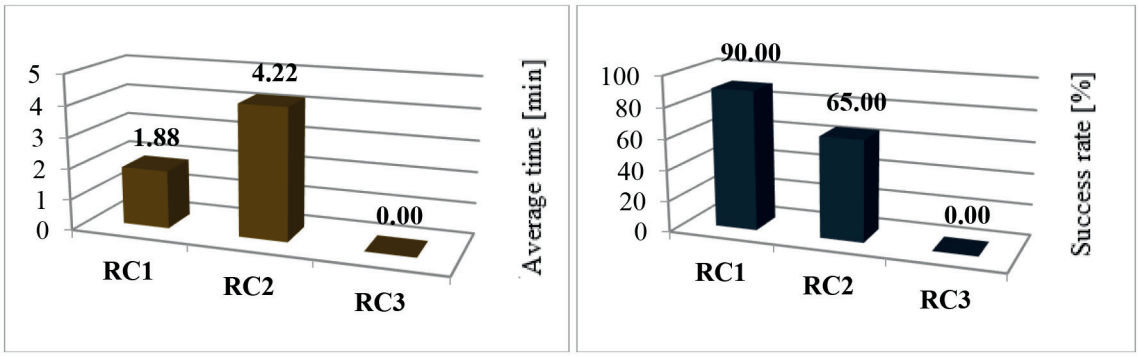


Figure 10 *left - Average breakthrough time and right - success rate using the raking method*

acquired in a relatively short time; this in turn creates a high level of risk in terms of securing objects. The main benefit of this article was the effort of the authors to point out to an absence of norms, which would regulate the testing of cylinder pin tumbler locks through non-destructive bumping, picking and racking methods and the need to address this situation. At the same time, these tests could be considered a starting point with the aim of creating a basis for further investigation.

Acknowledgments

This work was supported by the institutional grant project IGP 201701 and IGP 201704.

References

[1] MACH, V.: Security Systems - Passive Barriers (in Slovak), first edition. Multiprint, Kosice, p. 199, 2010.
[2] MITRIK, M., MACH, V.: Passive Barriers, first edition. VSBM, Kosice, p. 135, 2008.
[3] How to Pick a Lock (Basics) [online]. Available: www.instructables.com /id/How-to-Pick-a-Lock-Basics/ [accessed: 2018-02-10].
[4] Lock Basics and How to Work with them [online]. Available: www.digitalcitizen.life/book -review-practical-lock-picking-second-edition-deviant-ollam [accessed: 2017-12-22].
[5] IVANKA, J.: Passive Barriers (in Czech), second edition. UTB, Zlin, p. 148, 2014.
[6] LOVECEK, T., REITSPIS, J.: Designing and Assessing Object Protection Systems. EDIS, Zilina, 2011.
[7] GARCIA, M. L.: The Design and Evaluation of Physical Protection Systems. Elsevier, USA, 2001.
[8] Raking vs. Single Pin Picking [online]. Available: https://unitedlocksmith.net/blog/raking-vs-single-pin-picking [accessed: 2018-01-08].
[9] The Rake Method - A Brief Guide [online]. Available: https://www.bumpmylock.com/pages/the-rake-method-a-brief-guide.html [accessed: 2018-01-08].

Valeria Moricova - Monika Vaclavkova - Jana Studena - Bo Wang*

A SOFTWARE TOOL TO SUPPORT THE SELECTION OF CANDIDATES IN PRIVATE SECURITY SERVICES

Nowadays the protection of life, health and property of individuals is in the centre of public interest. There is not a distinction between the provision of such protection by private or public sector. The private security services play an important role in protection of persons and property. The subjects of protection are not only people and property, but also sensitive information which is relevant for the state interest or business entities. Based on research, the private security services do not make a selection of employees systematically. One of the reasons is the absence of an analysis of candidates' personal competencies which should take into account the requirements of the protected subject. The aim of the article is therefore a software solution for modelling the personal competencies of applicants for the job in private security services.

Keywords: *security services, selection of employees, software*

1. Introduction

The problem of selection of security service employees and their competencies is solved by the project research team (employees of the Faculty of Security Engineering and Faculty of Management Science and Informatics) in the project „Optimisation of the competencies in correlation with the particularity of the type positions in security services“ (VEGA 1/0064/15). The main goal of the project is to *create a tool enabling modelling of the personal competencies of the applicants for private security services depending on requirements of the security environment and protected interest.* The software tool is created in the conditions of the Slovak Republic, in Slovak language, and it consists of adatabase system and aweb application.

Private security in Slovakia operates as a *private security service and technical service* to protect persons and property. Requirements for running a security service (professional, physical and mental) are stated in the Directives [1], [2]:

- Act No. 473/2005 Coll. On providing services in the field of private security and on modification and amendment of certain Acts,
- Regulation of the Ministry of Internal Affairs No. 634/2005 Coll., which is used to implement the provisions of the Act No. 473/2005 Coll. On providing services in the field of private security and on modification and amendment of certain Acts.

In the Act on providing services in the field of private security (Act No. 473/2005 Coll.), system requirements in terms of the qualification of private security service providers are not specified. Guard duty and detective services are considered the same. Fundamental differences in the subject matter, personnel competencies and expertise are not respected. The Act demoted the more demanding detective service to the level of the standard physical protection (e.g. qualification requirements, professional knowledge, general eligibility). Hereby the system of personnel selection and educational preparation of the detective service providers is depreciated.

2. Selection of security staff

The selection and recruitment of new employees is a significant step for an organization and can be understood as an investment into its development. Even the process of employee selection for private security service providers is quite problematic. Nevertheless, there is an effort to identify basic competence requirements for some type positions, which can be evaluated positively (National Occupation System http://www.sustavapovolani.sk). Based on theoretical knowledge, surveys and practical experience, an algorithm for the selection of security staff was created. This algorithm contains the following subsequent steps [3]:

* [1]Valeria Moricova, [2]Monika Vaclavkova, [1]Jana Studena, [3]Bo Wang
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Faculty of Management Science and Informatics, University of Zilina, Slovakia
[3]Ningbo University Of Technology, China
E-mail valeria.moricova@fbi.uniza.sk

Preliminary phase:

a) Job analysis;
   - Security analysis of an object and its environment:
     - Job description;
     - Job specification;
b) Defining the suitability of employees;
c) Recruitment.

Selection phase:

a) Examining a structured Curriculum Vitae and a personal questionnaire;
b) Preliminary (initial) interview;
c) Testing the applicants;
d) Selective (continuous) interview;
e) Examining references.

Evaluation phase:

a) Selection assessment;
b) Selective (final) interview;
c) Decision on applicant selection;
d) Informing the applicant of the selection.

Using the above algorithm, for the needs of the National System of Professions by the expert group of the Slovak Chamber of Private Security, 10 type positions were updated and **6 type positions were newly established** [3]: Manager in the field of guard and detective services and self-protection; Project Specialist in the field of private security; Lecturer in the field of security services; Detective Specialist; Trainee Detective; Chief Detective.

Subsequently, private security staff files were created for all type positions. Each file contains the characteristics of a type position, a job description, occupational regulation, the ISCO-08 and ISCO-08 specification as well as the required level of education in terms of the European Qualifications Framework and the National Qualifications Framework. The file also lists the general capabilities, expertise, and skills that an ideal security employee should have. For a particular type position, the preferred level of the selected general competencies (elementary, advanced, high) and the Head of Physical Protection Change level of the qualification framework (professional knowledge and skills) are assigned. The defined requirements were the starting point for creating a software tool to support personnel selection in security services.

3. Software tool to support personnel selection in the security services

Information systems are an inseparable part of human activity in nearly all fields [4]. For example, in the field of Crisis Management, it is obvious that the management of crisis situations is undergoing rapid changes due to advances in Information Technology. After over three decades of application of computer based information systems to the crisis management, these systems are getting wider acceptance by the community of emergency managers [5]. In the field of Security Management, various supportive software tools are more and more frequently used [6].

Firms engaged in security services such as Private Security Service (further SBS) also belong to the field of security technologies. Within the optimisation of SBS services in the Slovak Republic, there is an effort to deal with the competencies of the hired employees. To simplify the activities connected with the mentioned problem, within the project VEGA 1/0064/15 supportive software tool was designed and implemented. Figure 1 depicts the data model of the designed software tool database.

4. Development of the software tool database

When developing software systems, it is necessary to set basic system requirements at the beginning. That is why the very first step of the software tool creation was defining requirements for the functionality of the respective tool.

Since the experts from various fields take part in the project, it was necessary to create a set of requirements, so that it would suit the needs of the experts from the security management and psychology. At the same time, it was necessary to specify the requirements, so that it would also follow the needs and suggestions of the experts from the field of informatics. Therefore, the initial phase of the project included several project team member meetings to specify the requirements.

The basic part of the tool is the database of individual type positions as well as the database of all attributes, specifics and characteristics of individual type positions. Based on the Act No. 473/2005 Coll., which puts emphasis on integrity, reliability, health and required professional eligibility of the employees of SBS, the basic structure of the database was created. The second source of creating the basic structure of the database was the register of occupations of the National Occupation System – area SBS. The two respective sources formed the part of the database which was named *legal requirements.* Requirements of this part of the database are necessary for the creation of the software tool as early as the first step of its implementation.

The second group of requirements for the data and the database were the specifics of individual objects from the point of view of risk analysis. To be more precise, it is the specification of inner and outer security risks, sources of danger in the respective object and the whole of the situation from inner or outer point of view in the respective object where the type position will be carried out. The methods and forms of protection required in the respective object will result from identified security risks and dangers. These methods and forms will then indicate certain supplementary requirements for the corresponding type positions. This part of the database was named *specific requirements.* The listed group of requirements is currently in the process of extension and will be implemented in the near future. Within the

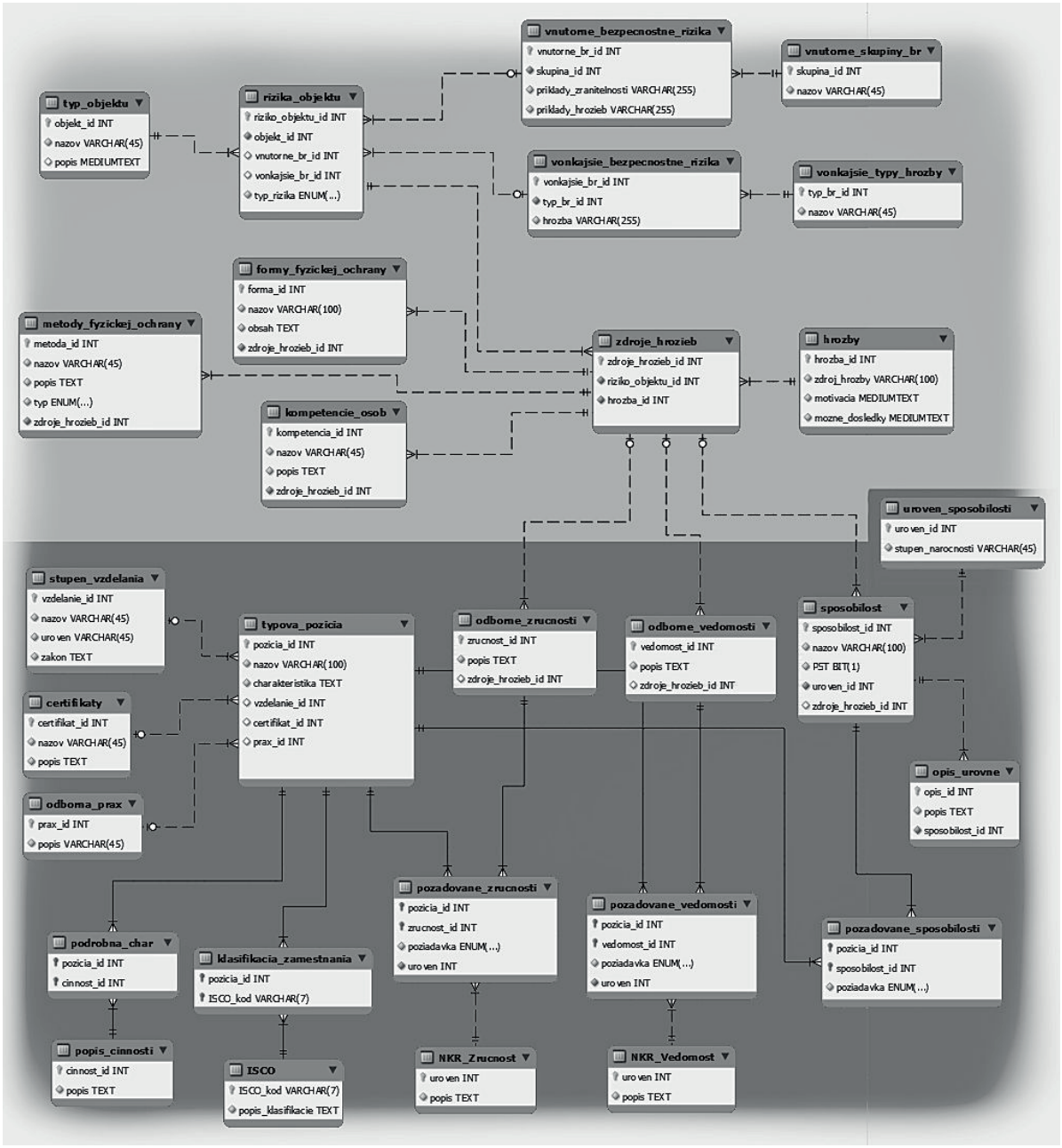


Figure 1 *Data model of the database of the designed software tool - see Annex for English equivalents of the tokens and collocates*

project, our goal was to take into account all the requirements, the legal group as well as the group of specific requirements. However, the project had limited human and time capacities and that is why, in the first phase, our attention was focused on the group of legal requirements.

The database of the software tool consists of data of various nature and in the present, the most appropriate tool to accomplish this task is the relational database system. Before developing the database, it was necessary to design its structure by the means of the data model. The development of the data model underwent several phases of modification and, as a result, several alternatives were created. The eventual alternative consisted of 29 database tables so this data model can be considered large.

Based on the data model, the database system which enables administration of individual dials in the database was developed. The database system MySQL is the system in which the database is implemented. This system is at the moment the most popular and freely spreadable from all SQL systems in the field of

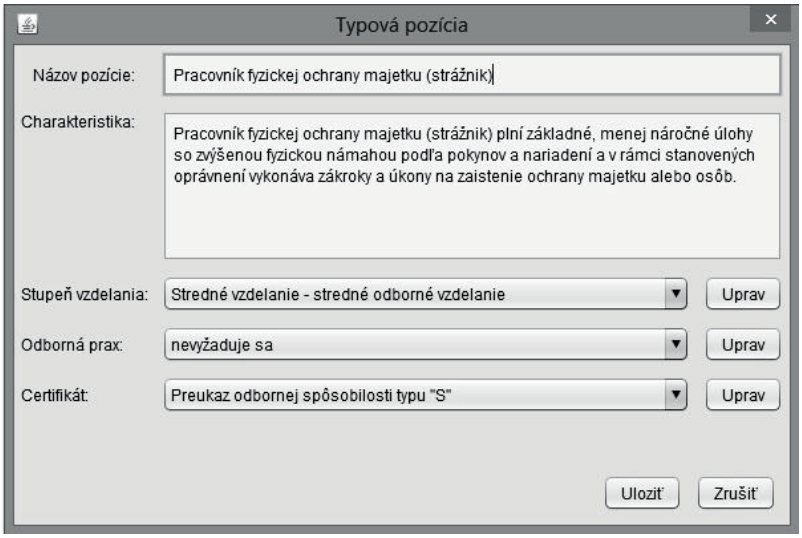


Figure 2 *Form for modifying the type position - see Annex for English equivalents of the tokens and collocates*

the database administration. It is developed, distributed and supported by Oracle Corporation. When developing the database, the tool MySQL Workbench was used, which is the graphic tool for the work with MySQL servers and databases. It fully supports MySQL Server, versions 5.1 and higher. It is compatible with MySQL Server 5.0, but it does not support all its functions. It is not compatible with MySQL Server, versions 4.x.

For developing the application of the database system working over the database, the programming language Java was selected. Java is an object oriented programming language, originally created by Sun Microsystems. The advantage of the language Java is that the source codes are independent from the computer architecture and they can be activated on any device which has virtual Java machine (JVM) available.

The environment that was used when developing the respective application was the environment of NetBeans which currently is one of the most used development environments. NetBeans is officially the development environment for Java 8. It is a simple tool for development of Java desktop, mobile and web applications, but also HTML5 applications with HTML, JavaScript and CSS. The main advantage of the NetBeans environment compared to other rival environments is the fast development of user interface, which is enabled by the graphic editor with a drag-and-drop tool.

When developing the database system, the technology Hibernate was used and it is one of the fastest developing information system technologies. The Hibernate ORM is an object-relational mapping framework for the Java language. Its main task is to map Java classes to database tables and data of Java types to SQL data types.

In Figure 2, there is one of the forms for editing the database, to be more specific, for editing the type position and its attributes. The respective form is connected with other forms, so that it copies the relations among individual dials in the database.

The database system was designed as a part of a software tool unit in the form of one common component. The database system enables creation of new items in the database, removal of unnecessary items as well as the change of desired items. The database system was tested at the Faculty of Security Engineering, University of Zilina (further FSE) and the verification was successful. The database system will be placed on the FSE server and it will be administered by an administrator (the main administrator/administrator) to prevent changes in the system by any of the users. The administrator will have an authorization for editing the database entries and will become the database manager.

5. Completion of other parts of the software tool

After developing the database, it was necessary to create an application for other users of the software tool. Since in our conditions it is a standard to expect a common user to be able to operate web browsers and web applications, the next part of the software unit was designed as a web application. The advantage of such application is that the website is accessible to a wide range of users without necessity of further installation of a new application to the personal computer, whereby it is accessible for various devices with the Internet access. Nowadays, the web applications are a growing trend in the field of IT technologies.

Initially, the application was implemented for the part of the database which deals with legal requirements. In the near future, the web application will be extended with the definition of requirements, placed in the group of specific requirements.

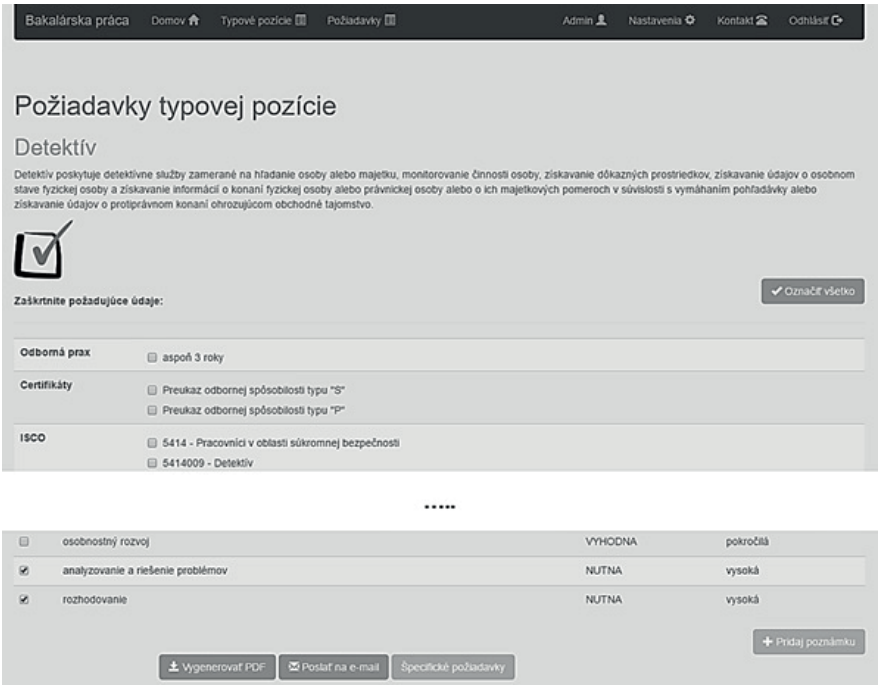


Figure 3 *Part of the form for creating a file with the requirements for the type position - see Annex for English equivalents of the tokens and collocates*

There are various different methods how to create a web application. In our project, the most common and the most popular type of web application architecture – Model – View – Controller (MVC) was used. The basic idea of MCV architecture is to detach the application logic from the presentation logic. This is the reason why the application is so well-arranged. It is divided into three components: Model, View, Controller. These components are presented as separate classes apart from the View component.

For back-end (the server part), PHP script language was selected, which is widely used for creating the dynamic web applications, specifically open source PHP framework CodeIgniter with the utilization of HTML5, CSS3, JS and library jQuery. In terms of front-end (the client part), Bootstrap was applied, which is HTLM, CSS and JS framework creating responsive applications on the Web.

The web application again copies the strategy of the database part, so that it enables the work of users on three different levels:

- common user can use the limited number of operations which he/she can conduct,
- administrator can implement changes in the data,
- main administrator can manage the administration rights for the common administrator.

Potential users of the web application are personnel managers in security services (common users).

After loading the website, in the window of the browser, the registration window with the possibility of authentication will display. After filling in the respective form, the user will be sent the file with the registration data.

If the user clicks on the icon „type positions“, the list of 16 type positions identified within security services in the National Occupation System will display. Each type position is described and there is also an icon of magnifier. The icon of magnifier enables the user to display the form with respective requirements for the selected type position. The form is quite large.

For each item, which defines the category of requirements for the selected type position, the title of the specific item is stated as well as respective options of particular requirements. With each requirement, there is a tick window which the user can mark. In the top right corner of the form, the user can mark all the requirements for the selected type position at once. In the right part under the last requirement, most of the requirement categories feature the option to add a note where the user can complete his/her notes, but also various additional specific requirements for the selected type position, which are not available in the database. If the user wants to create a file with selected requirements, he/she can do so in the bottom part of the window where there is a possibility to generate a file on the disc, which will encompass all the selected requirements according to the categories, in the PDF format. The second possibility is to have the respective file sent to the email address stated in the data.

Due to the form size, in Figure 3 only a part of the displayed field is presented. It is only one category of requirements. Further categories in the system are selected in a similar way, as in Figure 3.

The user with the authorization of the administrator or the main administrator has besides the stated possibilities also the right to conduct activities linked with editing specific items in the database. He/she can modify the list of requirements in some of the categories of requirements for specific type positions. Apart from this, administrators are responsible for delegating or taking away the authorization of a common user, as well as the administration of user accounts.

The process of selecting the most suitable job applicant can be supported by several methods of multi-criteria decision-making, e.g. Analytical Hierarchy Process (AHP), Decision Matrix Method (DMM), Forced Decision Matrix Method (FDMM), Potentially All Pairwise Rankings of All Possible Alternatives (PAPRIKA). An automated selection of candidates using the above methods may be an extension of the proposed software.

6. Conclusion

The solution of security problems and crises is influenced by various factors. The most significant features of crises are the lack of time and information, which puts a lot of pressure on the employees. These requirements on preparation of individuals for specific type positions are increasing. Itis the reason why the level of competencies required from employees of security services is also increasing, proportionally to their work activities [7], [8].

Creation of the software tool to support the selection of employees in security services was a part of the solution of the project VEGA 1/0064/15 for optimisation of competencies for type positions in SBS. A supportive software tool consisting of more components – modules, which were implemented with the use of current modern technologies, was developed. The created tool is easy to use and, supposedly, the users will not have problems to learn to operate it. In the first phase of the task solution, dials for the database system were prepared, even for specific requirements. However, because of the capacity of the project personnel as well as because of the project time horizon only legal requirements were included in the web part of the implemented software tool. Currently, an analysis of the specific requirements is being conducted, plan to include it in the advanced web application.

Due to the above mentioned reasons, the designed software tool has some limits. At the moment, the tool is available to specific SBS users so they can test it and comment on possible improvements. After delivering the comments in the form of a test protocol, the tool will be adjusted to the needs of the users. However, even the current solution can, when being correctly used, simplify the work of selection of employees for type positions in security services.

Acknowledgements

This work is supported by grant VEGA 1/0064/15 named “Optimisation of the competencies in correlation with the particularity of the type positions in security services”.

References

[1] Act No. 473/2005 Collection of Laws about Providing Services in the Field of Private Security and about Modification and Amendment of Some Laws [online]. 2017. Available: http://www.noveaspi.sk/products/lawText/1/60783/1/2 [accessed: 2017-09-02].

[2] Regulation of the Ministry of Internal Affairs SR No. 634/2005 Collection of Laws, which is Used to Implement the Provisions of the Law No. 473/2005 Collection of Laws about Providing Services in the Field of Private Security and about Modification and Amendment of Some Laws [online]. 2017. Available: http://www.noveaspi.sk/products/lawText/1/60948/1/2 [accessed: 2017-09-02].

[3] VIDRIKOVA, D., BOC, K.: Personnel Aspects of Selecting Human Resources for Private Security Services. University of Zilina, Zilina, p. 237, 2014.

[4] REITSPIS, J., MESAROS, M., BARTLOVA, I., CAHOJOVA, L., HOFREITER, L., SELINGER, P.: Management of Security Risks. EDIS, Zilina, 2004.

[5] RISTVEJ, J., ZAGORECKI, A.: Information Systems for Crisis Management - Current Applications and Future Directions. Communications - Scientific Letters of the University of Zilina. 13(2), 59-63, 2011.

[6] RISTVEJ, J., LOVECEK, T.: Software Products for Risk Assessment. Mathematical Methods and Techniques in Engineering & Environmental Science, Proceedings of 4th WSEAS International Conference on Natural Hazards (NAHA´11), Italy, 198-203, 2011.

[7] LOVECEK, T., RISTVEJ, J., SVENTEKOVA, E., SISER, A., VELAS, A.: Currently Required Competencies of Crisis and Security Managers and New Tool for Their Acquirement. Management Innovation and Business Innovation, Proceedings of 3rd International Conference on Management Innovation and Business, Philippines, 3-8, 2016.

[8] TITKO, M., ZAGORECKI, A.: Modelling Vulnerability of Transportation Network Using Influence Diagrams. Communications – Scientific Letters of the University of Zilina, 15(4), 97-100, 2013.

Annex for English equivalents of the tokens and collocates

Table A1 *English equivalents figure 1 Data model of the database of the designed software tool*

Slovak terms	English equivalent
Typ objektu	Object type
Riziko objektu	Facility risk
Vnutorne bezpecnostne rizika	Internal security risks
Vonkajsie bezpecnostne rizika	External security risks
Vnutorne skupiny	Inner groups
Vonkajsie typy hrozby	External types of threat
Metody fyzickej ochrany	Physical protection methods
Formy fyzickej ochrany	Forms of physical protection
Kompetencie osôb	Competence of persons
Zdroje hrozieb	Threat sources
Hrozby	Threats
Stupen vzdelania	Level of education
Certifikaty	Certificates
Odborna prax	Professional experience
Typova pozicia	Type position
Odborne zrucnosti	Professional skills
Odborne vedomosti	Professional knowledge
Spôsobilost	Competence
Uroven spôsobilosti	Level of competence
Opis urovne	Description of the level
Podrobna charakteristika	Detailed characteristics
Popis cinnosti	Activity description
Klasifikacia zamestnania	Job classification
Pozadovane zrucnosti	Required skills
Pozadovane vedomosti	Required knowledge
Pozadovane spôsobilosti	Required competences

Table A2 *English equivalents figure 2 Form for modifying the type position*

Slovak terms	English equivalent
Typova pozicia	Type position
Nazov pozicie: Pracovnik fyzickej ochrany majetku (straznik)	Job Title: Physical Property Protection Officer (Guardian)
Charakteristika: Pracovnik fyzickej ochrany majetku (straznik) plni zakladne, menej narocne ulohy so zvysenou fyzickou namahou podla pokynov a nariadeni a v ramci stanovenych opravneni vykonava zakroky a ukony na zaistenie ochrany majetku alebo osôb.	Characteristics: The Physical Property Protection Officer (Guardian) performs basic, less demanding tasks with increased physical effort according to instructions and regulations and, under authorization, performs interventions and actions to ensure the protection of property or persons.
Stupen vzdelania: Stredne vzdelanie - stredne odborne vzdelanie	Level of education: Secondary education - secondary vocational education
Odborna prax: nevyzaduje sa	Professional experience: not required
Certifikat: Preukaz odbornej spôsobilosti typu “S”	Certificate: Professional license type “S”
Uprav	Edit
Ulozit	Save
Zrusit	Cancel

Table A3 *English equivalents figure 3 Part of the form for creating a file with the requirements for the type position*

Slovak terms	English equivalent
Poziadavky typovej pozicie	Type position requirements
Detektiv	Detective
Detektiv poskytuje detektivne sluzby zamerane na hladanie osoby alebo majetku, monitorovanie cinnosti osoby, ziskavanie dôkaznych prostriedkov, ziskavanie udajov o osobnom stave fyzickej osoby a ziskavanie informacii o konani fyzickej osoby alebo pravnickej osoby alebo o ich majetkovych pomeroch v suvislosti s vymahanim pohladavky alebo ziskavanie udajov o protipravnom konani ohrozujucom obchodne tajomstvo.	The detective provides detective services: to search for a person or property, to monitor the activity of a person, to obtain evidence, to obtain data on the physical condition of a natural person, to obtain information on the conduct of a natural person or a legal person or on their assets in connection with recovery or collection of data on unlawful conduct threatening business secrets.
Odborna prax: aspon 3 roky	Professional experience: at least 3 years
Certifikaty: Preukaz odbornej spôsobilosti typu “S” / Preukaz odbornej spôsobilosti typu “P”	Certificates: Professional license type “S” / Professional license type “P”
Pracovnici v oblasti sukromnej bezpecnosti	Workers in the field of private security
Osobnostny rozvoj	Personality development
Analyzovanie a riesenie problemov	Analyzing and solving problems
Rozhodovanie	Decision making
Vyhodna	Advantageous
Nutna	Necessary
Pokrocila	Advanced
Vysoka	High
Oznacit vsetko	Mark everything
Pridat poznamku	Add note
Vygenerovat PDF	Generate PDF
Poslat na e-mail	Send to e-mail

Petr Hruza*

RESILIENCE AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

The article deals with resilience and protection of critical information infrastructure elements. The elements affect rapid recovery of the system to its original state and the increase of resistance during the subsequent emergency events. The article also deals with sectoral and cross-sectional criteria for determining the critical information infrastructure elements, which are closely related to resilience and protection. Risk assessment has been conducted in the area of critical information infrastructure. Finally, amendments of the Czech Cyber Security Act have been mentioned.

Keywords: *cybersecurity, resilience, protection, critical information infrastructure*

1. Critical infrastructure and criteria

According to the Act No 240/2000 Coll. on Crisis Management and on Amendments of Certain Acts (Crisis Management Act), **critical infrastructure (CI)** shall denote the **element of critical infrastructure or the system of elements of critical infrastructure, disruption of which would have a significant impact on the state security, on ensuring the basic living needs of the population, on health of people and state economy**. The CI elements are operated by state institutions or private entities. **The European critical infrastructure** shall denote the critical infrastructure within the territory of the Czech Republic, disruption of which would have a significant impact also on another member state of the European Union. **Element of critical infrastructure** shall denote primarily a building, an establishment, a vehicle or public infrastructure, determined in accordance with the cross-cutting and sectoral criteria. The Ministry of Interior (the General Headquarters of Fire Rescue System of the Czech Republic) administers the list of elements of CI. At present there are about 1300 of such elements [1].

In order for an element is to be determined as a part of critical infrastructure it has to meet **cross-cutting and sectoral criteria** having been set by the government regulation No 432/2010 Coll. on the criteria for determining the element of critical infrastructure [2].

The Cross-cutting criteria are considered to be the set of general criteria for assessing seriousness of impact of disruption or destruction of critical infrastructure element with the limit values which include the following [2]:

a) number of casualties (the injured and the dead);
b) economic impact (economic losses or deterioration of the quality of goods or services, including possible impacts on the environment);
c) impact on public (impact on public confidence, physical deprivation and disruption of everyday life, including the loss of necessary services).

The cross-cutting criteria include the aspects of casualties exceeding 250 dead or 2500 people treated in hospital for the period longer than 24 hours, economic impact with the limit value of state economic loss being higher than 0.5 % of GDP, or impact on public as a result of extensive restriction of provision of essential services or other serious intervention into everyday life affecting more than 125 000 people [2].

The Sectoral criteria shall denote technical or operational criteria determining critical infrastructure elements in particular CI sectors, such as e.g. energy, water management, food industry and agriculture, transport and public administration. Public administration then includes e.g. welfare system, state social support or social assistance [2].

The critical infrastructure is very extensive and it is assumed that the state will continuously protect it. The problem is that not all the CI entities belong to the state assets. Some CI entities are owned by the private sector. Even bigger disproportion can be seen in the area of **critical information infrastructure** (CII), in which the entities are owned mainly by the non-state (private)

* **Petr Hruza**
Department of Tactics, Faculty of Military Leadership, University of Defence in Brno, Czech Republic
Email: petr.hruza@unob.cz

sector. Therefore, the protection of the CI becomes a complicated process for the state [2].

2. Critical information infrastructure

Large computer networks, information systems and information services play absolutely essential role in a society. Their reliability and security is necessary for economic and social activities of individual states, and, mainly, for the functioning of state internal market.

The increasing range, frequency and impact of security incidents represent significant threats for the functioning of computer networks and information systems. Computer networks and mainly information systems may also become easy targets for intentional, detrimental actions aimed at damaging or disrupting the operation of systems. Such incidents may cause significant financial losses, breach users´ confidence and cause considerable damage to the state economy as a whole. Management of critical information infrastructure is complicated and mutually interconnected through all the sectors and with high number of participating entities and Czech public administration authorities. It requires a whole number of technical, organizational and other supporting elements with enough time necessary for its solution.

The **Critical information infrastructure** may be perceived as a complex of information and communication systems (meeting the determined cross-cutting and sectoral criteria in the area of cyber security), non-functioning of which may cause a significant impact on the state security, people´s basic necessities of life, health, and on state economy. Critical information infrastructure shall denote the element or the system of the CI elements (according to § 2, letter g) and letter i) of the Act No. 240/2000 Coll.) in the sector of communication and information systems, the area of cyber security (§ 2 letter b) of the Act No. 181/2014 Coll.). In practice they are such information or communication systems (e.g. ICS/SCADA systems), which meet criteria for determining the elements of critical information infrastructure [3].

There have not been signed any international agreements in the area of cyber security yet. The Council of Europe Convention on Cybercrime, known also as Budapest Convention, deals with cybercrime to a minor extent. The Act on Cybersecurity and its implementing regulations are rather non-binding recommendations and obligations to protect important information systems formulated e.g. in the reports of the UN Group of Governmental Experts (UN GGE) or in the confidence building measures taken by the OSCE member states. The judicature of the European Court of Human Rights does not deal directly with cyber security either [3].

The critical information infrastructure, as a subset of the critical infrastructure shares a number of characteristics with its other components (e.g. transport infrastructure or energy networks), but it shows some significant distinctions.

Common characteristics include e.g. the necessity to provide permanent power supply of the key sites, consider impacts of the elements and possible direct threats posed by hostile individuals. With regard to prediction and timely warning against the failure of function delivery the same procedures may be applied as elsewhere.

The question is what may be included into the above mentioned critical information infrastructure? There are mainly data networks, no matter how they are labelled. Central elements, mainly their control, are particularly sensitive sites. Computational systems cannot be disregarded, because they provide users with services (content) without which the significance of networks would not be so high.

Data networks help in daily life, e.g. in cashless payment systems. Longer failure of such systems would make arranging basic necessities of life impossible and would probably require improvised solutions, e.g. in case of food.

3. Resilience and protection of critical information infrastructure

Resilience is the ability to absorb, adapt to and recover fast from the impact of an emergency. Element resilience consists of technical resilience (determined by its robustness and renewability) and organizational resilience (i.e. the processes leading to the strengthening of technical resilience or its adaptability). The element resilience is the higher the lower is the decrease of its performance in the shortest time during an emergency. Vulnerability is the opposite of resilience. Resilience represents internal preparedness of an element for external emergency.

Resistance is the ability of a system to resist threats while maintaining its functionality. Resistance may be perceived also as the ability of a system not to lose its functionality. Infrastructure resistance may be perceived as the ability to reduce the range and time of an emergency. The critical infrastructure resistance is about supplying elementary goods and services regardless an emergency. The efficiency of infrastructure resistance lays in its ability to adapt to or recover fast from emergencies. The resistance of critical infrastructure is an indicator showing the ability to provide the functioning of a system or an element under the impact of external and internal elements. The resistant element provides its target function even under the conditions having degrading effects.

Protection and resilience of critical infrastructure are not contradictory concepts. They represent necessary elements of a complex risk management strategy. Strong foundations built for the protection and resilience of the critical infrastructure remain to be fundamental and decisive part of the risk management in all the areas of critical infrastructure. Suitably determined

impact and sectoral criteria contribute to effective and efficient protection and increased resilience of the critical infrastructure.

The Critical information infrastructure is special by its nonuniformity. Mainly the data networks are operated by many operators, who are in competition with each other. It results in the existence of several parallel area-wide data networks, following their own policies; however, the networks are interconnected in a defined way, e.g. based on the bilateral agreements or in peering centres.

In order to implement security measures in the case when the supply of functions fails, **it is necessary to carry out a rough classification of possible situations** as follows:

- large catastrophe having an impact on a large territory of state, mainly Prague and its surrounding area, where the majority of the network operators are located and the networks are controlled;
- smaller catastrophe having an impact on a part of the state territory;
- cyber attacks against data networks or information systems. Those attacks can be carried out against the networks of one or more operators and may have different goals.

Cyber attacks are special by the fact that **they cannot be specified demographically and their initiators, as well as their purpose are often unknown.** A mere detection is often a problem and includes mainly probes monitoring operation and searching for anomalies.

The issue of cyber attacks **has to be assessed individually** and from different aspect than the above mentioned classical critical infrastructure. The differences are as follows:

- possibility to carry out a massive attack in a few seconds;
- the targets may be area-wide;
- possibility to control key elements unnoticed by their operators;
- possibility to carry out a massive attack from inside the organization;
- the attack itself need not require large resources and may be carried out by individuals with not very high expertise. On the contrary, the preparation of an efficient attack, e.g. searching for weaknesses and vulnerabilities, requires excellent expertise.

It is important to have access to information on the capacity of a network in the real time in order to **build resistant networks**. The information has to be overall, not only from the part of the network. Automated tools should be available and enable comparing the current performance of network with particular metrics or parameters agreed within SLA. The tools should also be capable of determining such situations, which indicate the forthcoming problems.

The most resistant topology is such a topology, in which all the terminal nodes of networks (or the networks themselves) are mutually interconnected. This is the most expensive configuration, though. In practise it is necessary to find such configuration, which balances the cost efficiency and resistance and to provide the systems with the highest capacities of operation with alternative routes, possibly from various providers, being capable of fast activation and the same level of performance.

The resistance of networks can be achieved through the combination of partnerships of service providers, the elaborated design of network, the proactive network management and the recovery programme after an accident. Plans and regular testing are combined with operational philosophy, which connects performance with resistance and resilience capability.

4. Impact and sectoral criteria

Act No 205/2017 Coll. came into effect and amended the Act No 181/2014 Coll. on the Cybersecurity and on the Amendments of Related Acts (Cybersecurity Act), in line with Act No 104/2017 Coll., and other legislation, transposing the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). It became mandatory in the above mentioned Act on Cybersecurity to introduce new persons into the system of cybersecurity, i.e. operators of essential services, administrators of information systems of essential services and operators of information systems of essential services.

Act on Cybersecurity entrusts **The National Cyber and Information Security Agency** (NCISA) with the power to assign the operators of essential services and information systems of essential services in the same way as in the case of administrators of critical information infrastructure. The NCISA is empowered by the Regulation to determine the sectoral and impact criteria. The criteria should specify the level of impact the disturbed essential service has on providing the social and economic activities [4].

The National Cyber and Information Security Agency is the central body of the state administration for cybersecurity, including the protection of classified information in the area of information and communication systems and cryptographic protection. It was established on August 1, 2017 based on the Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts [4].

Chemical industry, medical facilities and gas industry have been beyond the system of critical information infrastructure regardless the cross-cutting criteria set by the government regulation No 432/2010 Coll. on the criteria for determining the element of critical infrastructure. Such a state is unsatisfactory, because information and communication systems in the above mentioned important sectors may cause serious problems both in the cyberspace and real space when ensuring the interests of the Czech Republic. These sectors have been included into a new Directive based on a new NIS Directive. It is necessary to assign

an operator of essential services and define sectoral and impact criteria for each sector.

New regulation shall determine impact and sectoral criteria for determining the operator of essential service and classify the levels of impacts the disturbed essential services have on providing the social and economic activities. It follows the process of determining the cross-cutting criteria according to § 1 of the government regulation No 432/2010 Coll., amended by the Amendment No 315/2014 Coll, and the process of determining sectoral criteria in line with the same government regulation. The reason for such a new regulation is also the obligation of the Czech Republic to implement legal regulations of the European Union, namely **the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016 concerning measures for a high common level of security of network and information systems across the Union** (the abovementioned NIS Directive). According to Article 5, § 1 of the NIS Directive the EU member states are obliged to identify the operators of essential services in each sector and sub-sector with an establishment on their territory by November 9, 2018 [5].

The sectors and sub-sectors are as follows [6]:

1. **Energy** (The sector of energy is further subdivided into sub-sectors of electricity, oil, gas and heating industry).
2. **Transport** (The sector of transport is further subdivided into sub-sectors of air transport, rail transport, water transport, and road transport.
3. **Health** (The sector of health is not further subdivided, although the NIS Directive includes the sub-sector of health care settings). The sector of health is a newly determined sector and its aim is the effort to increase the protection of health care facilities in the area of cybersecurity and thus reduce the risks, which could limit the functioning of facility and its services and consequently threaten patients´ health and lives.
4. **Water management** (The sector of water management is not further subdivided, although the NIS Directive includes the sub-sector of drinking water supply and distribution, namely the production, supply and distribution of drinking water and wastewaters drainage and treatment. The reason for including this sector on the list is its high dependency on ICT. The aim is to cover all the significant areas of this sector and subsequent population protection and provide people with access to safe drinking water, not harmful to their health. Casualties and the compromising of sensitive personal data are not considered as impact criterion in water management).
5. **Banking** - The aim is to cover significant areas of this sector and increase the protection of credit institutions in the area of cybersecurity. Banking is considered to be a significant sector both in the Czech Republic and the EU and thus the regulation and supervision of this sector is harmonized to a large extent. (The number of clients over 500 000 or the market share exceeding 1 % from the banking sector balance sheet).
6. **Financial market infrastructures** (The sector of financial market infrastructures is not further subdivided). They are the operators of trading venues as defined in the Act on Business Activities on the Capital Market. (6)
7. **Digital infrastructure** (Types of services in this sector include the interconnecting of technically self-sufficient networks, providing services to Domain Name System (DNS) on internet and administration or operation of top-level domain (TLD) name registries. Casualties and the compromising of sensitive personal data are not considered as impact criterion in digital infrastructure.
8. **Chemical industry** (Chemical industry is the only sector the regulation of which goes beyond the NIS Directive. Legislation of this sector stems from the authority awarded to the EU member states to regulate the areas considered to be significant beyond the sectors regulated by the NIS Directive. The types of services in this sector are divided as follows: production of technical gases; production of fertilizers and nitrogen compounds; production of pesticides and other agrochemical preparations; production of explosives; processing of nuclear fuel; production of basic pharmaceutical products; production of other inorganic substances; and production of other basic organic chemical substances). The compromising of sensitive personal data is not considered as impact criterion in chemical industry.

The impact criteria for the above mentioned sectors are perceived as impacts of cybersecurity incidents on information system or network of electronic communications in a given sector on the functioning of which a certain service is dependent. It may cause the following [6]:

- serious limitation or disruption of service affecting more than 50 000 people; or
- serious limitation or disruption of another basic service, or limitation or disruption of operation of the CI element; or
- economic loss higher than 0.25 % of GDP; or
- unavailability of service for more than 1 600 people in the case the service cannot be substituted in another way without disproportionate expenses; or
- over 100 dead or 1 000 injured people requiring medical treatment; or
- breach of public security in a significant part of municipality administrative district which would require rescue and disposal operations carried out by integrated rescue system; or
- the compromising of sensitive personal data on more than 200 000 people (this criterion is not in all sectors considered to be relevant).

5. Personnel

At one hand there is a legislation, legal norms and regulations, but on the other hand it is necessary to have also sufficient number of experts working in the area of critical information infrastructure and its protection. At present there is shortage of experts from the area of cybersecurity in all the required sectors (informatics, information security management, law, etc.). The problem is bigger in public administration, because the public administration cannot pay such experts well. Most experts, graduating from universities in the above mentioned sectors, go to private companies, which can offer them higher salaries and other benefits. The lack of experts may result in employing less qualified personnel and it may then be considered to be a cybersecurity threat, because unprofessional management or interventions into the systems belonging to the CI infrastructure or significant information systems may cause their failure. Lack of experts will necessarily lead to the disproportionate dependence of public administration and its information systems on private companies in the area of the ICT services. It may result in the increased costs of administration and thus the increasing burden for the state budget in relation to such suppliers.

6. Conclusion

It is an elementary task of a state to ensure the protection of critical infrastructure. The state has to ensure that the basic elements, connections and flows of the system within the state will remain operational under normal, abnormal and even critical conditions. Those elements are rudiments enabling the state to be capable of reaching stability and starting further development under any circumstances. Protection of critical infrastructure is part of the crisis management. An element has to meet both the cross-cutting and sectoral criteria to be included into the critical infrastructure. The cross-cutting criteria are a set of general standpoints with limit values determining the seriousness of impact disturbing or destroying the CI element. The sectoral criteria are technical or operational values for determining the CI elements in particular sectors of critical infrastructure. The National Cyber and Information Security Agency assigns the operators of essential services and information systems of essential services in the same way as in case of administrators of critical information infrastructure. For this purpose it determines sectoral and impact criteria in this area. On the grounds of the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016, concerning measures for a high common level of security of network and information systems across the Union, the EU member states are obliged to identify the operators of essential services in each sector and sub-sector with an establishment on their territory by November 9, 2018. Therefore a draft of the new regulation has been elaborated and discussed in the paper in more detail.

Acknowledgement

This contribution is part of the research project No VI20152019049 called "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" granted by the Ministry of Interior of the Czech Republic within the Czech Republic Security Research Programme in 2015 - 2020.

References

[1] Critical Infrastructure and its Protection [online]. Available: http://www.hzscr.cz/clanek/kriticka-infrastruktura-a-jeji-ochrana.aspx [accessed 2017-09-11].
[2] HROMADA, M., HRUZA, P., KADERKA, J., LUNACEK, O., NECAS, M., PTACEK, B., SKORUSA, L., SLOZIL, R.: Cyber Security: Theory and Practice (in Czech). Powerprint, Praha, 2015.
[3] Critical Information Infrastructure [online]. Available: https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf [2017-09-20].
[4] National Cyber and Information Security Agency [online]. Available: https://www.govcert.cz/cs/ [accessed 2017-09-28].
[5] Act No. 104/2017 Collection of Laws, amending the Act No. 365/2000 Collection of Laws, on Information Systems of Public Administration and on Amendment to Certain Acts, as amended, Act No. 181/2014 Collection of Laws, on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act), and Certain Acts [online]. Available: https://www.psp.cz/sqw/sbirka.sqw?cz=104&r=2017 [accessed 2017-10-1].
[6] New Cyber Security Notice - Call for Professional Public [online]. Available: https://www.govcert.cz/cs/nova-vkb/ [accessed 2017-10-10].

kamUNikácie
COMMUNICATIONS

Pawel Gromek*

INTRODUCTION TO VOLUNTARY EVACUATION RISK ASSESSMENT

Taking into consideration safety and security viewpoints of persons and property protection, evacuation as common protection mean is well known. Actually, object state-of-the-art comprises solutions generally based on experience gathered in countries much more affected by mass threats as Central Europe nationalities. Voluntary evacuation is treated as the most common evacuation form. Article presents the comparison of research conducted in USA and Poland defining voluntary evacuation scale as a significant risk factor. The evacuation risk influence determinants are described and risk assessment guidelines are performed. The guidelines are related to the state-of-the-art and the local Central Europe determinants.

Keywords: *voluntary evacuation, evacuation scale, risk assessment*

1. Introduction

In the case of emergency, there are generally two basic behaviour patterns – evacuation or sheltering in place [1], [2]. Particular countries have internal conceptions how to use these kinds of people protection measures in accordance with actual safety and security determinants. Common state-of-the-art is constituted in the great part by evacuation strategies elaborated in democratic countries most affected and experienced by mass threats on the world [3],[4],[5],[6]. Many of relevant conceptual elements are common with other countries' evacuation conceptions, including those in the Central Europe [7], [8].

Polish safety and security determinants emphasise the necessity of taking into consideration mostly the evacuation of people as a mean of protection. It is caused by considerably low level of shelters assurance. Based on the Supreme Audit Office data, only 4.37 % of Polish people are secured by shelters and other properly prepared places [9].

Concluding, evacuation will be the most common people protection mean in the case of an emergency in Poland. However, the evacuation action could have complex influence on people safety and security. At one hand, it is focused on protection human life and/or health as well as possessions. At the other hand, additional threats, organizational and non-organizational could be present [10]. In both cases, holistic risk assessment is necessary. All the positive and negative influence factors should be analysed as a starting point to make a decision: "evacuate or shelter in place".

The article presents preliminary research results concerning one of the most important, organizational aspect of evacuation of people. It is the voluntary evacuation. Its scale and determinants could be treated as the basic mass evacuation risk factors. The comparison of the results of research conducted in Poland and USA is described. Those two countries were chosen from the perspective of relating evacuation determinants in the Central Europe representative and the state much more affected by mass threats. Another reason was a similarity of the object kinds of threats and methodology. An attempt at explaining the author's rescue experience is made. The experience concerns many situations, when people in danger did not want to leave their homes and evacuate. A hypothesis of similar behaviour pattern in other Central Europe countries is put forward. It could generate an additional risk related with non-reflecting local evacuation determinants in the light of the world's, evacuation state-of-the-art.

Finally, the voluntary evacuation risk assessment guidelines are performed. Based on the Polish safety and security environment, they could be useful in optimization of evacuation conceptions in other Central Europe countries.

2. Voluntary evacuation venture and phenomenon as evacuation risk factors

Evacuation is defined as a movement of people from the danger zone to safer places [11]. It could be organized, partially-organized or unorganized. Organized evacuation forces

* **Pawel Gromek**
Faculty of Civil Safety Engineering, Main School of Fire Service, Warsaw, Poland
E-mail: pgromek@sgsp.edu.pl

Table 1 *Derivative evacuation threats and their importance priorities in Poland*

No	Derivative threat name	Importance priority (1 – the most important threat)
1	Loss of influence for all evacuation proceeding elements	1
2	Direct danger to life for evacuating and evacuated people	2
3	Information chaos referring to improper media usage	2
4	Administration decision making delays	3
5	Communication barriers appearing, communication collapse included	3
6	Decrease of crisis management efficiency	4
7	Transport system insufficiency	4
8	Morale decline among evacuating and evacuated people	5
9	Panic	6
10	Difficulties in evacuation flows, chaotic transport included	6
11	Personal decision making delays	6

local administration to ensure transportation means for all the dedicated evacuees. Object, potential difficulties lead to consideration that much more simple protection means are desired. The voluntary evacuation appears as an example of such a mean. It can be understood as both: partially-organized and unorganized evacuation manner [12].

The voluntary evacuation definition concerns movement of people from the danger zone to safer places with the use of personal transport means as well as accommodation possibilities. Local administration activity is mostly limited to make the decision, warn people about the threat and evacuation proceeding initialization, point out evacuation directions and routes, indicate gathering places, loading points, medical points, service points, unloading points, dislocating places, accommodation places, as well as to ensure safety and security in all the evacuation phases and organizational elements (points, places, etc.) [8]. Such an activity scope characterizes partially-organized voluntary evacuation proceeding (the venture).

Referring to the unorganized evacuation manner, voluntary evacuation is understood as phenomenon of people movement from danger zone to subjectively safer places. It is personally initiated because of critically low sense of security, what forces to use personal transportation means, as well as accommodation possibilities. The subjectivism is worth to highlight. Exemplifying, people could move to unsafe places because of information lack and threat dynamism [8].

Making the conclusion, the voluntary evacuation could take two faces: partially-organized venture initiated by the local administration decision makers and unorganized, behaviour related phenomenon. In both cases, potential, derivative threats' catalogue is constituted. Table 1 presents the object breakdown [10].

The above breakdown presents only the most important derivative threats. As each of them could give rise to causative – consecutive processes, the real catalogue would be much more complex. Since it could generate very serious consequences, the object risk assessment is required.

Taking present considerations, voluntary evacuation risk assessment should be one of the basic problematic aspects of evacuation risk assessment in general. Two questions at this stage appear [13], [14], [15]:

1. What is an unreliability measure?
2. What is a threat (effect) measure?

There are two ways of the unreliability measure assumption. At one stage, it is relatively easy to determine. It is voluntary evacuation initialization itself. This assumption reflects the experience-related fact that people do not want to evacuate in Poland, even if local administration leaders made the evacuation decisions. It does not matter if partially-organized or unorganized evacuation is taken into account. However, on the other stage, the unreliability measure could be measured as a primary threat probability. The effect measure is the voluntary evacuation scale – a percentage magnitude characterizing how many people declare to evacuate in case of emergency. Relation between the two measures constitutes the voluntary evacuation risk measure:

$$R=f(U,E) \tag{1}$$

where:
R - risk measure,
U - unreliability measure, $U = 1$, if voluntary evacuation is initiated,
E - effect measure.

The next logical question refers to potential, voluntary evacuation risk determinants. Analysis of primary threats (the threats causing the evacuation need) is necessary.

3. The voluntary evacuation in Poland and the USA

The primary threats are basic evacuation determinants. Their scale, character and potential progress have the greatest influence for the decision makers. Table 2 presents the comparison of the threats that could lead formally to evacuation in USA and Poland [8], [5], [16], [17].

The comparison reveals that the primary threats catalogue in USA is broader than in Poland. The USA procedures take into account more evacuation initiators. That is understandable in the light of actual, both national security systems' environments. They are obviously different. The differences arise on, for instance, geographical location, population, climate, resources, infrastructure and safety/security culture. However, the Polish State Crisis Management Plan contains much more threats' examples than in evacuation documents. There are (besides ones mentioned in the comparison):

- electricity supply disturbances,
- liquid fuel supply disturbances,
- gas supply disturbances,
- hurricanes,
- landslides,
- dam failures,
- droughts,
- other radiation threats,
- and others.

Most of them could be evacuation initiators. As a matter of fact, in the Instruction of the Chief of the National Civil Defense primary threats' catalogue is open. However, the identified lack could be an evacuation efficiency barrier.

American and Polish scientists made independent researches focusing on other voluntary evacuation risk determinants. They took place, in turn, in 2008-2009 and 2013-2014. The determinants' influence was reflected in voluntary evacuation scale.

The USA research was made by J. Carnegie and D. Dekaand involved 3618 representative responders from chosen USA regions (7-country UASI Region, Newark Oversample, Jersey City Oversample and 14-country Non-UASI Region). The following threats were analyzed: hurricane + flooding, terroristic attack (IND, IED, dirty bomb), industrial accident: chemical plan and industrial accident: hazmat train. The results were presented at National Evacuation Conference in New Orleans, LA (February 3-5, 2010) [18].

There was an assumption of gathering in the voluntary evacuation risk group following elements: official notification and communications, individual difference variables, access to resources, social influences, risk perception (related with primary threats) and proximity of threat. Based on that, it was proven, that voluntary evacuation scale in USA is in relation with the following factors:

- high risk perception (positive influence),
- living close to disaster (positive influence),

Table 2 *Comparison of catalogues containing primary threats in the light of evacuation in the USA and Poland*

Evacuation in the USA	Evacuation in Poland
Flood	Flood
Forest fire	Forest fire
Urban fire	-
Hazardous Materials Incidents	Hazardous Materials Incidents
Terrorism	Terrorism
Nuclear Power Plant Accident	Radiological incident
Hurricane	-
Earthquake	-
Severe Storm	Severe Storm
Dam failure	-
Snowstorms	-
Lake Effect Snows	-
Blizzard	-
Tsunami	-
Landslide	Landslide
-	Epidemic
-	Building collapses
	Gas supply limitations
Debris flow	-

- pet(s) present at home (negative influence),
- person with specific care need living at home (negative influence),
- homeowner living more than five years at current residence (negative influence),
- low-income (negative influence),
- zero-vehicle household (negative influence),
- educational attainment high (positive influence),
- English not-primary language spoken at home (positive influence),
- married with children under 18 living at home (positive influence),
- 65 years of age or older (negative influence).

In accordance with the research methodology, the positive influence means "more likely to evacuate" and the negative influence means "less likely to evacuate".

The voluntary evacuation scale magnitude was in range of 67 % (answer "Very likely" for the question: "How likely are you to voluntarily self-evacuate?") for the "Terror Attack" threat to 30 % for the "Industrial Accident: Chemical Plan" threat.

According to the Polish research results, they involved answers of 1034 country-representative responders. The research was made by the Safety Research Department team (the author included). The following threats were analyzed: flooding, forest fire, terrorist attack, hurricane and industrial accident: hazmat car tank. The results were enclosed in a statutory scientific report:

"Public Space Research – Scale and Influence of Voluntary Evacuation of People on Mass Evacuation" (number: S/E-422/5/13) at the Main School of Fire Service in Warsaw (Poland) in December 15, 2013 [19].

There was an assumption of gathering in the voluntary evacuation risk group the same elements as in the previous research, namely: official notification and communications, individual difference variables, access to resources, social influences, risk perception (related with primary threats) and proximity of threat. Based on that, it was proven, that voluntary evacuation scale in Poland is in relation with following factors:

- high risk perception (complex influence),
- living close to disaster (complex influence),
- emergency communicates in radio said by local authorities (positive in the case of women, lonely people, village and small towns' inhabitants),
- previous mass threat experience (positive influence),
- excluding information from different information sources (negative influence in the case of the biggest towns' inhabitants),
- clear and firm activities of local authorities and public services (positive influence in case of the youngest, maximum 20 years old responders),
- living in the middle-size town (positive influence for forest fires),
- non-alone living (positive influence for all the threats quite far from home),

In accordance with the research methodology, the positive influence means "decision of voluntary evacuation" and the negative influence means "decision of sheltering in place". The complex influences of risk perception and living close to disaster are exemplified by the following premises:

- 65 years of age or older inhabitants will more likely decide to evacuate in the case of the flood wave expected in 3 hours,
- 36-50 years of age inhabitants will less likely evacuate in the case of the flood wave expected in 0.5 h,
- women will more likely make the voluntary evacuation decision in case of weather warning concerning a hurricane likely to occur in 5 hours.

The premises could be explained by the Polish safety behavior patterns. Elderly inhabitants see their chance to voluntary evacuation owning to sufficient evacuation time (3 hours was the longest period with respect to the two others, i.e. 1 hour and 0.5 hour). The middle-aged inhabitants feel responsible for their possessions, especially in the face of a very short time between the risk perception and the threat coming. As far as the weather warning is concerned, women behavior is similar to the elderly inhabitants behavior pattern in the case of the flood threat. The analogy to voluntary evacuation decision in relation with sufficient evacuation time is observed.

The voluntary evacuation scale magnitude was in range of 48.5 % (answer "YES" for the question: "Will you self-evacuate?") for the situation: "Broken embankments, 1 hour to flooding wave coming" to 20.4 % for the situation "Numerous media news concerning possibility of terrorist attack without information about the attack reason".

The comparison of American and Polish research results leads to conclusion about:

- different threats' perception in both countries (low terrorist attack threat perception in Poland and relatively high in the USA, quite different relation for flood threat),
- higher voluntary evacuation scale in the USA than in Poland (this conclusion confirms author's observation during a catastrophic Polish flood in 2010),
- differences in the voluntary evacuation risk factors and their influence on the object risk.

The conclusions made aware of the necessity to create Polish voluntary evacuation strategy and executive documents based on the Polish safety and security environmental factors. They made probable the hypothesis concerning such necessity in other Central Europe countries', as well. Practical, field experience is crucial in this venture. The object state-of-the-art ought to be treated solely as a reference point.

4. The voluntary evacuation risk assessment guidelines

Concluding the research results, creation of the voluntary evacuation risk assessment guidelines is dependent on following criteria:

- local safety and security environmental factors,
- previous practical, field experience,
- historical, behavior-determined patterns,
- voluntary evacuation scale range (in Poland: 20.4 % - 48.5 %),
- particular voluntary evacuation risk determinants.

The guidelines focus on the unreliability measure and the effect measure. As far as the first one is concerned, two ways of assessment are proper:

1. $U = 1$, presumed magnitude reflecting the evacuation initialization.
2. $U \in (0.1>$, magnitude depended on local primary threat risk (especially probability).

According to the effect measure, voluntary evacuation scale determinants should be analysed as well as chosen state-of-the-art solutions implemented. Table 3 presents the suggested guidelines.

5. Conclusion

The basic volunteer risk assessment determinants were discussed in this paper. The focus was set on such risk factors as official notification and communications, individual difference variables, access to resources, social influences, risk perception (related to primary threats) and proximity of threats.

Table 3 *Guidelines for voluntary evacuation risk assessment*

No.	Voluntary evacuation risk assessment guidelines
1	Full primary and derivative threats' catalogues should be taken into consideration.
2	Every primary threat could give rise to causative – consecutive processes, leading to complex derivative threats. There is an opportunity to use the fault tree method and/or the event tree method to analyse risks referring to the derivative threats. Other risk assessment methods are allowed.
3	Local risk maps should be analyzed to highlight *U* magnitude as local primary threat risk (especially probability) for the second way of the risk assessment.
4	The potential evacuation zone ought to be shared into smaller parts facilitating detailed analysis of evacuees social structure and make possible an individualization of local voluntary evacuation scales' magnitudes.
5	Partially-organized and non-organized voluntary evacuation can both encompass maximum of 50 % of average (statistical representative) population. Results of the social structure determining the voluntary evacuation scale should be implemented.
6	The public evacuation means (cars, buses, trains, planes, boats, etc.) for at least 20 % of potential evacuees by the local administration are to be ensured. However, evacuation means' resources for 50 % of the local population are desired. Object lack is the next risk factor.
7	The warning time is a crucial voluntary evacuation determinant. The risk assessment ought to be based on 3 time-related scenarios: 1. Enough time to protect possessions and evacuate, 2. Enough time to evacuate, 3. Not enough time to evacuate.
8	The assessment should include scenarios with use of the local and/or public media to warn inhabitants by the local authorities.
9	Voluntary evacuation risk assessment results ought to be gathered and presented on risk maps as integral elements of local crisis management plans.
10	The assessment results should be tracked as helpful, decision support tips.

Differences between voluntary evacuation risk determinants in USA and Poland were proven. They have their sources in the local safety and security environments. The first conclusion is that the primary threats catalogue in USA is broader than in Poland. This fact constitutes the broader evacuation initiators group as well. Besides that, differences in magnitudes of voluntary evacuation scales in both countries were identified. In general, voluntary evacuation is not so common evacuation form in Poland than in the USA. One needs to emphasize, that this conclusion is opposite to the actual Polish evacuation conception. It seems to explain author's operational experience concerning situations, when people in danger did not want to leave their homes and evacuate.

Based on the Polish research and the comparison results, the guidelines for the voluntary evacuation risk assessment were elaborated. They include general directions for the assessment person who needs to take into account local risk determinants, using the state-of-the-art only as the additional solutions' source. Besides that, they could be useful reference point in creation of evacuation conceptions in other Central Europe nationalities.

Acknowledgments

This paper includes results of the statutory project work titled: Public Space Research – Scale and Influence of Voluntary Evacuation of People on Mass Evacuation – number: S/E-422/5/13, funded by the Ministry of Science and Higher Education of the Republic of Poland, and reflects only the view of the author.

References

[1] COVA, T. J., DENNISON, P. E., DREWS, F. A.: Modelling Evacuate versus Shelter-in-Place Decisions in Wildfires. Sustainability, 3, 1662-1687, 2011.

[2] PIETRANTONI, L., SACCINTO E.: Psychosocial Models of Evacuation Behaviours. KEPKA, P., JASKOLOWSKI, W. (Eds.), Emergency Evacuation of People from Buildings. The Main School of Fire Service, Warsaw, 2011.

[3] Evacuation Planning. Manual Number 11. Australian Emergency Manual Series 2005 [online]. Available: http://www.em.gov.au/documents/manual11-evacuation planning.pdf [accessed: 2014-08-29].

[4] Mass Evacuation Planning. Director's Guideline for Civil Defense Emergency Management Groups 2008 [DGL 07/08] [online]. Available: http://www.civildefence.govt.nz/assets/Uploads/publications/dgl-07-08-mass-evacuation-planning.pdf [accessed: 2017-06-21].

[5] Mass Evacuation Process Guide. Los Angeles Operational Area [online]. Available: catastrophicplanning.org/.../LAOA_Mass_Evacuation_Guide_SEP 2011.pdf [accessed: 2014-08-29].
[6] Evacuation and Shelter Guidance. Non-statutory Guidance to Complement Emergency Preparedness and Emergency Response & Recovery, Emergency Planning College 2014 [online]. Available: https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/274615/Evacuation_and_Shelter_Guidance_2014.pdf [accessed: 2017-06-21].
[7] Decree of the Ministry of the Interior of the Slovak Republic on April 13, 1995 on evacuation (No. 75/1995 Coll.).
[8] Instructions of the Chief of the National Civil Defense on the Evacuation of People, Animals and Possessions in Case of Mass Threat 2008 [online]. Available: www.ock.gov.pl/download/22/670/instrukcjawsprawieewakuacji.pdf [accessed: 2017-06-21].
[9] Preparedness of Civil Defense Structures to Tasks' Fulfillment at War and Peace. Information of Control Results. Supreme Audit Office 2012 [online]. Available: http://www.nik.gov.pl/plik/id,3953,vp,5028.pdf [accessed: 2017-06-21].
[10] GROMEK, P.: Organization of Mass Evacuation of People in Poland. Doctoral dissertation, National Defense Academy, 2014.
[11] FENG, W., CHAO, L., XUESONG, Z., MAHESH, N., XIAOMIN, Ch.: Effectiveness of Traffic Management Strategies at Destination during Emergency Evacuation. Journal of Transportation Safety & Security, 2, 152-170. 2010.
[12] GROMEK, P.: Mass Evacuation of People (multimedia presentation). Mykolo Romerio University Vilnius, 2013.
[13] SZOPA, T.: Foundations of Reliability Analysis. Warsaw University of Technology, 2008.
[14] ZANICKA HOLLA, K., RISTVEJ, J., SIMAK, L.: Risk Assessment in Industrial Processes. Iura Edition, Bratislava, 2010.
[15] ZANICKA HOLLA, K., RISTVEJ, J., SIMAK, L.: Systematic Method of Risk Assessment in Industrial Processes. Proceedings of International Conference Risk analysis VII: Simulation and Hazard Mitigation & Brownfield V: Prevention, Assessment, Rehabilitation and Development of Brownfield Sites, Great Britain, 115-125, 2010.
[16] Local Evacuation and Mass Care Planning Handbook, Emergency Management and Homeland Security Division. Michigan Department of State Police 2013 [online]. Available: http://www.michigan.gov/documents/msp/Local_Evacuation_and_ Mass_Care_Planning_Handbook_-_Pub_113_-_Final_Edition_ March_2013_420111_7. pdf [accessed: 2014-08-29].
[17] Polish State Crisis Management Plan. Government Centre for Security 2013-2015 [online]. Available: http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_.pdf [accessed: 2017-06-21].
[18] CARNEGIE, J., DEKA, D.: Evacuation vs. Shelter-in-Place: How will residents respond? (multimedia presentation). National Evacuation Conference, 2010.
[19] The Main School of Fire Service (Poland). Public Space Research – Scale and Influence of Voluntary Evacuation of People on Mass Evacuation (periodical Report, 2013).

kamUNikácie
COMMUNICATIONS

Sarka Krocova - Karla Barcova*

CHECKING THE HYDRAULIC EFFICIENCY AND IMPROVING SAFETY OF THE INTERNAL WATER SUPPLY

Water management systems in industrial facilities, industrial zones, hospitals and other internal water systems relatively frequently fail to meet the intended purpose for which they were built when an extraordinary event occurs. They may even pose a safety hazard. The causes of this condition may be of internal or external origin. Given that internal water supply systems of large premises always have a multipurpose character, i.e. to provide enough drinking water for drinking and sanitation purposes and also as a source of fire water for the fire safety of buildings, they must meet a wide range of hydraulic conditions and technical-operational capabilities. By what means and methods it is possible to achieve the desired state in economically-acceptable dimensions, while maintaining all the necessary hydraulic capabilities of the supply points of drinking and fire water, is briefly described in this article.

Keywords: *internal water supply network, water lines, water connection, hydraulics, risk, risk reduction, reliability*

1. Introduction

Important locations and extensive premises of public and private infrastructure of cities and towns cannot do without the construction and subsequent operation of an internal water supply network. The continuity and reliability of supplying drinking and fire water is one of the basic conditions of their operational functions and building safety. Even a short-term interruption of water (about 8-10 hours), required to repair damaged equipment of the waterworks system, causes serious or even critical problems for water consumers. It threatens food production, disrupts the functioning of accommodation and catering facilities and can seriously disrupt inter alia the operability of hospitals.

Since the occurrence of accidents and extraordinary events in water supply systems of the public water supply or water installations cannot be completely prevented, it is necessary to know and analyze the causes and conditions that give rise to these situations and prepare for their solution.

In some cases, it is possible to eliminate operational security risks via technical and investment funds during the construction of the given type of infrastructure of the built-up area. Other risks emerge during the operation of the systems as a result of errors and deficiencies in their use, when underestimating the changing characteristics of hydraulic piping systems over time, mainly due to changes in the surface roughness of the inner pipe walls and a subsequent change in flow capacity. Usually, in the case of a lack of the hydraulic efficiency control of the waterworks system‘s internal water supply system, problems are fully reflected in critical situations and, as a consequence, excessive damage is incurred [1].

To reduce or eliminate the operational and security risks of each internal water supply network, upon which the entire premises are dependent, it is necessary to understand and abide by at least the principles set out in this article.

2. Internal water supply as a comprehensive operating system

The reliability and flow volume capacity of water supply is always primarily dependent on the water source from which it draws water to be transported to individual structures or their complexes on the operated premises. In the Czech Republic and Slovakia, similarly to most other states, the source of water for internal water supply networks in public and private infrastructures, is almost always the water supply system for public needs, see Figure 1. It consists of a water line, which includes a system measuring water flow and a variously complex piping system of one or more pressure zones, depending on the technological needs of the premises.

* [1]Sarka Krocova, [2]Karla Barcova
[1]Department of Fire Protection, Faculty of Safety Engineering, VSB -Technical University of Ostrava, Czech Republic
[2]Department of Security Services, Faculty of Safety Engineering, VSB -Technical University of Ostrava, Czech Republic
Email: sarka.krocova@vsb.cz

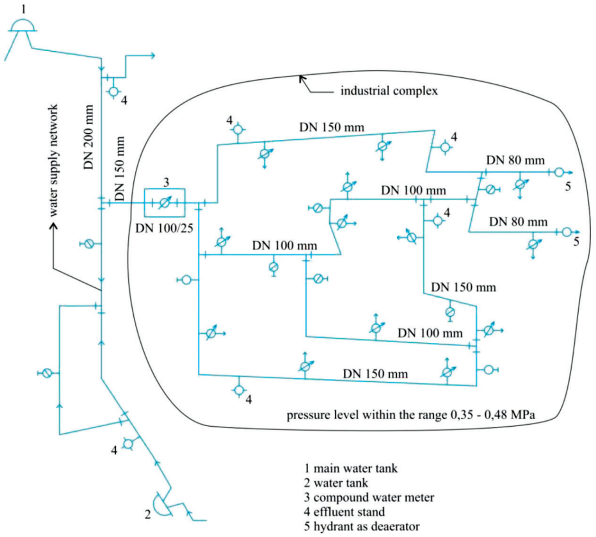


Figure 1 *Diagram of the internal water supply network of an industrial complex with fire water supply points*

In some specific situations, the source of potable and fire water can be an independent supply of surface or underground water. In such situations, the surface water must always be purified according to the parameters for drinking water in water treatment, which is an integral part of the internal water supply system. Underground water must be treated to obtain drinking water only in cases where it does not meet the requirements for drinking water laid down by law [2].

To meet the expected effect of the water supply network in the supply of drinking water and in many cases, fire water, it is necessary to view the system as one comprehensive system. Underestimating some parts of this system often produces a ripple effect. For example, a lack of water velocity in individual water lines reduces water quality and may give rise to serious health problems of consumers. Conversely, changes in flow capacities often cause technical glitches of control fittings of the water supply network or a change in the roughness of the inner pipe due to encrustation. The former hydraulic cause threatens the health and lives of people; the latter has the effect of compromising the fire safety of the entire premises due to a lack of fire water for fire hydrants or discharge pillars.

3. Hydraulics and its importance for the reliability and safety of water supply

For these and other reasons, each operator of an internal water supply network must know not only the hydraulic conditions of the entire system, but also of its individual distribution segments. The technical and operational parameters of water lines change over time. Significant changes and a reduction in the hydraulic efficiency of the water supply system occur primarily for the following reasons:

- the age of the pipeline systems,
- the quality of the flowing water,
- the operational load of the lines and water velocity.

The aforementioned root causes have various negative effects on the overall operating characteristics of the water supply network. If the age of the pipe is a fixed value, then the designer must respond to the known or suspected water quality while designing the structure of water lines (a branched, round or combined system) and calculate the dimensions of individual lines. When calculating the dimensions of the lines, the following procedure must be complied with.

Table 1 *Water flow in water lines*

dimension [mm]	water flow [l/s]
40	1.257
50	1.964
80	5.027
100	7.854

3.1 Dimensions proposal for water lines

A variety of calculation methods can be used for the dimension design of water lines of the internal water supply systems. One of the most progressive current methods is the mathematical modeling of the water supply network. It is particularly advantageous for the calculation of the new pipes with zero encrustation of the internal network, where it allows for achieving a high reliability of output calibrated values. Mathematical modeling gives designers and operators of water supply the answer to a number of fundamental questions. In particular, the speed of water flow in individual lines and the value of the hydrodynamic pressure at varying operating load (water flow inl/s).

For most internal water supplies providing only a supply of drinking, process and sanitary water, it is suitable to comply with the following principles when designing lines:

a) ensuring water velocity in the pipe system (the optimum is 0.8 to 1.1 $m.s^{-1}$)
b) maintaining the freshness of drinking water in the entire system (max. delay - 24 hours).
c) maintaining the secondary level of the health safety of drinking water throughout the entire water residence time in the internal water supply system, including its water supply connections (0.2 mg/l Cl_2).

These parameters of water quantity and quality can be achieved in the design and implementation of pipe lines and water connections of the following dimensions are listed in Table 1.

Table 2 *Water line dimension depending on the supply points of fire water*

	branch water supply network	circular water supply network
	water flow [l/s]	water flow [l/s]
dimension	fire hydrant	pump outflow stand
80	5.027	-
100	7.854	-
150	17.672	35.344
200	31.416	62.832

Figure 2 *An example of moderately encrusted piping*

The dimension design of internal water supply and individual water connections to buildings is always dependent on calculating the maximum and minimum water consumption connected to various branches of the water lines or water connections.

If the water system is currently designed as a multipurpose fire water supply for the area in question, it is necessary to consider the design of DN (diameter nominal) piping, depending on the type of withdrawal place of fire water, as shown inTable 2.

The dimension design of internal water pipelines, serving the purpose of the fire protection of buildings, is operationally very problematic. When the pipe dimensions are 100 mm, 150 mm, 200 mm, it is no longer possible, besides in exceptional cases, to maintain the freshness of drinking water and its health safety in the pipe system.

From the above significantly reduced procedure for the design of the suitable pipe dimensions depending on the desired quantity of water flow, a close connection between determination of the optimal dimensions of the pipeline and the pressure losses in the operating system is evident. In the event of an underestimation of this bond and its interdependence, the situation shown in Figure 2 may occur in a relatively short period of time (the first third of the pipeline's lifetime)

Such a situation occurs on water installations with insufficient flow velocity, especially in the design of branched systems, in connection with mineralized water with higher content of Fe and Mg. Aside from a reduced water velocity in the pipe below 0.4 $m.s^{-1}$, a more rapid formation of or increased encrustation also occurs as a consequence of drawing water from local groundwater resources and a lack of sufficient demineralization of groundwater during the purification to drinking water.

The subsequent risk of changes in hydraulic efficiency of water supply due to excessive encrustation of the inner pipe and their effect on the hydrodynamic properties of the pipe network is shown in Figure 3.

From Figure 3 it is clear that even at a slightly above-average water flow in water lines, the water supply network is not able to maintain the sufficient hydrodynamic pressure of water. That fact is a risk not only for operational purposes and various appliances that utilize water, but mainly for fire safety of the premises. Of the whole range of specific threats that have the potential to disable each internal water supply, the most important are the following events:

- contamination of drinking water with organic or inorganic substances,
- reduction in the level of drinking water supply in the distribution system,
- limitation or interruption of the water supply from its source.

If the abovementioned and other extraordinary events cause „merely" economic damage for industrial and commercial consumers of drinking water, for hospital premises and long-term sickness facilities, they will almost always result in the complete or partial evacuation of patients. For healthcare facilities, it does not serve the intended purpose of a classic reserve water supply, but always only as a direct supply of water to individual pavilions.

4. The safety risks of operating an internal water supply network

Given the importance and indispensability of the operational functions of water supply to the utility values of the premises, it is necessary to conduct checks, as a part of an emergency prevention and reduction of consequential damage. This issue is addressed on a general level in particular by CSN ISO 31000 Risk Management - Principles and Directives, which sets out the binding procedure for risk assessment technique.

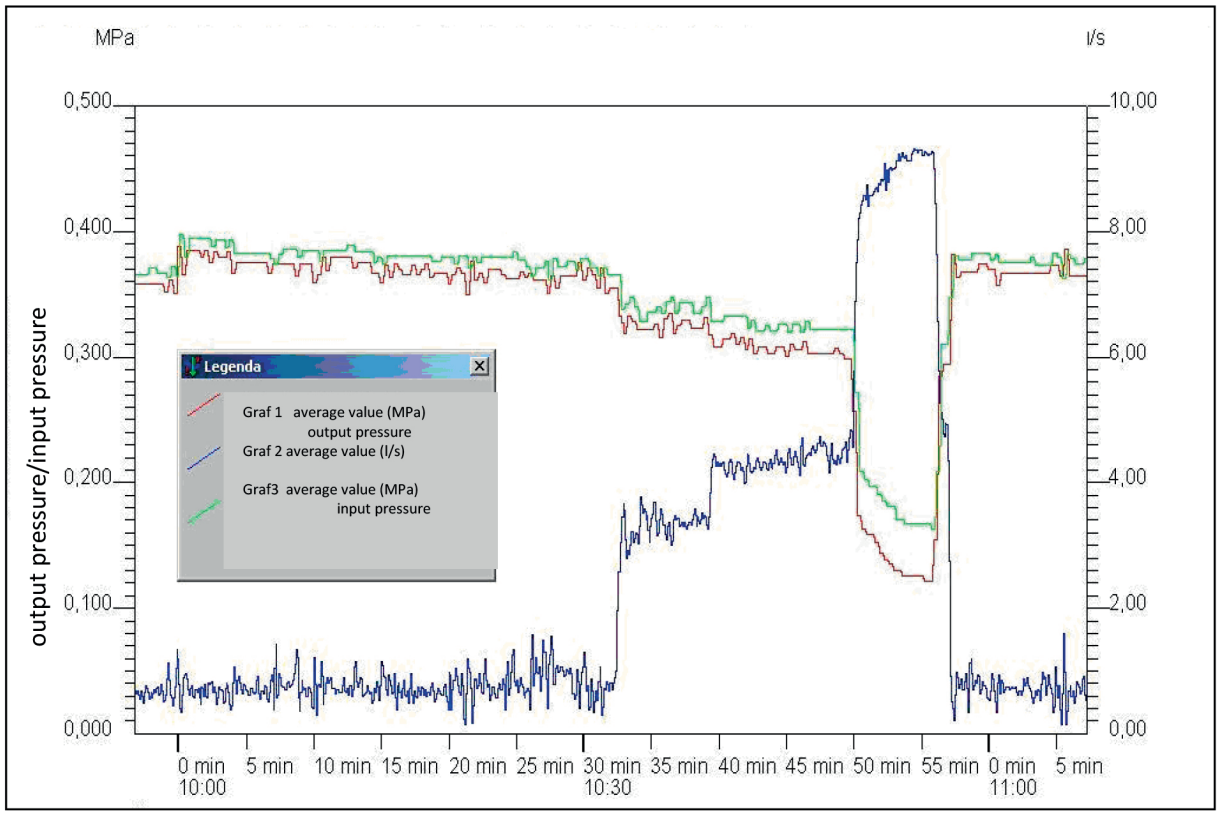


Figure 3 *Representation of the hydraulic efficiency of the water supply network during capacitive loading*

Checks should be focused primarily on exposing the weaknesses of the system and increasing its strengths.

Weaknesses

Internal water piping of industrial facilities, industrial zones and extensive technical-operational areas of various users, have a variety of weaknesses, with which one must be familiar and able to prepare operational plans to reduce them. The basic factors include the following:

- usually only one source of drinking and fire water,
- differing operating reliability of the water source, depending on its type,
- heavily undersized water connections in relation to the requirements of maximum supplies
- low hydraulic efficiency of water supply pipe systems,
- the risk of changes in the quality and safety of drinking water [3].

Strengths

Strengths are reflected primarily in optimally solved and constructed internal water piping, but they can be found to a lesser extent in essentially all waterpipes [4]:

- direct water supply to the place of consumption,
- fire safety of facilities on the premises,
- the possibility, upon agreement with the water supplier, to increase hydrodynamic water pressure in parts of the water supply network up to the parameters necessary for its technological use [5].

A relatively balanced state can be achieved if danger, stemming from the weaknesses, is recognized early and the potential of strengths is exploited, [6]. Attention should be focused on the following areas:

- monitoring of hydraulic and operating parameters of the internal water supply system,
- refinement of operational and handling rules,
- preparation of crisis preparedness plans of the subject in question.

The activity in question must not be segmented, however, it must be the output of a comprehensive risk analysis of the entire functional or utilized environment of the operator.

5. Discussion

Due to the irreplaceable significance of internal water supply systems for the functioning of production plants, shopping centers and hospitals, it is necessary not only to operate them optimally,

but also to seek ways of further rationalization. An extremely effective form could be national and international discussions of the professional public and the transmission of positive and negative experiences with the operation of these types of water cannons. Professional discussions could focus primarily on the following areas:

- how to avoid the danger of changes in the quality of drinking water and maintain its health security while preserving the hydraulic capacity of combined pipeline systems for drinking water and fire water for structures,
- economically acceptable and feasible ways to achieve a substantial increase in the reliability of water supply from internal water piping in the case of an extraordinary event or a crisis situation,
- finding new rational methods of using water in internal water supply networks during the technological utilization, before its conversion to waste water.

The topics proposed for discussion will become increasingly important in the light of occurring climate changes. Their meaning and scope transcends national boundaries and they are utilizable by everyone interested in increasing the economic efficiency and reliability of internal water supply systems.

6. Conclusion

The function of internal water supply of industrial and commercial complexes and industrial zones is irreplaceable. It does not only provide the drinking water to individual buildings on the premises, but it is also an important multipurpose source of fire water for the entire operating system. In order to be able to fulfill their specified purposes, they must be designed and implemented in accordance with the hydraulic principles mentioned in this article. These principles include, in particular, the following characteristics:

- a consistent overview of water losses throughout the distribution system,
- accurate knowledge of the amount of water in individual sectors or pressure zones of the internal water supply,
- the ability to operate only the strategic parts of the water supply network in crisis situations via the control system, for the most important premises of the operational area,

for selected and reduced supply points of fire water, to ensure their specified amount of supply during the crisis.

Failure to follow these principles not only significantly reduces the value of the entire construction work, it can also seriously disrupt the reliability requirements of the water supply for sanitary and technological purposes of the operator of the premises and, the last but not the least, the hydraulic reliability of the relevant multipurpose source of fire water.

The construction of the article and its structure defines the ways and means to minimize the risk that internal water supply will not meet the required and necessary technical and operational parameters upon commissioning.

Acknowledgement

This work was supported by the research project VI20152019049 „RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems“, supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019.

References

[1] STRELCOVA, S., REHAK, D., JOHNSON, E. A. D.: Influence of Critical Infrastructure on Enterprise Economic Security. Communications - Scientific Letters of the University of Zilina, 17(1), 105-110, 2015.
[2] Act no. 254/2001, Collection of laws: On Waters and Amending Some Laws (the Water Act), as amended.
[3] Act no. 252/2004, Collection of laws: Hygiene Requirements for Drinking and Hot Water and the Frequency and Extent of its Control.
[4] KROCOVA, S., REZAC, M.: Infrastructure Operation Reliability in Built-Up Areas. Communications - Scientific Letters of the University of Zilina, 18(1), 75-78, 2016.
[5] ADAMEC, V., MALEROVA, L., ADAMEC, M.: How to Assess Teritory Vulnerability. The Science for Population Protection 1, Population Protection Institute of Lazne Bohdanec, 17, 35-40, 2016.
[6] KROCOVA, S.: Industrial Landscape in the Period of Hydrological Drought. Inzynieria Mineralna, 18(1), 29-32, 2017.

COMMUNICATIONS – Scientific Letters of the University of Zilina
Author guidelines

1. Submitted papers must be unpublished and must not be currently under review for any other publication.
2. Submitted manuscripts should not exceed 8 pages including figures and graphs (in Microsoft WORD – format A4, Times Roman size 12, page margins 2.5 cm).
3. Manuscripts written in good English must include abstract and keywords also written in English. The abstract should not exceed 10 lines.
4. Submission should be sent by e-mail – as an attachment – to the following address: komunikacie@uniza.sk.
5. Uncommon abbreviations must be defined the first time they are used in the text.
6. Figures, graphs and diagrams, if not processed in Microsoft WORD, must be sent in electronic form (as JPG, GIF, TIF, TTF or BMP files) or drawn in high contrast on white paper. Photographs for publication must be either contrastive or on a slide.
7. The numbered reference citation within text should be enclosed in square brackets - in numerical order. The reference list should appear at the end of the article (in compliance with ISO 690).
8. The numbered figures and tables must be also included in the text.
9. The author's exact mailing address, full names, E-mail address, telephone or fax number, the name and address of the organization and workplace (also written in English) must be enclosed.
10. The editorial board will assess the submitted paper in its following session. If the manuscript is accepted for publication, it will be sent to peer review and language correction. After reviewing and incorporating the editor's comments, the final draft (before printing) will be sent to authors for final review and minor adjustments.

Errata: Communications – Scientific Letters of the University of Zilina, Vol. 20, No.1, 2018, „On Frequency Estimation for Partially Observed System with Small Noises in State and Observation Equations", pp. 67-72. The third author should have the number 3 at the name, i. e.

[3]Mariana Marcokova

and two affiliations as follows:

[3]Department of Structural Mechanics and Applied Mathematics, University of Zilina, Slovakia and Department of Electronics and Nanoelectronics, National Research University „Moscow Power Engineering Institute", Russia.

komunikácie
COMMUNICATIONS

VEDECKÉ LISTY ŽILINSKEJ UNIVERZITY
SCIENTIFIC LETTERS OF THE UNIVERSITY OF ZILINA
VOLUME 20

Address of the editorial office:
University of Zilina
EDIS – Publishing House
Univerzitna 8215/1
010 26 Zilina
Slovakia

E-mail: komunikacie@uniza.sk

Individual issues of the journal can be found on:
http://www.uniza.sk/komunikacie

Each paper was reviewed by two reviewers.

Journal is excerpted in **COMPENDEX, EBSCO Host** and **SCOPUS**.

Published quarterly by University of Zilina in
EDIS – Publishing House of University of Zilina

Registered No: EV 3672/09

ISSN (print version) 1335-4205
ISSN (online version) 2585-7878

ICO 00397 563

June 2018