Resistance of Passive Security Elements as A Quantitative Parameter Influencing The Overall Resistance and Resilience of A Critical Infrastructure Element

Tomáš Loveček
Faculty of Security Engineering/Department of Security Research
University of Zilina
Zilina, Slovakia
e-mail: Tomas.Lovecek@fbi.uniza.sk

Anton Šiser
Faculty of Security Engineering/Department of Security Management
University of Zilina
Zilina, Slovakia
e-mail: Anton.Siser@fbi.uniza.sk

David Řehák
Faculty of Safety Engineering/Department of Public Safety
VŠB – Technical University of Ostrava
Ostrava, Czech Republic
e-mail: david.rehak@vsb.cz

Martin Hromada
Faculty of Applied Informatics/Department of Security Engineering
Tomas Bata University in Zlín
Zlín, Czech Republic
e-mail: hromada@fai.utb.cz

***Abstract*— The character of protection and resilience of critical infrastructure is an important parameter, which directly affects the functioning and operational status of modern states. This article specifies the meaning of resistance indicator within the overall resilience of critical infrastructure element. In this paper, resistance indicator expresses the resistance of mechanical barriers and building construction and it is useful in creating a model of quantitative assessment of the level of protection of critical infrastructure elements.**

Keywords- resistance; resiliance; delay time; barriers; indicator.

I. INTRODUCTION

According to the 2007 decree of the European Council, critical infrastructure has to include primarily such physical resources, services, IT equipment and communication networks damage to or destruction of which would severely influence the critical social functions including the supply chain, healthcare, security, safety, economic and social well-being of the population or functioning of the European Union (EU) or its member states [1]. Protection of these elements or objects, deemed strategic for the state, is dealt with through individual solutions in various legal regulations but with different approaches to their protection. Such objects include nuclear plants, objects and areas for storage and manipulation with state secrets or objects housing financial institutions [2].

However, the critical infrastructure can include other elements/objects, the specific protection of which has not yet been covered by laws (such as line and node objects and elements of road, air, water or rail transport, chemical plants, suppliers of various forms of energy, hydraulic engineering objects, food and grocery businesses, industrial companies, mobile network providers, hospitals and other providers of care, etc.); the responsibility for their protection should be on the shoulders of the public sector, as well as the owners and managers of the individual elements of critical infrastructure [3] [5].

The paper structure includes 8 important sections. After the introduction, Section II focuses on assessing the current state, reviewing laws and European standards. Section III defines the relation between the terms "resistance" and "resilience". Section IV defines the options for evaluation of security systems and Section V then expands on the properties of passive barriers. Sections VI and VII are focused on collecting delay time data using a matrix, statistics and operation analysis. The final section summarizes the possible future developments in this area.

II. PROTECTION OF CRITICAL INFRASTRUCTURE – LEGISLATION AND STANDARDS

The existing EU standards approach the physical and object protection of the elements of the critical infrastructure through proclamations and do not specify specific proposals for its solutions. The Green Book

ISBN: 978-1-61208-493-0

document [2] states several possible means (tools) of improving preventive measures, security, preparedness and response in terms of the protection of the critical infrastructure within the EU conditions, but does not specify them further. This approach is similar on the national level, where according to [3] [4] [5], tools which can be used to lower the endangerment of the critical infrastructure can be technical elements for discouragement, detection, verification, signalization and elimination of the violator (mechanical and electronic) as well as the activity of security services (such as an intervention by a security force or the military); there is no further specification however what the resulting level of protection should be.

The analysis of the legal regulations of both the European and national levels of individual member states of the EU shows that the main focus is placed on implementing safety measures against anthropogenic threats (threats sources caused by person acting to damage or destroy an element of critical infrastructure), which are classified as tools increasing the resistance of the elements of critical infrastructure.

III. Resistance and Resiliance

The Resistance of a system can be understood as the ability of the system to resist the effect of negative factors, which do not lead to the change in the ability of the system to function. It is an ability of the system to resist changes that would lead to the system itself visibly changing. The resistance of a system is one of the many factors influencing the system's overall resilience. System resilience can be understood as the ability of a system to secure and maintain its functionality under the effects of negative factors as well as retain the functions of the system if changes to the system do occur.

The resistance of a system can be divided into structural and safety resistance. Structural resistance is the ability of a system to withstand the effects of negative factors based on the construction of its various elements, their placement in the system and the technologies utilized. Security resistance is the ability of a system to withstand the effects of negative factors using a system of security measures (Security Resistance) with minimal impact on the public safety (Safety Resistance).

IV. Evaluation Of Security Resistance Level

The existing tools, which evaluate the necessary or existing security resistance level use one of the two main approaches [6]:

- qualitative approach,
- quantitative approach.

There are several tools around the world using one of the aforementioned approaches [6] [11]:

- tools using the qualitative approach: RiskWatch (USA), CRAMM: CCTA Risk Analysis and Management Method (Great Britain),
- tools using the quantitative approach: SAVI: Systematic Analysis of Vulnerability to Intrusion, ASSESS: Analytic System and Software for Evaluation of Safeguards and Security (Sandia National Laboratories, USA), Sprut (Scientific and Production Enterprise ISTA SYSTEMS JS Co., Russia), SAPE (Korea Institute of Nuclear Non-proliferation and Control, South Korea), SATANO: Security Assessment of Terrorist Attack in a Network of Objects, (University of Žilina, Faculty of Security Engineering Slovakia, TLP spol. s r.o., Czech Republic).

Tools utilizing the qualitative approach are based on the evaluators' expert estimates when it is not possible to confirm the exact security resistance level and it is necessary to rely on the expert skills of the authors of these approaches. In such case it is impossible to verify whether the protection system is understated or overstated from in terms of the proposed protective measures.

Tools based on the quantitative approach allow the exact evaluation of the proposed protective measures based on measurable input and output parameters. In such cases, in contrast to the qualitative approach, the adequacy of a proposed solution can be confirmed. The basic parameter of the quantitative approach to resistance evaluation is the object protection level, which is judged based on structural and security resistance.

Structural resistance is evaluated separately by means of evaluation the individual elements of the object protection system such as the breakthrough resistance of a given object, i.e., the resistance of such object to various ways and methods of unwanted breakage [7]. The safety resistance is evaluated by evaluating the overall object protection level [8]. Figure 1 shows the visual classification of the basic evaluation parameters of critical infrastructure object resistance.

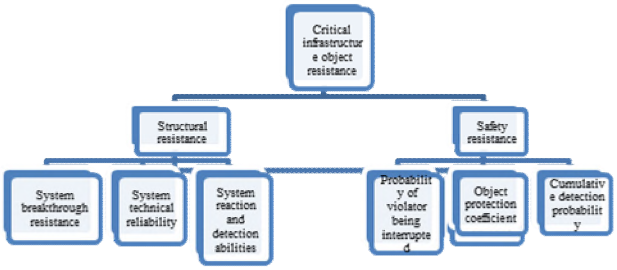
Critical infrastructure object resistance
Structural resistance
Safety resistance
System breakthrough resistance
System technical reliability
System reaction and detection abilities
Probability of violator being interrupted
Object protection coefficient
Cumulative detection probability

Figure 1. Basic evaluation parameters of a critical infrastructure resistance

The advantage of the quantitative approach is that subjectivity and influence of the evaluator is minimized and such amount and structure of protective measures is used so that the violator is detected and apprehended by a response unit before reaching his goal. Ironically, this approach is least used in practice.

The main reason for not using the quantitative approach is the fact that the evaluation tools do not have access to a basis of probability and temporal parameters of two main factors, which are the vector of approach and the protection system, both of which influence the overall required level of protection.

Other missing bases on parameters of factors influencing the overall protection level include:

- times of breakthrough resistance of passive protection elements, which change based on the type of tools used to break through them,
- the likelihood of being detected by active protection elements, which changes based on the violator's knowledge of the technology utilized (such as the way physical changes are evaluated as a result of a protected area being broken into) [10],
- reaction times of response units, changing based on the strategy of the response,
- reliability of the technical protection elements,
- reliability of the human factor.

The reason for the absence of these bases of input probability and temporal parameters is the fact that there are no methodical approaches specifying a simple way of acquiring them and up until recently, there was no research infrastructure, which would allow the creation of polygons and their subsequent filling with relevant data.

V. Delay Time Of Passive Barriers

Upon closer examination of the selected indicators influencing the resilience and general level of protection of an object, there are several links emerging that lead to the used mechanical security measures and structural barriers. The main task of these systems is to discourage, set back or completely prevent a potential violator reaching the protected object. The common element of all mechanical security systems and structural barriers is their attribute known in professional literature as delay time. This variable expresses the time in which a passive protective elements (such as doors, vaults, locks, etc.) has the ability to resist any tool or applied physical strength and depends on the mechanical properties of the materials used, abilities, skills and knowledge of the violator, effects of weather and other factors. The delay time value is expressed mathematically as:

$$DT= T_2 – T_1 \qquad (1)$$

i.e., the subtraction of T_1 – which is the time at which the violator began penetrating the passive protective element from, T_2 – which is the time at which the passive protective element has been penetrated.

The emphasis placed on studying the delay time of passive elements is rendered necessary by the fact that it is the only measurable attribute, which can also be used in the process of qualitative evaluation of the level of protection of an object. With the knowledge of exact values of delay time of each individual obstacle placed on the critical path we can - with a high degree of precision – determine whether a task force or a response team is able to act against a potential threat in time, whether it is caused by natural processes or is anthropogenic in its nature before this threat reaches its ultimate goal, i.e., the object under protection; this can be represented by tangible assets, intangible assets or human resources. In case of a standard violator interested in stealing valuables or some other form of property with high liquidity, the time of this theft path will consist of the studied delay time values of all existing passive security elements, the time of transitioning between them, but also the time necessary for retreat.

If the overall theft path is T_A – the time of action – then this value represents the maximum time within which the response team must perform a successful intervention against the violator. This time for intervention can be expressed as T_R – the reaction time – and will include the time from the first detection, evaluation, verification of the alert message and also the time necessary for transit and apprehension of the suspect through the means of the response unit. By comparing the times T_A and T_R we can then evaluate the level and effectiveness of the physical protection system. It can be concluded that for an effective case of property protection, the following must be true [9]:

$$T_A > T_R \qquad (2)$$

i.e., the action time - T_A, which the violator needs to reach the protected object must always be longer than T_R necessary to apprehend the violator. For more precise quantitative evaluation of the level of protection, it is necessary to return to the delay time value of passive protection elements and structural barriers in relation to the tools or means utilized.

VI. Delay Time Data Matrix

As part of the professional and publishing activities of the Faculty of Security Engineering, University of Zilina, a new method of evaluation for the effectiveness and level of physical protection of systems is being developed; this method would be based on exact time values expressed as delay time presented in a matrix using the 'tool versus the passive security element' relation. Part of the matrix proposal is represented in Figure 2.

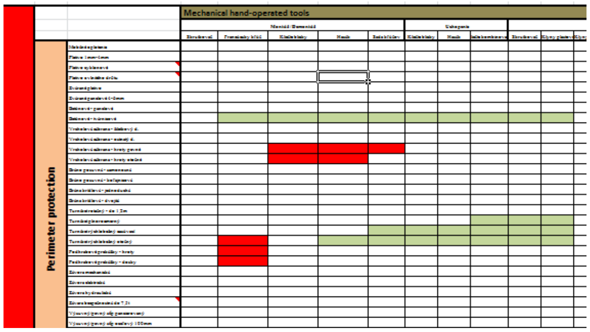

Figure 2. Proposal of delay time data matrix

In compiling and completing this matrix, several issues arise. Before we get to the most important one, which is the great amount of missing data, let us begin with the complications related to the selection of suitable representatives, both on the side of passive security elements and structural barriers, as well as on the side of tools used to breach them.

Since it is impossible to take into account the existence of all available security systems and the tools to break them, it proved necessary to divide them into categories from which the following elements best represent the overall character of their respective categories. This step simplified the entire process significantly and did not, in fact, decrease the quality of the end result. The current state of categories is not final and requires further modifications alongside continuous updates concurrent with the market development.

The first axis of the matrix consists of passive security elements divided into groups based on its location:

- perimeter protection (different types of fences, gates, turnstiles, ramps, etc.),
- outer protection (security doors, locks, windows, grilles, shutters, gates, security window films, etc.),
- object protection (safes, cabinets, boxes, etc.).

This axis also contains a separate group consisting of the most popular structural barriers.

The second axis focuses on tools, means and resources used to overcome passive security elements. They are divided into the following groups:

- physical load (breakage, kicking, etc.),
- improvised tools (ladder, rock, pole, etc.)
- mechanical hand-operated tools (axes, hammers, crowbar, screwdriver, etc.),
- motor tools (electric saw, drills, grinders, petrol saws, special hydraulic tool, etc.),
- thermal tools (liquid nitrogen, hot-air pistols, oxy-acetylene tools, etc.),
- firearms (.22LR, 9x19 Luger pistols, 5.56x45 rifles, etc.),
- explosives,
- means of transport (cars, trucks and special vehicles),
- specialized tools developed specifically to negotiate locks, doors, etc.

After the axes have been finalized, the matrix needs to be completed with specific values using all the currently known data accumulated in technical standards as well as resulting from tests performed. Where technical standards are concerned, it is necessary to point out their norms are not synchronized due to various reasons. There are several technical commissions and approval boards working in the field of development of technical standards focused on passive security elements. Some of these organizations have members who are also producers of such elements, which open up the potential for lobbying as well as directly influencing the normalization process for personal gains. As such, the delay time value may be skewed by testing parameters being set up in a way that is more suitable for certain products or in favour of their manufacturers.

Another problem found in detailed study of European standards is performing the tests in ideal conditions, which do not take into account real effects of the environment as well as the use of a limited amount of tools, as it is with the EN 1627 standard. This standard for penetration tests only involves some types of widely available tools. The use of specialized tools or high-performance thermal tools is not included in this case.

There is a specific issue in cases where the standard does not show resistance of passive security elements, as is the case in glass panes, against the effects of explosives or firearms using a measure of time but rather the maximum pressure or number of repeated impacts that the element is able to successfully resist. In case of explosives, the effects are shown immediately, therefore the only temporal value that can be measured is the time necessary to prepare and set the charge. The effects themselves on the passive security elements can only be assumed in realistic conditions, because all values listed in the standards have been measured in open areas or using pressure tubes and only using TNT-based explosives. The effects of other explosives will likely have to be calculated using the actually known coefficients [12]. Additionally, influence of the environment on the propagation of a pressure wave in real conditions will have to be taken into account. The largest task in the process of filling in the values of delay time is acquiring the missing data, which cannot be found in the norms or were not processed in any other way.

VII. Collecting Data Methods

A big contributing factor in collecting the data is selecting a method, which will lead to this data in the most effective way possible.

A. Expert opinions and valuation

Currently, the Faculty of Security Engineering of the Zilina University is focused on studying various approaches. One of them is using expert opinions. For this approach to be feasible, a larger number of professionals have to be selected, specialists in specific fields with extensive practical experience; they would then be answering prepared and unambiguous questions. Based on the responses and after their subsequent evaluation, relevant values could be achieved. The disadvantage of this approach is its organizational and managerial complexity as well as a large number of persons involved.

B. Fuzzy logic application

A second approach of gathering usable data for the delay time value is the use of fuzzy logic. Fuzzy logic is a system in mathematical theory, which uses the many-valued logic containing real values from the <0 ; 1> interval and elements of approximate deduction based on the rules of human logic. The term fuzzy logic came to be in 1965 based on scientific activities of a mathematician and scientist of Azerbaijani descent, L.A. Zadeh at the University of California, Berkeley. The first indications of this theory can be found in the early 20th century and it found its use in the subsequent years in various fields such as engineering, logistics, economics and computer sciences. Similarly, it can be used in risk analysis and evaluating the physical protection systems and their level of effectiveness. The advantage of fuzzy logic je its simple application to any values with no regard as to whether they are expressed as time, pressure or otherwise. The entire process takes place in mutually related steps, which are shown in Figure 3.

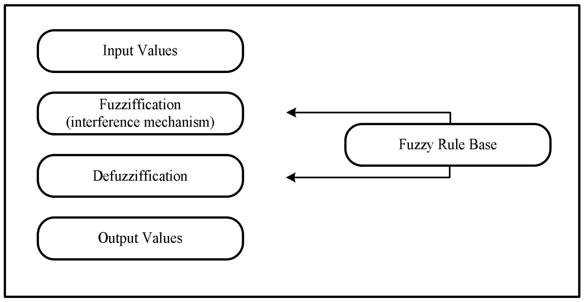

Figure 3. Fuzzy logic application steps

Entry data of random nature are assigned a level of adjacency through the use of evaluation language operators based on the regulation strategy defined by the rule base. Through the process of defuzzification, we create quantifiable results and obtain output values. This entire process seems simple, but each step allows for use of several methods. This puts high demands on the knowledge of the field of general logic, mathematics and statistics.

For a higher evaluation of accuracy of results obtained with the use of fuzzy logic, verification is needed, e.g., in the form of case studies, which would simulate realistic conditions and their influence on a real object. Penetration tests of selected passive security elements with the use of specific tools may serve as another kind of verification tool. The Faculty of Security Engineering at the Zilina University has performed similar tests as part of the PACITA and VEGA projects focused on acquiring delay time values of the most often used fences, safety walls, and other security elements. All missing delay time data could be acquired this way though this seems unrealistic due to high financial cost of the process. Therefore, the verification through selected tests is the biggest asset of the process.

VIII. CONCLUSION

Creating a database that would exactly present the quality of security elements based on their delay time values when being negotiated by a specific set of tools means a huge advancement in the abilities of quantitative evaluation of the quality of physical protection systems. In terms of evaluating resilience, i.e., the ability of an object or system to maintain its functionality against the influence of negative factors, the process of determining delay time values offers possibilities to highlight links to other indicators of resilience, specifically in case of structural resistance. Relations are, however, also clear in case of other indicators such as readiness, security or safety; and as was previously mentioned, it has a considerable importance when determining the reaction time. All acquired data will serve as an important step forward in the field of object security, especially in the application of quantitative evaluation of the physical protection systems.

ACKNOWLEDGMENT

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] Council Decision 2007/124/EC, Euratom, Council decision of 12 February 2007, establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks,

Accessed on 15 Feb. 2016, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0001:0006:EN:PDF.

[2] Green paper on a european programme for critical infrastructure protection.

Accessed on 30 March 2016, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&rid=8

[3] National concept of protection and defense methods of critical infrastructure in the Slovak Republic, Accessed on 18 April

2016, Available at: http://www.economy.gov.sk/narodny-program-pre-ochranu-a-obranu-kritickej-infrastruktury-v-slovenskej-republike--pdf-/136156s

[4] National program of protection and defense of critical infrastructure in the Slovak Republic

Accessed on 18 March 2016, Available at: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-186499?prefixFile=m_

[5] L. Simak, J. Ristvej, (2009). The Present Status of Creating the Security System of the Slovak Republic after Entering the European Union, Journal of Homeland Security and Emergency Management: Vol. 6 : Iss. 1, Article 20, ISSN: 1547-7355. DOI: 10.2202/1547-7355.1443

[6] T. Lovecek, at al. Qualitative approach to evaluation of critical infrastructure security systems. In: European journal of security and safety. ISSN 1338-6131. - Vol. 1, no. 1

[7] M. Hromada et al. The system and method of resilience evaluation of critical infrastructure / Systém a způsob hodnocení odolnosti kritické infrastruktury. Ostrava, 2014. 177 p. ISBN 978-80-7385-140-8.

[8] D. Řehak, L. Hadacek. Uniform methodology for determining the equipment for the production, transmission and distribution of national and european critical infrastructure and physical protection of these devices / Metodika jednotného určování zařízení pro výrobu, přenos a distribuci elektřiny národní a evropskou kritickou infrastrukturou a zajišťování fyzické ochrany těchto zařízení. [certified methodology]. Prague, 2013. 51 p. Č.j.: MV-104188-1/PO-OKR-2013

[9] M. L. Garcia, The design and evaluation of physical protection systems. USA: Elsevier. (2001). ISBN 0-7506 – 7367 – 2.

[10] G. Honey, Intruder alarms. 3rd edition. USA: Elsevier. (2007). ISBN – 13: 978-0-7506-8167-4

[11] T. Lovecek, J. Reitspis, Design and evaluation of physical protection systems / Projektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS- University of Žilina. (2011). ISBN 978-80-554-0457-8

[12] V. Kavicky, L. Figuli, S. Jangl, Z. Zvakova, Analysis of the field test results of ammonium nitrate: fuel oil explosives as improvised explosive device charges. In: Structures under shock and impact XIII: (13th international conference, SUSI 2014: New Forest, United Kingdom, 3 June 2014 through 5 June 2014). – Southampton, Boston: WITpress, 2014. – ISBN 978-1-84564-796-4. – P. 297-309. – (WIT Transactions on the Built Environment, Vol. 141. – ISSN 1746-4498). Available online with ISBN 978-1-84564-797-1.