Ing. Nikola Chovančíková – prof. Ing. Zdeněk Dvořák – PhD.**, doc. Ing. Bohuš Leitner, PhD.****

Safety indicators as a basis for increasing the resilience of critical infrastructure

Introduction

Critical infrastructure is a very large and complicated system that is increasingly attracting the attention of the general public in the 21st century. The current functioning of critical infrastructure (CI) elements can be negatively affected by the various threats that exist in society. The energy network, the transport network, information and communication systems, and many other establishments are classified as "critical infrastructures" which are necessary for the maintenance of vital social functions. Damage or destruction of CIs by natural disasters, terrorism, and crime can have negative effects on the safety of the European Union (EU) and the well-being of its citizens. Under Directive 2008/114 EC, critical infrastructure has been defined as an asset or system that is necessary to maintain vital social functions without which the functioning of the state would be significantly disrupted [1]. Due to the great importance of critical infrastructure elements for the functioning of the country's economy, it is necessary to increase their safety. The way to increase safety is to focus on the assessment of resilience. The article deals with the design of a framework for the evaluation of static resilience, which aims to create a basis for a possible solution to enhance the dynamic resilience of CI elements. The complexity of the solution should be determined by a framework based on the pillars of safety and protection.

Judicial analyses of critical infrastructure protection in Slovakia

In the past, the term critical infrastructure was not used in the Slovak Republic. Instead, such establishments and systems were generally referred to as important or vital infrastructure. The first milestone that can be considered as a serious step to deal with the issue of CI in Slovakia is the year 1999. In 1999, the central state administration bodies under the responsibility of the Ministry of the Interior of the Slovak Republic began to address the issue of CI. The primary task was to develop and coordinate the activities needed to ensure the protection of critical infrastructure, or vital infrastructure. Vital infrastructure was also addressed in Act no. 319/2002 Coll. on the defence of the Slovak Republic, in which §27 identified objects of special importance, which can historically be considered as the first elements of CI. Objects of special importance were within the framework of Act no. 319/2002 defined as strategic objects of defence infrastructure, the damage or destruction of which will limit the provision of state defence [2].

The very process of developing a legal instrument to address the problem of critical infrastructure security began with the approved document Concept of CI in the Slovak Republic and the method of its protection and defence. The concept was approved by Resolution no. 120 of 14 February 2007 of the Government of the Slovak Republic. Further adjusted in the process of the development of CI issues, the National Program for Critical Infrastructure Protection and Defence in the Slovak Republic was prepared in 2008. The program identified and detailed nine sectors of critical infrastructure located in Slovakia. The current legal instrument regulating the issue of CI is Act no. 45/2011 on Critical Infrastructure, the aim of which is in line with Directive 2008/114 / EC to improve the existing protection of critical infrastructure, in particular against the stronger threat of terrorist attacks [3] [5]. In order to improve the protection of critical infrastructure, two guidelines have emerged, which are rather of a recommendatory nature. Operators of CI elements can follow the given guidelines when implementing safety measures and handling sensitive information. The first guideline is Methodological guideline no. 29014 / 2014-1000-53190 MH SR on safety measures for the protection of CI elements in the energy and industry sectors. The second methodological guideline regulating the conditions of work with sensitive information is Methodological Guideline no.

ÖSSZEFOGLALÁS: A cikk a kritikus infrastruktúra védelme területén végzett kutatások eredményeit taglalja. A rugalmassági kutatás célja a statikus ellenálló képesség értékelési kereteinek létrehozása. A megoldás bonyolultságát ez a védelem (veszélytelenség, üzembiztonság) és a biztonság pilléreiből adódó keret határozza meg. A cél a kritikus infrastruktúra-létesítmények rugalmasságának dinamikus értékeléséhez szükséges műszaki előfeltételek megteremtése.

KULCSSZAVAK: statikus rugalmasság, a biztonság pillérei, kritikus infrastruktúra

ABSTRACT: The article discusses the results of research in the field of critical infrastructure protection. The resilience research is aimed at creating a framework for the assessment of static resilience. The complexity of the solution should be given by the framework, which derives from the pillars of safety. The aim is to create technical prerequisites for a possible dynamic assessment of the resilience of critical infrastructure facilities.

KEY WORDS: static resilience, pillars of safety, critical infrastructure

* University of Zilina, Faculty of Safety Engineering, Department of Technical Sciences and Informatics, 1. May 32, 010 26 Zilina; nikola.chovancikova@fbi.uniza.sk; ID: https://orcid.org/0000-0002-1982-6115

** University of Zilina, Faculty of Safety Engineering, Department of Technical Sciences and Informatics, 1. May 32, 010 26 Zilina; zdenek.dvorak@fbi.uniza.sk; ID: https://orcid.org/0000-0002-8320-1419

*** University of Zilina, Faculty of Safety Engineering, Department of Technical Sciences and Informatics, 1. May 32, 010 26 Zilina; bohus.leitner@fbi.uniza.sk; ID: https://orcid.org/0000-0001-5314-5666

08884 / 2018-1021-04943 of 7 March 2018 of the Ministry of Economy of the Slovak Republic on the protection of sensitive information on critical infrastructure and on the manner of handling this information in the conditions of the operator of the CI element of infrastructure in the energy and industry sectors. In connection with the protection of information, it is necessary to mention Act no. 69/2018 Coll. on Cyber Safety and on Amendments to Certain Laws Related to Critical Infrastructure [4]. In addition to legislation, there is a need to focus on possible ways to increase the safety of CI elements. An increase in the safety of CI elements can be achieved by increasing their resilience. Resilience ensures that the elements retain their basic functions even under the influence of adverse events and helps to prevent a failure of the overall infrastructure network.

Literature review

Scientific and professional literature has a large number of definitions for resilience. In most cases, the definition of resilience is adapted to the study area. In the area of critical infrastructure, it is appropriate to follow the definition developed in the Critical Infrastructure Resilience Final Report and Recommendations of 2009. Resilience is defined as the ability to absorb, adapt and / or recover rapidly from a potential adverse event [6]. Resilience has been addressed by many authors abroad. In the Czech Republic, the book Resilience of Critical Infrastructure: Theory, Principles and Methods was published, focusing on the issue of resilience of critical infrastructure. Dávid Řehák, in cooperation with a team of experts in the publication of the book, presents the critical infrastructure system, which includes the definition of the development of CI, the description of individual links in the system and the network layout of CI. A substantial part of the book is devoted to defining resilience in the CI system and evaluating cascading and synergistic effects in the CI system. The authors developed the CIERA method to evaluate the resilience of CI elements. The method makes it possible to quantify the level of robustness, adaptability and recoverability for different types of threats and from this determine the resulting level of resilience of the element. In the paper Resilience of Critical Infrastructure Elements and Its Main Factors, the authors focus on defining the conditions for building and strengthening the resilience of critical infrastructure elements. Subsequently, the factors determining the resilience of the elements are identified. The article concludes with case studies focusing on the energy, gas, ICT and road transport sectors [7]. Virenda Proag in Assessing and Measuring Resilience also assesses and measures the resilience of critical infrastructure elements. The publication deals with infrastructure systems that affect our daily lives, and thus draws attention to the problem of resilience. To define, quantify, and design an overall design to improve resilience, it focuses on properties such as absorption, adaptation, and recovery. The paper also includes steps to carry out an assessment of the resilience of socio-economic systems, e.g. defining the system – understanding the components of the system and how resilience affects the system, evaluating resilience – identifying the recovery path and performing recovery using models, etc. Furthermore, the publication lists indicators within the individual infrastructures, e.g. rescue services – number of lives saved, telecommunications – number of interrupted telephone calls and others. The publication includes a quantitative and qualitative assessment of resilience. In quantitative assessment, it addresses the effectiveness of resilience, and in qualitative assessment, a risk analysis is performed to identify the sources of risk [8]. In other publications, the issue of increasing the safety of critical infrastructures is addressed by Vidriková and colleagues in the book Critical Infrastructure and Integrated Protection [9]. The first results on the topic of safety indicators were published by the authors in the publications Indicators as a Tool for Evaluating the Pillars of the Safety Management System and in the article Research of Safety Management Indicators [10] [11].

Regarding the resilience of critical infrastructure, it is relatively safe to say on the basis of the analysis of available information sources that no one has so far comprehensively addressed this issue in Slovakia. That is why there is enough space here for new ideas that would be able to take the question of resilience and the protection itself to a higher level. Therefore, we think that creating a framework for assessing static resilience will have its benefits for practical purposes as well.

Materials and methods

When processing the framework for the evaluation of static resilience and the subsequent creation of assumptions for the solution of dynamic resilience, we propose to start from the pillars of safety, see *Figure 1*. The safety pillars make it possible to comprehensively cover the area of protection and defence of elements. By increasing resilience, we can also increase the safety of CI elements.

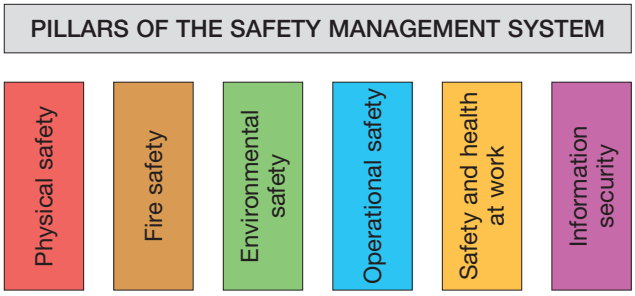

Figure 1 Pillars of the safety management system [12]

Within the individual pillars of safety, indicators will be set that are specific to the given area and determined by the entire area of complex coverage. The values of individual indicators would be determined fixedly on the basis of *Table 1*. The values of all indicators are added together and calculated as a percentage. The height of the static resilience value is determined according to *Table 2*.

The above three-level evaluation is more suitable for experts in practice; in our experience, a five-level scale would be too detailed. The aim of the practice is to gradually improve the setting of parameters so that most of the indicators used in practice are evaluated effectively.

The setting of the boundaries for the overall evaluation was determined by a group of experts, with the proviso that the stated values are recommended to be set again for a specific solution according to national and company practices.

Results

Based on the performed analysis and expert discussions, we came to the conclusion that the solution of static resilience through safety pillars has a real informative value

Table 1 Indicator rating scale (created by authors)

Verbal expression	Description	Value
Excellent	The indicator rated 1 (excellent) is a sign of quality assurance and coverage of all important requirements within the evaluated area. It is not characterized by serious deficiencies that would affect the deterioration of the value of the indicator.	1
Good	An indicator rated 2 (good) is a sign of good safety, but some areas are not sufficiently covered and may represent potential sources of risk in the future. It is characterized by minor shortcomings.	2
Bad	An indicator rated 3 (bad) is a sign of unsatisfactory safety. Some indicators are not covered at all. It is characterized by shortcomings that can have a significant impact on reducing the durability of the object.	3

Table 2 Overall evaluation of the level of resilience of the object (created by authors)

Value	Verbal expression	Description
33%-57%	Excellent level of resilience	Objects included in this group are characterized by high to very high static resilience within the individual evaluated pillars. Their shortcomings are defined and have no impact on the effectiveness of the evaluated object.
58%-79%	Good level of resilience	Objects included in this group are characterized by a good level of resilience within the individual evaluated pillars. The evaluation identified a number of shortcomings which partially reduced the level of resilience in the pillars. These shortcomings need to be remedied in the future by taking preventive measures, as they may represent the possibility of disrupting some functions of the building.
80%-100%	Bad level of resilience	Objects included in this group are characterized by low resilience within the evaluated pillars. Deficiencies can represent significant sources of risk that can lead to disruption of the operation of the object.

in practice. The proposed evaluation of individual indicators is relevant and the relevant values can adequately evaluate the given indicator. An increase in the informative value of indicators leading to the evaluation of the resilience of a given area can be achieved by an arithmetic mean. Arithmetic averages in the pillars of physical, fire, environmental, information safety, operational safety and health and safety will be applied in the final evaluation of resilience. An example of the application of the proposed method will be given in the following part of the paper in the case study. When studying the issue, the first impression is that it is a too subjective form of evaluation. Therefore, it is necessary to perform several evaluations on real objects. These case studies aim to set real practice-friendly values in an appropriate way.

Case study

The paper deals with the design of a method for assessing static resilience through the use of safety pillars. The proposed method of static resilience assessment will be applied to a potential element of critical infrastructure. In the case study, only 12 indicators will be included, i.e. two indicators will be set in each area. To ensure a comprehensive informative value, it is necessary to have at least 20-30 indicators in each area.

The proposed procedure will be applied to the Varín power plant, which is a very important element of the electrical infrastructure and can even be considered as a potential element of critical infrastructure. The display of the evaluation of individual areas is given in *Table 3*. The evaluation given in Table 3 includes the research results that were collected by the authors.

The evaluation based on the set indicators has led to the conclusion that the object has an excellent level of resilience, because its final value is 42% and is in the range of 33%-57%, see *Table 2*. In reality, the building is characterized by high durability because it is a relatively new building, which is very important for the energy infrastructure, and it is constantly maintained and undergoing modernization. If there are any shortcomings, they are certainly minimal and do not have a significant impact on reducing the durability of the object.

Discussion

The objectification of safety, vulnerability and resilience assessment is a common research topic. Teams of researchers around the world are looking for effective methods, procedures and tools to realistically measure safety, vulnerability and resilience. In each real life event, everyone evaluates the subjective safety assessment separately. The level of threat perception is different for each person. The objectification of evaluation is therefore very complicated because it requires a comprehensive approach. In the research conducted at the University of Žilina, we came to the conclusion that in principle, two approaches are possible in the creation and design of indicators for measuring the level of safety, vulnerability and resilience.

The first requires the measurement of specific physical quantities and the setting of limits for excellent (green), good (orange) and unsatisfactory evaluation (red). As an example, it is possible to mention the ambient temperature for a building located in Žilina (northwest of the Slovak Republic). During the year, temperatures from -5 to +30 degrees are common here. In this range, it is possible to evaluate the outdoor temperature excellent (green) depending on the season. If an anomaly occurs when negative temperatures drop to -15 to -6 degrees, or positives rise above 30 to 35 degrees, then it is possible to rate the temperature as good (orange), all other cases would be rated as unsatisfactory (red). Extreme negative

Table 3 Design of a comprehensive resilience assessment (created by authors)

PILLAR	INDICATOR	DESCRIPTION	VALUES	RESULT VALUE
Physical safety	Unauthorized entry into the premises	*a)* the building is 400 m away from the access road, which is separated by a barrier and a fence.The entrance is checked by an employee at the gatehouse. Including camera system.	1	1
		b) the building is separated from the access road by a barrier and a fence. The barrier is opened by attaching an employee card. There is no camera system that records the movement of vehicles.	2	
		c) access to the premises is not protected by abarrier, physical protection, camera system.	3	
	Fencing the perimeter of the complex	*a)* the perimeter fencing of the premises is made of welded panels in combination with other wire	1	1
		b) the fencing of the perimeter of the area is made of plastic-coated mesh, including a system for detecting the crossing of the fence, e.g. microphone cable	2	
		c) the perimeter fencing is made of plastic-coated mesh	3	
Fire safety	Equipment of the building according to the regulations on fire safety of the building	*a)* The building is equipped in accordance with applicable fire safety regulations. They abound with all basic and prescribed equipment for indicating and extinguishing fire in the building. According to valid standards.	1	1
		b) The building is equipped with valid fire safety regulations. They abound in basic equipment for indicating and extinguishing fire in the building.	2	
		c) The building is equipped with fire safety regulations. They provide only the necessary and most necessary equipment for indicating and extinguishing a fire.	3	
	Electrical fire alarm system	*a)* Equipment of the building in each production (steamboiler space, steamturbine, ...) and non-production space (offices, halls, ...) with electric fire alarm	1	1
		b) The electric fire alarm system is installed only in the production premises, i.e. only where there is the highest probability of a fire	2	
		c) The building is not equipped with electric fire alarm due to high financial resources	3	
Environ-mental safety	Periodicity of drainage system inspection	*a)* The drainage system anditsmaintenance intermsof protec-tionof the building is complied with in accordance with all regulations, emphasis is placed on inspections, prevention in all directions. Inspection and maintenance is performed once a month or as needed.	1	2
		b) The drainage system and its maintenance are inspected as needed and according to meteorological conditions. Inspec-tion and maintenance is performed once every six months or if necessary.	2	
		c) Drainage system and its maintenance is insufficient or none at all (it is neglected, the runways are often flooded). Inspection and maintenance is performed once a year or if necessary.	3	
	Threat to the building by floods	*a)* The building is located in very good outdoor conditions and there is no risk of flooding near the building (eg on a hill)	1	1
		b) The object is located near a river or water reservoir, but in case of floods the object can be endangered only by the least risk	2	
		c) The building is built in very close proximity to the river or in a location where there is a high flood risk (a few meters from the river)	3	

PILLAR	INDICATOR	DESCRIPTION	VALUES	RESULT VALUE
Operational safety	Occurrence of malfunction of the system for proving identity? check-in	*a)* "Check-in" or identity verification works at a top level, without more serious failure. The technology is more modern and the failure rate is minimal (once every 5 years).	1	1
		b) "Check-in" or identity check works at a high level, without failure. The technology is modern, but not as before, failures can occur (once every 1).	2	
		c) "Check-in" or identity check works ata sufficient level, failures are more frequent. The technology is outdated and the failure rate is very likely. (once every six months).	3	
	Time interval for maintenance of facility equipment	*a)* Maintenance of production process equipment is performed at intervals (4 months)	1	2
		b) Maintenance of production process equipment is performed at intervals (12 months)	2	
		c) Maintenance of production process equipment is performed at intervals (24 months)	3	
Safety and health at work	Expertise of employees	*a)* The employees of the building have all mandatory training, which is a basic prerequisite for the quality performance of security protection of the building.They are retrained regularly, exactly according to valid standards.	1	1
		b) The employees of the building have provided only the necessary and basic training for the quality performance of the safety of the building protection.They are retrained as needed, or at the request of the employer, according to applicable standards.	2	
		c) The employees of the building have only basic training provided, for sufficient performance of the safety of the building protection. They are trained at the request of the employer.	3	
	Failure to use personal protective equipment in the workplace	*a)* The regulation is drawn up, complied with and wears personal protective equipment in accordance with it	1	1
		b) The regulation is drafted, they do not comply with it, but they wear personal protective equipment	2	
		c) The regulation is not drafted, therefore personal protective equipment is not observed and is not worn	3	
Information security	Protection against misuse of data and information	*a)* The object has a complete backup of data, which is understood as a process in which copies of source data are created, can usually be stored in a different storage than the source data. The main reason for backup, in contrast, is the fast recovery of source data.	1	2
		b) Data backup is performed only when necessary and not all data is backed up, but only necessary.	2	
		c) Insufficient security against loss of data and information. The loss of any company data can mean great financial damage for a given company, or in extreme cases even liquidation	3	
	Security information software for information flow processing	*a)* The object of interest has a secure software solution for information flow together with a professional administrator for incident resolution,	1	1
		b) The object of interest has a secure software solution for information flow without a professional administrator for incident resolution,	2	
		c) The object of interest does not have a secure software solution for the information flow and does not even have a designated person to deal with incidents,	3	
			Sum	15
			Percentage expression of resilience	42%
			Verbal expression of resilience value	Excellent level of resilience

and positive temperatures affect not only people, but also technical systems and operating technologies.

The second approach is applied when it is not possible to measure real physical values; then an expert evaluation takes place, which requires the team of experts to determine the current evaluation for the proposed indicators with points of 1, 2 or 3.

To explain the practical use, if we choose, for example, road transport presented by individual use of passenger cars, or public transport presented by buses, then winter temperatures below minus 15 degrees in possible combination with wind and snow are a big problem. Measuring real outdoor temperatures is a standard task, a combination with wind (it is necessary to set the limits in m/s) and snow (it is necessary to set the limits of snow intensity).

Temperatures below minus 15 degrees are unique to our conditions and have a short duration. If, however, temperatures below minus 15 degrees came for ten or more days combined with heavy snowfall and strong winds, then it is possible that this would significantly reduce road traffic in the region concerned.

Conclusion

Safety research is a multidisciplinary and multi-level issue. The first step is to define the place (system) where we want to examine safety. In the past, experience has been crucial for safety decisions. Every entrepreneur / manager considers safety to be something that reduces profits and creates barriers to free enterprise. Sooner or later, everyone will face real safety issues. Their scope is presented in the article by the individual pillars of the safety management system. These six pillars are the basic framework within which the individual indicators have been prepared and tested.

The main intention of the researchers is to open a professional discussion in order to objectify the measurement of safety for the future. Our vision is that, thanks to the technology of the Internet of Things and the Internet of Everything, usable real-time physical measurements will be available in a short time. The measured values of individual quantities will be shared in expert information systems, where they are used by safety managers to support decision-making. In case of unavailability of some quantities, it will be possible to use learning software tools, where the initial values are set by experts and will be gradually improved by learning software. The goal should be to create expert information systems that will help safety managers in real time to decide how to proceed at a given moment. For the future, a technical standard should be prepared to address various scenarios in detail in order to enhance the safety of critical infrastructure.

Acknowledgement

Publication of this paper was supported by project IGP 2019/02 Proposal for a methodology for assessing the resilience of infrastructure object in the transport sector.

References

[1] Official Journal of the European Union. “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection.” Accessed March 3, 2021. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF , (Accessed 15.3.2021);

[2] Legal and information portal. “Act No. 319/2002 Coll. Defence of the SR as Amended.” Accessed March 3, 2021. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/319/, (Accessed 15.3.2021);

[3] Legal and information portal. “Act No. 45/2011 Coll. Regarding Critical Infrastructure.” Accessed March 3, 2021. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20210301, (Accessed 15.3.2021);

[4] Legal and information portal. “Act No. 69/2018 Coll. On Cyber Safety and on Amendments to Certain Acts.” Accessed March 3, 2021. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20200701, (Accessed 15.3.2021);

[5] Ministry of Interior of the Slovak Republic. “Critical infrastructure Protection.” Accessed March 3, 2021. https://www.minv.sk/?Ochrana_kritickej_infrastruktury, (Accessed 15.3.2021);

[6] National Infrastructure Advisory Council. “Critical Infrastructure Resilience Final Report and Recommendations.” Accessed March 3, 2021. https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf, (Accessed 15.3.2021);

[7] Řehák Dávid, Senovsky Pavel, Slivkova Simona. “Resilience of Critical Infrastructure Elements and Its Main Factors.” [online]. *Systems* 6, no.2 (May 2018):1-13. https://doi.org/10.3390/systems6020021, (Accessed 15.3.2021);

[8] Proag Virendra. „Assessing and Measuring Resilience. “ *Procedia Economics and Finance* 14, no. 18. (December 2014): 222-229. https://doi.org/10.1016/S2212-5671(14)00934-4, (Accessed 15.3.2021);

[9] Vidrikova, Boc, Dvořák and Řehák. *Critical Infrastructure and Integrated Protection*. 1st edit. Ostrava, Czech Republic: The Association of Fire and Safety Engineering, 2017;

[10] Chovančíková and Hoterová. “Indicators as a tool for assessing the pillars of the safety management system.” *The Science for Population Protection* 12, no.1 (October 2020);

[11] Dvořák and Chovančíková. “Research of safety management indicators.” *Technium social sciences journal* 8, no. 1 (June 2020);

[12] Belan Ľubomír. *Safety management. Safety and risk management*. University of Zilina, 2015.