

Measuring Resilience in Emergency Service Critical Infrastructure Elements in the Context of the Population Protection

Alena Splichalova^{a,*}, David Rehak^a, Jarmil Valasek^b, Frantisek Paulus^b

^aCharles University, Faculty of Social Sciences, Smetanovo nabrezi 6, 110 01 Prague 1, Czech Republic

^bPopulation Protection Institute, Na Luzci 204, 533 41 Lazne Bohdanec, Czech Republic

alena.splichalova@vsb.cz

Emergency service critical infrastructure elements are central elements in the systems used to protect the population. All branches of the integrated rescue system in the Czech Republic, especially the Fire Rescue Service of the Czech Republic (FRS), belong to this group of elements as key elements that specify and fulfil tasks to protect the population. The buildings used by FRS units face a considerable number of threats that increase their vulnerability and can subsequently disrupt their operations. In order to ensure the preparedness and subsequent operability of FRS stations, knowing the resilience of these elements, i.e. their preparedness against the effects of internal or external threats, is necessary. The article reviews various currently described resilience evaluation methods as well as the CIERA method and their application in selected elements of critical infrastructure emergency services.

1. Introduction

The fundamental task of every European state is to protect the life, health and property of its population. Under the subsidiarity declared in the Treaty of European Union (Council and Commission of the European Communities, 1992), protection of the population is administered by the individual European Union member states who create the legal regulations in this area and establish the branches for fulfilling individual tasks (Rehak et al., 2016). Measures to protect the population in the Czech Republic are performed by branches of the integrated rescue system and primarily the FRS (Act 239, 2000), which plays a key role in this system. Disruption to the system and failure to protect the population, especially in the ability of its branches to act in as the need arises, would have far-reaching consequences for the entire society (Rehak and Novotny, 2016). The preparedness and subsequent responsiveness of the FRS is closely linked to the functionality of its fire stations. In the Czech Republic, these buildings are designated as critical infrastructure elements (Government Decree, 2010). The buildings provide round-the-clock availability, and all means required for interventions during emergencies and crisis situations are located here. If the functionality of these elements is disrupted, the population cannot be sufficiently protected. Protecting these stations and ensuring sufficient resilience against emergent threats is therefore essential (IRDR, 2014).

The level of the resilience in critical infrastructure elements can currently be evaluated using several various methods (e.g. Nan and Sansavini, 2017; Bertocchi et al., 2016). The latest method is CIERA (Rehak et al., 2019), which was developed in the Czech Republic. This method provides a comprehensive picture of resilience in an element against specific threats and can indicate the overall status of the element. The present article therefore presents the results of applying the CIERA method to a selected, unspecified FRS station and proposes measures to strengthen its level of resilience.

2. Methods of evaluating resilience in critical infrastructure elements

Resilience, otherwise the ability of an element to absorb, adapt to and quickly recover from potentially disruptive events (NIAC, 2009), is an important part of the system for protecting critical infrastructure

elements. Resilience evaluation methods are currently non-homogeneous due to a lack of uniformity and absence of a standard framework. This has brought about several current methods and strategies for measuring, evaluating and subsequently specifying the level of resilience in critical infrastructure elements.

Wolter et al. (2002) studied resilience evaluation in the context of information and communication technologies in the monograph *Resilience Assessment and Evaluation of Computing Systems*. Ouyang et al. (2012) published an article proposing a multi-stage framework for analysing resilience in elements over individual periods. Petit et al. (2013) published the study *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, which comprehensively assessed the threat and consequences to a system. The applied method was based on a process similar to the Resilience Index. Comes et al. (2013) also examined the comprehensive assessment of resilience. Their methodological approach, which specifies the most critical points of a system, can be applied to any element.

Ouyang and Wang (2015) presented a new method for resilience evaluation, based on a holistic approach and comprehensive examination of the specific environment. Brauner et al. (2015), by contrast, strictly separated the environment that critical infrastructure vulnerabilities are assessed under into internal and external areas. Prior (2015) also divided the process of resilience evaluation, according to the time before the effects of negative factors begin and the period after the effects end. In the *Guidelines for Critical Infrastructure Resilience Evaluation*, Bertocchi et al. (2016) presented a foundation and combination of resilience dimensions, models and components with the aim of creating a unified concept of resilience evaluation that could be adapted to a specific sector of critical infrastructure. The method applies physical, logical, personal, organisational and cooperation indicators. The *Critical Infrastructure Resilience Index* method was also published in the same year. This method is compatible with all types of critical infrastructure and can be used to provide a cumulative resilience value (Alheib et al., 2016).

Over the last decade, several methods designed to specify the level of resilience in elements have been developed and proposed. Most of these, however, did not include all the resilience phases or components. Nan and Sansavini (2017) therefore created a quantitative method that consisted of integrated and hybrid modelling metrics. Cai et al. (2018) also proposed a new methodological solution based on the principle of a Bayes network evaluation method. The authors suggested that the main factors were the engineering system structure and means to maintain it. The most recent method, created for the purpose of comprehensive resilience evaluation in critical infrastructure system elements, is CIERA method (Rehak et al., 2019). CIERA is described in the following section of the article.

The specified resilience factor is not the only determining factor which maintains preparedness and responsiveness in the FRS. Another factor, for example, is the mobility of individual fire trucks, which depends directly on the performance of critical traffic elements (Patman et al., 2019).

3. Description of the CIERA method

Critical Infrastructure Element Resilience Assessment (Rehak et al., 2019) is a method designed to comprehensively evaluate resilience level. The process relies on suitable knowledge of the underlying data and clearly defined procedures. The method preserves the principles of complexity, tangibility, adequacy, objectivity and expertise. It also requires information about the structural and performance parameters of the element, its safety measures, organisational processes, and importantly, the specific threats that resilience is evaluated against. The method therefore enables resilience to be measured against seven groups of threats: geological, meteorological, procedural/technological, cascade, personnel, cybernetic and physical threats (IRDR, 2014).

Resilience is evaluated according to two areas, which are subsequently broken down into components and variables (Table 1). The first area is robustness (i.e. the ability of an element to absorb the effect of a disruptive event) and the recoverability of the element. The second area is adaptability, which is determined by examining the internal management processes that create the suitable conditions for adapting a critical infrastructure element to a disruptive event already underway.

Table 1: Components and variables determining resilience in critical infrastructure elements

Areas	Technical resilience	Technical resilience	Organisational resilience
Components	Robustness	Recoverability	Adaptability
Variables	Crisis preparedness	Material resources	Risk management
	Redundancy	Financial resources	Innovation processes
	Detection capability	Human resources	Education and development processes
	Responsiveness	Recovery processes	
	Physical resistance		

Each of the variables specified in Table 1 contains a different number of measurable items, which are evaluated progressively according to previously defined point values on a scale of 1 to 5. Individual measurable items are assigned specific weights in order to lower the subjective influence of the evaluation process. Weights are also assigned to variables. These variables take into account the topologies of the elements and thus represent the importance of the variables in determining the components.

The method's important steps are evaluating the level of resilience in the critical infrastructure element, identifying weaknesses, and proposing new measures for strengthening its resilience. Table 2 is used to evaluate resilience level.

Table 2: Comparison table for evaluating the resilience level of an element

Qualitative expression of resilience	Percentage expression of resilience
High level	85–100%
Acceptable level	69–84 %
Low level	53–68 %
Insufficient level	37–52 %
Critical level	≤ 36%

The resilience level indicates the current total status of the critical infrastructure element. If this level is 68% or lower, weaknesses should be identified. This process involves decomposition of the resilience evaluation results, whereby measures to strengthen the resilience of the element can then be proposed.

4. Application of the CIERA method to a selected critical infrastructure element

An unspecified FRS station located in a region of the Czech Republic was selected for the purposes of measuring resilience in a critical infrastructure element (**Activity 1**). The resilience of this station was measured in cooperation with the fire station chief and the FRS safety manager of the given region.

This station was subsequently described in detail according to its role in the critical infrastructure system and structural and performance parameters (**Activity 2**). The structural parameters of this station specify its topological structure, and in the case of planar elements, a list of key technologies. In the case of the fire station, the performance parameter of the element is the number of people it protects in the population (Vichova et al., 2017). This information is presented in Table 3.

Table 3: Description of evaluated element of emergency critical infrastructure services

Name of element:	Fire Rescue Service Station of the Czech Republic
Sector/Subsector:	Emergency Services/Integrated Rescue System
Topological structure:	Areal element
List of key technologies:	Means of intervention System for activating means of intervention Dispatcher for receiving information
Number of protected people:	290 000

Resilience in this element was evaluated against seven selected threats (**Activity 3**); however, due to its large scope, only the results of the analysis of the fire station against the effects of cascade threats (Rehak et al., 2018), specifically, the disruption in electric power supply over a 24-hour period, is presented in this article. A description of this threat (**Activity 4**) is presented in Table 4.

Table 4: Description of evaluated element of emergency critical infrastructure services

Name of threat:	Disruption to electric power supply over a 24-hour period
Type of threat:	Technogenic
Group of threat:	Cascade threat
Specification of threat:	Disruption to electric power supply at the fire station over a 24-hour period

The following section presents the results for the robustness, recoverability and adaptability of the fire station. The robustness of this element was evaluated first (**Activity 5**). This consisted in analysing the current state (level) of individual variables, i.e. crisis preparedness, redundancy, detection capability, responsiveness and physical resistance of the element. The results of the evaluation are presented in Figure 1.

CIERA Critical Infrastructure Elements Resilience Assessment		Critical Infrastructure Elements Resilience Assessment		2015-2019 RESILIENCE Critical Infrastructure			
Station of the Fire Rescue Service of the Czech Republic		Disruption of electricity supply for 24 hours					
Element name		Threat name					
1. Assessment of Robustness							
Number	Variables	Measurable items	Score MP_k [1-5]	Weight w_k [0,1-1,0]	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_i = \sum P_j v_j$ [%]
1.1.1	Crisis preparedness	Security plans	5	0,6	100	P = 0,15 A = 0,15 L = 0,25	84%
1.1.2		Practices dealing with disruptive event	5	0,4			
1.2.1	Redundancy	Existence of substitute linkages	5	0,6	100	P = 0,15 A = 0,20 L = 0,25	
1.2.2		Activation rate substitute linkages	5	0,4			
1.3.1	Detection capability	Indication of service outages	3	1,0	60	P = 0,75 A = 0,25 L = 0,20	
1.4.1	Responsiveness	Decrease of function	5	0,4	100	P = 0,20 A = 0,25 L = 0,15	
1.4.2		Time characteristics of the use of linkage	5	0,6			
1.5.1	Physical resistance	Technical means	3	1,0	60	P = 0,25 A = 0,15 L = 0,15	

Figure 1: Evaluation of the fire station’s robustness during a disruption to the electric power supply

The recoverability of the element was then evaluated (**Activity 6**). This consisted in analysing the current state (level) of the individual variables, i.e. material resources, financial resources, human resources and recovery processes. The results of the evaluation are presented in Figure 2.

CIERA Critical Infrastructure Elements Resilience Assessment		Critical Infrastructure Elements Resilience Assessment		2015-2019 RESILIENCE Critical Infrastructure			
Station of the Fire Rescue Service of the Czech Republic		Disruption of electricity supply for 24 hours					
Element name		Threat name					
2. Assessment of Recoverability							
Number	Variables	Measurable items	Score MP_k [1-5]	Weight w_k [0,1-1,0]	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_i = \sum P_j v_j$ [%]
2.1.1	Material resources	Ability of the asset to recover its function	5	0,3	98	P = 0,2 A = 0,2 L = 0,3	97%
2.1.2		Reparability of the assets key technology	5	0,2			
2.1.3		Availability of the spare parts at the time of need	4	0,1			
2.1.4		Replaceability of assets key technology	5	0,2			
2.1.5		Time horizon of repairing or replacing key technology	5	0,1			
2.1.6		Reliability criterion	5	0,1			
2.2.1	Financial resources	Allocation of the financial resources/reserves for recovery	5	0,3	100	P = 0,2 A = 0,2 L = 0,3	
2.2.2		Availability of financial resources/reserves in time of need	5	0,5			
2.2.3		Preparedness of financial resources/reserves in time of need	5	0,2			
2.3.1	Human resources	Availability of human resources with required qualification	5	0,25	96	P = 0,3 A = 0,3 L = 0,2	
2.3.2		Capacity of human resources	4	0,2			
2.3.3		Qualification of human resources	5	0,2			
2.3.4		Personal security	5	0,1			
2.3.5		Availability of human resources in time of need	5	0,25			
2.4.1	Recovery processes	Planning for function recovery	5	0,3	96	P = 0,3 A = 0,3 L = 0,2	
2.4.2		Process of function recovery	5	0,5			
2.4.3		Crisis preparedness of the recovery processes	4	0,2			

Figure 2: Evaluation of the fire station’s recoverability during a disruption to the electric power supply

The adaptability of the element was the final resilience component evaluated (**Activity 7**). This consisted in analysing the current state (level) of the individual variables, i.e. risk management, innovation processes, and education and development processes. The results of the evaluation are presented in Figure 3.

The main activity in this evaluation was calculating element resilience (**Activity 8**). The resilience level in the critical infrastructure element was calculated as an arithmetic average of the values of its specific components. In this case, the resilience of the FRS station achieved 92%.

CIERA Critical Infrastructure Elements Resilience Assessment		Critical Infrastructure Elements Resilience Assessment		2015-2019 RESILIENCE Critical Infrastructure			
Station of the Fire Rescue Service of the Czech Republic		Disruption of electricity supply for 24 hours					
Element name		Threat name					
3. Assessment of Adaptability							
Number	Variables	Measurable items	Score MP_k [1-5]	Weight w_k [0,1-1,0]	Variable $P_j = 20 \sum MP_k w_k$ [%]	Weight v_j	Component $K_j = \sum P_j v_j$ [%]
3.1.1	Risk management	Risk management level	5	0,4	90	0,4	94%
3.1.2		Risk assessment methodology	5	0,2			
3.1.3		Implementation of security standards	3	0,1			
3.1.4		Level of scenarios for disruptive events	4	0,3			
3.2.1	Innovation processes	Organizational structure	3	0,1	92	0,3	
3.2.2		Implementation of management systems	5	0,1			
3.2.3		Management of organizational processes	5	0,1			
3.2.4		Innovation of management processes	5	0,1			
3.2.5		Technology innovation	5	0,2			
3.2.6		Innovation of security measures	4	0,2			
3.2.7		Research and development	5	0,1			
3.2.8		Innovation investment	5	0,1			
3.3.1	Education and development processes	Types of education provided or permitted by organization	5	0,2	100	0,3	
3.3.2		Scope of education	5	0,3			
3.3.3		Training to deal with the disruptive event	5	0,3			
3.3.4		Evaluation of the training's effectivity	5	0,2			

Figure 3: Evaluation of the fire station's adaptability during a disruption to the electric power supply

The final activity in evaluating resilience in the critical infrastructure element was evaluating the resilience level, identifying weaknesses and proposing measures to strengthen the element's resilience (**Activity 9**). The resilience level was gradually evaluated according to comparative values (Table 2) on three levels.

The highest level which the resilience is evaluated against is the element level. In this case, we can say that the resilience of the fire station during disruption to the electric power supply was 92%. This indicates a high level of resilience and implies we can expect a permanent supply of service in the system to protect the population for the entire duration of the effects of the threat.

Resilience can then be evaluated according to the component and variable level. The resilience level due to robustness was 84%, which indicates an acceptable level. The resilience level due to recoverability and adaptability were 97% and 94%, respectively, which represents a high level. The resilience levels of most of the variables were high. The weakest variables were detection capability, physical resistance and organisational structure, resilience level being only 60%. For these variables, the weaknesses in element resilience should be identified and subsequently removed.

5. Conclusions

In most European countries, the population is protected by a system of emergency service branches, especially the Fire Rescue Service, which performs numerous tasks under its obligations. The preparedness and responsiveness of these branches is directly proportional to the resilience of the individual Fire Rescue Service stations. The resilience level defines the vulnerability of the stations to specific threats. The higher the resilience level of these stations, the lower their vulnerability, and vice versa. Resilience in critical infrastructure elements can currently be evaluated using various methods, though for the purposes of the article, the CIERA method was applied. This method can identify weakness in an element's internal system, among other things. Measures that lead to strengthening the element's resilience can be subsequently applied on the basis of the results.

Acknowledgments

The article was elaborated within a Ministry of the Interior of the Czech Republic Project, filed under: VI20152020009, entitled 'Targeted applied research of new advanced technologies, methods and procedures to increase the level of skills of the FRS'.

References

- Act 239 of 28 June 2000 on the Integrated Rescue System (Czech Republic).
- Alheib M., Baker G., Bouffier C., Cadete G., Carreira E., Gattinesi P., Guay F., Honfi D., Eriksson K., Lange K., Lundin E., Malm A., Melkunaite L., Merad M., Miradasilva M., Petersen L., Rodrigues J., Salmon R., Theocharidou M., Willot A., 2016, Report of Criteria for Evaluating Resilience, Ref. Ares 2519174.
- Bertocchi G., Bologna S., Carducci G., Carrozzi L., Cavallini S., Lazari A., Oliva G., Traballesi A., 2016, Guidelines for Critical Infrastructure Resilience Evaluation, Italian Association of Critical Infrastructures Experts, Roma, Italy.
- Brauner F., Münzberg T., Wiens M., Fiedrich F., Lechleuthner A., Schultmann F., 2015, Critical Infrastructure Resilience: A Framework for Considering Micro and Macro Observation Levels. In: International Conference on Information Systems for Crisis Response and Management (ISCRAM 2015), Kristiansand, Norway.
- Cai B., Xie M., Liu Y., Liu Y., Feng Q., 2018, Availability-based Engineering Resilience Metric and its Corresponding Evaluation Methodology. *Reliability Engineering & System Safety*, 172, 216-224, DOI: 10.1016/j.ress.2017.12.021
- Comes T., Bertsch V., French S., 2013, Designing Dynamic Stress Tests for Improved Critical Infrastructure Resilience. In 10th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2013), Baden-Baden, Germany, 307-311.
- Council and Commission of the European Communities, 1992, Treaty on European Union, Office for Official Publications of the European Communities, Brussels, Luxembourg.
- GD, 2010, Government Decree 432/2010 of 22 December 2010 on criteria for determination of the critical infrastructure element (Czech Republic).
- IRDR, 2014, Peril Classification and Hazard Glossary, Integrated Research on Disaster Risk, Beijing, China.
- Nan C., Sansavini G., 2017, A Quantitative Method for Assessing Resilience of Interdependent Infrastructures, *Reliability Engineering & System Safety*, 157, 35-53, DOI: 10.1016/j.ress.2016.08.013
- NIAC (National Infrastructure Advisory Council), 2009, Critical Infrastructure Resilience Final Report and Recommendations, The Department of Homeland Security, Washington, DC.
- Ouyang M., Dueñas-Osorio L., Min X., 2012, A Tree-stage Resilience Analysis Framework for Urban Infrastructure Systems. *Structural Safety*, 36-37: 23-31, DOI: 10.1016/j.strusafe.2011.12.004
- Ouyang M., Wang Z., 2015, Resilience Assessment of Interdependent Infrastructure Systems: With a Focus on Joint Restoration Modelling and Analysis. *Reliability Engineering & System Safety*, 141, 74-82, DOI: 10.1016/j.ress.2015.03.011.
- Patman D., Splichalova A., Rehak D., Onderkova V., 2019, Factors Influencing the Performance of Critical Land Transport Infrastructure Elements. *Transportation Research Procedia*, 40, 1518-1524, DOI: 10.1016/j.trpro.2019.07.210
- Petit F., Bassett G., Black R., Buehring W., Collins M., Dickinson D., Fisher R., Haffenden R., Huttenga A., Klett M., Phillips J., Thomas M., Veselka S., Wallace K., Whitfield R., Peerenboom J., 2013, Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience, Argonne National Laboratory, Chicago, IL.
- Prior T., 2015, SKI Focus Report 9: Measuring Critical Infrastructure Resilience, Eidgenössische Technische Hochschule Zürich, Switzerland.
- Rehak D., Hromada M., Novotny P., 2016, European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice, *Chemical Engineering Transactions*, 48, 943-948, DOI: 10.3303/CET1648158
- Rehak D., Novotny P., 2016, Bases for Modelling the Impacts of the Critical Infrastructure Failure, *Chemical Engineering Transactions*, 53, 91-96, DOI: 10.3303/CET1653016
- Rehak D., Senovsky P., Hromada M., Lovecek T., Novotny P., 2018, Cascading Impact Assessment in a Critical Infrastructure System, *International Journal of Critical Infrastructure Protection*, 22, 125-138, DOI: 10.1016/j.ijcip.2018.06.004
- Rehak D., Senovsky P., Hromada M., Lovecek T., 2019, Complex Approach to Assessing Resilience of Critical Infrastructure Elements, *International Journal of Critical Infrastructure Protection*, 25, 125-138, DOI: 10.1016/j.ijcip.2019.03.003
- Vichova K., Hromada M., Rehak D., 2017, The Use of Crisis Management Information Systems in Rescue Operations of Fire and rescue system in the Czech Republic. In: 12th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2017), *Procedia Engineering*, 192, 947-952, DOI: 10.1016/j.proeng.2017.06.163
- Wolter K., Avritzer A., Vieira M., van Moorsel A., 2012, Resilience Assessment and Evaluation of Computing Systems, Springer Heidelberg, Berlin, Germany, DOI: 10.1007/978-3-642-29032-9