Safety Science 123 (2020) 104573

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic

David Rehak*

VSB – Technical University of Ostrava, Faculty of Safety Engineering, Czech Republic

ARTICLE INFO

Keywords:
Critical infrastructure
ASOR Method
Organisational resilience
Risk management
Innovation processes
Educational and development processes

ABSTRACT

Critical infrastructure is a system that consists of civil infrastructures in which disruption or failure would have a serious impact on the lives and health of the population. It includes, for example, electricity, oil and gas, water supplies, communications and emergency or healthcare services. It is therefore important that technical resilience and organisational resilience is provided continuously and at a high level by the owners and operators of these civil infrastructures. Organisational resilience management mainly consists of continuously assessing determinants in order to identify weak points early so that adequate security measures can be taken to strengthen them. In the context of the above, the article presents a method for Assessing and Strengthening Organisational Resilience (ASOR Method) in a critical infrastructure system. The essence of this method lies in defining the factors that determine organisational resilience and the process of assessing and strengthening organisational resilience. The method thus allows weaknesses to be identified and the subsequent quantification of positive impacts that strengthen individual factors in organisational resilience. A benefit from applying this method is minimizing the risk and subsequent adverse impact on society of critical infrastructure system disruption or failure. The article also contributes to achieving the UN Sustainable Development Goal 9, namely Building Resilient Infrastructure. The ASOR method namely contributes to the development of quality, reliable, sustainable and resilient infrastructure, including regional and trans-border infrastructure. Finally, the article presents the results of this method's practical application on a selected electricity critical infrastructure entity in the Slovak Republic.

1. Introduction

A critical infrastructure (CI) means an asset, system or part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions (European Council, 2008). An important factor of risk management and critical infrastructure protection is continually strengthening its resilience (Public Safety Canada, 2018; Labaka et al., 2015).

In a critical infrastructure system, resilience is understood as a situation that reduces its vulnerability, minimises the consequences of active threats, accelerates response and recovery and facilitates adaptation to a given disruptive event (NIAC, 2009). The resilience cycle in a critical infrastructure system (Fig. 1) thus enables cyclic restoration and continuous strengthening of the critical infrastructure element's resilience through prevention, absorption, recovery and adaptation. In this regard, resilience management is an important factor of risk management in a critical infrastructure (ISO, 2018).

The reference point for high-quality and effective resilience management is the ability to assess it for the purpose of identifying weaknesses. Resilience in the critical infrastructure system should be assessed at two levels. The first level consists of critical infrastructure elements,[1] where 'technical resilience' is assessed (Rehak et al., 2018). The second level consists of critical infrastructure entities,[2] where 'organisational resilience' is assessed (ASIS, 2009; Denyer, 2017).

Organisational resilience is defined as the ability of an organisation to absorb and adapt in a changing environment (ISO, 2017) and/or to survive and strengthen in times of crisis (Seville et al., 2008; Gonçalves et al., 2019). In the context of critical infrastructure it may be perceived

* Address: Lumirova 13, 700 30 Ostrava-Vyskovice, Czech Republic.
E-mail address: david.rehak@vsb.cz.

[1] A critical infrastructure element refers in particular to a structure, facility, resource or public infrastructure determined according to cross-sectional and sector criteria.

[2] A critical infrastructure entity refers to the operator of a critical infrastructure element.

https://doi.org/10.1016/j.ssci.2019.104573
Received 25 September 2019; Received in revised form 22 November 2019; Accepted 4 December 2019
Available online 25 December 2019

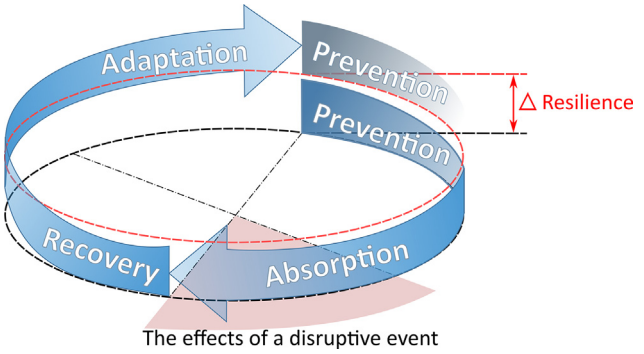

Fig. 1. Resilience cycle in a critical infrastructure system (Rehak et al., 2019).

as a management process leading to the increased adaptability of critical infrastructure elements to the recurring impact of past, disruptive events. Organisational resilience should be managed collectively for all the critical infrastructure elements operated by a given organisation. This type of resilience should be shaped, assessed and strengthened by the organisation's management in the prevention phase.

Several specialized publications concerning the assessment of resilience in a critical infrastructure system are currently available (e.g., Nan and Sansavini, 2017; Labaka et al., 2015; Petit et al., 2013), but the methods discussed focus on assessing the technical resilience of elements while only touching on or not looking at organisational resilience at all. Another group of approaches studies the assessment of organisational resilience (e.g., Bertocchi et al., 2016; Prior, 2015; ASIS, 2009), but only qualitatively, which does not allow the positive impacts of strengthening individual factors of organisational resilience to be quantified. Based on the foregoing, the aim of this article is to create a method of assessing and strengthening organisational resilience in a critical infrastructure system.

2. Factors determining organisational resilience

The starting point for assessing organisational resilience in a critical infrastructure system is setting the factors that determine this type of resilience (see Fig. 2). It is important to note that these factors should be defined in the context of the purpose that the results of organisational resilience assessment will serve, i.e. to increase the adaptability of critical infrastructure elements to disruptive events that have occurred in the past. Hence, these factors should reflect an entity's preparedness to risks, the environment's preparedness in defining and implementing adaptation processes, and the preparedness of personnel in increasing the adaptability of critical infrastructure elements. To this end, these factors should be categorized into three basic processes that include managing risk, innovation and employee (e.g., Kalowski, 2015; Boylan and Turner, 2017; NIAC, 2009; McManus et al., 2008).

Risk management is an important internal organisational process essential to ensuring safety and strengthening resilience already in the prevention stage. Risk management means coordinating the activities of leadership and organising management with regard to risks (ISO, 2018). In relation to risk management of organisational resilience, their level is determined by four factors, namely the level of risk management, the level of risk assessment methods applied, the level of safety standards implemented, and the level of specification of the disruptive event scenarios, which are the key starting points for creating contingency plans.

Other internal processes that significantly contribute to strengthening the resilience of critical infrastructure elements in the prevention stage is an organisational innovation processes. These can be separated from a practical point of view into product, process, marketing and organisational innovations (OECD/Eurostat, 2005). Process and organisational innovations are particularly important for strengthening resilience in terms of adaptability and focus on the reliability and external security of the technologies used. From this point of view, the level of the innovation process can be described by eight basic factors (Fig. 2).

Educational and development processes are the last group of processes that shape and strengthen the organisational resilience of critical infrastructure elements. The educational and development processes can be categorized into three basic types (Armstrong, 2014): knowledge (explicit and tacit), skills (e.g. technical, managerial, analytical, conceptual), and attitudes (reflecting the values a particular person recognizes). The key forms of educational and development activities include long-term education, study abroad, soft skills development, professional (of preventive and repressive nature) and employee training. Factors determining the level of education and development processes are shown in Fig. 2.

A principle of these factors is analysing an organisation's preparedness in increasing the adaptability of critical infrastructure to the recurring impact of past, disruptive events. For this reason, the factors focus on risk management processes (which preventatively and operationally minimise risks and their impact on CI elements), innovation

Fig. 2. Factors determining organisational resilience.

processes (which increase the technical resilience of CI elements), and processes for educating and developing personnel (which increase awareness of safety in CI elements, thereby minimising personal risks). Besides these processes, attention could also be given to planning, implementation and inspection processes (ASIS, 2009). These, however, do not correspond directly with resilience in critical infrastructure elements. For this reason, we may conclude that these factors are sufficient for assessing the organisational resilience of critical infrastructure.

Subsequently, the author defined individual factors, which included a description and setting the assessment parameters to indicate level with a score ranging between 1 and 100 points (the value 1 represents the minimum level of positive impact of the parameter on the creation of resilience and the value 100 represents the maximum positive impact). These scores were categorized into five levels. The score is based on the principle of linear ascension, where the difference between categories is directly proportional.

Defining the factors was primarily based on analysing the relevant documents above (i.e., ISO, 2018; OECD/Eurostat, 2005; Armstrong, 2014; McManus et al., 2008) and implemented by co-operating with experts from selected energy and transport critical infrastructure entities. Specifically, these were security directors and crisis managers of ČEPS (Czech Transmission System), SŽDC (Czech Railway Infrastructure Administration) and ŘSD (Road and Motorway Directorate), and the Security Liaison Officers of the ministries concerned, i.e. the Ministry of the Interior of the Czech Republic, the Ministry of Industry and Trade of the Czech Republic and the Ministry of Transport of the Czech Republic. Stakeholders' analysis was conducted using *A Guide to Stakeholder Identification and Analysis Techniques* (Bryson, 2004). An example of defining a factor at the level of risk management is presented in Table 1.

The final step in defining the factors that determine organisational resilience was to establish the weighting coefficients that take into account their different levels of significance (Table 2). To establish the weighting coefficients, simple methods can be used. For example, the Point Allocation Method, Weighted Ranking Method, Basic Variant Method or Fuller Triangle Method. More complex methods based on pairwise comparisons of variants can also be applied. For example, the Analytic Hierarchy Process – AHP (Saaty, 2008) or Analytic Network Process – ANP (Saaty, 2004). Methods based on utility function quantification or combinations of them are also useful (Weil and Apostolakis, 2001). In certain cases, the application of fuzzy logic (Djapan et al., 2013) may be an advantage.

Determining the weighting coefficients and subsequently standardizing them was conducted under an expert assessment of the expected future users of the method (i.e. the above-mentioned entities) using the Analytic Hierarchy Process method (Saaty, 2008), which is based on a pairwise comparison of variants supporting the assessment of criteria hierarchies. This method specifically allows realistic weight estimates to be set. It is therefore often applied in practice and achieves good results (De La Canal and Ferraris, 2013). One advantage of the AHP method is the support for preferential evaluation, which allows involved parties to assess resilience subjectively according to their preferred weights (Rehak and Senovsky, 2014).

The advantage of the AHP method is in supporting preferential evaluation that allows interested parties to carry out a subjective assessment of resilience based on preferred weights (Rehak and Senovsky, 2014). By their very nature, expert evaluations and the weights derived from them will always be subjective to some extent. Given that there is still intense research in this area, there is no widely accepted hierarchy of items, therefore the evaluation must be to some extent subjective. However, the use of such methods in management is not uncommon (Grabinski, 2007). The weighting coefficient specification allows this subjectivity to be transparently collected in one place and acknowledged. If required, the weighting system can be revised in the future.

3. Method for assessing and strengthening organisational resilience

The ASOR method was created by the author for the needs of Assessing and Strengthening Organisational Resilience in critical infrastructure system. The principle of this method lies in assessing factors that determine organisational resilience, identifying weak points and proposing measures for strengthening organisational resilience in a critical infrastructure entity. This method is mainly intended for security managers at critical infrastructure entities, but some aspects of the method are suitable for other managerial positions (e.g., personnel managers or innovation managers).

The fundamental part of the ASOR is its framework (Fig. 3), which defines the inputs necessary to achieve the assessment process itself. The use of the aforementioned factors is conditional on good knowledge of the critical infrastructure entity, defining a disruptive event scenario against which resilience can be assessed, and knowledge of the processes suitable for strengthening organisational resilience.

The central part of this method is the process of assessing and strengthening organisational resilience in a critical infrastructure system. This procedure is based on the available resources, focusing especially on critical infrastructure resilience factors (Bertocchi et al., 2016; Rehak et al., 2018), organisational resilience factors (ISO, 2017; ASIS, 2009), critical infrastructure resilience indicators (Prior, 2015; Petit et al., 2013; Rehak et al., 2017) and processes enhancing critical infrastructure resilience (Public Safety Canada, 2018; Labaka et al., 2015). From these documents, six steps were defined that allowed the level of organisational resilience to be assessed, weak points to be identified, and measures for strengthening organisational resilience to be proposed (Fig. 4).

Step 1: Analysing the selected critical infrastructure entity

The initial step in assessing and strengthening organisational resilience is to analyse a selected critical infrastructure entity. The analysis should focus on risk management, organisational innovation processes and educational and development processes. Attention should be given to individual factors under which these processes are determined within

Table 1
Defining the "Level of Risk Management" factor.

Factor Description	Assessment parameters and their scores
The aim is to assess the level of coordinated activity to manage and monitor the organisation with respect to risk. Particular attention is given to the level of implementation and execution of risk management strategies, risk analysis, risk management, risk monitoring and risk management optimization.	81–100: A risk management system is in place at the organisation. It is regularly optimized and includes strategies. 61–80: A risk management system is in place at the organisation. It is regularly optimized but lacks strategies. 41–60: A risk management system is in place at the organisation. It is not regularly optimized. 21–40: Risks are monitored at the organisation, but no risk management system is in place. 1–20: Risks are not assessed at the organisation.

Table 2
Standardized weights of processes and factors determining organisational resilience.

Weights of the organisational resilience processes (w)	Weights of the organisational resilience factors (v)
Risk management (0,4)	Level of risk management (0,4)
	Level of risk assessment methods applied (0,2)
	Level of safety standards implemented (0,1)
	Level of specification of disruptive event scenarios (0,3)
Organisational innovation processes (0,3)	Flexibility of the organisational structure (0,1)
	Level of management systems implemented (0,1)
	Methods of organisational process management (0,1)
	Level of innovation in management processes (0,1)
	Scope of technological innovations implemented (0,2)
	Level of innovation in security measures (0,2)
	Level of the organisation's involvement in science and research (0,1)
	Level of the organisation's investment into specific innovations (0,1)
Educational and development processes (0,3)	Level of education provided or supported to the organisation's employees (0,4)
	Level of employee training and maintenance of practical skills (0,4)
	Method of evaluating the effectiveness of employee training (0,2)

the context of their usability in order to increase the adaptability of critical infrastructure elements to the repeated effects of past disruptive events.

Step 2: Defining the disruptive event scenario

Not only the technical resilience of the elements but also the organisational resilience of the critical infrastructure entity needs to be assessed in the context of a particular disruptive event. This is because some factors (notably the Disruptive Event Scenario Specification Level and the Security Innovation Measures Level) can only be set in the context of certain threats. For this reason, it is important to define a disruptive event scenario before assessment. Specific methods such as Event Tree Analysis (IEC, 2010) or Failure Tree Analysis (IEC 61025, 2006b) can be applied in this area.

Step 3: Determining the level of organisational resilience

The key step in the process described is to calculate the level of organisational resilience. For this purpose, a semi-quantitative approach of assessment was selected. This approach is based on the expression as a percentage of individual factors determining organisational resilience. These expressions already include comparative values and are suitable for further use, i.e. to identify weak points. The calculation of organisational resilience itself is based on an easy to follow principle of linear aggregation of weighted values (Nasibova and Nasibov, 2010), whose results are relatively easy to interpret (Eq. (1)).

$$OR = \sum_{i=1}^{n} P_i w_i = \sum_{i=1}^{n} w_i \sum_{j=1}^{m} F_j v_j \quad (1)$$

where OR = organisational resilience of the critical infrastructure entity [%]; P_i = the i-th process of organisational resilience [%], w_i = the i-th normalized weight of the i-th process of organisational resilience [⟨0;1⟩], n = total number of processes determining organisational resilience; F_j = the j-th factor of organisational resilience [⟨1;100⟩], v_j = the j-th normalized weight of the j-th organisational resilience factor [⟨0;1⟩]; and m = total number of factors in the i-th organisational resilience process. The potential level of organisational resilience of a critical infrastructure entity is presented in graphical form in Fig. 5.

When using the principle of linear aggregation of weighted values, it is necessary to take into account that this calculation method may be encumbered by some problems. Especially significant is the implicit possibility of substitution, that is, the possibility of compensating for the lower value of one variable by the higher value of the second variable. This is a problem especially if the result is to be compared, for example, to different critical infrastructure entities. Another possible problem may be in the attempt of an evaluator to "deceive" the system. This choice is technically possible, but it is practically meaningless, because nothing forces the critical infrastructure entity to use this evaluation system. It is an informative tool providing information of a preventive nature in order to strengthen organisational resilience against selected disruptive events.

Step 4: Assessing the level of organisational resilience

The final step in assessing organisational resilience is assessment of

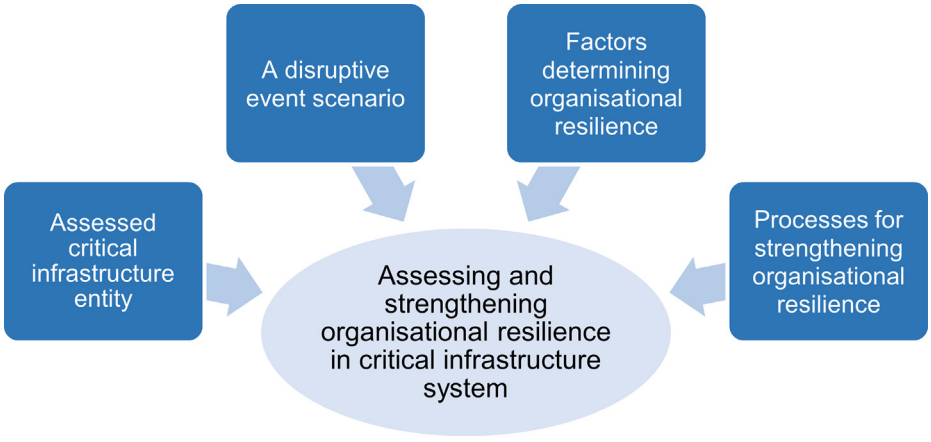

Fig. 3. Framework for the method of assessing and strengthening organisational resilience in a critical infrastructure system.

Fig. 4. The process of assessing and strengthening organisational resilience in a critical infrastructure system.

the achieved level and the adoption of adequate conclusions. To this end, an acceptance grading scale was created, which includes five categories analogous to the cases that define factors. The methodology for determining organisational resilience acceptability levels is based on the Failure Mode, Effects and Criticality Analysis method (IEC, 2006a), which uses multiple variables to determine the level of risk and is based on variations in their extreme values when assessing states. Individual levels of resilience were determined similarly, taking into account variations in extreme values in the number of classification categories (Table 3).

The above scale of acceptability levels shows that if organisational resilience reaches 69% or more (i.e. acceptable or high level), there is no need to take fundamental steps towards strengthening it. Conversely, if organisational resilience reaches a level of 68% or less (i.e. low, insufficient or critical), it is necessary to identify weaknesses (see step 5), which consists in decomposing the assessment results at the level of individual factors.

Table 3
Determination of the acceptance grading scale of organisational resilience.

Verbal expression of level	Calculation of levels by FMECA	Numeric expression of level
Critical level	1,1,1,1,5 = > ∅ 1.8	0–36%
Insufficient level	1,1,1,5,5 = > ∅ 2.6	37–52%
Low level	1,1,5,5,5 = > ∅ 3.4	53–68%
Acceptable level	1,5,5,5,5 = > ∅ 4.2	69–84%
High level	5,5,5,5,5 = > ∅ 5.0	85–100%

Step 5: Identifying weak points

Identifying weaknesses lies in decomposing the results of individual factors. Factors that have a resilience level of 68% or less (i.e. factors that do not reach the minimum acceptable level), need to be reviewed and a setup or recovery process should be initiated (see step 6).

Fig. 5. Example of expressing the level of organisational resilience of a critical infrastructure entity.

Step 6: Designing measures to strengthen organisational resilience

Based on decomposition of the assessment's results, measures to strengthen organisational resilience can be proposed. Strengthening resilience should be done as follows:

- Low level of resilience (53–68%): factors in this category embody sufficient parameters but improving them would significantly enhance the organisational resilience of the critical infrastructure entity.
- Insufficient level of resilience (37–52%): factors found in this category exhibit very poor parameters that significantly reduce the resilience of the affected processes.
- Critical level of resilience (0–36%): factors in this category are either completely absent or show critically low parameters. These factors need to be completely revised and their recovery process started as soon as possible.

To this end, not only applying the standard principles and requirements for strengthening organisational resilience (e.g., ISO, 2017; ASIS, 2009; Tasic et al., 2019) but also the specific requirements related to strengthening critical infrastructure is appropriate. In these circumstances, two initial documents can be recommended, namely the *National Cross Sector Forum 2018–2020 Action Plan for Critical Infrastructure* (Public Safety Canada, 2018) and *A Framework to Improve the Resilience of Critical Infrastructures* (Labaka et al., 2015).

The *2018–2020 Action Plan* (Public Safety Canada, 2018) continues to support the three strategic objectives identified in the national strategy for enhancing resilience in the critical infrastructure in Canada, i.e. building partnerships, sharing and protecting information and implementing an all-hazards risk management approach. A framework (Labaka et al., 2015) defines eight policies for improving organisational resilience: CI Organisational Procedures for Crisis Management; CI Top Management Commitment; CI Crisis Manager Preparation; CI Operator Preparation; First Responder Preparation; Government Preparation; Trusted Network Community; and Crisis Regulation and Legislation.

4. Example of the ASOR method's practical application in a selected electricity critical infrastructure entity

The ASOR method has been successfully applied by some critical infrastructure entities in the Czech Republic and Slovak Republic, among the most significant being, for example, the Czech Transmission System Operator, Czech Railway Infrastructure Administration, Regional Hospital Ostrava, Central Slovak Power Distribution Company and Railways of Slovak Republic. The presentation below of the ASOR method's practical application and obtained results have been anonymised to protect the critical infrastructure entity concerned.

A critical infrastructure entity was selected from the energy sector in order to assess its organisational resilience and strength **(step 1)**. The selected entity is a company operating in the territory of three regions of the Slovak Republic, distributing electricity nearly to 740,000 customers (i.e. contractors and households). Mainly the individual factors determining the processes for risk management, innovation and education and development at the organisation were examined in the analysis.

A specific disruptive event scenario was defined and then assessed against the entity's resilience **(step 2).** This event was "Disruption to SCADA (Supervisory Control and Data Acquisition) system functioning at the technical dispatch centre of a distribution system operator". The scenario was defined using the Event Tree Analysis method (IEC, 2010). A description of the disruptive event's scenario is given in Fig. 6.

After completion of steps 1 and 2, the level of organisational resilience of the critical infrastructure entity under assessment could be determined **(step 3)**. First, according to the analysis, organisational resilience factors in the context of the above-mentioned disruptive event were assessed. Based on pre-defined parameters (e.g., Table 1 for assessing the Level of Risk Management), the factor levels were assessed by the security manager of the critical infrastructure entity. Each factor was assigned a suitable number of points on a scale of 1–100, where 1 represented the minimum level of the parameter's positive effect in creating resilience, and 100 represented the maximum positive effect. The assessment results are presented in Table 4 below.

Applying equation (1), the level of organisational resilience was subsequently defined. The resulting scores of organisational resilience and determining processes are presented in Fig. 7.

The next step in assessing the organisational resilience and strength was assessing the levels achieved and adoption of adequate solutions **(step 4)**. The values achieved were compared with an acceptance grading scale of organisational resilience (see Table 3). The comparison showed that the level of organisational resilience of the rated critical infrastructure entity reached 53%, i.e., the lower limit of the lowest level. The reason for such a low level is mainly because of poorly established risk management processes, which, achieving just 24%, fall into a critical level. Organisational innovation processes reached 64%, which is also low. By contrast, educational and development processes achieved 80%, which is an acceptable level and does not need any immediate attention.

From this assessment, the weak points in the organisation's risk management and innovation processes were identified **(step 5)**. The results of the assessment of organisational resilience factors showed that the entity's critical organisational resilience factors are as follows:

- Level of risk management (32 points),
- Level of risk management methods applied (18 points),
- Level of safety standards implemented (36 points),
- Level of specification of disruptive event scenarios (12 points),
- Flexibility of the organisational structure (10 points),
- Level of the organisation's involvement in science and research (19 points).

The entity needs to revise these factors and commence recovery or renewal processes **(step 6)**. In terms of risk management, defining the risk management framework and principles, the strategic plan, the implementation of risk management processes and the tasks and responsibilities in these processes (ISO, 2018) were highlighted as urgent and proposed. In terms innovation, innovating in management processes (ASIS, 2009), increasing the flexibility of the entity's organisational structure (Denyer, 2017) and involving the organisation in science and research in energy infrastructure security (OECD/JRC, 2018) were proposed.

After partially implementing the measures above, the organisational resilience of the critical infrastructure entity was re-assessed. The results from re-assessment showed that organisational resilience increased significantly by 24%. Now achieving 77%, organisational resilience could be considered acceptable. Achieving this level of resilience was limited by time and the entity's current capabilities. For this reason, further strengthening of organisational resilience up to a high level may be assumed in the future.

In terms of risk management, a strategic basis (i.e. framework, principles, strategic plan, responsibilities) was defined as required. On this basis, risk management processes could be implemented (focusing on the risk assessment methodology, safety standards implementation, and specification of disruptive event scenarios). This process was necessary so that the entity's organisational resilience could be increased in the context of the disruptive event under assessment, i.e. "Disruption to SCADA (Supervisory Control and Data Acquisition) system functioning at the technical dispatch centre of a distribution system operator". As a result of these measures, the resilience of the process increased by 55%.

In the case of innovation processes, innovating the management processes was initiated (monitoring and self-assessment methods for the

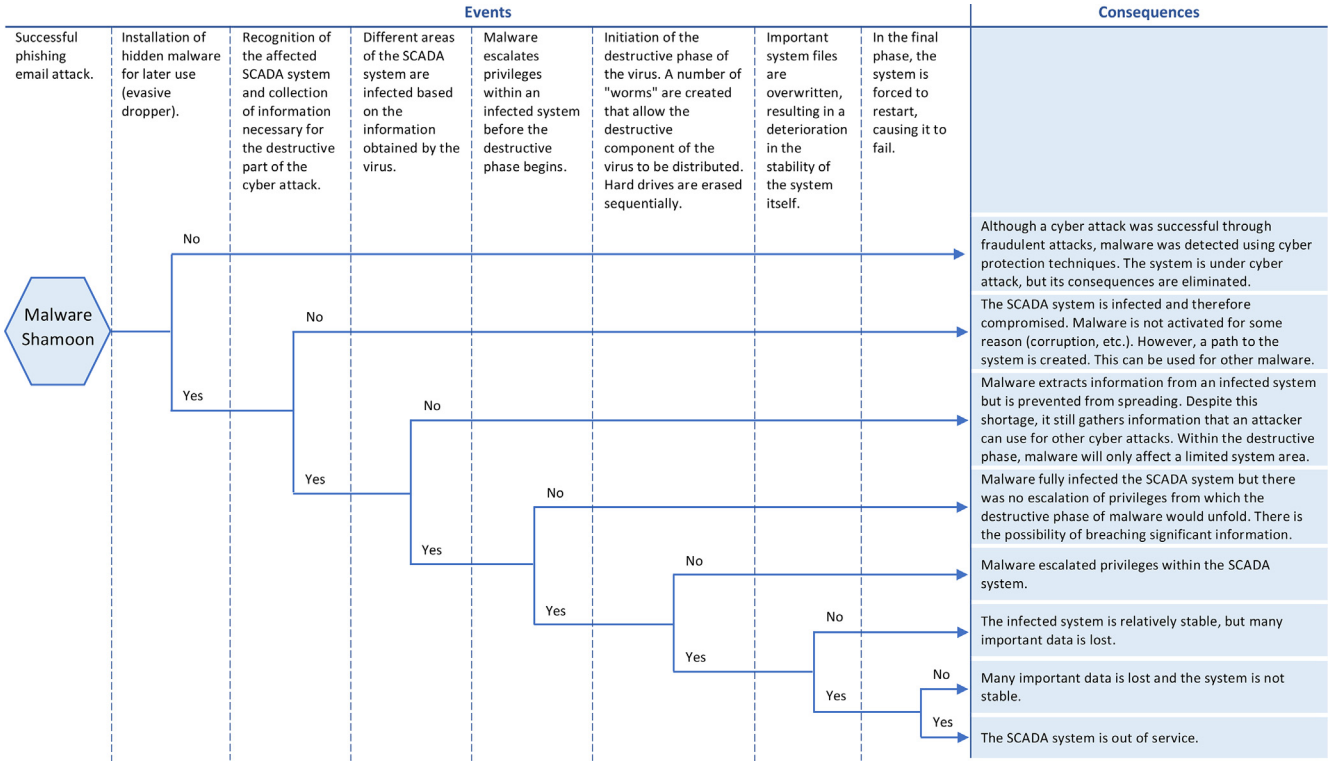

Fig. 6. Description of the disruptive event scenario.

Table 4
Results of the organisational resilience factor assessment.

Organisational resilience processes	Organisational resilience factors	Number of points
Risk management	Level of risk management	32
	Level of risk assessment methods applied	18
	Level of safety standards implemented	36
	Level of specification of disruptive event scenarios	12
Organisational innovation processes	Flexibility of the organisational structure	10
	Level of management systems implemented	73
	Methods of organisational process management	57
	Level of innovation in management processes	38
	Scope of technological innovations implemented	82
	Level of innovation in security measures	91
	Level of the organisation's involvement in science and research	19
	Level of the organisation's investment into specific innovations	95
Educational and development processes	Level of education provided or supported to the organisation's employees	90
	Level of employee training and maintenance of practical skills	76
	Method of evaluating the effectiveness of employee training	69

organisation were implemented). The entity was indirectly involved in some projects dealing with security for electricity infrastructure (mainly in practical verification of the project's results and feedback to the author). Increasing the organisational resilience in entities of this type was impossible. Process resilience increased by 7% as a result of these measures.

It follows from the case study above that organisational resilience in critical infrastructure entities is an important part of security for critical infrastructure elements. For example, Bruneau et al. (2003), even in 2003, identified organisational resilience as a key dimension of infrastructure (and then also community) resilience. This is because the importance of organisational resilience consists in strengthening an organisation's ability to absorb and adapt in a changing environment (ISO, 2017) or surviving and strengthening in times of crisis (Seville et al., 2008; Gonçalves et al., 2019). This creates a resilient environment for strengthening the technical resilience of critical infrastructure elements. Consequently, the impact of disruption to or failure of elements dependent on critical infrastructure (such as information and communications technology or transport infrastructure) is minimised. Real world examples demonstrating the need for a high level of organisational resilience in the electricity sector are nuclear facilities (disasters at Chernobyl, 1986, Fukushima, 2011). Cyber-attacks on power systems (Mullane, 2019) also pose a threat to nuclear power stations (Iran, 2010), power distribution systems (Ukraine, 2015) and operations technologies (Saudi Arabia, 2017).

5. Conclusion

The paper presents a method for assessing and strengthening organisational resilience in a critical infrastructure system (ASOR Method). The method enables weaknesses to be identified and the subsequent quantification of positive impacts that strengthen individual organisational resilience factors. This method is especially intended for the security managers of critical infrastructure entities who conduct

Fig. 7. Resulting organisational resilience level of the critical infrastructure entity.

assessment procedures in cooperation with managers responsible for individual organisational processes. The method is applicable to any critical infrastructure entity and enables organisational resilience to be assessed and strengthened against any disruptive event. Currently, the ASOR Method has already been successfully applied by several critical infrastructure entities in the Czech Republic (e.g. Transmission System Operator of the Czech Republic, Czech Railway Infrastructure Administration, and Regional Hospital Ostrava) and Slovakia (e.g. Central Slovak Power Distribution Company and Railways of the Slovak Republic).

Besides describing the ASOR method, the article also presented an example of the method's practical application in a selected critical infrastructure entity in the energy sector. The assessment results showed a critical level in organisational resilience, particularly in risk management concerning cyber threats. Because of SCADA's high vulnerability, disruption to its system may occur and result in huge power outages or blackouts (such as in 2012 when the Shamoon virus disabled tens of thousands of computers at middle-eastern energy companies). A critical level in organisational resilience in some innovation processes resulting in inflexibility in managing security systems, innovation and risk management was also identified.

In conclusion, it is worth noting that high quality and effective management of organisational resilience is the starting point and an integral part of effectively strengthening technical resilience elements already during their planning and construction stages. Strengthening complex resilience elements in a critical infrastructure system depends on an organisation's level of management and the availability of necessary resources. However, in a broader context, resilience should be seen as an indispensable part of risk management that significantly contributes to minimizing the risk of critical infrastructure system disruption or failure and the subsequent adverse impact on society.

Acknowledgments

This work was supported by the Ministry of the Interior of the Czech Republic, [Grant No. VI20152019049: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems].

Declarations of interest

No potential conflict of interest was reported by the author.

References

Armstrong, M., 2014. Armstrong's Handbook of Human Resource Management Practice. Kogan Page, London, United Kingdom.
ASIS. 2009. The Organizational Resilience Standard [ASIS SPC.1-2009]. American National Standards Institute, Washington, DC.
Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, A., Lazari, A., Oliva, G., Traballesi, A., 2016. Guidelines for Critical Infrastructure Resilience Evaluation. Italian Association of Critical Infrastructures' Experts, Roma, Italy.
Boylan, S.A., Turner, K.A., 2017. Developing organizational adaptability for complex environment. J. Leadership Educ. 16 (2), 183–198. https://doi.org/10.12806/V16/I2/T2.
Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., Von Winterfeldt, D., 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra 19 (4), 733–752. https://doi.org/10.1193/1.1623497.
Bryson, J.M., 2004. What to do when stakeholders matter: a guide to stakeholder identification and analysis techniques. Public Manage. Rev. 6 (1), 21–53.
De La Canal, M.D., Ferraris, I.C., 2013. Risk analysis holistic approach as a base for decision making under uncertainties. Chem. Eng. Trans. 33, 193–198. https://doi.org/10.3330/CET1333033.
Denyer, D., 2017. Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management, Cranfield, United Kingdom.
Djapan, M., Tadic, D., Macuric, I., Jerenic, B., Giaglon, E., 2013. A new model for evaluation of safety grade of indicators based on fuzzy logic. Chem. Eng. Trans. 33, 463–468. https://doi.org/10.3303/CET1333078.
European Council, 2008. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. European Union, Brussels, Belgium.
Gonçalves, L., Navarro, J.B., Sala, R., 2019. Spanish validation of the Benchmark Resilience Tool (short-form version) to evaluate organisational resilience. Saf. Sci. 111, 94–101. https://doi.org/10.1016/j.ssci.2018.09.015.
Grabinski, M., 2007. Management Methods and Tools. Springer Gabler, Wiesbaden, Germany. DOI: 10.1007/978-3-8349-9295-6.
IEC 60812, 2006a. Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). International Electrotechnical Commission, Geneva, Switzerland.
IEC 62502, 2010. Analysis techniques for dependability – Event tree analysis (ETA). International Electrotechnical Commission, Geneva, Switzerland.
IEC 61025. 2006b. Fault Tree Analysis (FTA). International Electrotechnical Commission, Geneva, Switzerland.
ISO 22316, 2017. Security and resilience – Organizational resilience – Principles and attributes. International Organization for Standardization, Geneva, Switzerland.
ISO 31000, 2018. Risk management – Guidelines. International Organization for Standardization, Geneva, Switzerland.
Kalowski, A., 2015. Structure determining factors of business organization. Int. J. Innovat., Manage. Technol. 6 (3), 206–212. https://doi.org/10.7763/IJIMT.2015.V6.603.
Labaka, L., Hernantes, J., Sarriegi, J.M., 2015. A framework to improve the resilience of critical infrastructures. Int. J. Disaster Resil. Built Environ. 6 (4), 409–423. https://doi.org/10.1108/IJDRBE-07-2014-0048.
McManus, S.T., Seville, E., Vargo, J., Brunsdon, D., 2008. Facilitated process for improving organizational resilience. Nat. Hazard. Rev. 9 (2), 81–90. https://doi.org/10.1061/(ASCE)1527-6988(2008) 9:2(81).
Mullane, M.A., 2019. Cyber attacks targeting critical infrastructure. < https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-

infrastructure > (Feb. 1, 2019).
Nan, C., Sansavini, G., 2017. A quantitative Method for Assessing Resilience of Interdependent Infrastructures. Reliab. Eng. Syst. Saf. 157, 35–53. https://doi.org/10.1016/j.ress.2016.08.013.
Nasibova, R.A., Nasibov, E.N., 2010. Linear aggregation with weighted ranking. Autom. Control Comput. Sci. 44 (2), 96. https://doi.org/10.3103/S0146411610020057.
NIAC (National Infrastructure Advisory Council), 2009. Critical Infrastructure Resilience: Final Report and Recommendations. U.S. Department of Homeland Security, Washington, DC.
OECD/Eurostat (Organisation for Economic Co-operation and Development), 2005. Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data. OECD Publishing, Paris, France. DOI: 10.1787/9789264013100-en.
OECD/JRC, 2018. System thinking for critical infrastructure resilience and security (Workshop). Organisation for Economic Co-operation and Development/Joint Research Centre, Paris, France/ Brussels, Belgium. < http://www.oecd.org/gov/risk/workshop-oecd-jrc-system-thinking-for-critical-infrastructure-resilience-and-security.htm > (Aug. 22, 2019).
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. Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9). Eidgenössische Technische Hochschule Zürich, Zurich, Switzerland.
Public Safety Canada, 2018. National Cross Sector Forum 2018–2020 Action Plan for Critical Infrastructure. Public Safety Canada, Ottawa, Canada.
Rehak, D., Hromada, M., Ristvej, J., 2017. Indication of Critical Infrastructure Resilience Failure. In: Cepin, M., Bris, R. (Eds.), Safety and Reliability – Theory and Application (ESREL). Taylor & Francis Group, London, United Kingdom, pp. 963–970.
Rehak, D., Senovsky, P., 2014. Preference risk assessment of electric power critical infrastructure. Chem. Eng. Trans. 36, 469–474. https://doi.org/10.3303/CET1436079.
Rehak, D., Senovsky, P., Slivkova, S., 2018. Resilience of critical infrastructure elements and its main factors. Systems 6 (2), 21. https://doi.org/10.3390/systems6020021.
Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., 2019. Complex approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Prot. 25, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003.
Saaty, T.L., 2004. Fundamentals of the analytic network process — multiple networks with benefits, costs, opportunities and risks. J. Syst. Sci. Syst. Eng. 13 (3), 348–379. https://doi.org/10.1007/s11518-006-0171-1.
Saaty, T.L., 2008. Decision making with the analytic hierarchy process. Int. J. Serv. Sci. 1 (1), 83–98. https://doi.org/10.1504/IJSSci. 2008.01759.
Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S., Vargo, J., 2008. Organisational resilience: researching the reality of New Zealand organisations. J. Bus. Contin. Emerg. Plan. 2 (2), 258–266.
Tasic, J., Amir, S., Tan, J., Khader, M., 2019. A multilevel framework to enhance organizational resilience. J. Risk Res. https://doi.org/10.1080/13669877.2019.1617340.
Weil, R., Apostolakis, G.E., 2001. A methodology for the prioritization of operating experience in nuclear power plants. Reliab. Eng. Syst. Saf. 74 (1), 23–42. https://doi.org/10.1016/S0951-8320(01)00064-3.