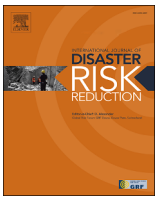
International Journal of Disaster Risk Reduction 111 (2024) 104748

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

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



Critical Entities Resilience Assessment (CERA) to small-scale disasters

David Rehak [a, *], Alena Splichalova [a], Heidi Janeckova [a], Alena Oulehlova [b], Martin Hromada [c], Miltiadis Kontogeorgos [d], Jozef Ristvej [e]

[a] VSB – Technical University of Ostrava, Faculty of Safety Engineering, Lumirova 13, 700 30 Ostrava - Vyskovice, Czech Republic
[b] University of Defence, Faculty of Military Leadership, Kounicova 65, 662 10 Brno, Czech Republic
[c] Tomas Bata University of Zlin, Faculty of Applied Informatics, Nad Stranemi 4511, 760 05 Zlin, Czech Republic
[d] RINA Consulting S.p.A., Via Santa Valeria 5, 20123 Milano, Italy
[e] University of Zilina, Faculty of Security Engineering, 1. maja 32, 010 26 Zilina, Slovakia

ARTICLE INFO

Keywords:
Critical entities
Resilience assessment
Resilience factors
Small-scale disasters
CERA support tool

ABSTRACT

Since 2022, there has been a significant increase in the importance of critical entities in terms of critical infrastructure protection. The adoption of the Critical Entities Resilience Directive must in EU member states ensure not only the protection of critical infrastructure, but also a sufficient resilience level of the entities themselves. This directive obliges critical entities to take measures to increase their resilience but does not provide any methodological support. A necessary starting point for fulfilling this obligation is knowledge of the current state of critical entities resilience to small-scale disasters. The results of the resilience assessment will then enable critical entities to identify vulnerabilities on the basis of which adequate technical, security and organisational measures can be defined. Therefore, this article presents an entirely new semi-quantitative method, CERA, which has been developed for the comprehensive assessment of entity and infrastructure resilience of critical entities. At the core of this method is a procedure that allows critical entities to self-assess their internal resilience through individual factors, which are defined in detail in this article. In order to facilitate the assessment process, the authors of the article have created the CERA Support Tool, which is supplementary material to this article. The Results section of the article also includes a presentation of a practical application example of the proposed procedure.

1. Introduction

As a result of high levels of urbanisation, contemporary society is increasingly dependent on the provision of essential services that are required to maintain the most important societal functions and economic activities, as well as public health and safety, while also taking care of the environment [1]. These essential services are provided through critical infrastructures whose owners or operators are designated as critical entities [1]. These critical entities and their associated infrastructures are constantly exposed to the negative effects of threats [2], that can cause incidents of varying intensity from minor accidents up to more significant small-scale disasters [3]. For this reason, it is necessary to ensure a sufficient resilience level of critical entities that enables these entities and their associated infrastructures not only to prevent the occurrence of small-scale disasters, but also to respond to them, to withstand them, to re-

* Corresponding author.
E-mail address: david.rehak@vsb.cz (D. Rehak).

https://doi.org/10.1016/j.ijdrr.2024.104748
Received 29 May 2024; Received in revised form 7 August 2024; Accepted 8 August 2024
Available online 9 August 2024

cover from them and to adapt to their further possible impact [4]. In this context, it is therefore possible to talk about the transition from the critical infrastructure protection to the critical entities resilience [5].

As a result of this transition, critical entities need to know their current resilience level to small-scale disasters. Several tools and methods can currently be used for this purpose, but these only allow for separate resilience assessments, either technical or organisational. In the context of technical resilience, the most widely used methods are quantitative [6–12], which are highly indicative of the current state of infrastructures, i.e. they mainly provide technical calculations. In addition to these methods, semi-quantitative methods [13–18] that allow easier evaluation through index values are also often used. In contrast, qualitative methods are used only occasionally, e.g. to identify threats and opportunities [19].

In this context, it should be mentioned that some methods in the framework of technical resilience assessment also partially consider the resilience of the organisation, but only of selected processes related exclusively to the infrastructure under assessment [20–22]. Within the framework of organizational resilience, the most used methods are qualitative [23–25] and semi-quantitative [26–32]. In contrast, quantitative methods [33] are rarely used due to differences in the degree to which each factor is fulfilled.

It is clear from the above that as a result of the change in the perception of resilience, i.e. its transition from critical infrastructure to critical entities, there is currently no tool that explicitly addresses the comprehensive assessment of technical and organisational critical entities resilience to small-scale disasters. Based on this fact, the aim of this article is to define the factors determining the entity and infrastructure resilience of critical entities and to develop a semi-quantitative method of self-assessing the critical entities internal resilience to small-scale disasters.

2. Background and methods

The essence of this part of the article is to acquaint the reader with the issue at hand. To this end, first a description of the critical entities and the essential services provided by them is made. Subsequently, attention is paid to small-scale disasters and their impacts on critical entities. In the last part, an analysis of approaches suitable for defining critical entities resilience factors is carried out.

2.1. Critical entities and their essential services

Society, especially in highly urbanised areas, has long been dependent on the provision of essential services. These essential services are provided through critical infrastructure [34], which are classified at the strategic level into technical (essential) and socio-economic [35]. Technical infrastructure provides services necessary for the normal functioning of society, in particular the supply of energy and drinking water, but also ensuring the availability of digital and transport services, amongst others. In contrast, the importance of socio-economic infrastructure rises particularly in times of disasters, when this type of infrastructure primarily ensures the availability of health care which is provided by hospitals, or emergency services which are provided by the fire brigade and the police force.

The owners and operators of these critical infrastructures are referred to as critical entities in all 11 sectors. However, a condition for the designation of an owner or operator as a critical entity is fulfilment of the three criteria set out in the Directive (EU) [1]. These criteria are as follows: 1) the entity provides one or more essential services, 2) the entity operates, and its critical infrastructure is located, on the territory of a Member State of the European Union, and 3) an incident would have significant disruptive effects on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors that depend on that or those essential services.

While the second and third criterion are binary, to assess the first criterion it is necessary to define the essential services for each sector. For this purpose, it is necessary to rely on the definition of an essential service, which is defined by Directive (EU) [1] as *„a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment“*. Determining the criteria for defining essential services in each sector is currently a task for each Member State. An example of the definition of essential services provided in the land transport sector is as follows [36].

- operation of TEN-T infrastructure;
- operation of services related to the transport of passengers and freight within TEN-T;
- operation of intelligent transport systems within TEN-T.

Infrastructure owners and operators that will be designated as critical entities from 2025 onwards are subsequently required to 1) conduct their own risk assessments to identify risks that could disrupt their ability to provide essential services, 2) take technical, security and organisational measures to enhance their resilience, and 3) report significant incidents to national authorities [1].

In the context of this article, it is necessary to pay particular attention to the second point, which obliges critical entities to take measures to increase their resilience. The essence of this obligation is knowledge of the current level of critical entities resilience to small-scale disasters. The results of the resilience assessment will then enable critical entities to identify vulnerabilities on the basis of which adequate technical, security and organisational measures can be determined.

2.2. Small-scale disasters and their impacts on critical entities

Critical entities are constantly exposed to hazards from the external and internal environment throughout their lifetime. These hazards can be generally classified as natural or man-made [3]. These hazards may result in accidents or incidents. A critical infrastructure accident is understood as *„an event that causes changing the critical infrastructure safety state into the safety state worse than the critical safety state that is dangerous for the critical infrastructure itself and its operating environment as well“* [37]. Whereas a critical infrastructure incident means *„an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, in-*

cluding when it affects the national systems that safeguard the rule of law" [1]. Depending on the scale of impacts (i.e. economic, human, and environmental impacts that may include death, injuries, disease and other negative effects on human physical, mental and social well-being) incidents can be further classified as small-scale disasters and large-scale disasters [38].

A small-scale disaster is *„a type of disaster only affecting local communities which require assistance beyond the affected community*" [38]. The impacts of small-scale disasters are mostly of a low to medium nature. For this reason, it is possible to ensure a sufficient resilience level to such events for critical entities. In particular, their preparedness, robustness, recoverability and adaptability [4]. In contrast, a large-scale disaster is *„a type of disaster affecting a society which requires national or international assistance*" [38]. These include major earthquakes, tsunamis and large-scale terrorist attacks. The impact of these disasters or combinations of disasters can be extreme and even catastrophic. Examples include the disaster at the Fukushima nuclear power plant in 2011 or the terrorist attacks of September 11, 2001. Ensuring the critical entities resilience to incidents of this magnitude is very challenging and in the vast majority of cases not even technically feasible. For this reason, the focus in the following text is on critical entities resilience to small-scale disasters.

Similar to hazards, small-scale disasters are also classified as natural or man-made [39]. Natural small-scale disasters are most often the result of gradual climate change, and among the most significant in the context of critical entities are floods, landslides, storms, and wildfires [40]. In contrast, man-made small-scale disasters are the result of intentional and/or unintentional actions, and among the most significant in the context of critical entities are fires, structural collapse of buildings, severe accidents, technological disasters, and terrorist attacks [41].

The impacts of these disasters primarily affect critical entities and their technical infrastructure. As a result of this negative impact, the provision of essential services may be disrupted, which may result in an escalation of cascading impacts not only on the dependents of critical infrastructure, but also on society as a whole, i.e. economic and social activities, the environment, public safety and security in general, or public health [1]. However, these impacts can in turn be mitigated by the critical entities resilience through organisational and technical resilience factors. The relationship between the contexts discussed in this section of the article is presented in Fig. 1.

The defined research framework shows that small-scale disasters significantly disrupt the ability of critical entities to provide essential services. For this reason, critical entities resilience to small-scale disasters is addressed in the following text.

2.3. Analysis of approaches suitable for defining resilience factors of critical entities

The starting point for the analysis of approaches suitable for defining the critical entities resilience factors is an understanding of the phases through which this resilience is determined. This issue has been addressed by a number of authors who have a very similar view of this classification but use quite different terminology [42]. For example, according to Yazdani et al. [43] resilience is characterized by four infrastructure characteristics, i.e., robustness, redundancy, resourcefulness, and speed. Some authors consider the defining components of resilience as its capabilities such as the ability to anticipate, allocate resources to an adverse event, tolerate risks, absorb, preserve the function of an element, adapt and/or recover quickly [44–49]. Collectively, these characteristics can be divided into areas or capacities, i.e. absorption, adaptation and transformation [50]. In doing so, these characteristics should correspond to the underlying capacities, parameters or indicators that, according to Francis and Beker [51], form the resilience triangle, comprising absorptive, adaptive and reinforcing capacities. In contrast, Carlson et al. [52] consider these key parameters to be preparedness, mitigation, response and recovery, which characterise the process of increasing the resilient capacity of a system. Also, four assets, i.e., reliability, redundancy, responsiveness, and recovery, must be in place for the entire resilience system to function [49]. Hromada et al. [53], who consider robustness, preparedness, responsiveness, and recoverability as the basic indicators, also lean towards this idea.

In the following text, the approaches are analysed, on the basis of which specific resilience factors for critical entities will be defined. In the context of the problem addressed, these approaches are analysed on two levels, namely organisational resilience and

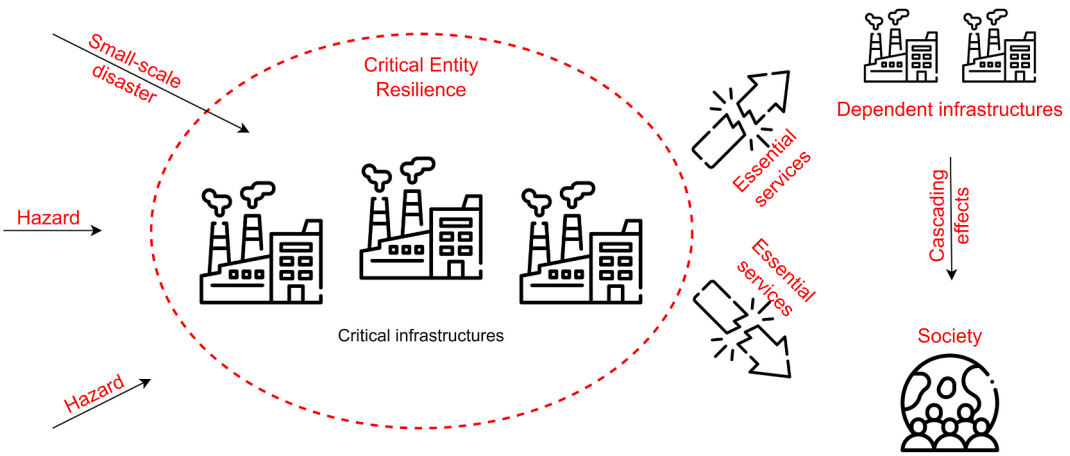


Fig. 1. Impact of small-scale disasters on critical entities, their critical infrastructure and society.

technical resilience. The organisational resilience factors can be broadly divided into structural-organisational, economic, social, legislative, political, human resources, leadership, communication and environmental factors [54]. However, these factors include elements that are much more specific. Factors that are common to all approaches are risk perception and crisis communication [55–58]. These factors are necessarily related to subconscious awareness of incidents, management of key processes, adaptive capacity, system stability or the capacity for reflection and organisational change [59–61]. Necessarily, incident investigation, emergency response reporting, availability of adequate human resources or information management are also linked to these factors [62].

In order to maintain the delivery of essential services, it is also necessary to pay attention to factors such as anticipation, solution development and implementation, reflection and learning [63]; understanding the environment, reference state, acceptance of system failure [64]; functional knowledge, flexibility of reaction, operational awareness, organisational responsiveness, strategic attention or strategic adaptation [65]; interaction and cooperation in learning from failures [66]; participatory planning [67]; employee engagement, innovation and creativity, planning strategies, leveraging knowledge, effective partnerships [68,69].

The factors mentioned so far are assumed to be used more by the critical entity management. Based on current knowledge, it is possible to state the importance of the personnel aspect of increasing the resilience level. This fact was confirmed by the authors of Lengnick-Hall et al. [70], who state that the knowledge, skills and abilities of employees are an important aspect of organizational resilience. The development and management of human resources then becomes a logical prerequisite for the development of organizational resilience. According to Refs. [71–73], creative thinking, flexibility and mindfulness or other soft and interpersonal skills can therefore be considered important. At the same time, it is possible to consider knowledge and experience at all levels of the entity's functioning as an important factor of organizational resilience [74,75]; employee bonuses, cooperation, knowledge development, management culture [76]; social bonds and emotional intelligence [77], psychological resilience [78] and well-being [79,80], social bonds and emotional intelligence [77] can also be considered essential.

In contrast, technical factors focus only on infrastructure, i.e. the ability of infrastructure to prevent or respond adequately to incidents. In this context, the most important factors are those that affect the functionality and performance of infrastructure [7,11]. Such factors may include robustness, adaptability, flexibility, survivability, system performance or infrastructure absorption capacity [9,12]. Other important factors are reliability and security of delivery [81], reparability and resourcefulness [9] or system characteristics of key technologies [13]. Also important from the perspective of infrastructure performance are the resilience threshold, the emergency system characteristics, the identity and function of the systems, the inherent and adaptive response to a disaster, or the degree of self-organisation capability [82,83].

Systems that are directly linked to infrastructure security also contribute to the required technical resilience level. Such factors can be considered as reactivity, detection capability, physical resilience [22], type of security [84], risk impact scenario on the infrastructure under consideration, penalty factors [18], and monitoring or security systems [85]. However, technical capabilities and parameters [18,21] or infrastructure design and maintenance [20] are also very important. Related to these factors is the combination of assets, resources and routine setup [17]. Ensuring redundancy [10,22] or backing up technologies, maintaining backup and contingent system components or storing operational spare parts is also an integral part of the infrastructure [21].

Based on the analysis of the approaches presented above, it can be concluded that the organisational and technical level permeates resilience as a whole, i.e. fundamentally influences the response to incidents, not only after the occurrence of incidents, but also before, during and after [61,86,87]. However, most of the authors mentioned so far understand organisational resilience in a monotonous way, in close connection with the processes of the organisation, especially managerial or purely operational processes, so we cannot talk about a truly comprehensive approach. Such an understanding of organisational resilience is currently not sufficient, even in view of the adoption of the critical entities resilience Directive (EU) [1]. Therefore, it is important to rethink this current approach and to see organisational and technical resilience as one.

3. Results

This part of the article presents the results of the research, which was the work of the author's team. Initially, attention is paid to the classification and definition of factors determining the critical entities resilience. Subsequently, the semi-quantitative CERA method is introduced to self-assess the critical entities resilience to small-scale disasters.

3.1. Classification and definition of factors determining the critical entities resilience

Critical infrastructure resilience has received much attention in the past from many authors (for example [88–99]). However, with the adoption of a new EU Directive [1], this focus needs to be shifted to critical entities. In the context of critical entities, resilience is defined as *„ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident“* [1]. Based on this definition, it is necessary to view the critical entities resilience broadly, i.e. on multiple levels. Resilience perceived in this way can be in terms of individual functions compared to the human brain (see Fig. 2). Just as the human brain is divided into hemispheres and lobes, resilience can also be divided into spheres and components. This comparison must be seen from a functional, not a medical, point of view. In this context, the resilience of critical entities is determined by two spheres, where one sphere is responsible for subject resilience, and the second sphere is responsible for infrastructural resilience. At the same time, in both spheres, the resilience of critical entities is determined by four components (i.e. resistance, robustness, recoverability, adaptability) which cover individual phases of crisis management, i.e. prevention, response, recovery, and adaptation of critical entities to small-scale disasters.

Entity resilience can be defined as the ability of critical entities to anticipate, prepare, respond, recover, and adapt to the occurrence, impact and effects of small-scale disasters, particularly in the area of an organisation's processes and resources. In contrast, in-

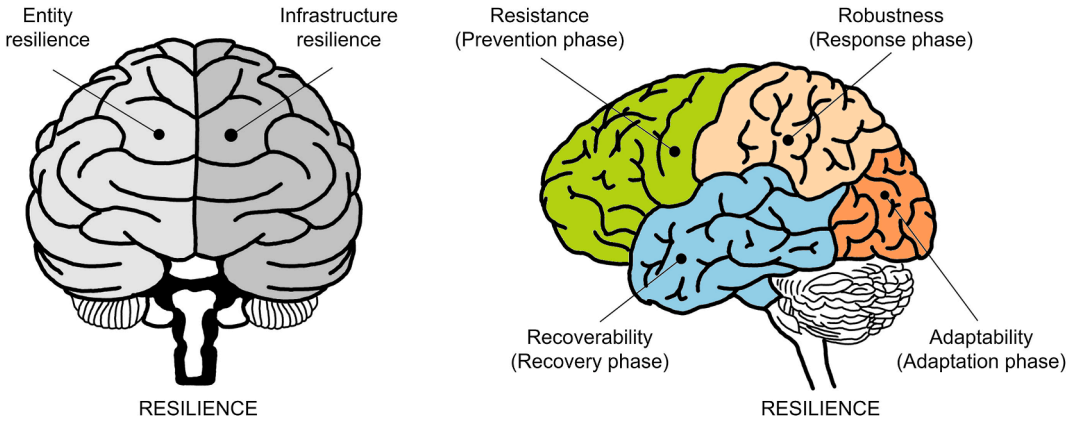


Fig. 2. Perception of critical entities resilience.

frastructure resilience can be defined as the ability of critical entities to monitor, detect, and absorb the impacts of small-scale disasters on their infrastructure, as well as the ability of critical entities to recover from these impacts.

In the following part of the article, attention is paid to defining the factors determining both entity and infrastructure resilience of critical entities. The starting point for this phase of the research was the analysis of approaches suitable for defining critical entities resilience factors, the results of which are presented in the previous section of the article. The results of this analysis show that both entity and infrastructure resilience are determined at a basic level by four fundamental components [4,42].

- resistance, the essence of which is to prevent small-scale disasters;
- robustness, the essence of which is to absorb the impacts of small-scale disasters;
- recoverability, the essence of which is to restore the critical entity function and resilience;
- adaptability, the essence of which is the critical entity adaptation to small-scale disasters that have already occurred.

In a more detailed breakdown, each component was further classified into secondary and tertiary factors, i.e. variables and their parameters. The classification of secondary factors is presented in Fig. 3.

A detailed description of secondary and tertiary factors which, according to the authors, are necessary for assessing the resilience of critical entities to small-scale disasters, is presented in Appendices A-D. The conception of these factors enables the assessment of the critical entities resilience at all three levels of management of the organisation, i.e. strategic, operational, and tactical. On the basis of defining these factors determining the resilience of critical entities, the *CERA Support Tool* was created by the authors of this article, which is presented as supplementary material to this article. A detailed description of the work with this tool is presented in the next part of the article.

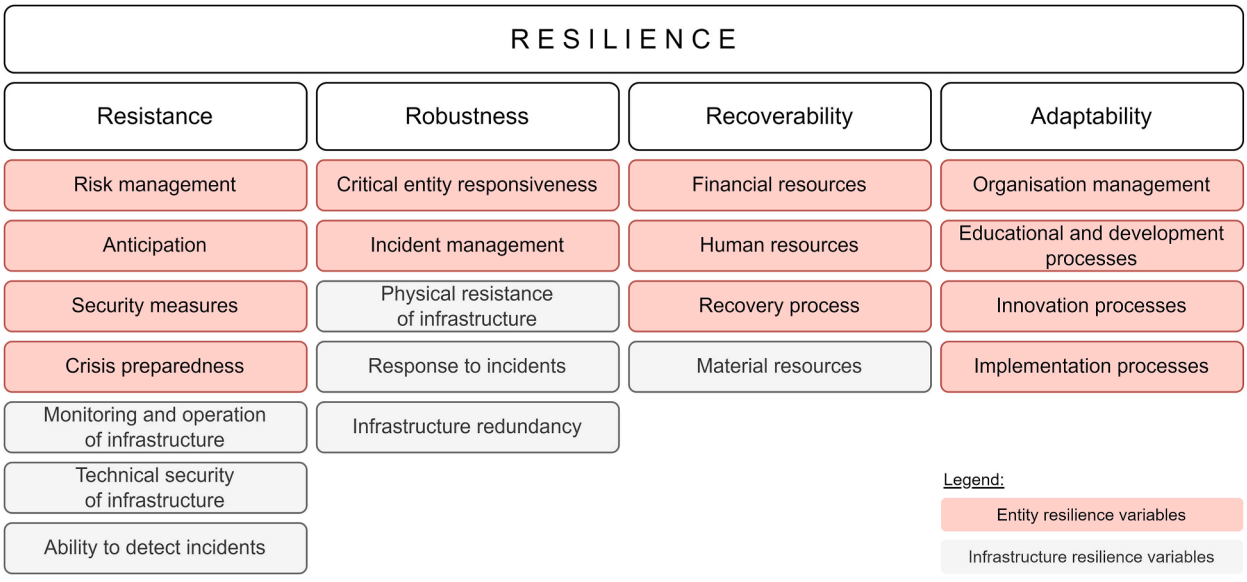


Fig. 3. Classification of components and variables determining the critical entities resilience.

3.2. Semi-quantitative method for critical entities resilience assessment to small-scale disasters

In order for critical entities to be able to take technical, security and organisational measures to increase their resilience in accordance with the Directive (EU) [1], it is necessary to first carry out a resilience assessment for each critical entity and establish the requirements for enhancing resilience. However, the defined research gap shows that there is currently no tool that can be used to comprehensively assess entity and infrastructure resilience. For this reason, the authors of this article developed a semi-quantitative *Critical Entities Resilience Assessment (CERA Method)*.

The CERA Method is intended exclusively for assessing the internal resilience of critical entities, for this reason it does not take into account external factors affecting resilience. At the core of this method is a procedure that is designed to self-assess the critical entities resilience to small-scale disasters. The basis of which is a semi-quantitative assessment of resilience factors that have been defined for each resilience component, i.e., resilience, robustness, recoverability, and adaptability. The procedure for assessing the critical entities resilience to small-scale disasters, including the recommended methodology, is presented in Fig. 4.

In the following part of the text, a detailed description of the individual steps of the process of assessing the critical entities resilience to small-scale disasters is made. This description is presented in the form of a case study of a terrorist attack on an electricity substation. In this context, it is important to emphasize that the critical entities resilience assessment must always be carried out only for one critical entity infrastructure against one specific small-scale disaster.

Step 1: Selection and analysis of the specific infrastructure

The essence of this step is the selection of the specific infrastructure that is operated by the critical entity. The selection of this infrastructure should be carried out using a Multi-Criteria Analysis [100] or a Functional Analysis [101]. The selected infrastructure must then be analysed for structural and topological parameters. The essence of the structural analysis is the categorisation of the infrastructure by type (i.e. classification into the relevant sector and sub-sector) and performance and the identification of key infrastructure technologies. The essence of topological analysis is the categorisation of infrastructure according to its topological structure, i.e. linear, point, areal [102,103]. An example of the analysis of the selected infrastructure is presented in Fig. 5.

Step 2: Hazard selection and small-scale disaster scenario processing

Once a specific infrastructure is selected by the critical entity, it is necessary to proceed to a risk analysis, based on which a specific high-risk hazard with the potential to cause a small-scale disaster will be selected. A risk analysis should be carried out using one of the recommended methods [104]. Based on the selection of a specific hazard, it is possible to proceed to the elaboration of a scenario of the small-scale disaster expected course, i.e. the effect of the selected hazard on the selected infrastructure. For this purpose, the Event Tree Analysis method [105] can be chosen, which allows the analysis of events and consequences leading to a small-scale disaster. An example of scenario processing for a selected man-made small-scale disaster is presented in Fig. 6.

Step 3: Identification of parameters and assessment of their level

The essence of this step is to identify the measurable items and assess the level of their fulfilment by the critical entity for all four components of resilience. For this purpose, it is appropriate to use the CERA Support Tool (see Fig. 7), which was created by the authors of the article based on the results of defining and classifying factors determining the critical entities resilience. Identification of parameters consists of selecting those measurable items that the evaluator considers adequate for the assessment, i.e. the activities/

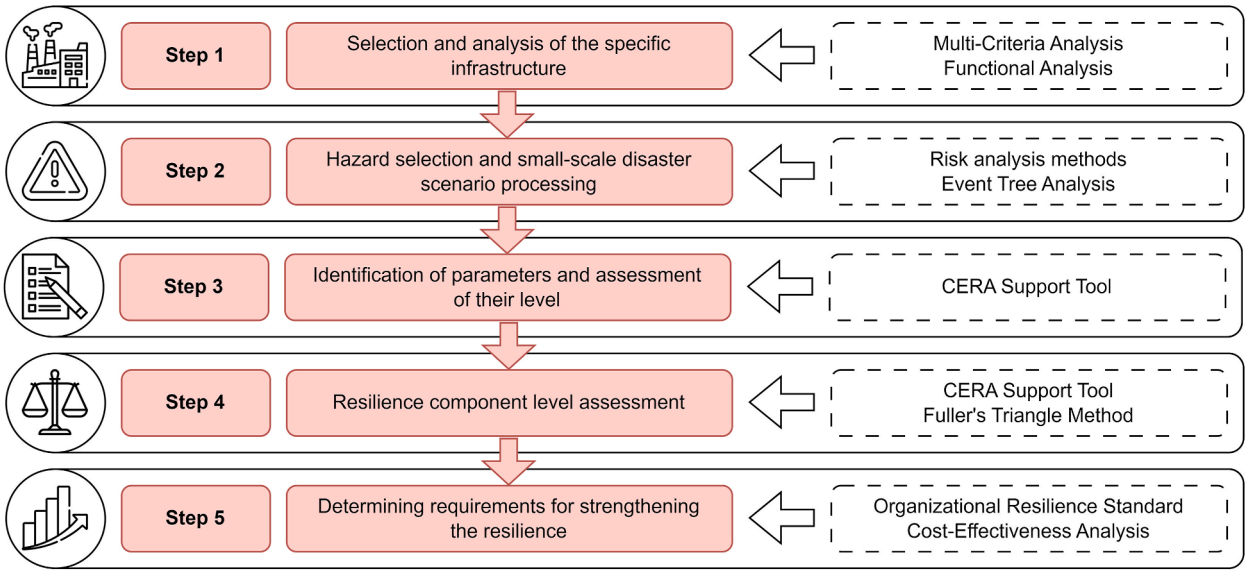


Fig. 4. Process for assessing the critical entities resilience to small-scale disasters.

Infrastructure name	Transmission system electrical station
Sector / Subsector	Energy / Electricity - Transmission
Key technologies	1. Transformers 2. Voltage instrument transformers 3. Current instrument transformers 4. Compensation chokes 5. Disconnectors and grounding switches 6. Busbars and branches 7. Circuit breakers
Performance	400/220 kV
Topological structure	Areal arrangement of infrastructure

Fig. 5. Example of selected infrastructure analysis.

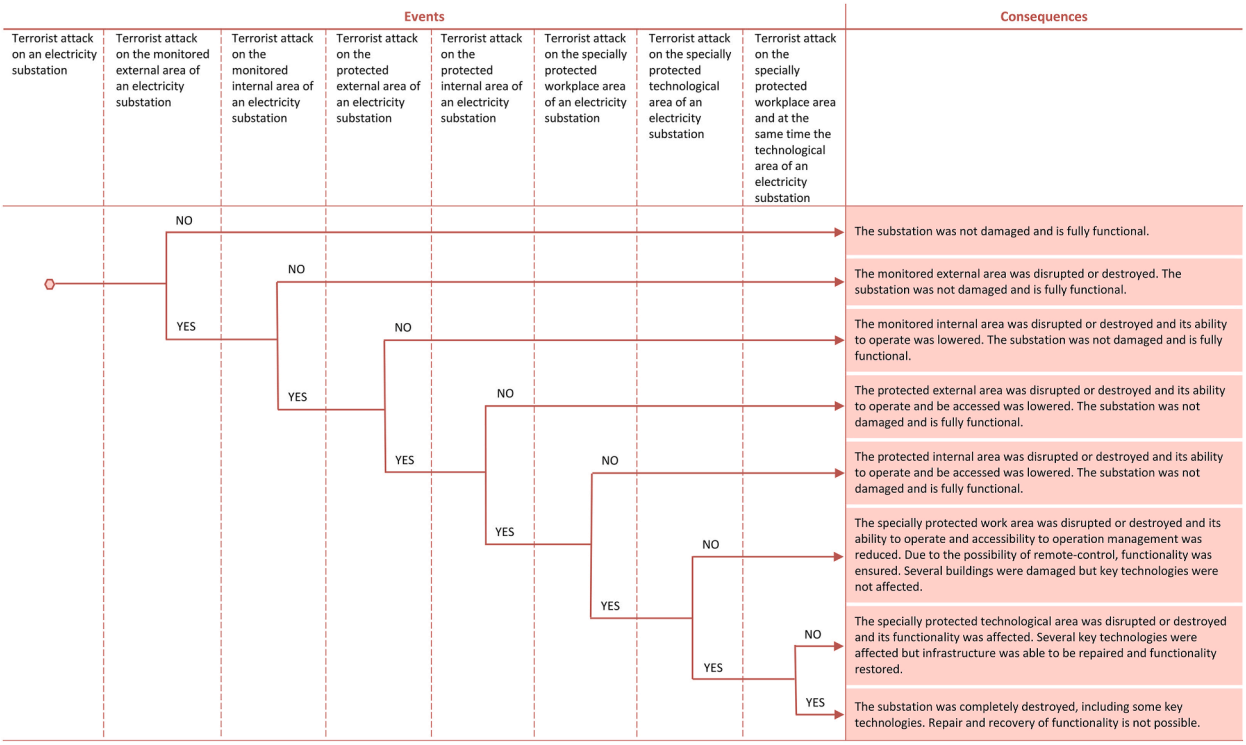


Fig. 6. Example of scenario processing for a selected small-scale disaster.

measures are implemented by the critical entity. For these parameters, the answer YES is selected in the column Identification of factors. Parameters that have not been identified by the evaluator are selected as NO and receive a value of zero in the level assessment.

For the parameters where a YES answer has been selected, it is then necessary to assess at what level the critical entity meets the activities/measures defined by these parameters. This level is expressed as a score from 1 to 5, where the points assigned have the following significance.

- 1: The critical entity does not meet any activities/measures defined by the parameter.
- 2: The critical entity meets only the minimum range of activities/measures defined by the parameter (approximately 25%).
- 3: The critical entity meets the activities/measures defined by the parameter only partially (about 50%).
- 4: The critical entity meets most of the activities/measures defined by the parameter (approximately 75%).
- 5: The critical entity fully meets the activities/measures defined by the parameter.

The identification of parameters and the assessment of their level should be primarily carried out by the security liaison officer in cooperation with the responsible managers of the infrastructure and processes concerned. However, the assessment process should

RESISTANCE
of the critical entity

CERA Support Tool

Resilience spheres	Variables	Parameters	Identification [YES/NO]	Level assessment [1-5]
Entity resilience	Risk management	Risk management level	Yes	5
		Risk assessment methodology	Yes	5
		Implementation of safety and security standards	Yes	3
		Incident modelling	Yes	2
	Anticipation	Preventive check	Yes	4
		Indicating disruption of critical entity resilience	No	
	Security measures	Physical protection	Yes	4
		Regime measures	Yes	4
	Crisis preparedness	Responsibilities, obligations, and powers	Yes	5
		Staff education and training	Yes	5
		Security planning and documentation	Yes	3
		Continuity planning	Yes	2
Infrastructure resilience	Monitoring and operation of infrastructure	Technical condition of infrastructure	Yes	5
		Maintenance, servicing, and testing of equipment	Yes	5
	Technical security of infrastructure	Mechanical barriers	Yes	4
		Electronic surveillance and alarm devices	Yes	5
		Cyber security	Yes	4
	Ability to detect incidents	Monitoring of surroundings	Yes	5
		Incident detection	Yes	4
Resistance level				**79%**

Fig. 7. Example of identifying parameters and assessing their level determining the critical entities resistance.

also involve external actors who depend on the delivery of essential services from the critical entity. In this way, the subjectivity of the assessment will be partially counteracted. At the same time, it should be noted that the use of such approaches in management is not uncommon [106]. This way of assessment allows this subjectivity to be transparently gathered in one place and acknowledged.

Step 4: Resilience component level assessment

Following the identification of the parameters and the assessment of their level, it is possible to proceed to the assessment of the level of the individual components. To this end, weighting coefficients have been established for each parameter (see Tables 1–4). These weighting coefficients reflect not only the significance of the parameters but also the variables that are determined by these parameters. The determination of the weighting coefficients was carried out in two phases using multi-criteria assessment methods, namely Metfessel's allocation [107] and Fuller's triangle [108]. In the first stage, 100 points were distributed among the variables within each component. In the second phase, the allocated points were further divided between individual parameters. The distribu-

Table 1
Weighting coefficients of parameters determining the critical entities resistance.

Variables	1st phase	Parameters	2nd phase	Weighting coefficients
Risk management	19	Risk management level	5	0.05
		Risk assessment methodology	5	0.05
		Implementation of safety and security standards	4	0.04
		Incident modelling	5	0.05
Anticipation	10	Preventive check	6	0.06
		Indicating disruption of critical entity resilience	4	0.04
Security measures	11	Physical protection	6	0.06
		Regime measures	5	0.05
Crisis preparedness	18	Responsibilities, obligations, and powers	4	0.04
		Staff education and training	4	0.04
		Security planning and documentation	5	0.05
		Continuity planning	5	0.05
Monitoring and operation of infrastructure	10	Technical condition of infrastructure	6	0.06
		Maintenance, servicing, and testing of equipment	4	0.04
Technical security of infrastructure	17	Mechanical barriers	6	0.06
		Electronic surveillance and alarm devices	6	0.06
			5	0.05
Ability to detect incidents	15	Monitoring of surroundings	7	0.07
		Incident detection	8	0.08
∑	**100**		**100**	**1.00**

Table 2
Weighting coefficients of parameters determining the critical entities robustness.

Variables	1st phase	Parameters	2nd phase	Weighting coefficients
Critical entity responsiveness	17	Time interval for activation of protective measures	9	0.09
		Status of forces and assets	8	0.08
Incident management	12	Crisis management preparedness	6	0.06
		Communication and sharing of information	6	0.06
Physical resistance of infrastructure	24	Fire resistance	8	0.08
		Seismic resistance	8	0.08
		Explosive resistance	8	0.08
Response to incidents	23	Incident mitigation	11	0.11
		Maintaining the functionality of key technologies	12	0.12
Infrastructure redundancy	24	Reliability criterion	7	0.07
		Redundant capacity availability	9	0.09
		Temporary substitution of key technologies	8	0.08
∑	**100**		**100**	**1.00**

Table 3
Weighting coefficients of parameters determining the critical entities recoverability.

Variables	1st phase	Parameters	2nd phase	Weighting coefficients
Financial resources	22	Allocation of financial resources for recovery	12	0.12
		Availability of financial resources on time	10	0.10
Human resources	26	Human resources capacity	9	0.09
		Human resources expertise	9	0.09
		Availability of human resources in time	8	0.08
Recovery process	17	Disaster preparedness recovery processes	9	0.09
		Restoring infrastructure function	8	0.08
Material resources	35	Ability to recover infrastructure functions	8	0.08
		Repairability of key infrastructure technologies	10	0.10
		Substitutability of key infrastructure technologies	9	0.09
		Availability of spare parts and repairs on time	8	0.08
∑	**100**		**100**	**1.00**

Table 4
Weighting coefficients of parameters determining the critical entities adaptability.

Variables	1st phase	Parameters	2nd phase	Weighting coefficients
Organisation management	18	Analysis of organisational processes	8	0.08
		Management of organisational processes	10	0.10
Educational and development processes	32	Extent of vocational training	8	0.08
		Quality of vocational training	8	0.08
		Incident management training	10	0.10
		Evaluation of training effectiveness	6	0.06
Innovation processes	21	Management process innovation	6	0.06
		Innovation of measures and technologies	8	0.08
		Investing in innovation	7	0.07
Implementation processes	29	Implementation of new processes	7	0.07
		Implementation of management systems	7	0.07
		Software implementation	7	0.07
		Implementation of security measures	8	0.08
∑	**100**		**100**	**1.00**

tion of points in both phases was implemented using Fuller's triangle and the resulting values were subsequently consulted with interested parties, i.e. selected critical entities.

The assessment of the critical entities resilience level through the individual components is then calculated by a weighted average of the individual parameters (Formula 1).

$$C_i = 20 \sum_{j=1}^{k} P_j w_j \tag{1}$$

where C_i = i-th component of critical entity resilience [%]; P_j = j-th measurable item of critical entity resilience [score]; w_j = j-th weighting coefficient of the j-th measurable item of critical entity resilience in the interval ⟨0;1⟩; k = total number of parameters in the i-th component.

At the end of the assessment, it is necessary to assess the achieved levels of each component. These resulting levels need to be scaled into one of five categories that reflect the levels of resilience acceptability. The division of these levels is philosophically based

on the FMECA method [109], which uses a five-point scale to determine the level of risk. By varying the extreme values of this scale (i.e., the largest and smallest values of the set, i.e., 1 and 5 points), categories of acceptability levels of resilience components are established see Fig. 8).

For components that have been categorised as low, inadequate or critical, it is necessary to retrospectively analyse their parameters and establish resilience-building requirements.

Step 5: Determining requirements for strengthening the resilience

After selecting a component with a low, insufficient, or critical resilience level, it is necessary to proceed to the determination of requirements for strengthening the resilience of the parameters determining this component. The requirements for strengthening the resilience of the parameters are derived from the results of the assessment of their current state and are defined in the context of the Organisational Resilience Standard [110].

- for measurable parameters with a value of 1 or 2, resilience strengthening through appropriate tools is required. These tools will be defined as part of the follow-up research of this author team.
- for parameters with a value of 3 or 4, it is appropriate to strengthen resilience through appropriate tools, but based on the results of a Cost-Effectiveness Analysis [111].
- for parameters with a value of 5, there is currently no need to strengthen their resilience.

The fifth step completes the process of assessing the critical entities resilience to small-scale disasters. It is appropriate to repeat this process if the resilience of some parameters have been strengthened or the time period requiring a cyclical resilience assessment, i.e. one year, has elapsed.

4. Conclusion

With the adoption of the Critical Entities Resilience Directive, a fundamental change in the perception of resilience in the critical infrastructure system is taking place in the European Union. The existing approach based on the protection of critical infrastructure is thus replaced by a new approach based on the critical entities resilience who are the owners or operators of this infrastructure. This Directive obliges critical entities to take measures to increase their resilience but does not provide any methodological support. In this context, however, it should be noted that a necessary starting point for fulfilling this obligation is knowledge of the current state of critical entities resilience to small-scale disasters. The results of the resilience assessment will enable critical entities to identify vulnerabilities on the basis of which adequate technical, security, and organisational measures can be defined. For this purpose, the authors of this article created the CERA (Critical Entities Resilience Assessment) method.

The essence of the CERA method is a comprehensive assessment of the entity and infrastructure resilience of critical entities. At the core of this method is a procedure that allows critical entities to semi-quantitatively self-assess their internal resilience through the individual factors that determine this resilience. The classification and definition of these factors is part of the CERA method. In order to facilitate their application in the evaluation process, the authors of this article created the CERA Support Tool, which is supplementary material to this article. A presentation of an example of a practical application of the proposed procedure is included in the Results section of the article.

The CERA method is primarily designed to assess the internal resilience of critical entities providing essential services in technically oriented sectors. However, with some modification, it could also be used to assess the resilience of critical entities providing essential services in socio-economically oriented sectors. The resilience assessment process should be carried out primarily by the security liaison officer of the assessed critical entity in cooperation with the responsible managers of the affected infrastructures and processes. However, the assessment process should also involve external actors who depend on the delivery of essential services from the critical entity. In this way, the subjectivity of the assessment will be partially counteracted.

Finally, it should be noted that follow-up research should focus on identifying and analysing tools suitable for resilience building at the level of individual factors. These tools should focus on both entity and infrastructure resilience. In the area of entity resilience,

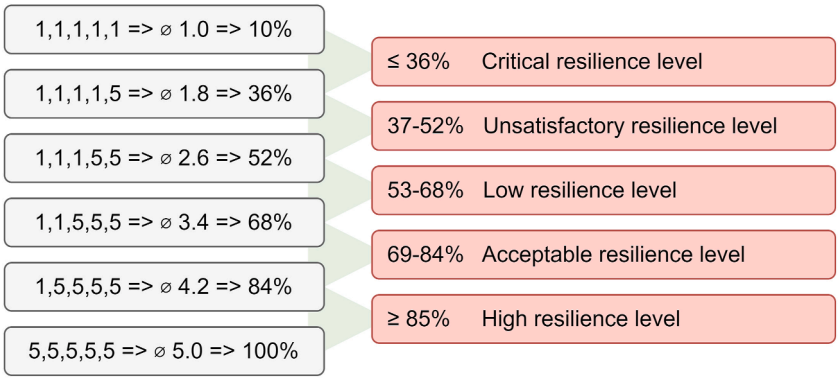


Fig. 8. Categories of acceptability levels of resilience components.

particular attention should be paid to the processes and resources of the organisation. In contrast, in the area of infrastructure resilience, attention should be paid in particular to technical and security measures.

Funding

This work was supported by the Ministry of the Interior of the Czech Republic [grant number VK01030014] and by the VSB – Technical University in Ostrava [grant number SP2024/039].

CRediT authorship contribution statement

David Rehak: Writing – review & editing, Writing – original draft, Visualization, Supervision, Software, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Alena Splichalova:** Writing – review & editing, Writing – original draft, Software, Resources, Methodology, Formal analysis, Conceptualization. **Heidi Janeckova:** Writing – review & editing, Writing – original draft, Resources, Formal analysis, Data curation. **Alena Oulehlova:** Writing – review & editing, Writing – original draft, Validation, Resources, Formal analysis, Data curation. **Martin Hromada:** Writing – review & editing, Writing – original draft, Validation, Software, Investigation, Conceptualization. **Miltiadis Kontogeorgos:** Writing – review & editing, Writing – original draft, Validation, Software, Formal analysis, Data curation. **Jozef Ristvej:** Writing – review & editing, Writing – original draft, Validation, Resources, Investigation, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: David Rehak reports financial support was provided by the Ministry of the Interior of the Czech Republic. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Appendix A. Factors determining the critical entities resistance

Variables and their parameters determining the critical entities resistance are presented in Table A.1.

Table A.1
Factors determining the critical entities resistance

Resilience spheres	Variable	Variable description	Parameters
Entity resilience	Risk management	A set of processes for early risk assessment and management, including the specification of incident scenarios.	Risk management level Risk assessment methodology Implementation of safety and security standards Incident modelling
	Anticipation	A set of organisational measures and procedures for predicting the occurrence of an incident due to exposure to a hazard.	Preventive check Indicating disruption of critical entity resilience
	Security measures	A set of organisational and regime measures for monitoring and physical/cyber protection of infrastructure.	Physical protection Regime measures
	Crisis preparedness	A set of analytical-planning documents to increase the preparedness of a critical entity for incidents and the fulfilment of connected security measures.	Responsibilities, obligations, and powers Staff education and training Security planning and documentation Continuity planning
Infrastructure resilience	Monitoring and operation of infrastructure	A set of technical measures for monitoring the technical condition of equipment, its maintenance, servicing and testing.	Technical condition of infrastructure Maintenance, servicing, and testing of equipment
	Technical security of infrastructure	A set of technical measures for monitoring and physical/cyber protection of infrastructure.	Mechanical barriers Electronic surveillance and alarm devices Cyber security
	Ability to detect incidents	A set of technical measures for infrastructure monitoring for early fault detection and incident detection.	Monitoring of surroundings Incident detection

Risk management level consists of assessing the level of risk management activities coordination in order to increase the organisation resilience [112]. Attention is paid in particular to the level of implementation and execution of risk management strategy, risk analysis, risk management, risk monitoring and risk management optimization.

Risk assessment methodology consists of assessing the level of applied risk assessment methodology [104]. As there are a number of methodologies that allow risk analysis to be undertaken with different objectives, the assessment of the methodology is largely based on the primary objective of the analysis (for the purposes of this assessment), i.e. assessing the extent to which the methodology used allows an understanding of the risks leading to a significant reduction or interruption in the service provision of the asset.

The implementation of safety standards consists of assessing the level of implementation of safety standards in the organisation. Focal areas include risk management [113], information security [114] and health and safety [115]. In addition to the core safety standards, standards from other specific safety-oriented areas can also be implemented, e.g. machinery safety [116].

Incident modelling consists of assessing the level of incident scenarios processing for identified risks. These scenarios can be developed at either a basic or detailed level. The essence of the basic level of scenario development is a qualitative or semi-quantitative assessment of the incident development. These scenarios are developed using simpler methods [117] and intended, for example, as input to further analyses or as a basis for understanding the problem. The essence of the detailed level of scenarios developed is a multivariate quantitative assessment of the likelihood and severity of the incident impact. These scenarios are developed using more sophisticated assessment methods, are based on quantitative data and are back-tested. Currently, digital twins are increasingly being used for this purpose [118].

Preventive checks should be implemented by critical entity managers at all levels of management. The essence of preventive checks is to obtain feedback on the current state of infrastructure, production and safety processes and the knowledge and skills of employees [119].

Indication of critical entity resilience disruption involves the use of methods and tools aimed at predictive indication of potential disruption of entity and infrastructure resilience [120,121].

Physical protection is the set of security services performed by security personnel to protect the infrastructure [122]. *Regime measures* is possible to divide into physical and cyber. In the field of physical protection, it is set of security measures that mainly secure the entry and exit to the infrastructure area, as well as the movement of people and assets within these areas [123]. In the field of cyber protection, it is a set of security measures for the systematic protection of electronic or printed data of a critical entity, e.g. information security management systems [114].

Responsibilities, obligations and powers consist of an assessment of the extent to which responsibilities, duties, authorities and roles are defined when dealing with incidents and crisis situations [124].

Staff training and education consists of assessing the extent of training, the level of training and maintaining the practical skills of staff to deal with incidents and crisis situations. To this end, occupational health and safety, fire protection, information technology and, for technical staff, practical incident and crisis management training should be implemented by the critical entity management [124].

Security planning and documentation consists of assessing the level of preparation of security documentation, in particular the emergency plan and crisis preparedness plan of the critical entity [125].

Continuity planning involves assessing the ability of the organisation to continue to provide essential services, within an acceptable timeframe and at a predefined volume, during an incident. It is primarily concerned with setting continuity policy, establishing continuity objectives at relevant functions and levels, planning, implementing and managing processes to provide essential services, or establishing guidelines and information for responding to an incident [126].

Technical condition of infrastructure consists of an assessment of the ability of the equipment to operate safely in terms of its technical condition [116]. This includes, in particular, verifying the current technical condition of the equipment according to the accompanying documentation or the local operating safety regulations, whether the equipment is still capable of fulfilling its purpose and whether its condition or operation endangers the safety of work and operational activities.

Maintenance, servicing and testing of equipment consists of carrying out checks on the technical condition of the infrastructure, its function and the services provided [127]. Based on the results of the technical inspection of the equipment, the required maintenance and servicing should be carried out. It is also advisable to test the equipment by means of regular functional and stress tests.

Mechanical barriers include in particular fencing (i.e. protection of the perimeter of the element), grilles, roller shutters or locks (i.e. protection of the shell of the element) to such an extent and with such technical parameters as to form a system of barriers which, by their design and mechanical resistance, will meet the safety functions specified by the technical standards [128].

Electronic surveillance and alarm devices include in particular CCTV and access control systems, electrical fire alarms, alarm and emergency systems, equipment for the detection of hazardous gases and vapours, equipment to limit the extent of leakage of hazardous substances, special technical measures against unauthorized manipulation or a system for rapid shutdown of the facility or equipment to such an extent as to provide protection of persons and infrastructure to enable timely and effective intervention in the disrupted facility or equipment (for example [129]).

Cyber security is a set of measures to protect the computer systems and networks of a critical entity from unauthorized access and from cybercrime, i.e. disruption, theft or misuse of the services provided or damage to hardware, software or electronic data [130].

Monitoring of surroundings is a set of methods, measurements, and tools (active/passive monitoring), including visual monitoring, which identifies the current state of events in the vicinity of individual infrastructures, i.e. determining the status of their systems, processes, and activities [131]. They also ensure the systematic collection of information over time to prevent incidents, pro-

vide a general overview and produce statistics on the current state of individual infrastructures and their surroundings/environment.

Incident detection involves a set of technical measures and tools for early detection of an impending incident (for example [132]). These include sensors, detectors, alarms, software tools, warning systems, but also suitable tools for the analysis of undesirable conditions.

Appendix B. Factors determining the critical entities robustness

Table B.1 and the following text present the variables and parameters determining the critical entities robustness.

Table B.1
Factors determining the critical entities robustness

Resilience spheres	Variable	Description of variable	Parameters
Entity resilience	Critical entity responsiveness	A set of organisational measures and procedures for reporting and managing incidents.	Time interval for activation of protective measures Status of forces and assets
	Incident management	A set of crisis management competencies and skills and methods of communication and information sharing during incident management.	Crisis management preparedness Communication and sharing of information
Infrastructure resilience	Physical resistance of infrastructure	The ability of infrastructure to withstand the negative effects of natural, anthropogenic and technogenic hazards through the material and structural resistance of these constructions.	Fire resistance Seismic resistance Explosive resistance
	Response to incidents	The ability of the facility to prevent the spread of the effects of incidents and ensure the repairability of key technologies.	Incident mitigation Maintaining the functionality of key technologies
	Infrastructure redundancy	The ability to immediately substitute the performance of a disrupted part of the infrastructure or to reinforce its capacity.	Reliability criterion Redundant capacity availability Temporary substitution of key technologies

The time interval for activation of protective measures is used to assess the system response time for activation of key (primary) protective measures to ensure that losses are minimized when an incident occurs [22].

The status of forces and assets consists of an assessment of the availability of forces and assets available to the critical entity to minimize the impact of the incident [22]. Forces and assets are required to interrupt the causes and address the impacts of an incident in the production process.

Crisis management preparedness is used to assess the level of capability and skills of the critical entity's crisis management to deal with incidents and crisis situations [133].

Communication and Sharing of Information is used to assess the procedures, methods, and methods/channels for exchanging information between internal and external stakeholders during an incident, through voice and data transmission of information over public and non-public telecommunications networks [134]. In crisis communication, the key is whether people's perceptions match the reality of the situation and their ability to assimilate information during the incident.

Fire resistance is pragmatically assessed in the context of the ability of building structures to withstand the effects of fire, provided that the load-bearing capacity, stability, integrity, and insulating capacity of the building structure are not impaired [135].

Seismic resistance of the building structure is then based on the ability to withstand the effects of an earthquake, and this due to sufficient tensile strength and ductility [136].

Explosive resistance of the building structure is subsequently expressed by the ability of the structure to resist the effects of the explosion through active or passive protection against explosion [137].

Incident mitigation is the assessment of the ability of technology to prevent the spread of the consequences of an incident. In the case of critical infrastructures, this includes, for example, automatic firefighting systems or automatic incident detection for bridges and tunnels [138].

Maintaining the functionality of key technologies involves assessing the possibility of implementing repairs to key technologies during an incident or crisis situation, e.g. through Public-Private Partnerships [139].

The reliability criterion consists of assessing whether the element meets the so-called reliability criterion. The higher the criterion, the higher the safety can be expected. A system with N elements meeting the N-1 criterion is then able to operate without any disruption of function when any one element of the system (of this N-value) is disabled, i.e. with any combination of N-1 elements [140].

Redundant capacity availability consists of an assessment of the sufficiency of the capacity and speed of backup systems and measures to ensure the required performance/capacity of the infrastructure [141]. The basic ways to increase reliability include increasing the faultlessness of systems by selecting the lowest possible serial reliability model, backing up key technologies, fuses, etc.

Temporary substitution of key technologies consists of assessing the possibility of immediate substitution of key technologies without disrupting the performance of the infrastructure, e.g. by redirecting production to a backup system [142].

Appendix C. Factors determining the critical entities recoverability

The variables and parameters determining the critical entities recoverability are presented in Table C.1.

Table C.1
Factors determining the critical entities recoverability

Resilience spheres	Variable	Variable description	Parameters
Entity resilience	Financial resources	Availability of financial resources or reserves to finance rapid infrastructure recovery.	Allocation of financial resources for recovery Availability of financial resources on time
	Human resources	Availability of human resources with the necessary qualifications.	Human resources capacity Human resources expertise Availability of human resources in time
	Recovery process	Processes that support rapid recovery of required infrastructure performance.	Disaster preparedness recovery processes Restoring infrastructure function
Infrastructure resilience	Material resources	Availability of the necessary components to repair or replace damaged or destroyed parts of the infrastructure.	Ability to recover infrastructure functions Repairability of key infrastructure technologies Substitutability of key infrastructure technologies Availability of spare parts and repairs on time

The allocation of financial resources for recovery consists of an assessment of the level and sources of funds allocated to the rapid restoration of the required performance of the infrastructure [143]. Closely related to the allocation of financial resources is the timeliness of financial resources, which is an assessment of how quickly and in what way financial resources are allocated to restore infrastructure performance. Financial resources may or may not be earmarked and/or accumulated for a given (calendar) year in advance on an ongoing basis (voluntary or statutory, etc.) (if not used, the funds are returned).

Human resource capacity consists of an assessment of the personnel amount that can be allocated to infrastructure renewal and an assessment of their dislocation within the infrastructure [144]. Also related to human resource capacity is *human resource expertise*, which is an assessment of the personnel qualifications in relation to infrastructure performance recovery requirements, and human resource time availability, which is an assessment of the timeliness of the availability of the required personnel.

Disaster preparedness recovery processes consists of assessing the level of processes that control or deal with material resources, financial resources/reserves and human resources. It is an assessment of the process of securing these resources for the recovery of infrastructure functions from the perspective of emergency preparedness and preparation for the recurrence of small-scale disasters [145].

Restoring infrastructure function consists of assessing the level of planning and recovery of infrastructure function due to small-scale disasters [146]. This is the time and progress of infrastructure performance recovery after the incident has ended. The shorter the recovery time and the faster the performance increase, the faster the infrastructure performance is restored to the desired level.

Ability to recover infrastructure functions is an assessment of the level of infrastructure function recovery without the need for major repairs. In particular, it involves restoring settings or resetting electronic parts of the system. If infrastructure function recovery is not possible, it is necessary to have information on the repairability of key infrastructure technologies, which consists of an assessment of whether a repair of a key infrastructure technology can be performed and what level of performance can be achieved after the repair [147].

Substitutability of key infrastructure technologies consists in assessing whether each key infrastructure technology or part of it can be replaced [148]. That is, whether it already exists on the market or can be manufactured and whether a replacement or spare part to repair it can be installed at all (in particular, if there are any physical barriers to installation). Replacement means removing the damaged part or the whole technology and replacing it with a part with an identical function. Capacity is in the sense of the (maximum) value for which the infrastructure is included in the critical infrastructure system (e.g. transport capacity or road capacity or maximum flow of a distribution pipeline). *The availability of spare parts and repairs on time* is an assessment of how quickly damaged key technology can be repaired or replaced and infrastructure performance restored to the desired level [149]. It is also necessary to assess the speed of delivery of spare parts or technology components, as well as specialised instruments, tools and installation aids.

Appendix D. Factors determining the critical entities adaptability

Variables and parameters determining the critical entities adaptability are presented in Table D.1.

Table D.1
Factors determining the critical entities adaptability

Resilience spheres	Variable	Variable description	Parameters
Entity resilience	Organisation management	Processes related mainly to setting up the entire management system, values, and rules of the organisation, setting up the organisational structure, managing resources, processes, and performance.	Analysis of organisational processes Management of organisational processes
	Educational and development processes	Processes that support the knowledge, skills, and attitudes of critical infrastructure entity employees.	Extent of vocational training Quality of vocational training Incident management training Evaluation of training effectiveness
	Innovation processes	Processes that support invention, science and research and the implementation of safety measures.	Management process innovation Innovation of measures and technologies Investing in innovation
	Implementation processes	Processes of preparing the introduction of theoretically planned ideas, projects, processes, systems, or solutions for further use.	Implementation of new processes Implementation of management systems Software implementation Implementation of security measures
Infrastructure resilience	In the infrastructure resilience sphere, no factors determining the adaptability of critical entities have been defined.		

The analysis of organisational processes consists of assessing the flexibility of the critical entity's organisational structure [150]. Modern forms of organisational structure make companies more adaptable and able to meet the expectations of internal and external customers. Following the analysis of organisational processes, it is also necessary to analyse the *management of organisational processes*, which consists in assessing the way organizational processes are managed. Each organisation or part of it is managed in a certain way which can be assessed [151].

Extent of vocational training consists of an assessment of the extent of training within the critical entity to enable the acquisition of specific expertise necessary for the reactiveness and restoration of infrastructure function. The assessment focuses primarily on the number of personnel trained and the target group, i.e. for whom the training is intended [152]. In the context of the extent of vocational training, it is also necessary to assess its quality. *The quality of vocational training* consists of an assessment of the level of training that is provided or facilitated to the critical entity's workforce.

Incident management training consists of assessing the level of training and maintaining the practical skills of the organisation's personnel to deal with small-scale disasters [153]. Also very closely related to incident response training is the assessment of training effectiveness, which consists of assessing how the effectiveness of training critical entity personnel is evaluated.

Management process innovation consists of assessing the level of management process innovation in a critical entity. Innovations can be implemented at different time points, resulting in two ways of implementation. The first way is Business Process Reengineering, which assumes that a one-time change is necessary to "straighten out" processes that will cause a dramatic change in performance in the organisation [154]. This is a radical intervention in the structure of the process and should bring immediate change. The second approach is Business Process Improvement, which assumes that a one-time change in the organization is not only ineffective but also insufficient and even harmful. Therefore, it seeks only gradual business process change that is more acceptable to the organisation [155].

Innovation of measures and technologies consists of assessing the extent of measures implementation and technological innovations [156], which may focus, for example, on product innovation (which focuses on the creation or modification of the services provided), technology innovation (i.e. the equipment that creates the products) or process innovation (i.e. the ways in which the products are created).

Investing in innovation involves assessing the investment level by the critical entity in particular innovations (i.e., management processes, technologies, and safety measures) and research and development [157]. A key indicator is not only the amount of these resources, but also their adequacy, effectiveness and timeliness of expenditure.

A significant role in entity resilience is played by implementation processes [63], which include the implementation of new processes, management systems, software, and security measures.

Implementation of new processes consists of a comprehensive assessment of implementation procedures and the use of implementation tools. Implementation of management systems consists of an assessment of the level of management systems implementation in the critical entity. It is a complex set of interrelated requirements of quality, environmental and occupational health and safety stan-

dards embedded in the overall corporate management system. *Software implementation* consists of an assessment of the level of implementation of new or upgrade of existing software (programming) based on the analysis of incidents, requirements and critical entity needs. It also involves the implementation of actions aimed at ensuring security in cyberspace, such as securing information in information systems, availability and reliability of electronic communications services and networks. *Implementation of security measures* consists of an assessment of the level/status of implementation of solutions and security measures for the provision of essential services, which have been designed on the basis of the information obtained about the incident.

The essence of critical entity adaptability is the strengthening of the organisation's processes in the face of incidents. For this reason, no determining factors have been defined in the infrastructure resilience sphere.

Appendix E. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijdrr.2024.104748.

References

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC.
[2] V. Panevski, L. Nedelchev, Increasing the resilience of critical entities in response to the Dynamic spectrum of threats, Innovations 11 (3) (2023) 79–82.
[3] UNDRR, Sendai Framework for Disaster Risk Reduction 2015-2030, United Nations Office for Disaster Risk Reduction, 2015 Geneva.
[4] D. Rehak, A. Splichalova, M. Hromada, N. Walker, H. Janeckova, J. Ristvej, Critical entities resilience failure indication, Saf. Sci. 170 (2024) 106371, https://doi.org/10.1016/j.ssci.2023.106371.
[5] C. Pursiainen, E. Kytömaa, From European critical infrastructure protection to the resilience of European critical entities: what does it mean? Sustainable and Resilient Infrastructure 8 (1) (2023) 85–101, https://doi.org/10.1080/23789689.2022.2128562.
[6] I. Häring, S. Ebenhöch, A. Stolz, Quantifying resilience for resilience engineering of socio technical systems, Eur. J. Sci. Res. 1 (2016) 21–58, https://doi.org/10.1007/s41125-015-0001-x.
[7] C. Nan, G. Sansavini, A quantitative method for assessing resilience of interdependent infrastructures, Reliab. Eng. Syst. Saf. 157 (2017) 35–53, https://doi.org/10.1016/j.ress.2016.08.013.
[8] C. Johansen, I. Tien, Probabilistic multi-scale modelling of interdependencies between critical infrastructure systems for resilience, Sustainable and Resilient Infrastructure 3 (2018) 1–15, https://doi.org/10.1080/23789689.2017.1345253.
[9] B. Cai, M. Xie, Y. Liu, Y. Liu, Q. Feng, Availability-based engineering resilience metric and its corresponding evaluation methodology, Reliab. Eng. Syst. Saf. 172 (2018) 216–224, https://doi.org/10.1016/j.ress.2017.12.021.
[10] S.A. Argyroudis, S.A. Mitoulis, L. Hofer, M.A. Zanini, E. Tubaldi, D.M. Frangopol, Resilience assessment framework for critical infrastructure in a multi-hazard environment, Sci. Total Environ. 714 (2020) 136854, https://doi.org/10.1016/j.scitotenv.2020.136854.
[11] S. Geng, M. Yang, S. Liu, A quantitative framework for resilience assessment of complex engineered systems under uncertainty, Chemical Engineering Transactions 91 (2022) 31–36, https://doi.org/10.3303/CET2291006.
[12] S. Geng, M. Yang, M. Mitici, S. Liu, A resilience assessment framework for complex engineered systems using graphical evaluation and review technique (GERT), Reliab. Eng. Syst. Saf. 236 (2023) 109298, https://doi.org/10.1016/j.ress.2023.109298.
[13] E.D. Vugrin, D.E. Warren, M.A. Ehlen, A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane, Process Saf. Prog. 30 (3) (2011) 280–290, https://doi.org/10.1002/prs.10437.
[14] F. Petit, G. Bassett, R. Black, W. Buehring, M. Collins, D. Dickinson, R. Fisher, R. Haffenden, A. Huttenga, M. Klett, J. Phillips, M. Thomas, S. Veselka, K. Wallace, R. Whitfield, J. Peerenboom, Resilience Measurement Index: an Indicator of Critical Infrastructure Resilience, Argonne National Laboratory, 2013 https://doi.org/10.2172/1087819, Lemont.
[15] T. Prior, Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9), Eidgenössische Technische Hochschule, 2015 Zurich.
[16] E. Hollnagel, Rag – the resilience analysis grid (chapter 5), in: Safety-II in Practice: Developing the Resilience Potentials, Routledge, London, 2017, https://doi.org/10.4324/9781315201023.
[17] I. Kozine, B. Petrenj, P. Trucco, Resilience capacities assessment for critical infrastructures disruption: the READ framework, Int. J. Crit. Infrastruct. 14 (3) (2018) 199–220, https://doi.org/10.1504/IJCIS.2018.10015604.
[18] M. Hromada, D. Rehak, L. Lukas, Resilience assessment in electricity critical infrastructure from the point of view of converged security, Energies 14 (2021) 1624, https://doi.org/10.3390/en14061624.
[19] F. Anvarifar, M.Z. Voorendt, Ch Zevenbergen, W. Thissen, An application of the Functional Resonance Analysis Method (FRAM) to risk analysis of multifunctional flood defences in The Netherlands, Reliab. Eng. Syst. Saf. 158 (2017) 130–147, https://doi.org/10.1016/j.ress.2016.10.004.
[20] L. Labaka, T. Comes, J. Hernantes, J.M. Sarriegi, J.J. Gonzalez, Implementation Methodology of the Resilience Framework, in: 47th Hawaii International Conference on System Sciences, 6-9 January 2014, Waikoloa, HI, USA, pp. 139-148. https://doi.org/10.1109/HICSS.2014.26.
[21] S.E. Van der Merwe, R. Biggs, R. Preiser, A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems, Ecol. Soc. 23 (2) (2018) 12. https://www.jstor.org/stable/26799110.
[22] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek, Complex approach to assessing resilience of critical infrastructure elements, International Journal of Critical Infrastructure Protection 25 (2019) 125–138, https://doi.org/10.1016/j.ijcip.2019.03.003.
[23] S. Tillement, C. Cholez, T. Reverdy, Assessing organizational resilience: an interactionist approach, M@n@gement 12 (2009) 230–264, https://doi.org/10.3917/mana.124.0230.
[24] A. Annarelli, C. Battistella, F. Nonino, A framework to evaluate the effects of organizational resilience on service quality, Sustainability 12 (3) (2020) 958, https://doi.org/10.3390/su12030958.
[25] S. Janzen, A. Harig, N. Gdanitz, H. Stein, N. Öksüz-Köster, W. Maass, Decoding resilience: a graph-based approach for organizational resilience assessment, in: 42nd International Conference on Conceptual Modeling: ER Forum, 7th SCME, Project Exhibitions, Posters and Demos, and Doctoral Consortium, 06-09 November 2023, Lisbon, Portugal.
[26] R. Patriarca, G. Gravio, F. Costantino, A. Falegnami, F. Bilotta, An analytic framework to assess organizational resilience, Safety and Health at Work 9 (3) (2018) 265–276, https://doi.org/10.1016/j.shaw.2017.10.005.
[27] J. Tasic, S. Amir, J. Tan, M. Khader, A multilevel framework to enhance organizational resilience, J. Risk Res. 23 (6) (2020) 713–738, https://doi.org/10.1080/13669877.2019.1617340.
[28] D. Rehak, Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the Slovak republic, Saf. Sci. 123 (2020) 104573, https://doi.org/10.1016/j.ssci.2019.104573.
[29] W. Eljaoueda, N.B. Yahiaa, B.B. Saouda, A qualitative-quantitative resilience assessment approach for socio-technical systems, Procesia Computer Science 176 (2020) 2625–2634, https://doi.org/10.1016/j.procs.2020.09.305.
[30] M. Marchi, F. Friedrich, M. Riedl, H. Zadek, E. Rauch, Development of a resilience assessment model for manufacturing enterprises, Sustainability 15 (24) (2023) 16947, https://doi.org/10.3390/su152416947.
[31] N. Komatina, N. Nikolic, V. Paunovic, Organizational resilience assessment from the perspective of process realization and key performance indicators, in: 22nd International Symposium INFOTEH-JAHORINA, 15-17 March 2023, East Sarajevo, Bosnia and Herzegovina, pp. 13-17.
[32] ICOR, Organizational Resilience Framework, The International Consortium for Organizational Resilience, 2023 Lombard, IL.

[33] R. Chen, Y. Xie, Y. Liu, Defining, conceptualizing, and measuring organizational resilience: a multiple case study, Sustainability 13 (5) (2021) 2517, https://doi.org/10.3390/su13052517.
[34] F. De Felice, I. Baffo, A. Petrillo, Critical infrastructures overview: past, present and future, Sustainability 14 (2022) 2233, https://doi.org/10.3390/su14042233.
[35] M. Mukherjee, K. Abhinay, M.M. Rahman, S. Yangdhen, S. Sen, B.R. Adhikari, R. Nianthi, S. Sachdev, R. Shaw, Extent and evaluation of critical infrastructure, the status of resilience and its future dimensions in south asia, Progress in Disaster Science 17 (2023) 100275, https://doi.org/10.1016/j.pdisas.2023.100275.
[36] D. Rehak, H. Janeckova, Perceiving the resilience of land transport critical entities, in: O. Prentkovskis, I. Yatskiv, Jackiva, P. Skačkauskas, M. Karpenko, M. Stosiak (Eds.), TRANSBALTICA XIV: Transportation Science and Technology. TRANSBALTICA 2023. Lecture Notes in Intelligent Transportation and Infrastructure, Springer, Cham, 2024, pp. 553–561, https://doi.org/10.1007/978-3-031-52652-7_55.
[37] M. Bogalecka, K. Kołowrocki, Integrated model of critical infrastructure accident consequences, Journal of Polish Safety and Reliability Association 8 (3) (2017) 43–52.
[38] UNDRR, Disaster Risk Reduction Terminology, United Nations Office for Disaster Risk Reduction, 2017 Geneva.
[39] I. Mohamed Shaluf, Disaster types, Disaster Prev. Manag. 16 (5) (2007) 704–717, https://doi.org/10.1108/09653560710837019.
[40] A. Fraser, M. Pelling, A. Scolobig, S. Mavrogenis, Relating root causes to local risk conditions: a comparative study of the institutional pathways to small-scale disasters in three urban flood contexts, Global Environ. Change 63 (2020) 102102, https://doi.org/10.1016/j.gloenvcha.2020.102102.
[41] A. Allen, L. Zilbert Soto, J. Wesely, T. Belkow, V. Ferro, R. Lambert, I. Langdown, A. Samanamu, From state agencies to ordinary citizens: reframing risk-mitigation investments and their impact to disrupt urban risk traps in Lima, Peru, Environ. Urbanization 29 (2) (2017) 477–502, https://doi.org/10.1177/0956247817706061.
[42] A. Mentges, L. Halekotte, M. Schneider, T. Demmer, D. Lichte, A resilience glossary shaped by context: reviewing resilience-related terms for critical infrastructures, Int. J. Disaster Risk Reduc. 96 (2023) 103893, https://doi.org/10.1016/j.ijdrr.2023.103893.
[43] A. Yazdani, R.A. Otoo, P. Jeffrey, Resilience enhancing expansion strategies for water distribution systems: a network theory approach, Environ. Model. Software 26 (12) (2011) 1574–1582, https://doi.org/10.1016/j.envsoft.2011.07.016.
[44] J. Fiksel, Sustainability and resilience: toward a systems approach, Sustain. Sci. Pract. Pol. 2 (2) (2006) 14–21, https://doi.org/10.1080/15487733.2006.11907980.
[45] C. Perrings, Resilience and sustainable development, Environ. Dev. Econ. 11 (4) (2006) 417, https://doi.org/10.1017/S1355770X06003020.
[46] DHS, Risk Steering Committee, DHS Risk Lexicon, United States Department of Homeland Security, Washington, DC, 2008.
[47] Y.Y. Haimes, On the definition of resilience in systems, Risk Anal. 29 (4) (2009) 498–501, https://doi.org/10.1111/j.1539-6924.2009.01216.x.
[48] A.R. Berkeley, M. Wallace, A Framework for Establishing Critical Infrastructure Resilience Goals, National Infrastructure Advisory Council, Washington, DC, 2010.
[49] Cabinet Office, Keeping the Country Running: Natural Hazards and Infrastructure, Civil Contingencies Secretariat, Cabinet Office, London, 2011.
[50] C. Bene, R.G. Wood, A. Newsham, M. Davies, Resilience: new utopia or new tyranny? Reflection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes, IDS Working Papers 405 (2012) 1–61, https://doi.org/10.1111/j.2040-0209.2012.00405.x.
[51] R. Francis, B. Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2014) 90–103, https://doi.org/10.1016/j.ress.2013.07.004.
[52] L. Carlson, G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, R. Whitfield, Resilience: Theory and Application, Argonne National Laboratory, 2012 https://doi.org/10.2172/1044521, Lemont.
[53] M. Hromada, L. Lukas, M. Matejdes, J. Valouch, L. Necesal, R. Richter, F. Kovarik, System and Method of Evaluating the Resilience of Critical Infrastructure, Association of Fire and Safety Engineering, Ostrava, 2013 (in Czech).
[54] J. Geciene, Social resilience assessment framework in the context of organizations operating in rural areas: conceptual review, Social Transformations in Contemporary Society 7 (2019) 142–149.
[55] M. Mills, K. Mutafoglu, V.M. Adams, C. Archibald, J. Bell, J.X. Leon, Perceived and projected flood risk and adaptation in coastal southeast queensland, Australia, Climatic Change 136 (2016) 523–537, https://doi.org/10.1007/s10584-016-1644-y.
[56] S. Fink, Crisis Communications: the Definitive Guide to Managing the Message, McGraw-Hill Education, New York, NY, 2013.
[57] W.T. Coombs, Protecting organization reputations during a crisis: the development and application of situational crisis communication theory, Corp. Reput. Rev. 10 (2007) 163–176, https://doi.org/10.1057/palgrave.crr.1550049.
[58] R.R. Ulmer, T.L. Sellnow, M.W. Seeger, Effective Crisis Communication: Moving from Crisis to Opportunity, fifth ed., SAGE Publications, Thousand Oaks, CA, 2022.
[59] S.T. McManus, Organisational Resilience in New Zealand, University of Canterbury, Christchurch, 2008, https://doi.org/10.26021/1351.
[60] D.A. Kerner, J.S. Thomas, Resilience attributes of social-ecological systems: framing metrics for management, Resources 3 (4) (2014) 672–702, https://doi.org/10.3390/resources3040672.
[61] M.K. Linnenluecke, A. Griffiths, Assessing organizational resilience to climate and weather extremes: complexities and methodological pathways, Climatic Change 113 (2012) 933–947, https://doi.org/10.1007/s10584-011-0380-6.
[62] A.S. Jovanovic, S. Chakravarty, M. Jelic, Resilience and situational awareness in critical infrastructure protection: an indicator-based approach, in: V. Rosato, A.D. Pietro (Eds.), Issues on Risk Analysis for Critical Infrastructure Protection, IntechOpen, London, 2021, https://doi.org/10.5772/intechopen.97810.
[63] S. Duchek, Organizational resilience: a capability-based conceptualization, Business Research 13 (2020) 215–246, https://doi.org/10.1007/s40685-019-0085-7.
[64] C. Catalan, R. Benoit, Evaluation of organizational resilience: application in quebec, in: E. Hollnagel, E. Rigaud, D. Besnard (Eds.), Proceedings of the Fourth Resilience Engineering Symposium (1–), Presses des Mines, Paris, 2011, pp. 50–57, https://doi.org/10.4000/books.pressesmines.975.
[65] M. Hepfer, T.B. Lawrence, The heterogeneity of organizational resilience: exploring functional, operational and strategic resilience, Organization Theory 3 (1) (2022), https://doi.org/10.1177/26317877221074701.
[66] J.L. Gressgård, K. Hansen, Knowledge exchange and learning from failures in distributed environments: the role of contractor relationship management and work characteristics, Reliab. Eng. Syst. Saf. 133 (2015) 167–175, https://doi.org/10.1016/j.ress.2014.09.010.
[67] M. Rahman, S. Ghosh, Increasing resilience by the participatory planning approach, in: Construction Research Congress, 2016, pp. 1538–1545, https://doi.org/10.1061/9780784479827.154.
[68] C. Brown, E. Seville, J. Vargo, Measuring the organizational resilience of critical infrastructure providers: a New Zealand case study, International Journal of Critical Infrastructure Protection 18 (2017) 37–49, https://doi.org/10.1016/j.ijcip.2017.05.002.
[69] A.V. Lee, J. Vargo, E. Seville, Developing a tool to measure and compare organizations' resilience, Nat. Hazards Rev. 14 (1) (2013) 29–41, https://doi.org/10.1061/(ASCE)NH.1527-6996.0000075.
[70] C.A. Lengnick-Hall, T.E. Beck, M.L. Lengnick-Hall, Developing a capacity for organizational resilience through strategic human resource management, Hum. Resour. Manag. Rev. 21 (3) (2011) 243–255, https://doi.org/10.1016/j.hrmr.2010.07.001.
[71] C.A. Lengnick-Hall, T.E. Beck, Adaptive fit versus robust transformation: how organizations respond to environmental change, J. Manag. 31 (5) (2005) 738–757, https://doi.org/10.1177/0149206305279367.
[72] O. Lindberg, O. Rantatalo, Competence in professional practice: a practice theory analysis of police and doctors, Hum. Relat. 68 (4) (2015) 561–582, https://doi.org/10.1177/0018726714532666.
[73] K.M. Sutcliffe, T.J. Vogus, E. Dane, Mindfulness in organizations: a cross-level review, Annual Review of Organizational Psychology and Organizational Behavior 3 (2016) 55–81, https://doi.org/10.1146/annurev-orgpsych-041015-062531.
[74] G.A. Bonanno, C.R. Brewin, K. Kaniasty, A.M. La Greca, Weighing the costs of disaster: consequences, risks, and resilience in individuals, families, and communities, Psychol. Sci. Publ. Interest 11 (1) (2010) 1–49, https://doi.org/10.1177/1529100610387086.
[75] T.A. Williams, D.A. Shepherd, Victim entrepreneurs doing well by doing good: venture creation and well-being in the aftermath of a resource shock, J. Bus. Ventur. 31 (4) (2016) 365–387, https://doi.org/10.1016/j.jbusvent.2016.04.002.

[76] B. Walker, V. Nilakant, K. Heugten, J. Kuntz, S. Malinen, K. Naswall, Becoming Agile: A Guide to Building Adaptive Resilience, University of Canterbury, Christchurch, 2019.
[77] K. O'Neill, Steps You Can Take to Build a Resilient Organization, Center for Creative Leadership, Greensboro, NC, 2020. https://www.ccl.org/articles/leading-effectively-articles/steps-you-can-take-to-build-a-resilient-organization/. (Accessed 10 May 2024).
[78] K.M. Connor, J.R. Davidson, Development of a new resilience scale: the connor-davidson resilience scale (CD-RISC), Depress. Anxiety 18 (2) (2003) 76–82, https://doi.org/10.1002/da.10113.
[79] E. Diener, Guidelines for national indicators of subjective well-being and ill-being, J. Happiness Stud. 7 (4) (2006) 397–404, https://doi.org/10.1007/s10902-006-9000-y.
[80] P. Dolan, R. Metcalfe, Measuring subjective wellbeing: recommendations on measures for use by national governments, J. Soc. Pol. 41 (2) (2012) 409–427, https://doi.org/10.1017/s0047279411000833.
[81] M. Nardo, M. Saisana, A. Saltelli, S. Tarantola, Handbook on Constructing Composite Indicators: Methodology and User Guide, Organisation for Economic Co-operation and Development, Paris, 2008, https://doi.org/10.1787/9789264043466-en.
[82] A. Clark, S. Zonouz, Cyber-physical resilience: definition and assessment metric, IEEE Trans. Smart Grid 10 (2) (2019) 1671–1684, https://doi.org/10.1109/TSG.2017.2776279.
[83] L. Petersen, D. Lange, M. Theocharidou, Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators, Reliab. Eng. Syst. Saf. 199 (2020) 106872, https://doi.org/10.1016/j.ress.2020.106872.
[84] K. Kampova, T. Lovecek, D. Rehak, Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak republic, International Journal of Critical Infrastructure Protection 30 (2020) 100376, https://doi.org/10.1016/j.ijcip.2020.100376.
[85] H. Li, G.E. Apostolakis, J. Gifun, W. VanSchalkwyk, S. Leite, D. Barbe, Ranking the risks from multiple hazardsin a small community, Risk Anal. 29 (3) (2009) 438–456, https://doi.org/10.1111/j.1539-6924.2008.01164.x.
[86] G.M. Alliger, C.P. Cerasoli, S.I. Tannenbaum, W.B. Vessey, Team resilience: how teams flourish under pressure, Organ. Dynam. 44 (3) (2015) 176–184, https://doi.org/10.1016/j.orgdyn.2015.05.003.
[87] T.A. Williams, D.A. Gruber, K.M. Sutcliffe, D.A. Shepherd, E.Y. Zhao, Organizational response to adversity: fusing crisis management and resilience research streams, Acad. Manag. Ann. 11 (2) (2017) 733–769, https://doi.org/10.5465/annals.2015.0134.
[88] C. Nan, G. Sansavini, W. Kroger, H.R. Heinimann, A quantitative method for assessing the resilience of infrastructure systems, in: PSAM 2014 - Probabilistic Safety Assessment and Management, June 2014 Honolulu, Hawai.
[89] M. Panteli, P. Mancarella, The grid: stronger, bigger, smarter? Presenting a conceptual framework of power system resilience, IEEE Power Energy Mag. 13 (3) (2015) 58–66, https://doi.org/10.1109/MPE.2015.2397334.
[90] I. Häring, G. Sansavini, E. Bellini, N. Martyn, T. Kovalenko, M. Kitsak, G. Vogelbacher, K. Ross, U. Bergerhausen, K. Barker, I. Linkov, Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies, in: NATO Science for Peace and Security Series C: Environmental Security, Springer, Netherlands, 2017, pp. 21–80, https://doi.org/10.1007/978-94-024-1123-2\textunderscore2.
[91] K. Fischer, S. Hiermaier, W. Riedel, I. Häring, Morphology dependent assessment of resilience for urban areas, Sustainability 10 (6) (2018) 1800, https://doi.org/10.3390/su10061800.
[92] D. Rehak, P. Senovsky, S. Slivkova, Resilience of critical infrastructure elements and its main factors, Systems 6 (2) (2018) 21, https://doi.org/10.3390/systems6020021.
[93] P. Klimek, J. Varga, A.S. Jovanovic, Z. Szekely, Quantitative resilience assessment in emergency response reveals how organizations trade efficiency for redundancy, Saf. Sci. 113 (2019) 404–414, https://doi.org/10.1016/j.ssci.2018.12.017.
[94] M.H. Oboudi, M. Mohammadi, M. Rastegar, Resilience-oriented intentional islanding of reconfigurable distribution power systems, Journal of Modern Power Systems and Clean Energy 7 (4) (2019) 741–752, https://doi.org/10.1007/s40565-019-0567-9.
[95] N.U.I. Hossain, R. Jaradat, S. Hosseini, M. Marufuzzaman, R.K. Buchanan, A framework for modeling and assessing system resilience using a bayesian network: a case study of an interdependent electrical infrastructure system, International Journal of Critical Infrastructure Protection 25 (2019) 62–83, https://doi.org/10.1016/j.ijcip.2019.02.002.
[96] A. Jovanovic, P. Klimek, O. Renn, R. Schneider, K. Øien, J. Brown, M. DiGennaro, Y. Liu, V. Pfau, M. Jelic, T. Rosen, B. Caillard, S. Chakravarty, P. Chhantyal, Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards, Environment Systems and Decisions 40 (2) (2020) 1–35, https://doi.org/10.1007/s10669-020-09779-8.
[97] M. Braun, C. Hachmann, J. Haack, Blackouts, restoration, and islanding: a system resilience perspective, IEEE Power Energy Mag. 18 (4) (2020) 54–63, https://doi.org/10.1109/MPE.2020.2986659.
[98] D.K. Mishra, M.J. Ghadi, A. Azizivahed, L. Li, J. Zhang, A review on resilience studies in active distribution systems, Renew. Sustain. Energy Rev. 135 (2021) 110201, https://doi.org/10.1016/j.rser.2020.110201.
[99] A. Mottahedi, F. Sereshki, M. Ataei, A. Nouri Qarahasanlou, A. Barabadi, The resilience of critical infrastructure systems: a systematic literature review, Energies 14 (6) (2021) 1571, https://doi.org/10.3390/en14061571.
[100] J. Figueira, S. Greco, M. Ehrogott, Multiple Criteria Decision Analysis: State of the Art Surveys, Springer, New York, NY, 2005, https://doi.org/10.1007/b100605.
[101] C.L. Dozier, A.M. Briggs, K.M. Holehan, N.A. Kanaman, J.F. Juanico, Functional analysis methodology: best practices and considerations, in: J.B. Leaf, J.H. Cihon, J.L. Ferguson, M.J. Weiss (Eds.), Handbook of Applied Behavior Analysis Interventions for Autism, Autism and Child Psychopathology Series, Springer, Cham, 2022, https://doi.org/10.1007/978-3-030-96478-8_22.
[102] D. Rehak, S. Slivkova, R. Pittner, Z. Dvorak, Integral approach to assessing the criticality of railway infrastructure elements, Int. J. Crit. Infrastruct. 16 (2) (2020) 107–129, https://doi.org/10.1504/IJCIS.2020.107256.
[103] A. Fekete, Urban Disaster Resilience and Critical Infrastructure, Julius-Maximilians-Universität Würzburg, Würzburg, 2018.
[104] IEC 31010, Risk Management – Risk Assessment Techniques, International Electrotechnical Commission, Geneva, 2019.
[105] IEC 62502, Analysis Techniques for Dependability – Event Tree Analysis (ETA), International Electrotechnical Commission, Geneva, 2010.
[106] M. Grabinski, Management Methods and Tools, Gabler Verlag, Wiesbaden, 2007, https://doi.org/10.1007/978-3-8349-9295-6.
[107] M. Metfessel, A proposal for quantitative reporting of comparative judgments, J. Psychol. 24 (2) (1947) 229–235, https://doi.org/10.1080/00223980.1947.9917350.
[108] P.C. Fishburn, A comparative analysis of group decision methods, Behav. Sci. 16 (6) (1971) 538–544, https://doi.org/10.1002/bs.3830160604.
[109] IEC 60812, Failure Modes and Effects Analysis (FMEA and FMECA), International Electrotechnical Commission, Geneva, 2018.
[110] ASIS, Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use, American National Standards Institute, Washington, DC, 2009.
[111] H.M. Levin, P.J. McEwan, in: Cost-Effectiveness Analysis: Methods and Applications, second ed., SAGE Publications, Washington, DC, 2000.
[112] ISO/TS 31050, Risk Management – Guidelines for Managing an Emerging Risk to Enhance Resilience, International Organization for Standardization, Geneva, 2023.
[113] ISO 31000, Risk Management, International Organization for Standardization, Geneva, 2018.
[114] ISO/IEC 27001, Information Security, Cybersecurity, and Privacy Protection – Information Security Management Systems – Requirements, International Organization for Standardization, Geneva, 2022.
[115] ISO 45001, Occupational Health and Safety Management Systems – Requirements with Guidance for Use, International Organization for Standardization, Geneva, 2018.
[116] ISO 12100, Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction, International Organization for Standardization, Geneva, 2010.
[117] M. Iturriza, L. Labaka, J.M. Sarriegi, J. Hernantes, Modelling methodologies for analysing critical infrastructures, J. Simulat. 12 (2) (2018) 128–143, https://

doi.org/10.1080/17477778.2017.1418640.
[118] E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, M. Hellmann, Digital twin conceptual framework for improving critical infrastructure resilience, Automatisierungstechnik 69 (12) (2021) 1062–1080, https://doi.org/10.1515/auto-2021-0104.
[119] D. Denyer, Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking, BSI and Cranfield School of Management, Cranfield, 2017.
[120] Z. Yang, B. Barroca, A. Weppe, A. Bony-Dandrieux, K. Laffr′echine, N. Daclin, V. November, K. Omrane, D. Kamissoko, F. Benaben, H. Dolidon, J. Tixier, V. Chapurlat, Indicator-based resilience assessment for critical infrastructures – a review, Saf. Sci. 160 (2023) 106049, https://doi.org/10.1016/j.ssci.2022.106049.
[121] A. Splichalova, D. Patrman, N. Kotalova, M. Hromada, Managerial decision making in indicating a disruption of critical infrastructure element resilience, Adm. Sci. 10 (3) (2020) 75, https://doi.org/10.3390/admsci10030075.
[122] EN 15602, Private Security Services, European Committee for Standardization, Brussels, 2022.
[123] T. Lovecek, J. Reitspis, Designing and Evaluation of Object Protection Systems, University of Zilina, Zilina, 2011.
[124] ISO 9001, Quality Management Systems, International Organization for Standardization, Geneva, 2015.
[125] D. Philpott, Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity, second ed., Bernan Press, Lanham, MD, 2016.
[126] ISO 22301, Security and Resilience – Business Continuity Management Systems, International Organization for Standardization, Geneva, 2019.
[127] K. Tracht, G. Goch, P. Schuh, M. Sorg, J.F. Westerkamp, Failure probability prediction based on condition monitoring data of wind energy systems for spare parts supply, CIRP Annals 62 (2013) 127–130, https://doi.org/10.1016/j.cirp.2013.03.130.
[128] D. Vidrikova, K. Boc, Z. Dvorak, D. Rehak, Critical Infrastructure and Integrated Protection, the Association of Fire and Safety Engineering, Ostrava, 2017.
[129] EN 50398-1, Alarm Systems – Combined and Integrated Alarm Systems, European Committee for Electrotechnical Standardization, Brussels, 2017.
[130] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[131] V. Novotny, P. Sysel, J. Prinosil, J. Mekyska, K. Slavicek, I. Lattenberg, Critical infrastructure monitoring system, in: IEEE 17th International Colloquium on Signal Processing & its Applications (CSPA), 2021, pp. 165–170 https://doi.org/10.1109/CSPA52141.2021.9377303, Langkawi, Malaysia.
[132] O. ElSahly, A. Abdelfatah, A systematic review of traffic incident detection algorithms, Sustainability 14 (22) (2022) 14859, https://doi.org/10.3390/su142214859.
[133] A. Carmeli, J. Schaubroeck, Organisational crisis-preparedness: the importance of learning from failures, Long. Range Plan. 41 (2) (2008) 177–196, https://doi.org/10.1016/j.lrp.2008.01.001.
[134] R. Savolainen, Information sharing and knowledge sharing as communicative activities, Inf. Res. 22 (3) (2017) 9.
[135] S. Chaturvedi, A. Vedrtnam, M.A. Youssef, M.T. Palou, G. Barluenga, K. Kalauni, Fire-resistance testing procedures for construction elements – a review, Fire 6 (1) (2023) 5, https://doi.org/10.3390/fire6010005.
[136] A. Rasulo, A. Pelle, B. Briseghella, C. Nuti, A resilience-based model for the seismic assessment of the functionality of road networks affected by bridge damage and restoration, Infrastructures 6 (8) (2021) 112, https://doi.org/10.3390/infrastructures6080112.
[137] M.Y.H. Bangash, T. Bangash, Explosion-Resistant Buildings: Design, Analysis, and Case Studies, Springer, Berlin, Heidelberg, 2006, https://doi.org/10.1007/3-540-31289-7.
[138] Bosch, Automatic incident detection for bridges and tunnels, Bosch Security Systems, Fairport, NY (2020). https://media.boschsecurity.com/fs/media/pb/images/industries_2/transportation/APP-NOTE_Automatic_Incident_Detection.pdf. (Accessed 24 April 2024).
[139] P. Marana, L. Labaka, J.M. Sarriegi, Maintenance in critical infrastructures: the need for public-private partnerships, in: M. Carnero, V. González-Prida (Eds.), Optimum Decision Making in Asset Management, IGI Global, 2017, pp. 62–82, https://doi.org/10.4018/978-1-5225-0651-5.ch003.
[140] M. Ovaere, S.V. Proost, Electricity Transmission Reliability: the Impact of Reliability Criteria, Katholieke Universiteit, Leuven, 2016, https://doi.org/10.2139/ssrn.2874192.
[141] A. Daidone, S. Chiaradonna, A. Bondavalli, P. Veríssimo, Analysis of a redundant architecture for critical infrastructure protection, in: R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (Eds.), Architecting Dependable Systems V. Lecture Notes in Computer Science, vol. 5135, Springer, Berlin, Heidelberg, 2008, https://doi.org/10.1007/978-3-540-85571-2_4.
[142] F. Steinhauser, Redundancy for power utility communication networks, in: 26th International Conference and Exhibition on Electricity Distribution, CIRED, 2021, pp. 1742–1746, https://doi.org/10.1049/icp.2021.1917.
[143] Ch Zhang, J.J. Kong, S.P. Simonovic, Restoration resource allocation model for enhancing resilience of interdependent infrastructure systems, Saf. Sci. 102 (2018) 169–177, https://doi.org/10.1016/j.ssci.2017.10.014.
[144] V. Proag, Human resources management for infrastructure, in: Infrastructure Planning and Management: an Integrated Approach, Springer, Cham, 2021, pp. 563–593, https://doi.org/10.1007/978-3-030-48559-7_20.
[145] P.S. Mohan, Disasters, disaster preparedness and post disaster recovery: evidence from caribbean firms, Int. J. Disaster Risk Reduc. 92 (2023) 103731, https://doi.org/10.1016/j.ijdrr.2023.103731.
[146] C.R. Zorn, A.Y. Shamseldin, Post-disaster infrastructure restoration: a comparison of events for future planning, Int. J. Disaster Risk Reduc. 13 (2015) 158–166, https://doi.org/10.1016/j.ijdrr.2015.04.004.
[147] E. Ciapessoni, D. Cirio, A. Pitto, M. Sforna, A quantitative methodology to assess the process of service and infrastructure recovery in power systems, Elec. Power Syst. Res. 189 (2020) 106735, https://doi.org/10.1016/j.epsr.2020.106735.
[148] M. Hartmann, S. Maseberg, Replacement of components in public key infrastructures, in: 27th Annual Conference of the IEEE Industrial Electronics Society (IECON'01), vol. 3, 2001, pp. 2012–2016 https://doi.org/10.1109/IECON.2001.975600, Denver, CO.
[149] D. Lamghari-Idrissi, R. Basten, G.J. van Houtum, Spare parts inventory control under a fixed-term contract with a long-down constraint, Int. J. Prod. Econ. 219 (2020) 123–137, https://doi.org/10.1016/j.ijpe.2019.05.023.
[150] W. Chmielarz, M. Zborowski, A. Biernikowicz, Analysis of the importance of business process management depending on the organization structure and culture, in: Federated Conference on Computer Science and Information Systems, 2013, pp. 1079–1086 Krakow, Poland.
[151] L.A. Sincora, M.P.V.d. Oliveira, H. Zanquetto-Filho, M.Z. Alvarenga, Developing organizational resilience from business process management maturity, Innovation & Management Review 20 (2) (2023) 147–161, https://doi.org/10.1108/INMR-11-2021-0219.
[152] E.E. Yamoah, The link between human resource capacity building and job performance, Int. J. Hum. Resour. Stud. 4 (3) (2014) 139–146, https://doi.org/10.5296/ijhrs.v4i3.5938.
[153] J. Rodriguez, K. Walters, The importance of training and development in employee performance and evaluation, World Wide Journal of Multidisciplinary Research and Development 3 (10) (2017) 206–212.
[154] A. Fetais, G.M. Abdella, K.N. Al-Khalifa, A.M. Hamouda, Business process Re-engineering: a literature review-based analysis of implementation measures, Information 13 (2022) 185, https://doi.org/10.3390/info13040185.
[155] M. Syed Ibrahim, A. Hanif, F.Q. Jamal, A. Ahsan, Towards successful business process improvement – an extension of change acceleration process model, PLoS One 14 (11) (2019) e0225669, https://doi.org/10.1371/journal.pone.0225669.
[156] O.S.I. Fayomi, J.O. Adelakun, K.O. Babaremu, The impact of technological innovation on production, J. Phys. Conf. 1378 (2019) 022014, https://doi.org/10.1088/1742-6596/1378/2/022014.
[157] W. Lazonick, Investing in Innovation: Confronting Predatory Value Extraction in the U.S. Corporation, Cambridge University Press, Cambridge, 2023, https://doi.org/10.1017/9781009410700.