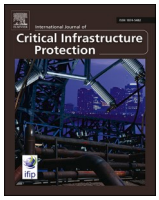
international journal of critical infrastructure protection 49 (2025) 100766

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

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



Critical entities resilience strengthening tools to small-scale disasters

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

[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] Czech Technical University in Prague, Faculty of Transportation Sciences, Konviktska 293/20, 110 00 Praha, Czech Republic
[d] Tomas Bata University of Zlin, Faculty of Applied Informatics, Nad Stranemi 4511, 760 05 Zlin, Czech Republic
[e] RINA Consulting S.p.A., Via Santa Valeria 5, 20123 Milano, Italy
[f] University of Zilina, Faculty of Security Engineering, 1. maja 32, 010 26 Zilina, Slovakia

ARTICLE INFO

Keywords:
Critical entities
Strengthening resilience
Strengthening tools
Small-scale disasters
CERA method

ABSTRACT

The issue of critical infrastructure protection is still largely based on the concept of critical infrastructure resilience. However, it is already clear that this concept must be restructured, primarily due to the adoption of a new European Union directive that focuses on the resilience of critical entities that are owners or operators of individual critical infrastructures. This directive stipulates, among other things, an obligation for critical entities to provide unlimited services necessary for maintaining the most important functions of the state. For this reason, it is necessary to pay increased attention not only to strengthening the resilience of infrastructures, but also to the management processes of critical entities. Based on these facts, 161 tools suitable for strengthening the critical entities internal resilience against small-scale disasters are classified and defined in this article. These strengthening tools are defined for both entities and infrastructural resilience. The article further defines the environment and procedure for strengthening the critical entities internal resilience, thus expanding the application of the existing CERA method, which was originally designed for the purpose of assessing the critical entities resilience to small-scale disasters. The design part of the article also includes a presentation of an example of a practical application of the proposed procedure.

1. Introduction

Critical entities, as owners or operators, play a pivotal role in the protection of critical infrastructures through which companies provide so-called essential services [1]. These infrastructures are permanently exposed to hazards that can cause accidents [2] or incidents [1]. Incidents can be further classified into small-scale disasters and large-scale disasters, depending on the extent of the impacts [3]. From the point of view of critical entities and the essential services provided by them, small-scale disasters are considered a greater risk, since their occurrence reaches a higher frequency [4]. For this reason, it is essential that these critical entities and their infrastructures have a high level of resilience, which should be cyclically assessed [5] and in case of indication of its violation [6] should be strengthened through appropriate tools. This resilience can be classified into internal and external in the context of the environment [7]. While the critical infrastructure internal resilience is ensured by the critical entities management processes, external resilience is determined by the external environment in which these critical entities and their infrastructures are located.

Strengthening resilience in connection with disasters is currently the focus of many states and multinational organizations operating in various fields, e.g. in the field of climate resilience [8], resilience for a changing climate [9], health resilience to climate change [10], resilience to disasters [11], resilience to natural disasters [12], resilience in post-disaster situations [13], resilience and response to crisis [14], etc. Strengthening resilience in this context mainly concerns society and territory. However, within urban areas, significant attention is also paid to the resilience of critical infrastructure [15,16].

The need to strengthen the resilience of critical infrastructure to the effects of disasters was already declared in 2015 as part of Sustainable Development Goal 9 [17]. From the beginning, however, attention was paid to the protection of critical infrastructure rather than its resilience, e.g. [18–22]. It was only in the following years that publications related to the resilience of critical infrastructure began to appear (e.g. [23–28])

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

https://doi.org/10.1016/j.ijcip.2025.100766
Received 20 February 2025; Received in revised form 16 April 2025; Accepted 22 April 2025
Available online 23 April 2025

and subsequently also tools for its strengthening (e.g. [29–31]). A fundamental change in the perception of this issue occurred in 2022, when, as a result of the adoption of the European Union directive [1] there was a transition from the protection of critical infrastructure to the resilience of critical entities [32]. Strengthening the resilience of these entities is currently possible mainly through general approaches to strengthening organizational resilience (e.g. [33–38]), however, tools designed explicitly for strengthening the critical entities resilience have not yet been published.

It is evident from the above that considerable attention has been paid to strengthening resilience to disasters for a long time, but only in the context of the resilience of society or territory. In the context of the critical infrastructure protection or resilience, several important publications have been published in the past period. However, in the context of the adoption of the directive on the critical entities resilience, no comprehensive study regarding strengthening the resilience of these entities has yet been presented. Based on these facts, the aim of the article is to define tools suitable for strengthening the internal resilience of critical entities, both in the field of entities and infrastructural resilience. For their practical implementation, the authors also proposed an extension of the CERA method, which can now be used not only for critical entities resilience assessment, but also for identifying key areas where these measures need to be taken to increase the resilience level. This concept can be compared to the NIST Cybersecurity Framework [39], where so-called controls are used for this purpose.

2. Critical entity resilience system

The essence of this part of the article is a brief definition of backgrounds, which will help the reader to better understand the following text. As already stated in the abstract, this article directly follows the publication dealing with Critical Entities Resilience Assessment (CERA) to Small-scale Disasters [5], thereby expanding this issue and providing the reader with a holistic approach to critical entities resilience. For this purpose, it is appropriate to perceive the critical entities resilience as a system (see Fig. 1), which can be compared to the human brain, where the left hemisphere is responsible for entities resilience, the right hemisphere for infrastructural resilience and the cerebellum for cyber resilience. Based on this concept, it is evident that the Critical Entity Resilience System (CERS) is determined by three dimensions (i.e. organizational, physical and cyber) that interact with each other.

The CERS is, like any other system, shaped by a set of related elements and the links between them [40]. In the case of CERS, these elements are the management, processes and critical entity infrastructures. However, for the proper functioning of the entire system and ensuring the required level of its resilience, financial, human and material resources are also necessary, which form inputs into this system. If the system is properly set up and sufficiently resilient, its output is essential services [1], which are necessary for the functioning of the society.

However, CERS is also influenced by the external environment, and the factors of this external environment can be both negative and positive. In the case of negative factors, these are mainly hazards that can cause accidents [2] or incidents [1], whereby incidents can be further classified into small-scale and large-scale disasters depending on the scale of the impacts [3]. A small-scale disaster is defined as *"a type of disaster only affecting local communities which can require assistance also beyond the affected community"*, while a large-scale disaster is defined as *"a type of disaster affecting a society which requires national or international assistance"* [3]. From these definitions it is clear that the critical entities resilience and the essential services provided by them can be addressed only against small-scale disasters because in the case of large-scale disasters, any level of critical entities resilience is completely insufficient.

As can be seen from Fig. 1, CERS is determined by three dimensions, but in the context of this article, only the organizational dimension (i.e., entity resilience) and the physical dimension (i.e., infrastructure resilience) are explicitly elaborated. The cyber dimension is not elaborated separately, but tools for strengthening resilience information and operational technologies are integrated into both of these dimensions. Resilience in these two dimensions is further determined by components (i.e. resistance, robustness, recoverability and adaptability), variables and parameters. Defining variables and their parameters was described in detail in the previous article [5]. If the level of resilience is insufficient, it is advisable to strengthen it through adequate tools, which in this context can be considered as positive factors of the external environment. However, in order to define these strengthening tools, it is necessary to first pay attention to the analysis of approaches suitable for strengthening the critical entities resilience.

3. Approaches suitable for strengthening the critical entities resilience

Currently, there are very few publications that explicitly deal with the issue of strengthening the critical entities resilience. Moreover, these

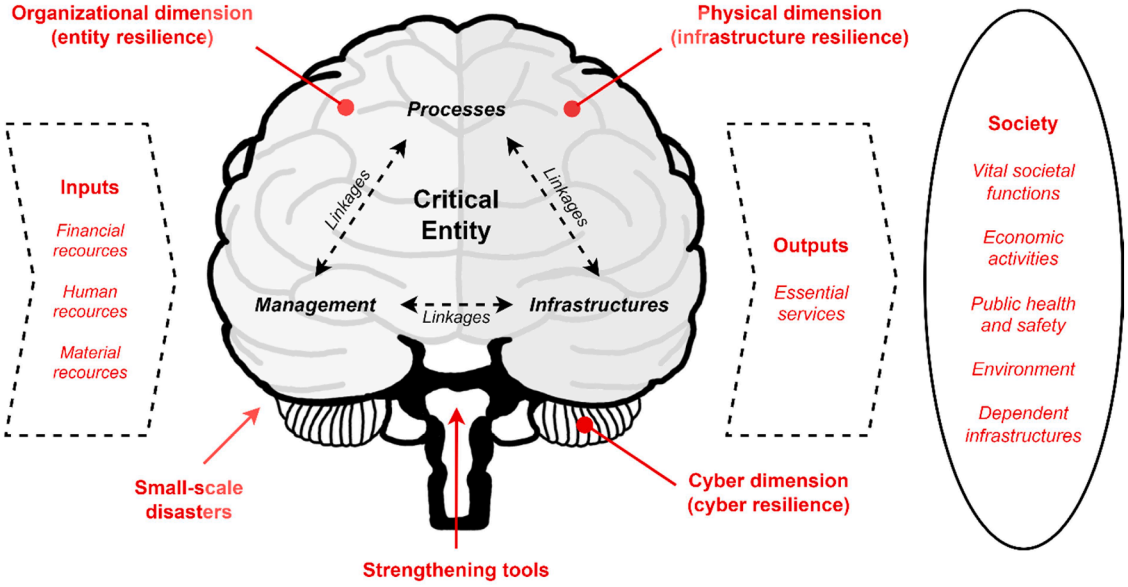


Fig. 1. Critical entity resilience system.

publications are very general in nature and provide only basic information about possible access [41], challenges for the near future [42] or starting points applicable for setting up a probable concept of strengthening the critical entities resilience [43]. From what has been said so far, it is clear that the analysis of approaches directly related to strengthening the critical entities resilience cannot be carried out, primarily because of their absence. For this reason, in the following text, attention is focused more on the analysis of approaches that are used to strengthen the resilience of infrastructures and strengthen the resilience of organizational management. Indeed, some of these approaches may include areas suitable for strengthening the critical entities resilience.

Across different areas, strengthening the resilience of infrastructures is carried out similarly. Most approaches are generic in nature, reflecting transnational recommendations or national resilience management concepts. Efforts to find suitable procedures and establish priorities or strategies for a resilient society are often presented in these types of documents, primarily through preventive management and the implementation of individual solutions [44]. Building this resilience can be done, for example, through the following categories, i.e. infrastructure, situational awareness, planning, procedures, management, training, communication and collaboration at horizontal and vertical levels, learning lessons, resources and assessment [45,46]. It is also necessary to coordinate the basic capabilities of adequate response to an incident, monitor, predict, learn and manage resilience itself (i.e. crisis management, operational risk management, security policies, risk reduction process, identification of critical assets, data protection, etc.), and that in the field of operation and the infrastructure organization itself [47–49].

For a comprehensive approach to risk management, it is advisable to use internationally recognized standards, such as ISO 31000 [50], ISO 28000 [51], ISO 22316 [52], COSO-ERM [53], ISO/TS 31050 [54] or ISO 9001 [55] or guidelines [56], which contribute to the provision of the essential services [57,58]. It is clear that it is appropriate to take a collaborative approach to incident resolution, create partnerships, build collaboration, use and share best practices, enhance decision-making capabilities and innovate risk management processes. Furthermore, it is necessary to ensure resilient communication systems (secure management of information systems, improvement of information exchange, etc.) and to have back-up plans for coordinating work in times of supply failures, whether at the input or output of the infrastructures [59–63]. It is also necessary that infrastructures are prepared for incidents (i.e. risk analysis, identification of vulnerable points, vulnerability reduction, use of business continuity plan, disaster recovery plan or incident response plan) and the management of the organization adapts its crisis communication not only towards employees, but also to stakeholders and state administration [61,64,65].

Another important area suitable for strengthening the critical entities resilience is the management of the organization, or their collective reaction, mainly at the time of the incident [66]. It is desirable that management at all levels be cohesive and that so-called team resilience training takes place [67]. At the same time, it is advisable to have resilience engineering in place, which significantly contributes to the prevention of incidents, using the operationalization of proposals (procedures used in operation can also be used in other spheres of the organization), development and testing of these proposals, environmental research or focusing on key (problem) components [68]. Organizational management must have established bodies, along with adaptive and flexible competencies [69,70], prepare for role improvisation [71] and actively work with risks based on the security policy or resilience concept [72,73], e.g. using a six-pack [74].

An approach such as resilience engineering perceives resilience as a system property, i.e. mainly as a setting for the organization of infrastructures. However, resilience can also be strengthened through individuals (employees), through the development of human resources and their sufficient capacity [65]. It is therefore necessary to provide adequate training, i.e. set up the training life cycle, create training programs [75–77], increase staff qualifications [78], raise and share awareness of risks, monitor employee behaviour and reactions to an incident, or assign responsibility to individual positions [49,79]. So-called resilience training is applied in this area [80], which can be divided into preparedness training [81], stress resilience training [82] and personal effectiveness training [83]. Team resilience training can also be part of this training [84] and resilience engineering training [85]. Through these approaches, the development of the ability to withstand non-standard situations and respond effectively to them is ensured [80].

To strengthen the critical entities resilience, in addition to the above-mentioned approaches, those that strengthen the technical resilience of individual infrastructures can also be used. In the field of incident response, this is, for example, early warning, for which sophisticated techniques based on artificial intelligence can be used [29], enabling, for example, dynamic adaptations or automatic reactions [86]. Modelling and simulation can also be used [87,88] and also the concept of digital training or digital twins [47,89,90]. At the same time, it is necessary to carry out regular security checks and audits, continuous monitoring and technology resilience testing [64], determine the status and performance of equipment, the status of resource reserves and material security, or plan equipment repairs [91]. Stress tests are also used to check resilience [92] or so-called quality functions (QFD), which are able to identify various resilience criteria and subsequently transform them into system requirements [93]. Diagnostic systems or technical checklists can be used to check the technical parameters of infrastructures [94].

The last important area for strengthening the resilience of infrastructures and organization management is innovation and resource sufficiency (financial, human and material). For this purpose, support for research and development, motivation for investment, monetization resilience or support for new approaches to subduction are crucial [65, 79,95,96].

The analysis of the approaches suitable for strengthening the critical entities resilience has shown that appropriate tools have not yet been explicitly defined and properly categorized. In recent years, have been noticed only one article that dealt more closely with specific tools for strengthening resilience [30]. Furthermore, it is not clear with the analysed approaches whether they are usable for the entities or infrastructural resilience. However, the analysis of approaches also shows that these two types of resilience are interconnected [97], and therefore influence each other. Nevertheless, it is appropriate to categorize future tools for strengthening the critical entities -resilience accordingly.

4. Results

From the analysis presented above, it is evident that there is currently no comprehensive study that explicitly deals with the description of tools and their application in strengthening the critical entities resilience. However, on a more general level, some approaches have been identified that could be used for this purpose. Based on these results, the essence of this part of the article is the classification and definition of tools suitable for strengthening the critical entities internal resilience against small-scale disasters. Based on their nature, these tools are broadly classified according to their applicability to strengthen subject or infrastructure resilience in the context of individual components, i.e. resistance, robustness, recoverability and adaptability. The classification of tools on a general level is presented in Fig. 2.

The figure also shows that the individual instruments are classified in more detail according to their relationship to specific variables and their parameters. A description of variables and parameters is available in the article Critical Entities Resilience Assessment (CERA) to Small-scale Disasters [5]. In this context, these tools can be likened to the neurons that make up the neural network of the brain, in this case the inner critical entities resilience. At the same time, however, it is necessary to realize that blood is necessary for the proper functioning of this neural network, which in the context of a critical entity represents external resources provided by the supply chain. Some of these tools can also be

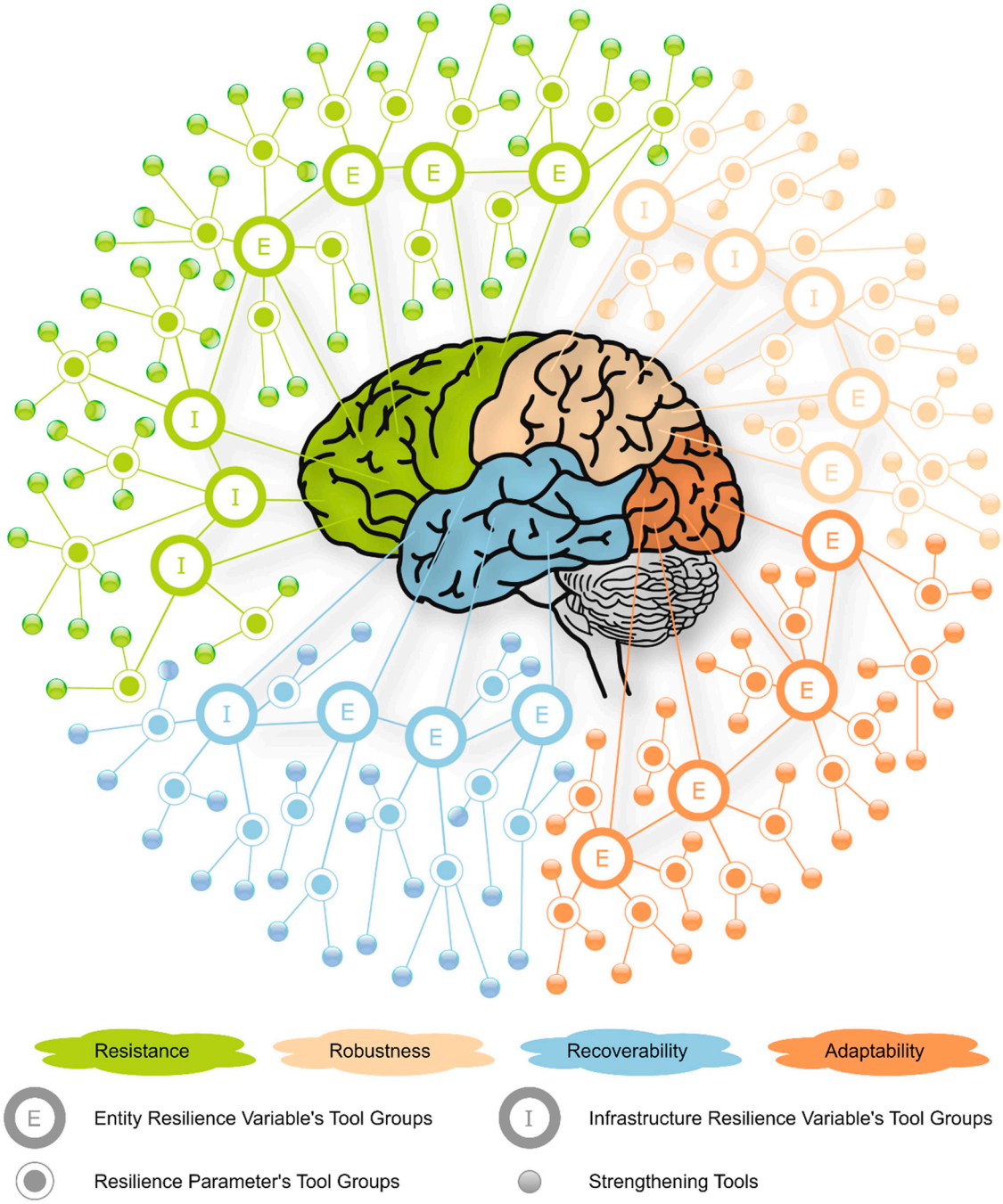


Fig. 2. An environment for strengthening the critical entities resilience.

used to strengthen the resilience of other parameters (similar to the case of synapses in the brain), but only on the condition that these are related areas of resilience, e.g. training and personnel training and training to deal with incidents. A detailed classification of strengthening tools, including their definition, is presented in the following text.

4.1. Classification and definition of tools for strengthening entities resilience

First, attention is paid to tools for strengthening entities resilience, which are further classified according to their relationship to individual components of resilience. The methodological procedure of classifying and defining tools was implemented in five steps. First, an analysis of approaches suitable for strengthening the critical entities resilience was carried out (see Section 3 of this article). Based on the results of this analysis, specific tools were selected and their classification was carried out. Subsequently, these tools were defined in relation to the critical entities resilience. As part of the fourth step, the instruments classified and defined in this way were consulted with selected critical entities from the Czech Republic and Slovakia. The final step was to incorporate the comments of critical entities into the text, which is presented in Sections 4.1.1. to 4.1.4. of this article.

4.1.1. Tools for strengthening entity resistance

In the context of the temporal arrangement of the phases of resilience, the tools for strengthening the entity resistance are first defined. These empowering tools are defined at the level of parameters (see Table 1).

Table 1
Tools for strengthening entity resistance.

Variables	Parameters	Strengthening tools
Risk management	Level of risk management	Risk management strategy Integrated risk management Software support tools
	Risk assessment methodology	Comparative methods Analytical methods based on a deterministic approach Analytical methods based on a probabilistic approach Risk prioritization tools
	Implementation of safety/ security standards	Technical standards Implementation plan Revising the implemented standards
	Incident modelling	Modelling programs Xtended Reality
Anticipation	Preventive control	Safety assurance system Internal control system
	Indicating a breach in the critical entity resilience	Protective measures index (PMI) Vulnerability index (V-index) Resilience measurement index (RMI) Strategic tensions assessment tool (STAT) Critical entities resilience failure indication (CERFI)
Security measures	Guarding	Technical standards Types of security guards
	Regime protection	Regime measures Background checks
Crisis preparedness	Responsibilities, duties and powers	Security and resilience – Crisis management
	Education and training of workers	Employee development and education system Employee training methods & techniques
	Safety planning and documentation	Critical entity crisis preparedness plan Internal emergency plan
	Continuity planning	Business continuity management system

The resilience of entity resistance is determined by four variables, which are risk management, anticipation, security measures and crisis preparedness. Tools for strengthening the resilience of these variables are presented in the following text.

4.1.1.1. Tools for strengthening risk management. One of the primary tools for strengthening the critical entity resilience in the field of risk management is a *Risk management strategy*. It is a tool that is primarily related to the prevention of risks and their minimization. A correctly set strategy helps not only with the solution of risks, i.e. with their identification, analysis, management, monitoring or communication, but also with the optimization of the entire risk management process [98]. It is clear that strategic thinking is used at the strategic level, which includes a systemic view, a specific goal, intelligent opportunism (flexibility to accept alternative solutions), hypothetical orientation (the ability to create and test optimal variants) and thinking in time [99].

Another important tool is *Integrated risk management*. Its essence is the combination of three program areas of risk management, i.e. technological/cyber risks, operational risks and corporate/strategic risks [100]. Integrated risk management is based on six key activities, i.e. strategy, assessment, response, communication and reporting, monitoring and technology.

For the organization's risk management, it is advisable to use *Software support tools* that enable effective management of not only corporate risks. These tools are primarily helpful in identifying risks, evaluating them and mitigating potential risks that could affect the provision of essential services. An example is Enterprise Risk Management Tools [101], which enable risk identification, risk assessment, scenario analysis and risk quantification. Additional features include integration with strategic planning processes and automated reporting and analytics.

Another important risk management tool for critical entities are risk assessment tools. These tools can be classified into three groups based on their purpose [102]:

- *Comparative methods*, e.g. Brainstorming, Checklist, Ishikawa (Fishbone), Multi-criteria Analysis, What-if?;
- *Analytical methods based on a deterministic approach*, e.g. Hazard and Operability Studies, Human Reliability Analysis, Preliminary Hazard Analysis, Cause-Consequence Analysis;
- *Analytical methods based on a probabilistic approach*, e.g. Bow Tie Analysis, Event Tree Analysis, Failure Tree Analysis, Layer Protection Analysis.

To evaluate the results of the risk assessment, it is advisable to use *Risk prioritization tools*. The prioritization of security risks is a process by which, with the help of criteria set by a critical entity, the order of identified risks is determined, based on their significance for infrastructure elements. This prioritization is of fundamental importance when choosing and implementing security measures, designing a security concept or creating/updating a security strategy or policy. For this purpose, methods of multicriteria analysis can be used in particular, e.g. Metfessel's allocation [103], Fuller's triangle [104], Analytic Hierarchy Process [105], or Failure Mode, Effects, and Criticality Analysis [106].

An important tool for the work of critical entities with risks is the use of available *Technical standards*. These are mainly standards supporting risk management not only in general, but also in specific areas:

- risk management system [50],
- risk assessment techniques [102],
- managing an emerging risk to enhance resilience [54],
- information security management systems [107],
- occupational health and safety management systems [108].

In order for the relevant technical standards to be implemented into the processes of the critical entity, it is necessary to develop an *Implementation plan*. This plan should include a set of activities aimed at effectively and systematically applying the selected standards at the required time. The core activities of the implementation plan are publication of an internal document, determination and notification of responsible persons, description of the process of implementation of technical standards, determination of the method of monitoring and determination of conditions for updating the implementation process [109].

In connection with the implementation of technical standards into the processes of a critical entity, attention must also be paid to *Revising the implemented standards*. A critical entity should permanently monitor the validity and up-to-dateness of all technical standards that have been implemented in its processes. When ensuring that any of these standards are updated or replaced by a new standard, they must conduct a preliminary analysis of the impact of this change and prepare a process review plan [110]. When revising processes, the opinions and comments of interested parties, such as experts, dependent organizations or customers, should also be considered.

The last significant area for strengthening risk management is incident modelling. *Modelling programs* such as ALOHA Software can be used for this purpose [111], OpenFlows FLOOD [112], or FLACS-CFD explosion, fire & dispersion modelling software [113]. It is also possible to use *Xtended Reality* tools to model incidents [114], which include Augmented Reality, Virtual Reality, and Mixed Reality.

4.1.1.2. Tools for strengthening anticipation. An important tool for

strengthening anticipation in the field of preventive control is the *Safety assurance system*. The essence of this system is the effective control of safety risks caused by a critical entity. The safety assurance system can be implemented in various areas, e.g. in the area of health protection at work [108] or in the railway sector [115].

Another important tool for strengthening anticipation is the *Internal control system*. With the help of this control system, critical entities can record, evaluate and manage risks related to their documented processes. The internal control system is a tool for comprehensive control of the process environment, which can be used in various areas of the entity, especially in the areas of risk assessment, process control, financial control, compliance control, information and communication, and monitoring [116].

Important tools for strengthening anticipation are tools for indicating the disruption of the critical entity resilience. Among those currently available are, for example:

- *Protective measures index – PMI* [117]. Here, attention is paid to comprehensive protection across component categories, i.e. physical security, security management, security unit, information sharing, protection measures- and dependencies.
- *Vulnerability index – V-index* [118]. This indicator is used in the systematic assessment of the position of protection and vulnerability of critical infrastructure and key resources. Within this methodology, a vulnerability indicator is used, which is central to the preparation of sector risk estimate, the analysis of vulnerabilities in the sector and sub-sector, to identify ways to reduce vulnerability or to reveal strengths and weaknesses in the area of security.
- *Resilience measurement index – RMI* [119]. The main goal of RMI is to measure the ability of critical infrastructure to reduce the size and/or duration of the impacts resulting from the action of hazards, using the response and assessment of individual components. RMI is composed of four main components, which are preparedness, mitigation measures, response capabilities and recovery mechanisms, which are broken down further.
- *Strategic tensions assessment tool – STAT* [120]. The essence of this tool is the assessment of the strategic tension of the organization through four basic strategies of resilience, i.e. progression, flexibility, defence and cohesion. Based on this model, the organization will gain insight into the perceptions of resilience from internal and external stakeholders. The result of the assessment is the identification of blind spots and risk factors of the organization.
- *Critical entities resilience failure indication – CERFI* [6]. The essence of this tool is a probabilistic algorithm that, through indicators, predicts the relationship between the intensity of hazard and the level of critical entity resilience. The result of this prediction is an indication of the critical point of failure of the critical entity resilience.

4.1.1.3. Tools for strengthening security measures. Tools for strengthening security measures can be classified into two groups. The first group is represented by guarding tools. In this area, *Technical standards*, such as the standard setting requirements for the provision of private security services for critical infrastructure, are important tools for strengthening resilience [121].

In addition to technical standards, another beneficial tool is the choice of an adequate *Types of security guards*. This can be performed either directly by the given critical entity or by an external security service. In both cases, the following types of Security guards may be used: Government Contract Security Guards, Contract Security Guards, Armed Security Guards, Unarmed Security Guards, Guard Dog Security, and Video Surveillance Operators [122].

The second group are tools for regime protection, which is defined as *"a set of regime measures implemented for the purpose of monitoring and physical/cybernetic protection of an organization"* [123,124]. Regime measures are the core tools of regime protection. These are in particular the following *Regime measures* (e.g. [125]):

- determining the authorization of persons and means of transport to enter the object, determining the authorization of persons to enter the secured area and the meeting area and the method of checking these authorizations;
- control measures at the entrance to the object, secured and meeting areas and the method of control of these measures;
- the conditions and method of controlling the movement of persons in the facility, secure areas and meeting areas and the method of checking and removing classified information from the facility, secure area and meeting areas;
- the mode of handling keys and means of identification, in particular the method of their labelling, allocation, safekeeping and records;
- mode of handling technical means and their use;
- the mode of movement of classified information in the object, secure area and negotiation area.

Background checks are also among the regime protection tools [1]. This tool serves to minimize the risk that critical entities employees or their contractors will abuse, for example, their access rights within the critical entity organization the to cause damage and harm. For this purpose, Member States should establish procedures for checks and determine the categories of persons who must undergo these checks. Appropriate training and qualification requirements for these persons should also be established.

4.1.1.4. Tools for strengthening crisis preparedness. An important tool of a general nature for strengthening crisis preparedness is a technical standard *Security and resilience – Crisis management* [126]. This standard provides crisis management guidance to help organizations plan, implement, maintain, review and continuously improve crisis management capability at a strategic level. Among other things, this document also focuses on determining responsibilities, duties and powers in the field of crisis management, crisis communication, and staff training and education.

In the field of employee training, it is also advisable to have an established *Employee development and education system*. This system should be focused especially on Preparedness and Readiness, Skill Development, Team Coordination, Risk Identification and Mitigation, Maintaining Reputation, Legal and Regulatory Compliance, Employee Well-Being, and Cost Reduction [127]. Available ones can be used for this purpose *Employee training methods & techniques*, such as Simulation training, Collaborative training, Video training, Cross-training, Job shadowing, Gamification, Mobile learning, Blended learning, Micro-learning, Adaptive learning [128].

In the field of security planning and documentation, the critical entity crisis preparedness plan and internal emergency plan can be considered the most effective tools for strengthening crisis preparedness. The *Critical entity crisis preparedness plan* serves to ensure the preparedness of the critical infrastructure entity for crisis situations that may threaten the function of the infrastructure (e.g. [129]). In particular, this plan should include:

- procedures for solving crisis situations identified in the hazard's analysis;
- plan of economic mobilization measures for suppliers of mobilization supplies;
- identification of possible hazards to the function of infrastructure elements;
- measures to protect infrastructure elements.

The *Internal emergency plan* serves as a planning document for such critical entities that handle hazardous substances and may experience a serious accident. The details of the internal emergency plan are available

in the Seveso-III Directive [130].

The last significant tool for strengthening crisis preparedness is the *Business continuity management system* [131]. This system represents a complex management process that identifies potential hazards for the critical entity as a whole and impacts on its business activities, i.e. the provision of essential services. This system also provides a framework for building the critical entity resilience with the ability to respond effectively to small-scale disasters and a framework for the availability of processes and resources to ensure the continuous provision of essential services.

4.1.2. Tools for strengthening entity robustness

Another group of tools are tools for strengthening entity robustness. These empowering tools are also defined at the level of parameters (see Table 2).

The resilience of entity robustness is determined by two variables, which are the critical entity responsiveness of the and incident management. Tools for strengthening the resilience of these variables are presented in the following text.

4.1.2.1. Tools for strengthening the critical entity responsiveness. The essence of strengthening the critical entity responsiveness is to minimize the time interval for the activation of protective measures and strengthening the state of forces and means usable for intervention. In order to minimize the time interval for the activation of protective measures, so-called smart systems can be used by the critical entity [132, 133]). In the field of physical protection, these are most often *Smart security systems* or *Smart fire protection systems*. In the field of cyber protection, this most often involves the use of the *Internet of things* or *Artificial intelligence*.

Strengthening the state of forces and means usable for intervention can be carried out both quantitatively and qualitatively. From a quantitative point of view, own forces and resources (e.g. company firefighters or protective service) can be strengthened by *Contractual forces and resources*, e.g. security agencies. From a qualitative point of view, the responsiveness of the critical entities can be strengthened by some modern technologies, e.g. *Unmanned systems* [134].

4.1.2.2. Tools for strengthening incident management. Crisis management readiness and communication and information sharing are key factors in incident management. Strengthening crisis management preparedness can be implemented, for example, by creating a suitable *Strategy for effective response and resilience* [135] or *Solving crisis scenarios based on simulation* [136].

In the area of communication and information sharing, the crisis communication plan and the warning and information plan are important tools. The *Crisis communication plan* is intended not only for internal crisis communication, but also for critical entity crisis communication with intervening components and other interested parties, e.g. dependent critical entities. The *Warning and information plan* is intended for the transmission of crisis information to the population. Other important strengthening tools are the correct setting of *Parameters of crisis communication* [137] and the use of *Modern communication technologies* [138].

4.1.3. Tools for strengthening entity recoverability

The third group is represented by tools for strengthening entity recoverability. In Table 3, these empowering tools are presented in the context of individual parameters.

The resilience of the entity's recovery is determined by three variables, which are financial resources, human resources and recovery processes. Tools for strengthening the resilience of these variables are presented in the following text.

4.1.3.1. Tools for strengthening financial resources. The essence of strengthening the resilience of financial resources in the area of recoverability is their adequate allocation for recovery and timely preparedness. For this purpose, it is possible to use several important tools that serve to prioritize the spending of financial resources or optimize expenses/costs. The most important tools can be considered, for example, the Lean Six Sigma methodology, asset management or software tools.

Lean Six Sigma is a performance improvement methodology that aims to eliminate waste, reduce variability and improve overall process efficiency [139]. By implementing Lean Six Sigma principles, a critical entity can streamline its operations, reduce costs and increase the quality of recovery processes.

Asset management enables critical entities to achieve the desired balance of cost, risk and performance in the recovery process [140]. Asset management also helps to value assets and supports the realization of value in balancing financial, environmental and social costs, risks, service quality and performance in relation to assets. Cost optimization can be used to manage and manage the assets of a critical entity [141].

In order to increase the visibility of incurred expenses and create adequate reserves for recovery, critical entities can use some of the available *Financial software tools* for automating expenses, such as Zoho Expense, Rydoo, Emburse Certify, Expensify, Everlance. The description and comparison of these tools is a suitable basis for their correct selection [142].

An important tool in terms of the timely availability of financial resources is their allocation from the external environment. *External financial resources* allow a critical entity to use financial resources that

Table 2
Tools for strengthening entity robustness.

Variables	Parameters	Strengthening tools
Critical entity responsiveness	Time interval for activation of protective measures	Smart security systems Smart fire protection systems Internet of things Artificial intelligence
	State of forces and means	Contractual forces and resources Unmanned systems
Incident management	Crisis management preparedness	Strategy for effective response and resilience Solving crisis scenarios based on simulation
	Communication and information sharing	Crisis communication plan Warning and information plan Parameters of crisis communication Modern communication technology

Table 3
Tools for strengthening entity recoverability.

Variables	Parameters	Strengthening tools
Financial resources	Allocation of financial resources for recovery	Lean Six Sigma Asset management Financial software tools
	Timeliness of financial resources	External financial resources
Human resources	Human resource capacity	SimMan simulation model External human resources
	Human resources expertise	Behavioural event interview Assessment centre Jack Welch matrix
	Timely availability of human resources	External human resources
Recovery process	Disaster preparedness recovery processes	Critical entity crisis preparedness plan Technical standards
	Recovery of infrastructure function	Disaster recovery plan Business impact analysis Work breakdown structure Network analysis methods

are not part of its management, i.e. external funding sources can be used. External sources of financing include, for example, shares, bonds, loans, grants, subsidies, investors or insurance [143].

4.1.3.2. Tools for strengthening human resources. Human resources are also necessary for recovery processes. They can be strengthened especially in the areas of their capacity, expertise and time availability. For workforce capacity planning, it is possible to use, for example, the *SimMan simulation model* [144]. It is a management tool that serves as a testbed for assessment the effectiveness and robustness of various scheduling options and human resource allocation rules. The insufficient capacity of human resources can also be supplemented from *external sources* (e.g. construction companies) if necessary, but in this case, it is necessary to have this form of outsourcing treated contractually.

It is advisable to check the expertise of human resources not only during the selection of employees, but also during their work in the personnel structure of a critical entity. When selecting employees, some of the tools for selecting candidates for a certain job position, such as the Behavioural event interview or the Assessment centre, may be used. *Behavioural event interview* [145] it assumes that future behaviour can best be predicted based on knowledge of past behaviour. This method can also be used to quickly determine the expertise of the staff. In contrast, the *Assessment centre* method [146] is based on comparing the applicant's skills with others who have been selected. This comparison takes place at the same time in the same place, where all applicants are engaged in group or individual tasks.

To check the expertise of human resources in the course of their work in the personnel structure of a critical entity, it is possible to use, for example, the *Jack Welch matrix* [147]. It is a tool based on the assessment of performance values. This matrix is used to classify and differentiate employees using two independent variables, i.e. performance level (how employees achieve their results) and corporate culture fit (how employees adhere to the organization's guiding principles, which to some extent reflects their typical behaviour).

The time availability of human resources can be solved in a similar way as the insufficient capacity of human resources, i.e. on the basis of the contract, *External human resources* can be used if necessary. This is, for example, a contractual arrangement for the provision of assistance within a pre-defined time horizon, with a pre-selected entity that has the necessary personnel of the required expertise.

4.1.3.3. Tools for strengthening recovery process. Last but not least, the recovery processes themselves are necessary. Their strengthening can be implemented especially in the field of disaster preparedness, recovery processes and by recovery the function of the infrastructure. Disaster preparedness of recovery processes should be implemented primarily on the basis of the *Critical entity crisis preparedness plan* (e.g. [129]). In the case of strengthening recovery processes, the procedures for solving crisis situations identified in the hazard analysis and the plan of economic mobilization measures for suppliers of mobilization supplies are central to this plan. Other important tools in the area of disaster preparedness for recovery processes can be selected *Technical standards*, e.g. Business continuity management systems [131], Crisis management [126] or Societal security [148].

A key tool for strengthening infrastructure recovery processes is the *Disaster recovery plan* [149]. This document contains detailed instructions on how to respond to unplanned events such as natural disasters, power outages, cyber-attacks and other small-scale disasters. It is used to minimize the impact of these disasters on infrastructure elements and to recovery their function. The aim of this plan is to help the critical entity solve the recovery of system functionality so that it is able to provide basic services again at least at the minimum required level after the incident.

Another effective tool that should be used before preparing a disaster recovery plan is *Business impact analysis* [150]. This document is used to predict the consequences of the disruption of the company's core business operations due to the occurrence of a small-scale disaster. This is an important part of the business continuity plan. It represents a tool to reveal vulnerable places and to create strategies to minimize risks. The result is an impact analysis report that describes potential risks specific to the organization.

For the infrastructure function restoration project itself, it is advisable to use, for example, the *Work breakdown structure* [151]. This tool represents a simple analytical technique, the aim of which is to break down the project, i.e. recovery of the element function, to individual activities up to such a level of detail that responsibilities, demands and time horizon can be assigned to them.

The last recommended tools for strengthening recovery processes are *Network analysis methods* [152]. It is a group of special analytical techniques that can be used to analyse or optimize interconnected and related processes, activities, networks or elements. The most important methods in the given context are Critical Path Method (CPM), Critical Chain Method (CCM) and Program Evaluation and Review Technique (PERT).

4.1.4. Tools for strengthening entity adaptability

The last group of tools related to entity resilience are tools for strengthening entity adaptability. An overview of these tools in the context of parameters is provided in Table 4.

The resilience of entity adaptability is determined by four variables, which are organizational management processes, educational and development processes, innovation processes and implementation processes. Tools for strengthening the resilience of these variables are presented in the following text.

4.1.4.1. Tools for strengthening organizational management processes. Strengthening the resilience of the organization's management processes should be implemented through their thorough analysis and management. In order to analyse the organizational processes of a critical entity, it is possible to use a number of analytical methods, the most important of which are Benchmarking, GAP analysis, EFQM excellence model, Process analysis, and SWOT analysis.

Benchmarking [153] is a method for systematically comparing the processes, organizational structure, products and performance of a given critical entity with other recognized organizations as a basis for comparison in order to define the goals of self-improvement. It provides an important link between establishing, identifying and understanding the key indicators for achieving change, i.e. improvement. Getting the right information and working with it is key to the success of this method.

GAP analysis [154] is an analytical and planning tool that serves to identify and examine the gaps (differences, deficits, shortcomings, disproportions) between the current state of fulfilment of a strategic goal (or achieved in some time horizon of its fulfilment) and the planned (required) state of fulfilment of this strategic goal. It therefore serves to identify and examine the differences between the current and planned state of fulfilment of the strategic goal through the target values of the indicators.

EFQM excellence model [155] was created as the primary framework for self-assessment and improvement of organizations so that they can achieve sustainable excellence. The EFQM model has a total of nine criteria and 32 sub-criteria. Each sub-criterion is broken down into individual questions or areas of focus that are assessed within the sub-criterion.

Process analysis [156] provides a comprehensive and detailed overview of existing processes, causes and consequences of their shortcomings for the critical entity. It includes methods that make it possible to analyse the described processes from different points of view and provides information on the possibilities of eliminating the identified shortcomings.

SWOT analysis [157] it pits the strengths and weaknesses of the

Table 4
Tools for strengthening entity adaptability.

Variables	Parameters	Strengthening tools
Organizational management processes	Analysis of organizational processes	Benchmarking GAP analysis EFQM excellence model Process analysis SWOT analysis
	Management of organizational processes	Quality management system Balanced ScoreCard Business process reengineering
Educational and development processes	Scope of professional education	Educational and development activities Tools for maintaining psychological and work well-being Personal development plan
	Quality of professional education	Cooperation with professional educational institutions Guidelines for competence management and people development Management systems for educational organizations
	Incident handling training	Incident modelling and simulation Digital twins
	Assessment of training effectiveness	Kirkpatrick model Kaufman model Phillips model
Innovation processes	Innovation of management processes	Total quality management Event-driven process chain Business process modelling notation
	Innovation measures and technologies	Support for research and innovation Innovation management
	Investment in innovation	Financial plan Investment plan Financial control tools
Implementation processes	Implementation of new processes	Business process modelling Business process management
	Implementation of management systems	Quality management system Environmental management system Occupational health and safety management system
	Software implementation	Information security management system
	Implementation of security measures	7FE method PDCA cycle Six Sigma (DMAIC) 8D Method 4Q Method

critical entity and/or its parts or processes against the identified opportunities and threats arising from the external environment. The results of this analysis serve as a starting point for defining strategies for further development of the critical entities.

To manage organizational processes, a critical entity can primarily use the proven *Quality management system* [55], which provides the critical entity with a basic quality management framework. Another important tool for managing organizational processes is the *Balanced ScoreCard* method [158]. This method creates a link between strategy and operational activities with an emphasis on performance measurement. It is based on the idea of monitoring strategic measures in addition to traditional financial indicators and thus obtaining an optimal view of performance. The advantage of this method is that it can define the connection between different components of strategic planning and management.

If serious deficiencies have been analysed in the organizational processes, it is recommended to readjust them. For this purpose, it is advisable to use *Business process reengineering* [159]. It is a tool suitable for radical redesign of business processes with the aim of achieving significant improvements in productivity, cycle time, quality and employee and customer satisfaction. This model assumes that a one-time change is necessary for the so-called "straightening" of processes to cause a dramatic change in the performance of a critical entity.

4.1.4.2. Tools for strengthening educational and development processes. Strengthening the critical entity resilience in the field of educational and development processes can be realized not only through the scope and quality of vocational training, but also through training to deal with incidents and assessment its effectiveness. The basic tool in the scope of education is individual types of *Educational and development activities* [160]. Among their key forms are long-term education, study stays abroad, development of skills (soft skills), professional training (preventive and punitive) and staff training.

Tools for maintaining psychological and work well-being can also be considered important, as psychologically balanced people achieve lower error rates and higher work performance [161]. Another suitable tool in the area of the scope of education is a *Personal development plan*. This is a document or a list of various activities aimed at increasing the competence of the worker. This plan may include forms of education, work activities of the employee leading to an increase in his qualifications, contribution of the employee to the organization, participation in development programs, etc.

The quality of professional education can be ensured either by self-help or by *Cooperation with professional educational institutions*. This cooperation can be established with universities, technical schools or other educational institutions. Thanks to this cooperation, it is possible to gain access to certified or professional personnel, who can subsequently provide various forms of training for the personnel of the critical entity. In both cases, it is possible to proceed with staff training in accordance with, among other things, the requirements of the relevant technical standards, e.g. *Guidelines for competence management and people development* [162] or *Management systems for educational organizations* [163].

In the area of training to deal with incidents, it is advisable to use modern technologies, especially available tools in the area of *Incident modelling and simulation* [87] or the concept of *Digital twins* [47,89,90]. Elements of virtual or augmented reality can be used to model and simulate incidents [164]. Some of the recognized assessment models can be used to assess the effectiveness of training, such as *Kirkpatrick model* [165], *Kaufman model* [166], or *Phillips model* [167]. Before choosing and implementing a particular model, it is recommended to read the publication A Critical Review on Training Evaluation Models [168].

4.1.4.3. Tools for strengthening innovation processes. An important area for strengthening the critical entities resilience are innovation processes, which are determined by innovations in management processes, innovations in measures and technologies, and investments in innovations. *Total quality management* is a suitable tool for the innovation of management processes [169]. It is a very complex technique that emphasizes quality management in all dimensions of the organization. It promotes the general use of general management principles and the application of modern process management, including the involvement of top managers in the form of leadership. Furthermore, it promotes the involvement of all employees, strongly promotes customer orientation and the quality of products and services, efficient use of the organization's resources, elimination of unnecessary costs, and also promotes continuous improvement efforts based on clear facts and indicators.

Another tool suitable for innovation of management processes is *Event-driven process chain* [170]. It is a kind of flowchart that can be used to show the structure of business process control flow as a chain of events and functions. It provides various connections that enable alternative and parallel implementation of processes. The tool also built on a similar principle is *Business process modelling notation* [171]. It is a

flowchart method that models the steps of a planned business process from start to finish. It is the key to business process management and visually depicts the detailed sequence of business activities and information flows required to complete a process. Its purpose is to model ways to improve efficiency, consider new circumstances or gain a competitive advantage.

In the area of innovation measures and technologies, the *Support of research and innovation* plays a key role. Based on this support, critical entities can participate in the solution of grant projects, the results of which can contribute, among other things, to strengthening their resilience. In the European Union, this is, for example, the Horizon Europe funding program, which allocated €93.5 billion for the years 2021–2027 [172]. At the national level, this support is provided mainly through state grant agencies or individual ministries. A technical standard [173], is also an important tool for *Innovation management*, which defines the principles of innovation management and their systematic implementation.

Investments in innovation are a significant area of strengthening innovation processes. In this area, it is appropriate to apply the following tools in particular: *Financial plan, Investment plan* and *Financial control tools* [174]. The financial plan is a summary of the individual innovation projects of the critical entity, the sales forecast for the services provided and the external financing budgets for the individual departments. The investment plan determines how to properly invest and work with assets in order to achieve innovation goals with an acceptable level of risk, and to invest the funds of the critical entity safely.

4.1.5. Tools for strengthening implementation processes

The last area for strengthening the critical entities resilience in the field of entity adaptability are tools for strengthening implementation processes. In this area, it is necessary to pay particular attention to tools for the implementation of new processes, the implementation of management systems, the implementation of software and the implementation of security measures.

An important initial tool in the field of implementing new processes is *Business process modelling* [175], which enables a general understanding of the processes of the critical entity. On the basis of process modelling, a description of the current state of the organization can be made, and then a suitable form of implementation of new processes can be designed, tested and selected. As part of this implementation, it is also appropriate to apply *Business process management* [176]. It is a tool whose essence is a structured approach to the optimization of already implemented processes. The essence of this tool is continuous monitoring and analysis of the functioning of these processes in various scenarios.

For the implementation of management systems, it is advisable to primarily use adequate technical standards. *Quality management system* [55] can be considered a key tool, which specifies the requirements for the quality management system, which provides the critical entity with an increase in credibility with an internationally recognized certificate. This system promotes the introduction of a process approach in the development, implementation and improvement of the effectiveness of the quality management system with the aim of increasing customer satisfaction by meeting their requirements. Other important tools are the *Environmental management system* [177] and *Occupational health and safety management system* [108]. By connecting these three technical standards, a so-called integrated management system is created [178].

Information security management system [107] is advisable to use for software safe implementation. This technical standard defines the risk management process and includes people, procedures and IT systems, providing a holistic approach to information security.

Security measures are procedures for dealing with cases of violation of established security rules by users, administrators and persons holding security roles. In this context, the implementation of security measures can be seen as a process improvement process through available methods [179]. For this purpose, it is possible to use e.g. *7FE method* [180], which combines the four main phases of 4F (i.e. Foundations, Findings and solutions, Fulfilment, and Future) and the three essential elements of 3E (i.e. Leadership, Project management, and People change management. Each of these elements is present for the entire time of the implementation process. Other suitable methods can be e.g. *PDCA cycle, Six Sigma (DMAIC), 8D Method, 4Q Method* [181].

4.2. Classification and definition of tools for strengthening infrastructure resilience

The following part of the article focuses on tools for strengthening infrastructure resilience. These tools are further classified according to their relationship to the individual components of resilience. The exception is infrastructure adaptability, for which no parameters are currently defined [5].

4.2.1. Tools for strengthening infrastructural resistance

The first group are tools for strengthening infrastructure resistance. Similar to entity resistance, in this case also the tools are defined at the level of parameters (see Table 5).

The resilience of infrastructure resistance is determined by three variables, which are monitoring and operation of the infrastructure, technical security of the infrastructure and the ability to detect incidents. Tools for strengthening the resilience of these variables are presented in the following text.

4.2.1.1. Tools for strengthening infrastructure monitoring and operation.

In order to strengthen the critical entities resilience, in addition to the above-mentioned tools for entity resistance, it is also necessary to monitor and ensure the optimal operation of the infrastructure, i.e. it is necessary to ensure adequate conditions for the operation of technical equipment. An important tool in this area is a technical standard *Functional safety of electrical / electronic / programmable electronic safety-related systems* [182], which sets more detailed requirements for the safe operation and use of equipment.

Checking the condition and performance of the infrastructure is no less important. Here, regular monitoring, assessment and comparison with expected parameters are required, which can be done, for example, using the following tools:

- *Root cause analysis to identify reliability issues* [183]. The essence of this tool is the identification of events that can cause a problem, and the subsequent development of an action plan for their effective solution.
- *Computerized maintenance management system* [184]. This tool uses so-called problem codes, which inform about the current state of the device in the event of a malfunction. These codes also show fault and maintenance history and are able to provide data for possible failures. This is a central record of all data from individual devices.
- *Remote monitoring and management* [185]. This tool is focused primarily on the field of information technology. In a large-scale digital asset management environment, it acts as a central "nervous system" that coordinates, oversees and controls various aspects to achieve optimal performance and security levels.

Ensuring its trouble-free operation is also an essential part of infrastructure operation. This is ensured by means of diagnostic systems that enable the detection of problems, or and identification of the cause of failures, which shortens the time needed to repair key technology. These systems can be secured using the following tools:

- *Equipment condition simulation – EQS* [186]. This tool determines the optimal time horizon and scope of maintenance in accordance with

Table 5
Tools for strengthening infrastructural resistance.

Variables	Parameters	Strengthening tools
Infrastructure monitoring and operation	Technical condition of the infrastructure	Functional safety of electrical / electronic / programmable electronic safety-related systems
		Root cause analysis to identify reliability issues
		Computerized maintenance management system
		Remote monitoring and management
	Equipment maintenance, service and testing	Equipment condition simulation (EQS)
		Service relationship management
		Reliability, availability and maintainability (RAM)
		Safety review (SR)
		Maintenance plan
Technical infrastructure security	Mechanical barriers	Technical means of protection
		Systematic analysis of vulnerability to intrusion (SAVI)
		Design and evaluation of physical protection systems
		Vega-2
		Systematic analysis of physical protection effectiveness (SEPA)
		Security design proposal
		Basics of soft targets protection guidelines
	Electronic monitoring and alarm devices	Surveillance means
		Alarm devices
	Cyber security	NIST Cybersecurity Framework
		Zero Trust Architecture
		Anti-virus tools
		Deep learning and machine learning
		Information security management system
		Cyber resilience framework: Strengthening defences and enhancing continuity in business security
		Cyber resilience assessment tool for industrial control systems (ICS-CRAT)
		Cyber resilience self-assessment tool (CR-SAT)
Incident detection capability	Environmental monitoring	Diagnostic devices
		Territorial vulnerability analysis
		Geographic information systems and spatial analysis
		Multi-risk assessment
		Unmanned aerial vehicle
		CIA Method
		CERBERUS Approach
	Detection of the occurrence of an incident	Handbook of incident and accident reporting
		Security incident management system
		Information technology infrastructure library (ITIL)
		Specialized shared databases

safety and economy, through a mathematical model and a simulation algorithm of the evolution of the state of the equipment.

- *Service relationship management* [187]. It is an effective system for optimizing and providing all maintenance information to improve decision making, reduce costs and ensure consistency of service events. This information is provided to all interested parties.
- *Reliability, availability and maintainability – RAM* [188]. The purpose of this tool is to ensure the continuity of the provision of basic services, while maintaining a high level of safety and quality. It assesses the capabilities of the system, identifies possible causes of failures and provides possible alternatives for solving them.
- *Safety review – SR* [189]. This tool determines whether a critical entity complies with established safety principles and identifies potentially dangerous locations. This is a two-part process involving a survey of the workplace for hazards and the effectiveness of safety processes and procedures.

Infrastructure maintenance can also be provided through a *Maintenance plan* [190], which stipulates the implementation of controls in a predetermined form and time frame. In this case, it is advisable to introduce at least one form of maintenance: preventive maintenance, i.e. cyclically recurring maintenance, determined on the basis of an algorithm [191], predictive maintenance, i.e. constant monitoring of equipment and provision of specific maintenance if necessary [192], or corrective maintenance, i.e. a reactive form of maintenance, solving malfunctions [190].

4.2.1.2. Tools for strengthening the technical infrastructure security. One of the important tools for strengthening the critical entities resilience in the field of technical security are *Technical means of protection* [193]. These are security systems, presented by a system of mechanical, electrical or electronic elements that form a permanent barrier preventing the entry/exit of a person or the entry/exit of a means of transport to a protected object or place, which cannot be overcome without expert knowledge or physical strength. Among these means of protection can be classified primarily perimeter protection means (fences, gates, barriers, passive infrared barriers, motion sensors, etc.), which represent means used mainly for perimeter protection [194].

Based on what has been said so far, it is necessary for the critical entity to actively work with tools to determine the current state of the infrastructure's technical security. The following tools can be used for this purpose:

- *Systematic analysis of vulnerability to intrusion – SAVI* [195]. This tool assesses all likely opportunities to breach strategic locations in the infrastructure while creating a list of the most vulnerable paths in terms of likelihood of breach. It also has an extensive database of resources that can be used to maximize infrastructure protection.
- *Design and evaluation of physical protection systems* [196]. This tool evaluates the infrastructure protection system using a quantitative approach, which is mainly used to protect strategic objects, such as nuclear or military facilities.
- *Vega-2* [197]. A software tool that determines the effectiveness of physical protection systems with regard to the nature of the intruder, both external and internal. On the basis of the information obtained, it provides suggestions and also options for possible strengthening of infrastructure protection. It also contains a database of physical barriers and other support elements with the possibility of custom settings.
- *Systematic analysis of physical protection effectiveness – SEPA* [198]. This software tool uses a 2D model of the guarded area combined with a heuristic algorithm to find the most vulnerable locations. This combination significantly increases the sensitivity analysis, through which the most critical points, i.e. the points of possible protection failure, are analysed.

In addition to the technical means mentioned above, it is also advisable to use *Security design proposal* [199]. This tool systematically manages security issues and unifies individual security measures into one comprehensive document, which ensures their interdependence within the entire security system. Within this tool, specific security measures for the threats found are also described. As supporting material for the creation of this security plan can be mentioned Protecting vulnerable targets from terrorist attacks [200] or Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks [201].

Mechanical barriers must always be fully functional. The ideal tool to

ensure these conditions are methodologies that ensure their required optimization and functionality. *Basics of soft targets protection guidelines* [202] adapts the object or territory using a suitable systematic approach to their security. It is based on an anti-terrorist approach, i.e. on knowledge of the attackers' progress, and is therefore primarily focused on preventing violent attacks and limiting their impact.

For complex technical security of the infrastructure, it is recommended to use object protection means. Tools for this area can be classified into surveillance and alarm devices. *Surveillance means* [203] they are a necessary tool for checking the infrastructure and its immediate surroundings. It is mainly about closed-circuit television (CCTV). *Alarm devices* are able to identify and report the emergence of a non-standard situation. These resources include, for example, alarm transmission systems and equipment [204], combined and integrated alarm systems [205], electronic access control systems [206], social alarm systems [207].

In connection with the development of information technologies, cyber security must also be included in the technical security of the infrastructure. Important tools in this area are the NIST Cybersecurity Framework [39], Zero Trust Architecture [208] and cyber security tools. The NIST Cybersecurity Framework presents a set of voluntary guidelines to help organizations assess and improve their ability to prevent, detect and respond to cybersecurity risks. Zero Trust Architecture is a model that approaches the design and implementation of IT systems based on distrust, caution and scepticism. The principle is distrust of all users, devices and services, whether they are outside or inside the network. Other important cyber security tolls are *Anti-virus tools* [209] or exploitation of *Deep learning and machine learning* [210].

The level of cyber security is closely related to *Information security management system* [107]. Through this tool, the required information security can be achieved with the help of best practices, security techniques, setting requirements, in relation to current cyber threats. However, technical standards cannot be relied upon at present. It is advisable to supplement these with other tools that reflect the dynamic development of cyber threats. Among such tools it is possible to include, for example:

- *Cyber resilience framework: Strengthening defences and enhancing continuity in business security* [64]. These tools provide strategies to strengthen defences against cyber threats. Adequate protection of the critical entity is achieved by setting and combining policies, management, cooperation with external stakeholders and continuous monitoring.
- *Cyber resilience assessment tool for industrial control systems – ICS-CRAT* [211]. This qualitative tool uses the R4 resilience framework, as well as metrics from the physical, technical and organizational domains. It represents a high-quality simulation tool with a full-fledged security analysis, even when considering the subjective approach.
- *Cyber resilience self-assessment tool – CR-SAT* [212]. It is a web-based tool developed to systematically operationalize cyber resilience through a continuous improvement process. This tool was primarily developed for small and medium-sized businesses that do not have sufficient funds to provide specialized cyber protection.

4.2.1.3. Tools for strengthening incident detection capability. The distinctiveness of incident detection significantly affects the critical entity resilience and its preparation for an incident. Monitoring enables a critical entity to actively monitor the environment, identify potential threats and opportunities, and quickly respond to changes. The environment can be monitored with the help of *Diagnostic devices* [213], which are able to record changes in the surrounding environment and communicate this information to the user in the form of a notification. These are, for example, sensors, detectors, warning systems or software tools that are able to detect meteorological and geological changes, concentrations and exceeding the limits of monitored substances or radioactivity.

In addition to the above-mentioned devices, which are capable of informing about the current state of the environment in real time, it is advisable to monitor other possible risks in the long term. Tools for territorial risk analysis and mapping can be used to monitor and assess risks in a certain territory [214]. Among the most important monitoring tools are *Territorial vulnerability analysis* [215,216], *Geographic information systems and spatial analysis* [217], and *Multi-risk assessment* [218]. Another important group of tools are methods for cascading impact analysis and assessment, such as Cascading Impact Assessment in a Critical Infrastructure System – *CIA Method* [219], Analyzing Cascading Effects among Critical Infrastructures – *CERBERUS Approach* [220], or Region-Based Cascading Impact Analysis in Critical Infrastructure Systems [221].

Unmanned aerial vehicles are currently increasingly used for monitoring [222], which can be controlled remotely by a human operator from a ground control station or can fly autonomously using an on-board computer. This unmanned aircraft has the required sensors (thermal cameras, hyperspectral and multispectral cameras and distance detection and measurement systems – LIDAR), directly destined for infrastructure monitoring.

The critical entities resilience of is also significantly influenced by the method and time horizon of incident detection. Incidents can be detected using a detection system that uses personnel. In the case of staff cooperation, it is necessary that the critical entity establishes clear reporting procedures that are usable for this method of incident detection. A good example is *Handbook of incident and accident reporting* [223].

Another very sophisticated tool is the *Security incident management system* [224]. That is a system of creating a security team to identify incidents and then eliminate them through innovative procedures. These security teams are often referred to as Security Operations Center (SOC), Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT). To ensure credibility, independent verification or standardization, the international Forum of Incident Response and Security Teams (FIRST) is available, bringing together security teams that have passed the verification process of the organization of the same name, or the organization Trusted Introduce, which is another representative bringing together mainly European security teams.

An incident is not always necessarily detected only by staff. Currently, there are software tools that are capable of independently recognizing dangerous events and recording these fluctuations. One of these tools is *Information technology infrastructure library – ITIL* [225], which, using proven procedures and concepts, describes and directs infrastructure information technology to effectively set processes and prevent incidents, not only in the area of improving the quality of information system service management. ITIL includes, for example, the Service Desk, which is responsible for receiving and classifying incidents, or the Problem Management Process, which manages the life cycle of all incidents.

Incident detection can also be significantly assisted by data from events that have already taken place. For this purpose, it is advisable to use *Specialized shared databases* [226]. These databases contain records of incidents that have taken place, their causes, consequences, and, where appropriate, how the incident was resolved. These are, for example, the Major Accident Reporting System (eMARS), Maper Hazard Incident Data Service (MHIDAS), Analysis, Research and Information on Accidents (ARIA) databases.

4.2.2. Tools for strengthening infrastructural robustness

Another group is represented by tools for strengthening infrastructural robustness. These empowering tools are also defined at the level of parameters (see Table 6).

Resilience of infrastructure robustness is determined by three variables, which are infrastructure physical resistance, response to incidents

Table 6
Tools for strengthening infrastructural robustness.

Variables	Parameters	Strengthening tools
Physical resistance of the infrastructure	Fire resistance	Fire protection
		Fire detection
		Fire safety
		Tools for assessing the fire resilience
		Fire resilient infrastructure constructions and materials
	Seismic resistance	Design of structures for earthquake resistance
		Finite element method
	Explosion resistance	Explosion resistant equipment
		Composite materials
		Strain-hardening cementitious composites
Incident response	Reduction of the consequences of the incident	Automatic systems
		Manual means
	Maintaining the functionality of key technologies	Public-private partnerships
Infrastructure redundancy	Reliability criterion	N-1 criterion
		Critical path method
	Availability of redundant capacity	Availability of parallel components
		Independent redundancy degree
	Temporary substitution of key technologies	Type plan
		Activation plan
		Operational management

and infrastructure redundancy. Tools for strengthening the resilience of these variables are presented in the following text.

4.2.2.1. Tools for strengthening physical resistance of the infrastructure. Strengthening physical resistance of critical infrastructure must be implemented in the context of three key dangers, which are the effects of fire, seismic activity and explosion. Important tools for strengthening the fire resistance of infrastructure include technical standards aimed at *Fire protection* [227], *Fire detection* [228], and *Fire safety* [229]. It is advisable to support the application of these standards with other tools that enable *assessing the fire resilience* [230] or research into new *Fire resilient infrastructure constructions and materials* [231].

When strengthening seismic resistance, it is advisable to start from the technical standard for *Design of structures for earthquake resistance* [232]. This technical standard consists of six parts, which are oriented towards ensuring the required level of resistance of buildings, bridges, silos, tanks, pipelines, towers, masts, and chimneys. Another important tool that can be used in the context of earthquake engineering, is *Finite element method* [233]. It is a numerical method that can be used to simulate the course of stress or deformations, based on the created physical model. This method is mainly used to check already designed devices, namely to identify critical points of the structure.

The last group are tools for strengthening explosion resistance. In the case of strengthening resistance to internal explosions, it is advisable to proceed from the technical standard *Explosion resistant equipment* [234]. This standard sets requirements for blast-resistant constructions that can withstand an internal explosion without bursting and prevent hazardous effects for the environment. It can be used for constructions in which the occurrence of an explosion is assumed to be an exceptional case of loading. When strengthening resistance to external explosions, it is more appropriate to use new *Composite materials* [235] or technology such as *Strain-hardening cementitious composites* [236].

4.2.2.2. Tools for strengthening incident response. Another important area for strengthening infrastructural robustness is incident response. In this area, robustness can be strengthened through tools related to reducing the consequences of an incident and maintaining the functionality of key technologies. Two categories of tools can be used to reduce the consequences of an incident and prevent major infrastructure damage, namely automatic systems and manual means. *Automatic systems* can be used in almost all areas of infrastructure protection, e.g. fire protection, physical security, prevention of serious accidents [237]. A significant advantage of these automatic systems lies in their independence, the so-called self-detection and measurement of the values of the monitored quantity or device according to predefined conditions. This is status monitoring with a retrospective check and assessment of whether the monitored device is capable of operation. In the case of *Manual means*, the actual control functions/operations are performed only by personnel [238]. For example, these can be pressure relief valves or collection sumps.

Maintaining the functionality of key technologies is also important in incident response. This is mainly the implementation of key technology repairs during an incident or crisis situation. The functionality of these key technologies can be maintained either by own forces and means (this requires financial reserves, availability of spare parts and human resources with technical expertise) or in the form of *Public-private partnerships* [239]. The advantage of PPP is primarily the more efficient allocation of public funds and the provision of quality services in the required time, expertise and material availability.

4.2.2.3. Tools for strengthening infrastructure redundancy. The last area for strengthening infrastructure robustness is infrastructure redundancy. In this area, robustness can be strengthened through reliability criteria, availability of redundant capacity and temporary substitution of key technologies. An important tool for strengthening the reliability criterion is the provision of infrastructure redundancy on principle *N-1 criterion* [240]. Criterion N-1 states that a system that is able to withstand an unexpected failure or failure of one system component at any time has an acceptable level of reliability.

Another important tool is *Critical path method* [241]. These are the basic deterministic methods of network analysis. The goal of this method is to determine the duration of a certain process, based on the length of the so-called critical path, which represents a series of interdependent activities with the smallest time reserve. The critical entity can then focus on those activities that are crucial for the reliability of the supply of the basic service.

Reinforcing the availability of redundant capacity should be primarily based on the *Availability of parallel components* [242], especially in the case of key infrastructure components. In the event of failure of one component, it is desirable to automatically replace it with a redundant component and ensure continuity without the need for a significant reduction in the provision of the basic service.

The availability of redundant infrastructure capacity can be assessed using the *Independent redundancy degree* tool [243]. It is a methodology for assessment system redundancy, specifically quantifying independent redundancy in complex systems. This approach considers the interactions between different factors that influence redundancy, treating different factors as distinct dimensions to comprehensively account for all potential impact factors.

The final area for strengthening infrastructure redundancy is the temporary substitution of key technologies. To successfully ensure temporary substitution, the *Type plan*, activation plan and operational management are the necessary tools [244]. A type plan provides recommended type procedures, policies and measures for handling a specific type of crisis situation. An *Activation plan* is a set of procedures or regulations that determine which components and in what order will be activated for immediate substitution needs. *Operational management* ensures a specific layout of the time requirement and provision of resources for the temporary substitution of key technologies in the very short term.

4.2.3. Tools for strengthening infrastructural recoverability

The last group of instruments related to infrastructural resilience are instruments for strengthening infrastructural recoverability. The presentation of these tools in the context of parameters is made in Table 7.

The resilience of infrastructural recoverability is determined by material resources. Tools for strengthening the resilience of this variable are classified into four areas. The first area is the ability to recover infrastructure function. In this area, it is appropriate to apply *Analytical modelling tools*. The use of analytical models and algorithms can be used to predict infrastructure recovery based on knowledge of its construction, materials and operating conditions, i.e. the time and conditions under which the infrastructure will recover can be estimated. An example would be the SimulationXpress tool [245], from which it is possible to obtain information about the critical points of the infrastructure from a material point of view, including the creation of a model of the expected deformation.

Analysis and simulation tools can be further used to enhance the recovery capability of the infrastructure function. The importance of these tools lies mainly in saving costs in the stage of development and introduction of production, when it is relatively easy to test the behaviour of virtual models at the level of parts, assemblies and entire technological units. Thanks to the graphical display of the results, critical points can be quickly evaluated and, after adjusting the virtual models, you can then proceed to recovery the function of the critical infrastructure [246].

The second area for strengthening infrastructural recoverability is the repairability of key infrastructure technologies. Core tools in this area are repairability scenario building tools. For this purpose it can serve, for example, *CAD simulation and analysis* [247], which enables the creation of a 3D model of a key infrastructure element and the subsequent simulation of its repairs. This procedure allows visualization of a potential repair problem and analysis of repair options.

Another suitable tool is *Finite element analysis* [248], which serves to simulate the mechanical properties of a key infrastructure element and predict its behaviour during various repair procedures. It makes it possible to assess, for example, the strength, flexibility and stability of the element after repair. FEA is a computer method for predicting how a product will respond to real-world forces, vibrations, heat, fluid flow, and other physical influences. The results of this analysis provide information on whether the product will break, wear out, or perform as designed.

The last tool suitable for analysing the repairability of key infrastructure technologies is *Monte Carlo* [249]. This simulation allows estimating the probability of success of different repair scenarios depending on various variables, such as cost or availability of resources.

The third area for strengthening infrastructural recoverability is the substitutability of key infrastructure technologies [250]. An important tool in this area is the *Emergency shutdown plan*. If an incident occurs, it is important that key technologies are shut down according to predetermined rules to avoid unintentional damage. In this plan, it must be clearly established which technologies and under which conditions can be shut down for the necessary period of time and which must be kept in operation. A follow-up tool is the *Key technology replacement plan*, which sets out the technological procedure for the exchange of key parts of the infrastructure.

The last area for strengthening infrastructural recoverability is the time availability of spare parts and the horizon of repairs. A key tool in this area is the *Spare parts inventory strategy* [251]. The essence of this strategy is to achieve a balance between minimizing stocks and minimizing the risk of their unavailability. Another important tool is the *Infrastructure repair plan*, which can be processed, for example, using dynamically updated damage estimates for optimal repair planning [252].

Table 7
Tools for strengthening infrastructural recoverability.

Variables	Parameters	Strengthening tools
Material resources	Ability to recover infrastructure function	Analytical modelling tools Analysis and simulation tools
	Repairability of key infrastructure technologies	CAD simulation and analysis Finite element analysis Monte Carlo
	Substitutability of key infrastructure technologies	Emergency shutdown plan Key technology replacement plan
	Time availability of spare parts and repair horizon	Spare parts inventory strategy Infrastructure repair plan

4.3. The process of strengthening the critical entities internal resilience

Based on the classification and definition of tools for strengthening entity and infrastructure resilience, it is possible to move on to defining the application procedure of these tools in order to strengthen the critical entities internal resilience. Methodologically, this procedure follows the CERA method [5], which it hereby extends by another four steps (see Fig. 3).

The essence of the first five steps of the CERA method is the procedure for assessing the resilience of critical entities to small-scale disasters. The essence of this procedure is a semi-quantitative assessment of the individual components determining the critical entities resilience, i.e. resistance, robustness, recoverability and adaptability. The result of this assessment is the identification of components that achieve low, insufficient or critical levels of resilience. It is then necessary to strengthen the resilience of these components at the measurable items level.

In the following part of the text, a detailed description of the steps 6–8, which present the procedure of strengthening the critical entities resilience to small-scale disasters is provided. This description is processed in the form of a case study of a terrorist attack on a transformer station and follows on from a case study of assessing the critical entities resilience against small-scale disasters [5]. The scenario of this case study was developed using the Event Tree Analysis method [253], which allows the analysis of events and consequences leading to the emergence of a small-scale disaster. The defined scenario predicts a terrorist attack on the specially protected workplace area of an electricity substation, as a result of which the serviceability of this area will be reduced, but key technologies will not be affected. Due to the possibility of remote management, the availability of operation control is reduced, but the functionality of the transformer station is ensured.

Step 6: Selecting a specific parameter

The selection of a specific parameter is implemented based on the requirements for strengthening resilience, which were determined by the CERA method in Step 5 [5]. Primarily, attention should be paid to all items that were not included in the assessment as part of the identification of parameters and assessment of their level (see Step 3). For these parameters, the reason for their non-inclusion should be determined, and if it is possible to take corrective action by implementing one of the strengthening tools, then it is appropriate to proceed to the next step (Step 7). A similar procedure should also be applied in the case of parameters whose resilience level has been assessed with a value of 1 or 2. 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 [254].

In the context of the case study presented in the previous article [5] three parameters have been selected within the Resistance component for which it is necessary to strengthen their resilience:

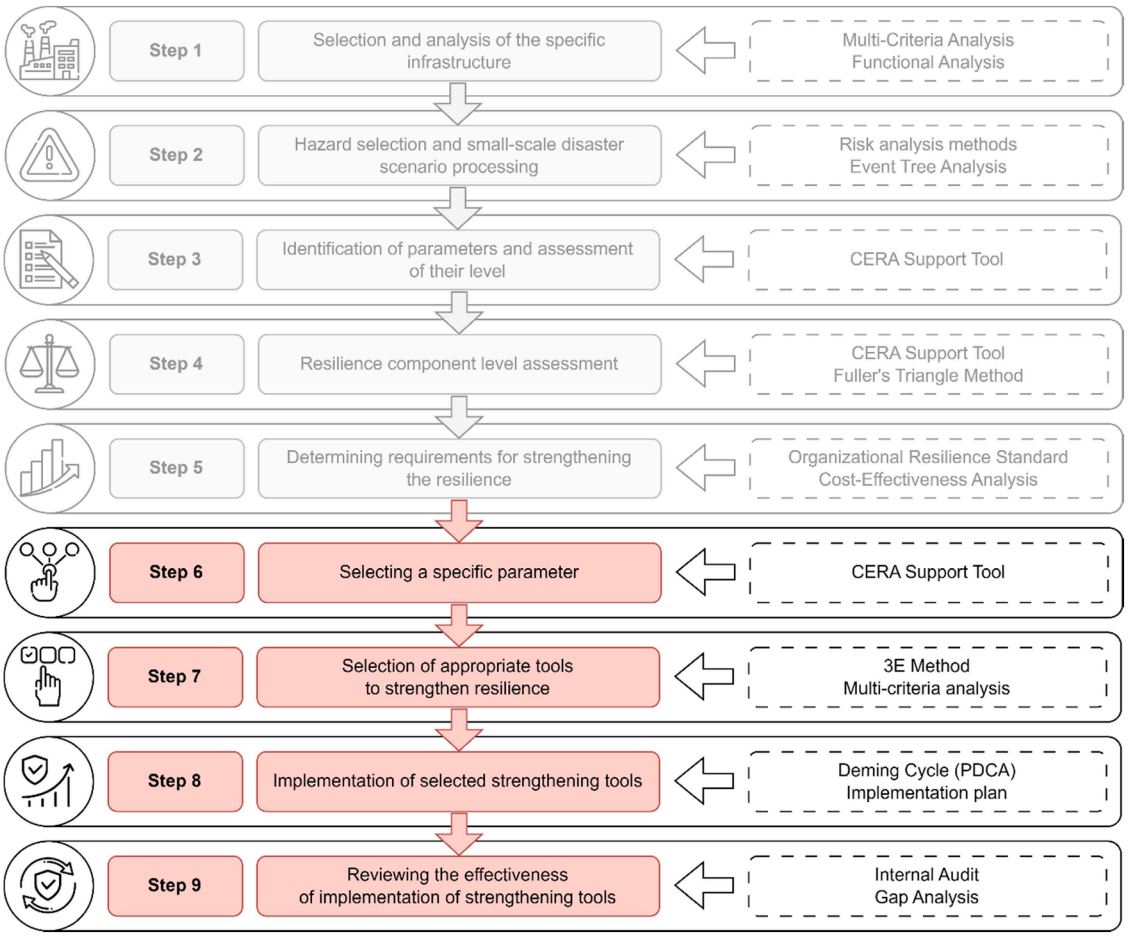


Fig. 3. Procedure for strengthening the critical entities internal resilience (extension of the CERA method).

- *Indicating disruption of critical entity resilience* (assessment level 0) – this parameter was selected because it was not included in the assessment because this activity is not implemented by the critical entity;
- *Incident modelling* (assessment level 2) – this parameter was selected because the critical entity implements only the minimum range of activities/measures defined by this parameter;
- *Continuity planning* (assessment level 2) – this parameter was selected because the critical entity implements only the minimum range of activities/measures defined by this parameter.

Step 7: Selection of appropriate tools to strengthen resilience

At the moment when specific parameters are selected by the evaluator, for which it is required to strengthen their resilience, it is possible to move on to the selection of appropriate tools. For this purpose, the authors primarily recommend method 3E [255], where the criteria are clearly defined, i.e. Economy, Efficiency, Effectiveness. If the evaluator does not meet these criteria, he can use Multicriteria Analysis [256], where he set his own criteria.

In the case of the application of the 3E method, the tools for strengthening the resilience of selected parameters are assessed from the point of view of their economy, efficiency and effectiveness. Economy considers the minimization of the costs of the critical entity resources (i.e. financial, human, material) while maintaining the required quality of resources and the expected result, i.e. strengthening the resilience of the parameter to the required level. Efficiency considers the optimization of the use of resources to achieve the expected result. In contrast, effectiveness considers the maximization of the level of the achieved result when allocating resources of the same quantity and quality.

An example of selecting a suitable tool for strengthening resilience using the 3E method is presented on the parameter "Indicating disruption of critical entity resilience" (see Fig. 4). In this case, indicating a violation of the critical entity resilience can be realized using five appropriate tools, which are Protective Measures Index (PMI), Vulnerability Index (V-index), Resilience Measurement Index (RMI), Strategic Tensions Assessment Tool (STAT), and Critical Entities Resilience Failure Indication (CERFI Tool). A description of these tools is provided in Section 4.1.1. of this article.

From the assessment presented above, it is evident that the most appropriate tool for strengthening the resilience of the parameter "Indicating disruption of critical entity resilience" is the Critical Entities Resilience Failure Indication (CERFI Tool) [6]. This tool achieves the highest level of economy (it is a freely available tool; the personnel and time requirements are minimal), a very high level of effectiveness (it is an intuitive tool designed directly for the self-assessment of disruption of critical entity resilience) and a very high level of expected resilience (the result of the assessment is immediately indicated potential disruptions of the critical entity resilience, which can be immediately minimized).

Step 8: Implementation of selected strengthening tools

Once appropriate tools have been selected to strengthen the resilience of parameters, it is necessary to implement them. The implementation process should generally fulfil the essence of the Deming cycle [257]. For this purpose, it is advisable to prepare an implementation plan, which should include a set of activities aimed at effectively and systematically applying the selected tools at the required time

The name of the parameter:	*Indicating disruption of critical entity resilience*				
Current level of resilience:	*0 (this parameter was not included in the assessment)*				
Evaluation criteria	**Strengthening tools**				
	PMI	**V-index**	**RMI**	**STAT**	**CERFI**
Economy (the cost of resource)	200 €	200 €	200 €	1 000 €	200 €
Efficiency (optimizing the use of resources)	40%	40%	60%	90%	100%
Effectiveness (expected level of resilience)	3	2	4	5	5
Ranking	**4**	**5**	**3**	**2**	**1**

Fig. 4. Selection of a tool suitable for strengthening the resilience of the parameter "Indicating disruption of critical entity resilience".

(see Fig. 5).

The first step in the process of implementing the strengthening tools is the publication of an internal document (policy, regulation, regulation) that will contain all the information necessary to implement the tools into the processes and resources of the critical entity. Furthermore, it is necessary to determine and inform responsible persons about the changes that will be made. Subsequently, the phase of the actual application of the strengthening tools can be started, which will be continuously monitored and, in case of deficiencies, will be adapted to the current conditions. If the conditions are updated during the implementation process, it is necessary to revise and re-implement the phase of application of strengthening tools.

In the case of the implementation of the selected tool to strengthen the resilience of the parameter "Indicating disruption of critical entity resilience", the procedure is carried out in accordance with the process presented above, in the following steps:

- an internal directive is issued by the critical entity director establishing the implementation procedure of the CERFI Tool in order to strengthen the critical entity resilience;
- in this directive 1) the specific processes to which the implementation is concerned are defined, 2) the responsible persons are determined, i.e. the Critical Entity's Security Liaison Officer and the administrators of individual processes, and 3) the amount of financial resources allocated for the implementation is determined;
- the application of the CERFI Tool to selected processes is implemented according to the procedure that is part of this tool, and is continuously monitored and coordinated by the Security Liaison Officer at all times;
- after the end of the CERFI Tool application, their monitoring is continued for the affected processes, which consists, among other things, in a time-graded reassessment of the critical entity resilience;
- in case the new resilience values do not reach the expected level, it is advisable to update the application of the strengthening tool, e.g. by choosing another suitable tool.

Step 9: Reviewing the effectiveness of implementation of strengthening tools

The final step in the resilience-building process is to review the effectiveness of the implementation of strengthening tools. Assessment of their effectiveness can be done based on the results of a critical entity internal audit [131]. An example can be a reference model for auditing organizational resilience [258]. However, for a more detailed review of effectiveness, it is advisable to apply the Gap Analysis method based on the results of the internal audit [259]. The essence of this method is the comparison of the required/planned level of critical entity resilience with the actual state.

In the case of the implementation of the CERFI Tool to strengthen the resilience of the parameter "Indicating disruption of critical entity resilience", it is sufficient to review the effectiveness of this implementation through an internal audit. As part of this review, attention should be paid in particular to the applicability of the newly defined indicators and the analysis of the indicated critical points of failure of the critical entity resilience.

The result of the assessment of the effectiveness of the implementation of strengthening tools can be, for example, a comparison table that provides an overall picture of the fulfilment of the expected benefit. If these expectations are not fulfilled, the process of strengthening the critical entity resilience becomes insufficient. In such a case, it is advisable to reassess the level of resilience components (see Step 4 of the CERA method), identify parameters with an insufficient level of resilience (see Step 5 of the CERA method) and repeat the process of strengthening the critical entity resilience (see Steps 6–9 of the CERA method). With this step, the entire process of strengthening the critical entities resilience against small-scale disasters is concluded.

4.4. *Summary – pros and cons*

The main part of the article presents a total of 161 tools suitable for strengthening the critical entities resilience to small-scale disasters. The following text is focused on defining their benefits, but also on the limitations that limit their implementation. Attention is paid in particular to the assessment of the financial requirements, knowledge and process requirements for implementation and operation, effectiveness, sustainability and, last but not least, the potential of these tools.

The main benefits of these tools include the fact that most of these tools are publicly available, thereby minimizing the acquisition costs for critical entities. The exceptions are various software solutions used for risk management, such as Enterprise Risk Management Tools, incident

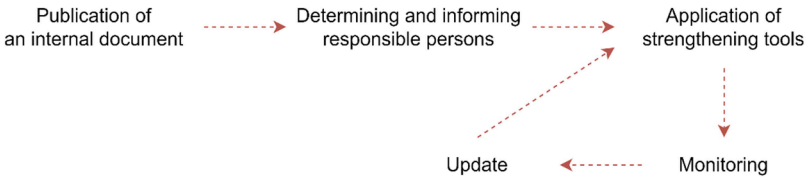


Fig. 5. The process of implementing tools to strengthen the resilience of parameters (created by [107]).

modelling, i.e. FLACS-CFD explosion, fire & dispersion modelling software, or financial software tools for expense automation, such as Zoho Expense, Rydoo, Emburse Certify, Expensify, Everlance. In addition, other necessary expenses can be considered, for example, the costs of implementing smart or unmanned systems or artificial intelligence, which represent significant investments in existing systems. Another financial burden can be seen in the implementation of simulation models, such as SimMan, digital twins, virtual or augmented reality, or the use of CAD Simulation and Analysis. It should also be mentioned that operating costs reach a standard level and are mainly related to personnel costs. Other not very high costs may be related, for example, to professional training or the purchase of support services. However, these costs may be partially offset by income from grant projects or subsidy programs.

A significant limitation in the implementation and operation of these tools is the knowledge and process complexity. Most tools require special professional knowledge or directly professional competence, which requires either long-term training of internal employees or the purchase of experts from the external environment. Specifically, these are tools focused on physical security, such as Security, unarmed or armed security guards, Guard Dog Security, and Video Surveillance Operators. The demands for increased knowledge of personnel also require tools that are associated with the so-called integrated management system, i.e. a combination of Quality management system, Environmental management system, and Occupational health and safety management system. Considerable knowledge and process complexity is also required in the case of a security incident management system. If special teams (SOC, CERT, CSIRT) are created or security documentation is created and subsequently managed (critical entity crisis preparedness plan, internal emergency plan, business continuity management system), it is essential that the responsible persons have the required expertise. Extended knowledge competencies are also required for the application of tools supporting investment in innovation, in particular financial and investment planning and financial control tools. These tools require an advanced level of expertise and knowledge. In contrast, professional competence is required for tools that are associated with the critical infrastructure resistance strengthening, i.e. securing the infrastructure against the three key hazards, i.e. against the effects of fire, seismic activity and explosion. Professional competence is also required when using unmanned systems. Here, it is a legal obligation for users of these systems to pass the appropriate tests and thus obtain the required authorization to use them.

Attention must also be paid to the assessment of the presented tools effectiveness. In the context of the previous two aspects, this is the most demanding phase of the assessment, because the resulting values may be considered to some extent subjective by some critical entities. The most appropriate way to assess the effectiveness of the applied tools is a comparative assessment of the critical entity internal resilience. The essence of this approach is to compare the resilience levels before and after the application of specific tools. The resilience assessment must always be carried out using the same method, and the resulting value can be further confronted with the amount of costs spent on the application of the tools. A significant limitation of this approach is the fact that only a limited number of methods are currently available for assessing the critical entities resilience.

For the effective use of tools, their long-term sustainability based on the flexibility of these tools is also important. Ensuring this sustainability is not easy, as it requires constant adaptation to dynamic changes in various areas, e.g. market changes, technological progress or changes in legislation. The flexibility of the tools therefore represents a certain limitation in their implementation. Based on this fact, the authors recommend primarily using the 3E method, through which long-term sustainability can be ensured to a certain extent. If any tool is to be truly sustainable in the long term, it is necessary to take these tools into account in the long-term budget, i.e. the tools should be part of the financial plan, require reviewing the functionality of the tools and, of course, setting up a feedback system.

The final topic of the summary is undoubtedly the assessment of the application tools potential. Primarily, these tools are intended to strengthen the critical entities resilience against small-scale disasters. However, it is necessary to point out that their secondary benefit should also be seen in strengthening the reliability and quality of the basic services provided. The implementation of tools contributes to the optimization of management processes and the effective allocation of resources. Critical entities thus strengthen not only the internal resilience, but also the microenvironment of the organization.

5. Conclusion

At the end of 2022, a new approach to the protection of critical infrastructure was adopted in the countries of the European Union, which is based on the critical entities' resilience. The essence of this approach is to strengthen resilience not only in the area of critical infrastructures, but also of critical entities that are their owners or operators. As a result of this change, it is therefore necessary to pay attention to strengthening resilience not only in the technical area, but also in managerial, process and resource areas. Based on these facts, 161 tools suitable for strengthening the critical entities internal resilience against small-scale disasters were classified and defined in this article.

Based on their nature, these strengthening tools are broadly classified according to their applicability to strengthen subject or infrastructure resilience in the context of individual components, i.e. resistance, robustness, recoverability and adaptability. In this context, the article defined the environment and procedure for strengthening the critical entities internal resilience. This procedure extends the application of the existing CERA method, which was originally designed for the purpose of assessing the critical entities resilience to small-scale disasters. An example of a practical application of the proposed procedure is presented at design part of the article.

The strengthening tools, as well as the procedure for their selection and implementation, are applicable to all critical entities providing essential services in technically oriented sectors. In the case of application to critical entities providing essential services in socio-economically oriented sectors, the tools strengthening entity resilience could be fully utilized. Tools designed to strengthen infrastructural resilience would have to be modified according to the specifics of individual socio-economic sectors. The process of strengthening resilience, as well as the possible modification of strengthening tools, should always be implemented in the presence of the Security Liaison Officer.

In conclusion, it should be noted that follow-up research should be focused primarily on detailed elaboration of the cyber dimension of the critical entity resilience system, including tools for strengthening the critical entities resilience within this dimension. Attention should also be paid to assessing the effectiveness of individual tools in strengthening the critical entity resilience as a whole. More attention should also be paid to tools for strengthening the critical entities resilience providing essential services in socio-economically oriented sectors.

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 SP2025/088].

CRediT authorship contribution statement

David Rehak: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Alena Splichalova:** Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Methodology, Formal analysis, Conceptualization. **Heidi Janeckova:** Writing – review & editing,

Writing – original draft, Resources, Investigation, Formal analysis, Data curation. **Ondrej Ryska:** Writing – review & editing, Writing – original draft, Resources, Investigation, Formal analysis, Data curation. **Alena Oulehlova:** Writing – review & editing, Writing – original draft, Validation, Investigation, Formal analysis, Data curation. **Lenka Michalcova:** Writing – review & editing, Writing – original draft, Validation, Investigation, Formal analysis, Data curation. **Martin Hromada:** Writing – review & editing, Writing – original draft, Validation, Methodology, Conceptualization. **Miltiadis Kontogeorgos:** Writing – review & editing, Writing – original draft. **Jozef Ristvej:** Writing – review & editing, Writing – original draft, 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 was provided by Ministry of the Interior of the Czech Republic. Ondrej Ryska reports financial support was provided by VSB-Technical University of Ostrava Faculty of Safety Engineering. Co-author (D.R.) is associate editor in the International Journal of Critical Infrastructure Protection. 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

No data was used for the research described in the article.

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] M. Bogalecka, K. Kołowrocki, Integrated model of critical infrastructure accident consequences, J. Polish Safety Reliabil. Assoc. 8 (2017) 43–52.

[3] UNDRR, Disaster Risk Reduction Terminology, United Nations Office for Disaster Risk Reduction, Geneva, 2017.

[4] IFRC, World Disasters Report 2022, International Federation of Red Cross and Red Crescent Societies, Geneva, 2023.

[5] D. Rehak, A. Splichalova, H. Janeckova, A. Oulehlova, M. Hromada, M. Kontogeorgos, J. Ristvej, Critical entities resilience assessment (CERA) to small-scale disasters, Int. J. Disaster Risk Reduct. 111 (2024) 104748, https://doi.org/10.1016/j.ijdrr.2024.104748.

[6] 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.

[7] M. Hromada, D. Rehak, C. Fuggini, N. Walker, External resilience assessment of energy critical infrastructures, in: D. Borge-Diez, E. Rosales-Asensio (Eds.), Energy Systems Resilience and Distributed Generation, Springer, Cham, 2024, pp. 109–142, https://doi.org/10.1007/978-3-031-67754-0_4.

[8] Strengthening Climate Resilience, Organisation for Economic Co-operation and Development, 2024. https://www.oecd.org/development/climate-resilience/ (accessed 29 September 2024).

[9] Global Resilience Forum: Strengthening Resilience for a Changing Climate, United Nations Office for Disaster Risk Reduction, 2023. https://www.undrr.org/event/global-resilience-forum-strengthening-resilience-changing-climate (accessed 29 September 2024).

[10] Strengthening Health Resilience to Climate Change, World Health Organization, 2015. https://www.afro.who.int/publications/strengthening-health-resilience-climate-change (accessed 29 September 2024).

[11] FMIC, German Strategy for Strengthening Resilience to Disasters, Federal Ministry of the Interior and Community, Berlin, 2022.

[12] United Nations Development Programme, Strengthening Resilience to Natural Disasters in Ukraine. https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Strengthening-resilience-to-natural-disasters.pdf, 2022 (accessed 1 October 2024).

[13] IDRC, Strengthening resilience in post-disaster situations, International Development Research Centre, Ottawa, 2011.

[14] Commonwealth Scholarship Commission in the United Kingdom, Strengthening Resilience and Response to Crises, 2024. https://cscuk.fcdo.gov.uk/dt-category/strengthening-resilience-and-response-to-crises/ (accessed 1 October 2024).

[15] K. Knodt, A. Stöckl, F. Steinke, M. Pietsch, G. Hornung, J.P. Stroscher, Power Blackout, Citizens' Contribution to strengthen urban resilience, Energy Policy 174 (2023) 113433, https://doi.org/10.1016/j.enpol.2023.113433.

[16] S.M.H.S. Rezvani, M.J.F. Silva, N.M. de Almeida, Urban resilience index for critical infrastructure: a scenario-based approach to disaster risk reduction in road networks, Sustainability. 16 (2024) 4143, https://doi.org/10.3390/su16104143.

[17] UN, Transforming our World: The 2030 Agenda for Sustainable Development, United Nations, New York, NY, 2015.

[18] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley, Hoboken, NJ, 2006.

[19] J. Lopez, R. Setola, S. Wolthusen, Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, Springer, Berlin, 2012, https://doi.org/10.1007/978-3-642-28920-0.

[20] G. Stergiopoulos, E. Vasilellis, G. Lykou, P. Kotzanikolaou, D. Gritzalis, Classification and comparison of critical infrastructure protection tools, in: M. Rice, S. Shenoi (Eds.), Critical Infrastructure Protection X. ICCIP 2016. IFIP Advances in Information and Communication Technology, Critical Infrastructure Protection X. ICCIP 2016. IFIP Advances in Information and Communication Technology, 485, Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-48737-3_14.

[21] L. Kruszka, M. Klosak, P. Muzolf, Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection, IOS Press, Amsterdam, 2019.

[22] T. Lovecek, L. Strakova, K. Kampova, Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens, Sustainability. 13 (2021) 5898, https://doi.org/10.3390/su13115898.

[23] R. Setola, E. Luiijf, M. Theocharidou, Critical infrastructures, protection and resilience, in: R. Setola, V. Rosato, E. Kyriakides, E. Rome (Eds.), Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, 90, Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-51043-9_1.

[24] F. Petit, D. Verner, J. Phillips, L.P. Lewis, Critical Infrastructure protection and Resilience: integrating interdependencies, in: A. Masys (Ed.), Security by Design. Advanced Sciences and Technologies for Security Applications, Springer, Cham, 2018, https://doi.org/10.1007/978-3-319-78021-4_10.

[25] Ch. Pursiainen, Critical infrastructure resilience: a nordic model in the making? Int. J. Disaster Risk Reduct. 27 (2018) 632–641, https://doi.org/10.1016/j.ijdrr.2017.08.006.

[26] D. Rehak, P. Senovsky, S. Slivkova, Resilience of critical infrastructure elements and its main factors, Systems. (Basel) 6 (2018) 21, https://doi.org/10.3390/systems6020021.

[27] D. Gritzalis, M. Theocharidou, G. Stergiopoulos, Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies, Springer, Cham, 2019, https://doi.org/10.1007/978-3-030-00024-0.

[28] B. Rød, D. Lange, M. Theocharidou, Ch. Pursiainen, From risk management to resilience management in critical infrastructure, J. Manag. Eng. 36 (2020), https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795.

[29] S. Mohrle, S.S. Ottenburger, T.O. Muller, D. Trybushnyi, E. Deines, W. Raskob, Strengthening resilience in critical infrastructure systems: a deep learning approach for smart early warning of critical states, in: B. Castanier, M. Cepin, D. Bigaud, C. Berenguer (Eds.), Proceedings of the 31st European Safety and Reliability Conference (ESREL), Angers, France, 2021, pp. 1894–1901, https://doi.org/10.3850/978-981-18-2016-8_239-cd, 19-23 September 2021.

[30] D. Rehak, S. Slivkova, H. Janeckova, D. Stuberova, M. Hromada, Strengthening resilience in the energy critical infrastructure: methodological overview, Energies. (Basel) 15 (2022) 5276, https://doi.org/10.3390/en15145276.

[31] B. Rathnayaka, Ch. Siriwardana, D. Robert, D. Amaratunga, S. Setunge, Improving the resilience of critical infrastructures: evidence-based insights from a systematic literature review, Int. J. Disaster Risk Reduct. 78 (2022) 103123, https://doi.org/10.1016/j.ijdrr.2022.103123.

[32] C. Pursiainen, E. Kytomaa, From European critical infrastructure protection to the resilience of European critical entities: what does it mean? Sustain. Resilient. Infrastruct. 8 (2022) 85–101, https://doi.org/10.1080/23789689.2022.2128562.

[33] ASIS, Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use, American National Standards Institute, Washington, DC, 2009.

[34] D. Denyer, Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking, BSI and Cranfield School of Management, Cranfield, 2017.

[35] J. Tasic, S. Amir, J. Tan, M. Khader, A multilevel framework to enhance organizational resilience, J. Risk. Res. 23 (2019) 713–738, https://doi.org/10.1080/13669877.2019.1617340.

[36] B. Walker, V. Nilakant, K. Heugten, J. Kuntz, S. Malinen, K. Naswall, Becoming Agile: A Guide to Building Adaptive Resilience, The University of Canterbury, Christchurch, 2019.

[37] S. Duchek, Organizational resilience: a capability-based conceptualization, Bus. Res. 13 (2020) 215–246, https://doi.org/10.1007/s40685-019-0085-7.

[38] The International Consortium for Organizational Resilience, Organizational Resilience Framework, 2023. https://www.build-resilience.org/organizational-resilience-framework.php (accessed 5 October 2024).

[39] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024, https://doi.org/10.6028/NIST.CSWP.29.

[40] A. Backlund, The Definition of System, Kybernetes 29 (2000) 444–451, https://doi.org/10.1108/03684920010322055.

[41] V. Panevski, L. Nedelchev, Increasing the resilience of critical entities in response to the dynamic spectrum of threats, Innovations 11 (2023) 79–82.

[42] Z. Dvorak, Strengthening the resilience of critical subjects, with a focus on transport and health, Mechanics Transport Communications 21 (2023) 2440.
[43] H. Janeckova, The basis for strengthening organisational resilience of critical transport infrastructure entities, Transport. Res. Proc. 74 (2023) 1300–1307, https://doi.org/10.1016/j.trpro.2023.11.275.
[44] L. Xing, Y. Fang, E. Zio, A hierarchical Resilience Enhancement framework for interdependent critical infrastructures, Reliab. Eng. Syst. Saf. 215 (2021) 107868, https://doi.org/10.1016/j.ress.2021.107868.
[45] A. Tomalska, Preparing critical infrastructure for the future: lessons learnt from the Covid-19 pandemic, Secur. Defence Quarterly 39 (2022) 21–32, https://doi.org/10.35467/sdq/146603.
[46] B. Adini, O. Cohen, A.W. Eide, S. Nilsson, L. Aharonson-Daniel, I.A. Herrera, Striving to Be resilient: what concepts, approaches and practices should Be incorporated in resilience management guidelines? Technol. Forecast. Soc. Change 121 (2017) 39–49, https://doi.org/10.1016/j.techfore.2017.01.020.
[47] D. Lichte, F.S. Torres, E. Engler, Framework for operational resilience management of critical infrastructures and organizations, Infrastructures. (Basel) 7 (2022) 70, https://doi.org/10.3390/infrastructures7050070.
[48] Operational Risk: Sound Practices to Strengthen Operational Resilience, Office of the Comptroller of the Currency, 2020. https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf (accessed 25 October 2024).
[49] Enhancing Canada's Critical Infrastructure Resilience to Insider Risk, Critical Infrastructure Directorate, 2019. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf (accessed 25 October 2024).
[50] ISO 31000, Risk Management, International Organization for Standardization, Geneva, 2018.
[51] ISO 28000, Security and Resilience — Security Management Systems — Requirements, International Organization for Standardization, Geneva, 2022.
[52] ISO 22316, Security and Resilience — Organizational Resilience — Principles and Attributes, International Organization for Standardization, Geneva, 2017.
[53] Compliance Risk Management: Applying the COSO ERM Framework, Society of Corporate Compliance and Ethics & Health Care Compliance Association, 2020. https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf (accessed 27 October 2024).
[54] ISO/TS 31050, Risk Management — Guidelines for Managing an Emerging Risk to Enhance Resilience, International Organization for Standardization, Geneva, 2023.
[55] ISO 9001, Quality Management Systems — Requirements, International Organization for Standardization, Geneva, 2015.
[56] Organisational Resilience: Practitioner Guide for NSW Public Sector Organisations, New South Wales Treasury, 2018. https://www.treasury.nsw.gov.au/sites/default/files/2018-09/TPP18-07%20Organisational%20Resilience%20-%20Practitioner%20guide%20for%20NSW%20Public%20Sector%20Organisations%20-pdf.pdf (accessed 27 October 2024).
[57] J. Marquez-Tejon, M. Jimenez-Partearroyo, D. Benito-Osorio, Organisational Resilience management model: A case study of joint stock companies operating in Spain, Int. Entrepreneur. Manag. J. 20 (2024) 1907–1934, https://doi.org/10.1007/s11365-024-00967-5.
[58] T. Gerginova, Building resilience – the NATO and European Union approach to Building resilience, in: International Scientific Conference the Strategic and Security Concept for the Countries of Southeast Europe, Struga, North Macedonia, 2023, pp. 27–40, https://doi.org/10.20544/ICP.8.1.23.P03, 27-29 September 2023.
[59] Resilience, Civil Preparedness and Article 3, North Atlantic Treaty Organization, 2023. https://www.nato.int/cps/en/natohq/topics_132722.htm#resilience (accessed 1 November 2024).
[60] A. Hansson, Effects of prolonged electricity supply disruptions on critical entities. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9125603&fileOId=9125617, 2023 (accessed 4 November 2024).
[61] V. Panevski, Organizational resilience and critical infrastructure Security systems, Security Future 7 (2023) 3–5.
[62] 2021-2023 Action Plan for Critical Infrastructure, Minister of Public Safety and Emergency Preparedness, 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf (accessed 4 November 2024).
[63] National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience, Cybersecurity and Infrastructure Security Agency, 2013. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf (Accessed 5 November 2024).
[64] A. Al-Hawamleh, Cyber Resilience Framework: strengthening defenses and enhancing continuity in business security, Int. J. Comput. Digital Syst. 15 (2024) 1315–1331, https://doi.org/10.12785/ijcds/150193.
[65] Interministerial Reference Document on the National Resilience Strategy in the Field of Defence and National Security: "Collective, Solid, Long-Term Resilience in the Face of a Crisis, General Secretariat for Defence and National Security, 2022. https://www.sgdsn.gouv.fr/files/files/3.%2020220315_NP_Document%20cadre_SNR_vf_EN_0.pdf (accessed 6 November 2024).
[66] R. Ranucci, S. Wang, Resilience in, Top management teams: responding to crisis by focusing on the future, Long. Range Plann. 57 (2024) 102268, https://doi.org/10.1016/j.lrp.2022.102268.
[67] V. Zemba, E.M. Wells, M.D. Wood, B.D. Trump, B. Boyle, S. Blue, C. Cato, I. Linkov, Defining, measuring, and enhancing resilience for small groups, Saf. Sci. 120 (2019) 603–616, https://doi.org/10.1016/j.ssci.2019.07.042.
[68] A.W. Righi, T.A. Saurin, P. Wachs, A Systematic Literature Review of Resilience Engineering: research areas and a research agenda proposal, Reliab. Eng. Syst. Saf. 141 (2015) 142–152, https://doi.org/10.1016/j.ress.2015.03.007.
[69] R. Bawantha, Ch. Siriwardana, D. Robert, A. Amaratunga, S. Setunge, Improving the resilience of critical infrastructures: evidence-based insights from a systematic literature review, Int. J. Disaster Risk Reduct. 78 (2022) 103123, https://doi.org/10.1016/j.ijdrr.2022.103123.
[70] J. Bergström, N. Dahlström, S. Dekker, K. Petersen, Training organisational resilience in escalating situations. Resilience Engineering in Practice, CRC Press, Boca Raton, FL, 2011, https://doi.org/10.1201/9781317065265.
[71] J. Lundberg, A. Rankin, Resilience and vulnerability of small flexible crisis response teams: implications for training and preparation, Cognition Technol. Work 16 (2014) 143–155, https://doi.org/10.1007/s10111-013-0253-z.
[72] T. Pavleska, G.P. Sellitto, H. Aranha, Crafting organizational security policies for critical infrastructures: an architectural approach, J. Surveillance, Secur. Safety 5 (2024) 116–139, https://doi.org/10.20517/jsss.2023.40.
[73] I.A. Herrera, T.O. Grøtan, R. Woltjer, B. Nevhage, S. Nilsson, J. Trnka, B. Adini, O. Cohen, R. Forsberg, C. Jonson, Applying resilience concepts in Crisis management and critical infrastructures-the DARWIN Project, in: Risk, Reliability and Safety: Innovating Theory and Practice - Proceedings of the 26th European Safety and Reliability Conference (ESREL), Glasgow, United Kingdom, 2017, pp. 2137–2144, https://doi.org/10.1201/9781315374987-324, 25 September 2016.
[74] A. Tatarowski, Building resilience of critical infrastructure in the light of asymmetric threats and terrorism, Terroryzm – Studia, Analizy, Prewencja 5 (2024) 391–409, https://doi.org/10.4467/27204383TER.24.014.19402.
[75] I. Scheuch, N. Peters, M.S. Lohner, C. Muss, C. Aprea, B. Fürstenau, Resilience Training Programs in Organizational contexts: A scoping review, Front. Psychol. 12 (2021) 733036, https://doi.org/10.3389/fpsyg.2021.733036.
[76] S. Forbes, D. Fikretoglu, Building resilience: the conceptual basis and research evidence for resilience training programs, Rev. General Psychol. 22 (2018) 452–468, https://doi.org/10.1037/gpr0000152.
[77] S. Flandin, G. Poizat, M. Durand, Improving resilience in high-risk organizations: principles for the design of innovative training situations, Develop. Learn. Organiz. 32 (2018) 9–12, https://doi.org/10.1108/DLO-03-2017-0027.
[78] S. Kermetchieva, Key quality criteria for private security in the protection and resilience of critical entities, in: International Scientific Conference the Strategic and Security Concept for the Countries of Southeast Europe, Struga, North Macedonia, 2023, pp. 301–310, https://doi.org/10.20544/ICP.8.1.23.P29, 27-29 September 2023.
[79] Cabinet Office, The UK Government Resilience Framework, 2023. https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html (accessed 15 November 2024).
[80] E. Ketelaars, C. Gaudin, S. Flandin, G. Poizat, Resilience training for critical situation management. An umbrella and a systematic literature review, Saf. Sci. 170 (2024) 106311, https://doi.org/10.1016/j.ssci.2023.106311.
[81] S. Fazeli, M. Haghani, M. Mojtahedi, T.H. Rashidi, The role of individual preparedness and behavioural training in natural hazards: a scoping review, Int. J. Disaster Risk Reduct. 105 (2024) 104379, https://doi.org/10.1016/j.ijdrr.2024.104379.
[82] A. Kozhan, M. Yerkinbekova, S. Omarova, Z. Turniyazova, A. Davletova, Development of stress resistance (on an Example of Athletes' Training), Retos 51 (2024) 211–218, https://doi.org/10.47197/retos.v51.100302.
[83] A.O. Chan, Y.H. Chan, J.P. Kee, Improving resistance and resiliency through Crisis Intervention training, Int. J. Emerg. Ment. Health 14 (2012) 77–86.
[84] D.L. Alderson, R.P. Darken, D.A. Eisenberg, T.P. Seager, Surprise is inevitable: how do we train and prepare to make our critical infrastructure more resilient? Int. J. Disaster Risk Reduct. 72 (2022) 102800 https://doi.org/10.1016/j.ijdrr.2022.102800.
[85] P. Gromek, Strategic training and exercises for critical infrastructure protection and resilience: a transition from lessons learned to effective curricula, Int. J. Disaster Risk Reduct. 65 (2021) 102647, https://doi.org/10.1016/j.ijdrr.2021.102647.
[86] E. Rios, E. Iturbe, A. Rego, N. Ferry, J.Y. Tigli, S. Lavirotte, G. Rocher, P. Nguyen, H. Song, R. Dautov, W. Mallouli, A.R. Cavalli, The DYNABIC Approach to resilience of critical infrastructures, in: ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security, 29 August –1 September 2023, New York, NY, 2023, pp. 1-8. https://doi.org/10.1145/3600160.36050.
[87] U.D. Ani, J.D. McK Watson, J.R.C. Nurse, A. Cook, C. Maple, A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape, in: Living in the Internet of Things (IoT 2019), London, United Kingdom, 2019, pp. 1–15, https://doi.org/10.1049/cp.2019.0131, 1-2 May 2019.
[88] D. Rehak, P. Novotny, Bases for modelling the impacts of the critical infrastructure failure, Chem. Eng. Trans. 53 (2016) 91–96, https://doi.org/10.3303/CET1653016.
[89] W.H.D. Ang, H.S.J. Chew, J. Dong, H. Yi, R. Mahendren, Y. Lau, Digital training for building resilience: systematic review, meta-analysis, and meta-regression, Stress Health 38 (2022) 848–869, https://doi.org/10.1002/smi.3154.
[90] E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, M. Hellmann, Digital Twin Conceptual Framework for improving critical infrastructure resilience, Automatisierungstechnik 69 (2021) 1062–1080, https://doi.org/10.1515/auto-2021-0104.
[91] W. Liu, Y. Hu, Q. Huang, Research on critical factors influencing organizational resilience of major transportation infrastructure projects: A hybrid fuzzy

DEMATEL-ISM-MICMAC approach, Buildings 14 (2024) 1598, https://doi.org/10.3390/buildings14061598.
[92] I. Linkov, B.D. Trump, J. Trump, G. Pescaroli, W. Hynes, A. Mavrodieva, A. Panda, Resilience stress testing for critical infrastructure, Int. J. Disaster Risk Reduct. 82 (2022) 103323, https://doi.org/10.1016/j.ijdrr.2022.103323.
[93] Q. Mao, N. Li, F. Peña-Mora, Quality function deployment-based framework for improving the resilience of critical infrastructure systems, Int. J. Crit. Infrast. Protect. 26 (2019) 100304, https://doi.org/10.1016/j.ijcip.2019.100304.
[94] Guidance Notes on Building Critical Infrastructure Resilience in Europe and Central Asia, United Nations Development Programme, 2022. https://www.undp.org/sites/g/files/zskgke326/files/2022-11/UNDP_Guidance%20notes_v4_0.pdf (accessed 28 November 2024).
[95] F.M. Baldursson, C. Banet, C.K. Chyong, Building Resilience in Europe's Energy System, 2023. https://cerre.eu/wp-content/uploads/2023/06/01062023_CERRE_REPORT_RESILIENCE.pdf (accessed 28 November 2024).
[96] Resilience of Critical Infrastructure Protection, European Union – Humanitarian Aid and Civil Protection, 2015. https://civil-protection-humanitarian-aid.ec.europa.eu/system/files/2017-11/recipe_guidelines.pdf (accessed 28 November 2024).
[97] J.E. Thomas, D.A. Eisenberg, T.P. Seager, E. Fisher, A resilience engineering approach to integrating Human and socio-technical system capacities and processes for national infrastructure resilience, J. Homel. Secur. Emerg. Manage 16 (2019) 20170019, https://doi.org/10.1515/jhsem-2017-0019.
[98] LogicGate, 6 Steps for Developing Effective Risk Management Strategies, 2024. https://www.logicgate.com/blog/developing-effective-risk-management-strategies/ (accessed 30 November 2024).
[99] D. Peljhan, M. Marc, Risk management and strategy alignment: influence on new product development performance, Technol. Anal. Strateg. Manage 35 (2021) 1547–1559, https://doi.org/10.1080/09537325.2021.2011192.
[100] V. Vicente, The Essentials of Integrated Risk Management, 2023. https://www.auditboard.com/blog/integrated-risk-management-irm/ (accessed 30 November 2024).
[101] MetricStream, The Top 5 Enterprise Risk Management (ERM) Tools For 2024, 2024. https://www.metricstream.com/blog/top-5-erm-tools.html (accessed 30 November 2024).
[102] IEC 31010, Risk Management – Risk Assessment Techniques, International Organization for Standardization, Geneva, 2019.
[103] M. Metfessel, A proposal for quantitative reporting of comparative judgments, J. Psychol.: Interdiscipl. Appl. 24 (1947) 229–235, https://doi.org/10.1080/00223980.1947.9917350.
[104] P.C. Fishburn, A comparative analysis of group decision methods, Behav. Sci. 16 (1971) 538–544, https://doi.org/10.1002/bs.3830160604.
[105] T.L. Saaty, How to make a decision: the analytic hierarchy process, Eur. J. Operat. Res. 48 (1990) 9–26, https://doi.org/10.1016/0377-2217(90)90057-I.
[106] IEC 60812, Failure Modes and Effects Analysis (FMEA and FMECA), International Electrotechnical Commission, Geneva, 2018.
[107] ISO/IEC 27000, Information Technology – Security Techniques – Information Security Management Systems, International Organization for Standardization, Geneva, 2018.
[108] ISO 45001, Occupational Health and Safety Management Systems – Requirements with Guidance for Use, International Organization for Standardization, Geneva, 2018.
[109] D. Blumenthal, R. Stoddard, Implementation planning: the critical step, PM Network 13 (1999) 80–86.
[110] E. Manten, 5 Steps to Plan a Process Review, 2020, in: https://www.linkedin.com/pulse/5-steps-plan-process-review-eric-manten (accessed 5 December 2024).
[111] ALOHA Software, United States Environmental Protection Agency, 2023. https://www.epa.gov/cameo/aloha-software (accessed 5 December 2024).
[112] Bentley, OpenFlows FLOOD: Integrated Flood Modeling Software, 2024. https://www.bentley.com/software/openflows-flood/ (accessed 5 December 2024).
[113] Gexcon, FLACS-CFD Explosion, Fire & Dispersion Modelling Software, 2024. https://www.gexcon.com/software/flacs-cfd/ (accessed 5 December 2024).
[114] S. Khanal, U.S. Medasetti, M. Mashal, B. Savage, R. Khadka, Virtual and augmented reality in the disaster management technology: a literature review of the past 11 years, Front. Virtual. Real. 3 (2022), https://doi.org/10.3389/frvir.2022.843195.
[115] Safety Management System Requirements for Safety Certification or Safety Authorisation, European Union Agency for Railways, 2022. https://www.era.europa.eu/system/files/2022-11/Guide%20on%20safety%20management%20system%20requirements.pdf (accessed 9 December 2024).
[116] Internal Control System: Ensuring Effective Risk Minimization and Compliance in Companies, GBTEC, 2024. https://www.gbtec.com/resources/internal-control-system-advantages/ (accessed 9 December 2024).
[117] R.E. Fisher, M. Norman, Developing measurement indices to enhance protection and resilience of critical infrastructure and key resources, J. Bus. Contin. Emer. Plan. 4 (2010) 191–206, https://doi.org/10.69554/OBLQ8823.
[118] F. Petit, W. Buehring, R. Whitfield, R. Fisher, M. Collins, Protective measures and vulnerability indices for the enhanced critical infrastructure protection programme, Int. J. Crit. Infrastruct. 7 (2011) 200–219, https://doi.org/10.1504/IJCIS.2011.042976.
[119] 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, Lemont, 2013, https://doi.org/10.2172/1087819.
[120] D. Denyer, M. Sutliff, Resilience Reimagined: A Practical Guide for Organisations, National Preparedness Commission, Cranfield University and Deloitte, Cranfield, 2021.
[121] EN 17483-1, Private Security Services – Protection of Critical Infrastructure, European Committee for Standardization, Brussels, 2021.
[122] J. Ferdinando, What Are The Types Of Security Guards?, 2024. https://www.buildingsecurity.com/blog/types-of-security-guards/ (accessed 10 December 2024).
[123] D. Rehak, A. Splichalova, T. Lovecek, M. Hromada, S. Jemelkova, A. Oulehlova, Convergence of safety and security within process plants, J. Loss. Prev. Process. Ind. 94 (2025) 105579, https://doi.org/10.1016/j.jlp.2025.105579.
[124] K. Kampova, T. Lovecek, D. Rehak, Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak Republic, Int. J. Crit. Infrast. Protect. 30 (2020) 100376, https://doi.org/10.1016/j.ijcip.2020.100376.
[125] Decree 528/2005 on physical security and certification of technical means. (in Czech).
[126] ISO 22361, Security and Resilience – Crisis Management, International Organization for Standardization, Geneva, 2022.
[127] Crises Control, Crisis Management Training: Empower Your Team with Crises Control, 2023. https://www.crises-control.com/blogs/crisis-management-training-8/ (accessed 10 December 2024).
[128] D. Gupta, 18 Best Employee Training Methods & Techniques, 2024. https://whatfix.com/blog/employee-training-methods/ (accessed 11 December 2024).
[129] Act 240/2000 on Crisis Management and on amendments of certain acts, Crisis Act, 2000. https://www.hzscr.cz/soubor/crisis-management-act-doc.aspx (accessed 11 December 2024).
[130] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.
[131] ISO 22301, Security and Resilience – Business Continuity Management Systems, International Organization for Standardization, Geneva, 2019.
[132] S. Mahendra, M. Sathiyanarayanan, R.B. Vasu, in: Smart Security System for Businesses using Internet of Things (IoT), in: 2nd International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, 2018, pp. 424–429, https://doi.org/10.1109/ICGCIoT.2018.8753101.
[133] K. Macnish, A. FernandezInguanzo, A. Kirichenko, Smart information systems in cybersecurity: an ethical analysis, The ORBIT Journal 2 (2019) 1–26, https://doi.org/10.29297/orbit.v2i2.105.
[134] P. Daponte, F. Paladi, Monitoring and Protection of Critical Infrastructure by Unmanned Systems, IOS Press, Amsterdam, 2023.
[135] K.C. Mizrak, Crisis management and risk mitigation: strategies for effective response and resilience, in: F. Mizrak (Ed.), Trends, Challenges, and Practices in Contemporary Strategic Management, IGI Global, 2024, pp. 254–278, https://doi.org/10.4018/979-8-3693-1155-4.ch013.
[136] M. Abdalla, L. Alarabi, A. Hendawi, Crisis management art from the risks to the control: a review of methods and directions, Information 12 (2021) 18, https://doi.org/10.3390/info12010018.
[137] W.T. Coombs, Parameters for crisis communication, in: W.T. Coombs, S. J. Holladay (Eds.), The Handbook of Crisis Communication, Blackwell Publishing, Oxford, 2010.
[138] A. Carreras-Coch, J. Navarro, C. Sans, A. Zaballos, Communication technologies in emergency situations, Electronics. (Basel) 11 (2022) 1155, https://doi.org/10.3390/electronics11071155.
[139] B.K. Kiang, M.S. Jusoh, S.S.M.M. Salleh, R. Ahmad, M.S.H. Din, Applying lean six Sigma approach: a study in recipe recovery and backup process environment, in: 8th International Conference on Advanced Materials Engineering & Technology (ICAMET 2020), Langkawi, Malaysia 2347, 2021 020285, https://doi.org/10.1063/5.0055628.
[140] ISO 55000, Asset management, International Organization for Standardization, Geneva, 2024.
[141] H. Adeli, A. Karim, Construction Scheduling, Cost Optimization and Management, CRC Press, Boca Raton, FL, 2001, https://doi.org/10.1201/9781482267686.
[142] K. Snyder, K. Main, Best Business Expense Tracker Apps 2024, 2024. https://www.forbes.com/advisor/business/software/best-business-expense-tracker-apps/ (accessed 15 December 2024).
[143] B.D. Grundy, P. Verwijmeren, The External Financing of Investment, Journal of Corporate Finance 65 (2020) 101745, https://doi.org/10.1016/j.jcorpfin.2020.101745.
[144] H. Huang, L. Lee, H. Song, B.T. Eck, SimMan: A simulation model for workforce capacity planning, Comput. Oper. Res. 36 (2009) 2490–2497, https://doi.org/10.1016/j.cor.2008.10.003.
[145] P.C. Susanto, N.H. Parmenas, R.F. Suryawan, I. Apriyani, Determinant attitude and employee recruitment: analysis psikotest, assessment, behavioral event interview and experience (Study Literarture), Int. J. Psychol. Health Sci. 1 (2023), https://doi.org/10.38035/ijphs.v1i1.83.
[146] H. Annen, The impact of selection and the assessment center method on leader development, in: M. Clark, C. Gruber (Eds.), Leader Development Deconstructed. Annals of Theoretical Psychology, Leader Development Deconstructed. Annals of Theoretical Psychology, 15, Springer, Cham, 2017, https://doi.org/10.1007/978-3-319-64740-1_11.
[147] A.A. Buchko, K.J. Buchko, Values-based management or the performance-Values matrix: was Jack Welch right? J. Bus. Leadership 8 (2012) 69–83, https://doi.org/10.58809/KUPD4878.

[148] ISO 22397, Societal Security, International Organization for Standardization, Geneva, 2014.
[149] H.E. Miller, K.J. Engemann, R.R. Yage, Disaster planning and management, Commun. IIMA 6 (2006) 25–36, https://doi.org/10.58729/1941-6687.1308.
[150] T. Williams, M. Resto-Leon, Cracking the code: the keys to a successful business impact analysis, J. Bus. Contin. Emer. Plan. 16 (2023) 313–319.
[151] N. Burghate, Work breakdown structure: simplifying project management, Int. J. Comm. Manag. Stud. 3 (2018) 2. Article.
[152] H. Dzwigol, Network analysis as a research method, in: 3rd International Interdisciplinary Scientific Conference "Digitalization and Sustainability for Development Management: Economic, Social, and Environmental Aspects, London, United Kingdom 456, 2023 03001, https://doi.org/10.1051/e3sconf/202345603001, 2023.
[153] C.A.S. Passos, R.B.B. Haddad, Benchmarking: a tool for the improvement of production management, in: IFAC Proceedings 46, 2013, pp. 577–581, https://doi.org/10.3182/20130911-3-BR-3021.00003. Volumes.
[154] M.J. Kami, Gap analysis key to super growth, Long. Range Plann. 1 (1969) 44–47, https://doi.org/10.1016/0024-6301(69)90045-4.
[155] J. Bocoya-Maline, M. Rey-Moreno, A. Calvo-Mora, The EFQM excellence Model, the knowledge Management process and the corresponding results: an explanatory and predictive study, Rev. Manag. Sci. 18 (2024) 1281–1315, https://doi.org/10.1007/s11846-023-00653-w.
[156] W. Grossmann, S. Rinderle-Ma, Process analysis. Fundamentals of Business Intelligence. Data-Centric Systems and Applications, Springer, Berlin, Heidelberg, 2015, https://doi.org/10.1007/978-3-662-46531-8_7.
[157] R.W. Puyt, F.B. Lie, C.P.M. Wilderom, The origins of SWOT analysis, Long. Range Plann. 56 (2023) 102304, https://doi.org/10.1016/j.lrp.2023.102304.
[158] S. Kumar, W.M. Lim, R. Sureka, Ch.J.Ch. Jabbour, U. Bamel, Balanced scorecard: trends, developments, and future directions, Review of Managerial Science 18 (2024) 2397–2439, https://doi.org/10.1007/s11846-023-00700-6.
[159] 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.
[160] M. Armstrong, Armstrong's Handbook of Human Resource Management Practice, 13th ed., Kogan Page, London, 2014.
[161] R.G. Ratnawat, P.C. Jha, Impact of job related stress on employee performance: a review and research agenda, IOSR J. Bus. Manag. 16 (2014) 1–6, https://doi.org/10.9790/487X-161150106.
[162] ISO 10015, Quality Management – Guidelines for Competence Management and People Development, International Organization for Standardization, Geneva, 2019.
[163] ISO 21001, Educational Organizations – Management Systems for Educational Organizations, International Organization for Standardization, Geneva, 2018.
[164] D. Scorgie, Z. Feng, D. Paes, F. Parisi, T.W. Yiu, R. Lovreglio, Virtual Reality for Safety Training: a systematic literature review and meta-analysis, Saf. Sci. 171 (2024) 106372, https://doi.org/10.1016/j.ssci.2023.106372.
[165] D.L. Kirkpatrick, Evaluating Training Program: The Four Levels, Berret-Koehler Publishers, San Francisco, CA, 1994.
[166] R. Kaufman, J.M. Keller, Levels of evaluation: beyond Kirkpatrick, Hum. Resour. Dev. Q. 5 (1994) 371–380, https://doi.org/10.1002/hrdq.3920050408.
[167] J.J. Phillips, Level four and beyond: an Roi model, in: S.M. Brown, C.J. Seidner (Eds.), Evaluating Corporate Training: Models and Issues. Evaluation in Education and Human Services, Evaluating Corporate Training: Models and Issues. Evaluation in Education and Human Services, 46, Springer, Dordrecht, 1998, https://doi.org/10.1007/978-94-011-4850-4_6.
[168] B. Ambu-Saidi, C.Y. Fung, K. Turner, A.S.S. Lim, A critical review on training evaluation models: a search for future agenda, J. Cognit. Sci. Human Develop. 10 (2024) 142–170, https://doi.org/10.33736/jcshd.6336.2024.
[169] A. Gunasekaram, S.K. Goyal, T. MArtikainen, P. Yli-Olli, Total Quality management: A new perspective for improving quality and productivity, Int. J. Quality & Reliabil. Manag. 15 (1998) 947–968, https://doi.org/10.1108/02656719810199033.
[170] J. Mendling, Event-driven process chains (EPC), in: metrics for process models, in: Lecture Notes in Business Information Processing, 6, Springer, Berlin, Heidelberg, 2008, https://doi.org/10.1007/978-3-540-89224-3_2.
[171] A. Vaisman, An introduction to business process modeling, in: M.A. Aufaure, E. Zimányi (Eds.), Business Intelligence. eBISS 2012. Lecture Notes in Business Information Processing, Business Intelligence. eBISS 2012. Lecture Notes in Business Information Processing, 138, Springer, Berlin, Heidelberg, 2013, https://doi.org/10.1007/978-3-642-36318-4_2.
[172] European Comission, Horizon Europe, 2024. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (accessed 19 December 2024).
[173] ISO 56000, Innovation Management, International Organization for Standardization, Geneva, 2020.
[174] A. Wójcik-Czerniawska, Financial innovations and new tools in finance, J. Manag. Financ. Sci. 46 (2023) 105–116, https://doi.org/10.33119/JMFS.2022.46.8.
[175] R.S. Aguilar-Savén, Business process modelling: review and framework, Int. J. Prod. Econ. 90 (2004) 129–149, https://doi.org/10.1016/S0925-5273(03)00102-6.
[176] M. Dumas, M. La Rosa, J. Mendling, H.A. Reijers, Introduction to Business Process management. Fundamentals of Business Process Management, Springer, Berlin, Heidelberg, 2018, https://doi.org/10.1007/978-3-662-56509-4_1.
[177] ISO 14001, Environmental Management Systems, International Organization for Standardization, Geneva, 2015.
[178] A.S. de Souza Barbosa, L.B. da Silva, V.F. de Souza, S.N. Morioka, Integrated management systems: their organizational impacts, Total Qual. Manag. Bus. Excellence 33 (2021) 794–817, https://doi.org/10.1080/14783363.2021.1893685.
[179] M. Malinova, S. Gross, J. Mendling, A study into the contingencies of process improvement methods, Inf. Syst. 104 (2022) 101880, https://doi.org/10.1016/j.is.2021.101880.
[180] J. Jeston, J. Nelis, Business Process Management: Practical Guidelines to Successful Implementations, 2nd ed., Routledge, Abingdon-on-Thames, 2008.
[181] A.B.E. Aichouni, F. Ramlie, H. Abdullah, Process improvement methodology selection in manufacturing: A literature review perspective, Int. J. Adv. Appl. Sci. 8 (2021) 12–20, https://doi.org/10.21833/ijaas.2021.03.002.
[182] IEC 61508, Functional Safety of Electrical /Electronic / Programmable Electronic Safety-related Systems, International Electrotechnical Commission, Geneva, 2010.
[183] B. Andersen, T. Fagerhaug, Root Cause Analysis: Simplified Tools and Techniques, 2nd ed., ASQ Quality Press, Milwaukee, WI, 2006.
[184] M. Wienker, K. Henderson, J. Volkerts, The Computerized maintenance Management system an essential tool for World class maintenance, Procedia Eng. 138 (2016) 413–420, https://doi.org/10.1016/j.proeng.2016.02.100.
[185] N.T. Minh, V. Zorin, Methods of remote monitoring of operability of mechanical systems, in: IOP Conference Series: Materials Science and Engineering 918, 2020 012080, https://doi.org/10.1088/1757-899X/918/1/012080.
[186] Y. Jin, J. Geng, Ch. Lv, Y. Chi, T. Zhao, A methodology for equipment condition simulation and maintenance threshold optimization oriented to the influence of multiple events, Reliab. Eng. Syst. Saf. 229 (2023) 108879, https://doi.org/10.1016/j.ress.2022.108879.
[187] Decisiv, Service Relationship Management: A Strategic Approach to Commercial Asset Maintenance, 2024. https://www.decisiv.com/wp-content/uploads/2018/08/2017_11-SRM_WhitePaper.pdf (accessed 4 January 2025).
[188] R.K. Sharma, S. Kumar, Performance modeling in critical engineering systems using RAM analysis, Reliab. Eng. Syst. Saf. 93 (2008) 913–919, https://doi.org/10.1016/j.ress.2007.03.039.
[189] T. Mishra, Safety Review, 2019. https://www.safeopedia.com/definition/6171/safety-review (accessed 4 January 2025).
[190] F. Camci, System maintenance scheduling with prognostics information using genetic algorithm, IEEe Trans. Reliab. 58 (2009) 539–552, https://doi.org/10.1109/TR.2009.2026818.
[191] C.H. Lie, Y.H. Chun, An algorithm for preventive maintenance policy, IEEe Trans. Reliab. 35 (1986) 71–75, https://doi.org/10.1109/TR.1986.4335352.
[192] T. Zonta, C.A. da Costa, R. da Rosa Righi, M.J. de Lima, E.S. da Trindade, G.P. Li, Predictive maintenance in the industry 4.0: A systematic literature review, Comput. Ind. Eng. 150 (2020) 106889, https://doi.org/10.1016/j.cie.2020.106889.
[193] D. Vidrikova, K. Boc, Z. Dvorak, D. Rehak, Critical Infrastructure and Integrated Protection, Association of Fire and Safety Engineering, Ostrava, 2017.
[194] D. Rehak, T. Lovecek, M. Hromada, N. Walker, I. Haring, Critical infrastructures resilience in the context of a physical protection system, in: R. Shinkuma, F. Xhafa, T. Nishio (Eds.), Advances in Engineering and Information Science Toward Smart City and Beyond. Engineering Cyber-Physical Systems and Critical Infrastructures, Advances in Engineering and Information Science Toward Smart City and Beyond. Engineering Cyber-Physical Systems and Critical Infrastructures, 5, Springer, Cham, 2023, https://doi.org/10.1007/978-3-031-29301-6_1.
[195] R.J. McAniff, W.K. Paulus, B. Key, B. Simpkins, The SAVI (systematic analysis of vulnerability to intrusion) software package, in: 28th INMM Annual Meeting on Safeguards: A Mature Technology, Newport Beach, CA, 1987 6449601.
[196] M.L. Garcia, Design and Evaluation of Physical Protection Systems, 2nd ed., Butterworth-Heinemann, Oxford, 2008.
[197] Y. Tarasov, Specialized Software Systems, Security, Reliability, Information, 78, 2008.
[198] S.S. Jang, S.W. Kwan, H. Yoo, J.S. Kim, W.K. Yoon, Development of a vulnerability assessment code for a physical protection system: systematic analysis of physical protection effectiveness (SAPE), Nuclear Eng. Technol. 41 (2009) 747–752, https://doi.org/10.5516/NET.2009.41.5.747.
[199] R. Nunes-Vaz, S. Lord, Designing physical security for complex infrastructures, Int. J. Crit. Infrastruct. Protect. 7 (2014) 178–192, https://doi.org/10.1016/j.ijcip.2014.06.003.
[200] United Nations, Protecting Vulnerable Targets from Terrorist Attacks, 2022. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod1-introduction_final-web.pdf (accessed 6 January 2025).
[201] A.P. Schmid, Layers of preventive measures for soft target protection against terrorist attacks. Handbook of Terrorism Prevention and Preparedness, International Centre for Counter-Terrorism, The Hague, 2021, https://doi.org/10.19165/2020.6.01.
[202] Kalvach, et al., Basics of Soft Targets Protection Guidelines, 2nd ed., Soft Targets Protection Institute, Prague, 2016.
[203] EN 62676, Video Surveillance Systems for Use in Security Applications, European Committee for Electrotechnical Standardization, Brussels, 2014.
[204] EN 50136, Alarm Systems – Alarm Transmission Systems and Equipment, European Committee for Electrotechnical Standardization, Brussels, 2012.
[205] EN 50398, Alarm Systems – Combined and Integrated Alarm Systems, European Committee for Electrotechnical Standardization, Brussels, 2017.
[206] EN 60839, Alarm and Electronic Security Systems, European Committee for Electrotechnical Standardization, Brussels, 2013.

[207] EN 50134, Alarm Systems – Social Alarm Systems, European Committee for Electrotechnical Standardization, Brussels, 2002.
[208] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture: NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://doi.org/10.6028/NIST.SP.800-207.
[209] S. Mukkamala, A. Sung, A. Abraham, Cyber-security challenges: designing efficient intrusion detection systems and anti-virus tools, in: V.R. Vemuri (Ed.), Enhancing Computer Security with Smart Technology, Auerbach Publications, Boca Raton, FL, 2006.
[210] S.A. Salloum, M. Alshurideh, A. Elnagar, K. Shaalan, Machine learning and deep learning techniques for cybersecurity: a review, in: A.E. Hassanien, A. Azar, T. Gaber, D. Oliva, F. Tolba (Eds.), Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020). Advances in Intelligent Systems and Computing 1153, Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-44289-7_5.
[211] M.A. Haque, S. Shetty, B. Krishnappa, ICS-CRAT: a cyber resilience assessment tool for industrial control systems, in: IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Washington, DC, 2019, pp. 273–281, https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
[212] J.F. Carías, S. Arrizabalaga, L. Labaka, J. Hernantes, Cyber resilience self-assessment tool (CR-SAT) for SMEs, IEEE Access. 9 (2021) 80741–80762, https://doi.org/10.1109/ACCESS.2021.3085530.
[213] S. Qiu, H. Zhao, N. Jiang, Z. Wang, L. Liu, Y. An, H. Zhao, X. Miao, R. Liu, G. Fortino, Multi-sensor information fusion based on machine learning for real applications in Human activity recognition: state-of-the-art and research challenges, Inf. Fusion 80 (2022) 241–265, https://doi.org/10.1016/j.inffus.2021.11.006.
[214] A. Bernatik, P. Senovsky, M. Senovsky, D. Rehak, Territorial risk analysis and mapping, Chem. Eng. Trans. 31 (2013) 79–84, https://doi.org/10.3303/CET1331014.
[215] C. Baldi, M. Martelli, M.C. Treu, Territorial vulnerability analysis: the environmental risk management systems, in: C.A. Brebbia (Ed.), Risk Analysis IV, WIT Press, Southampton, 2004, https://doi.org/10.2495/RISK040681.
[216] M.C. Treu, A. Colucci, S. Lodrini, Territorial vulnerability analysis: the methodological framework, in: C.A. Brebbia (Ed.), Risk Analysis IV, WIT Press, Southampton, 2004, https://doi.org/10.2495/RISK040691.
[217] S. Fotheringham, P. Rogerson, Spatial Analysis And GIS, 3rd ed., CRC Press, London, 2002.
[218] E. Pilone, M. Demichela, G. Baldissone, The multi-risk assessment approach as a basis for the territorial resilience, Sustainability. 11 (2019) 2612, https://doi.org/10.3390/su11092612.
[219] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek, P. Novotny, Cascading impact assessment in a critical infrastructure system, Int. J. Crit. Infrast. Protect. 22 (2018) 125–138, https://doi.org/10.1016/j.ijcip.2018.06.004.
[220] S. Schauer, S. Konig, M. Latzenhofer, S. Rass, T. Grafenauer, Analyzing cascading effects among critical infrastructures: the CERBERUS approach, in: Proceedings of the 15th International Conference on Information Systems for Crisis Response and Management (ISCRAM Conference), Rochester, NY, USA, 2018, pp. 428–437, 20–23 May 2018.
[221] Y.J. Hong, M. Choo, D.K. Yoon, Region-based cascading impact analysis in critical infrastructure systems, Sustain. Resilient. Infrastruct. 9 (2024) 293–307, https://doi.org/10.1080/23789689.2024.2303798.
[222] V.D. Rai, R. Ranjan, A.R. Gadhiya, B.M. Mote, Use of modern physical tools for mitigating the effect of abiotic stresses, in: A.Ch. Rai, A. Rai, K.K. Rai, V.P. Rai, A. Kumar (Eds.), Stress Tolerance in Horticultural Crops: Challenges and Mitigation Strategies, Elsevier, Amsterdam, 2021, pp. 387–397, https://doi.org/10.1016/B978-0-12-822849-4.00018-8.
[223] C.W. Johnson, A Handbook of Incident and Accident Reporting, Glasgow University Press, Glasgow, 2003.
[224] A. Liska, CERTs, ISACs, and Intelligence-Sharing Communities, in: Building an Intelligence-Led Security Program, Elsevier, Amsterdam, 2015, pp. 139–151, https://doi.org/10.1016/B978-0-12-802145-3.00008-9.
[225] R.A. Steinberg, ITIL Service Operation, 2nd ed., Cabinet Office, London, 2011.
[226] European Commission, Selection of Publicly Available Databases of Chemical Accident Data, 2023. https://minerva.jrc.ec.europa.eu/en/shorturl/minerva/chemical_accident_databases (accessed 12 January 2025).
[227] ISO 6182, Fire Protection – Automatic Sprinkler Systems, International Organization for Standardization, Geneva, 2021.
[228] ISO 7240, Fire Detection and Alarm Systems, International Organization for Standardization, Geneva, 2024.
[229] ISO/TR 17755, Fire Safety – Overview of National Fire Statistics Practices, International Organization for Standardization, Geneva, 2014.
[230] K. Himoto, K. Suzuki, Computational framework for assessing the fire resilience of buildings using the multi-layer zone model, Reliab. Eng. Syst. Saf. 216 (2021) 108023, https://doi.org/10.1016/j.ress.2021.108023.
[231] T. Gernay, S. Selamet, N. Tondini, N.E. Khorasani, Urban infrastructure Resilience to fire disaster: an overview, Procedia Eng. 161 (2016) 1801–1805, https://doi.org/10.1016/j.proeng.2016.08.782.
[232] EN 1998, Eurocode 8: Design of Structures for Earthquake Resistance, European Commission, Brussels, 2004.
[233] J.F. Hall, Finite element analysis in Earthquake engineering, Int. Geophys. 81 (2003) 1133–1158, https://doi.org/10.1016/S0074-6142(03)80183-3.
[234] EN 14460, Explosion Resistant Equipment, European Committee for Standardization, Brussels, 2018.
[235] A. Gargano, A.P. Mouritz, Comparative study of the explosive blast resistance of metal and composite materials used in defence platforms, Composites Part C: Open Access 10 (2023) 100345, https://doi.org/10.1016/j.jcomc.2023.100345.
[236] Y. Wang, Z. Zhao, H. Qiang, X. Wang, J. Guo, Blast resisting responses and upgrading technology for an underground structure subjected to external explosions, Structures 56 (2023) 105055, https://doi.org/10.1016/j.istruc.2023.105055.
[237] J. Laufs, H. Borrion, B. Bradford, Security and the smart City: A systematic review, Sustain. Cities. Soc. 55 (2020) 102023, https://doi.org/10.1016/j.scs.2020.102023.
[238] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, T. Baker, Security threats to critical infrastructure: the Human factor, J. Supercomput. 74 (2018) 4986–5002, https://doi.org/10.1007/s11227-018-2337-2.
[239] 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.
[240] M. Ovaere, S. Proost, Optimal electricity transmission reliability: going beyond the N-1 criterion, Energy J. 39 (2018) 211–234, https://doi.org/10.5547/01956574.39.4.mova.
[241] Y. Takakura, T. Yajima, Y. Kawajiri, S. Hashizume, Application of critical path method to stochastic processes with historical operation data, Chem. Eng. Res. Design 149 (2019) 195–208, https://doi.org/10.1016/j.cherd.2019.06.027.
[242] J. Shim, Ch.K. Kim, Y. Lee, Availability of a redundant system with two parallel active components under markovian assumptions, Int. J. New Technol. Res. 3 (2017) 17–18.
[243] H. Su, Quantifying independence redundancy in systems: measurement, factors, and impact analysis, ArXiv. 14 (2023) 04766, https://doi.org/10.48550/arXiv.2310.04766.
[244] J.J. Thakkar, Project Management: Strategic and Operational Planning, Springer, Singapore, 2022, https://doi.org/10.1007/978-981-15-3695-3.
[245] Solid Solutions, SimulationXpress, 2024. https://www.solidsolutions.ie/solidworks/3d-cad/features/simulationxpress.aspx (accessed 15 January 2025).
[246] J.E. Hannay, T. van den Berg, S. Gallant, K. Gupton, Modeling and simulation as a service infrastructure capabilities for discovery, composition and execution of simulation services, J. Defense Model. Simul. 18 (2021) 5–28, https://doi.org/10.1177/1548512919896855.
[247] PTC, CAD Simulation and Analysis, 2024. https://www.ptc.com/en/technologies/cad/simulation-and-analysis (accessed 17 January 2025).
[248] SimScale, What Is FEA | Finite Element Analysis?, 2024. https://www.simscale.com/docs/simwiki/fea-finite-element-analysis/what-is-fea-finite-element-analysis/ (accessed 17 January 2025).
[249] L. Chen, Q. Lu, D. Han, A Bayesian-driven Monte Carlo approach for managing construction schedule risks of infrastructures under uncertainty, Expert. Syst. Appl. 212 (2023) 118810, https://doi.org/10.1016/j.eswa.2022.118810.
[250] M. van den Boomen, M.T.J. Spaan, Y. Shang, A.R.M. Wolfert, Infrastructure maintenance and replacement optimization under multiple uncertainties and managerial flexibility, Construct. Manag. Econ. 38 (2019) 91–107, https://doi.org/10.1080/01446193.2019.1674450.
[251] V. Lukitosari, I.N.Pujawan Suparno, B. Widodo, Inventory strategy for spare parts redundancy to support server operations during production processes, Prod. Manuf. Res. 7 (2019) 395–414, https://doi.org/10.1080/21693277.2019.1630681.
[252] F. Kottmann, M. Kyriakidis, V.N. Dang, G. Sansavini, Enhancing infrastructure resilience by using dynamically updated damage estimates in optimal repair planning: the power grid case, ASCE-ASME J. Risk Uncertain. Eng. Syst., Part A: Civil Eng. 7 (2021) 04021048, https://doi.org/10.1061/AJRUA6.0001159.
[253] IEC 62502, Analysis Techniques for Dependability – Event Tree Analysis (ETA), International Electrotechnical Commission, Geneva, 2010.
[254] H.M. Levin, P.J. McEwan, Cost-Effectiveness Analysis: Methods and Applications, 2nd edit., SAGE Publications, Washington, DC, 2000.
[255] W.B. Liu, Z.L. Cheng, J. Mingers, L. Qi, W. Meng, The 3E methodology for developing performance indicators for public sector organizations, Public Money Manag. 30 (2010) 305–312, https://doi.org/10.1080/09540962.2010.509180.
[256] 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.
[257] P.M. Swamidass, Deming Cycle (PDCA), in: Encyclopedia of Production and Manufacturing Management, Springer, Boston, MA, 2000, https://doi.org/10.1007/1-4020-0612-8_229.
[258] I. van Maaren, A reference model for auditing organisational resilience, Maandblad voor Accountancy en Bedrijfseconomie 96 (2022) 201–211, https://doi.org/10.5117/mab.96.89573.
[259] G. Blokdyk, Gap Analysis: The Definitive Handbook, Createspace Independent Publishing Platform, Scotts Valley, CA, 2017.