Safety Science 170 (2024) 106371

Contents lists available at ScienceDirect

Safety Science

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

Critical Entities Resilience Failure Indication

David Rehak [a,*], Alena Splichalova [a], Martin Hromada [b], Neil Walker [c], Heidi Janeckova [a], Josef Ristvej [d]

[a] VSB – Technical University of Ostrava, Faculty of Safety Engineering, Lumirova 13, 700 30 Ostrava – Vyskovice, Czech Republic
[b] Tomas Bata University in Zlin, Faculty of Applied Informatics, Nad Stranemi 4511, 760 05 Zlin, Czech Republic
[c] International Association of Critical Infrastructure Protection Professionals, 200 Ware Road, Hoddesdon Herts EN11 9EY, United Kingdom
[d] University of Žilina, Faculty of Security Engineering, 1. maja 32, 010 26 Zilina, Slovakia

ARTICLE INFO

Keywords:
Critical entities
Resilience
Resistance
Robustness
Failure
Indicators
CERFI tool

ABSTRACT

The adoption of the new Directive (EU) 2022/2557 on the resilience of critical entities has raised the question of how to assess the level of resilience of these entities in relation to current security threats. Until now, approaches have focused only on assessing the resilience of critical infrastructure elements. However, the new Directive exemplifies the need to pay attention not only to the element resilience, but also and more importantly to the resilience of their owners and operators, i.e., critical entities. Based on this fact, the authors of the article created a tool for Critical Entities Resilience Failure Indication (CERFI Tool). The essence of this tool is a probabilistic algorithm that predicts the relationship between the threat intensity and the protective part of critical entity resilience through indicators (to be created by the assessors themselves). The result of this prediction is an indication of the critical point of failure of the critical entity's resilience in phases of prevention and absorption of impacts. The CERFI Tool thus contributes to increasing the safety of technically oriented infrastructures, especially those of an energy and transport nature. The paper concludes with an example of the practical application of the developed tool on a selected critical entity in the energy sector.

1. Introduction

People living in large urban agglomerations are increasingly dependent on a reliable supply of essential services that are necessary to maintain vital social functions and economic activities, along with public health and safety services (Directive (EU), 2022). These essential services are provided through critical infrastructure (CI), which can be classified as technical and socio-economic. The most important technical CI systems have long included energy and transport (Council Directive, 2008). For example, the energy sector was identified as a uniquely critical sector in 2013 (The White House, 2023), as a failure of its services would cause cascading impacts on the provision of essential services of all other CI systems (Vichova and Hromada, 2019; Rehak et al., 2018a).

Owners or operators of CI systems are referred to as critical entities. The ability of these critical entities to prevent, respond to, withstand, mitigate, absorb, adapt to and recover from incidents is referred to as resilience (Directive (EU), 2022). This resilience can be perceived on two basic levels. The first level is technical resilience, which focuses on the physical protection of CI elements (NIAC, 2009; Kampova et al., 2020). The second level is organisational resilience, which is concerned with the managerial and procedural areas of critical entities (ASIS, 2009; Rehak, 2020). However, the same determinant components can be identified for both types of resilience, which are resistance, robustness, recoverability and adaptability (Rehak et al., 2018b; Rehak et al., 2022a).

In the context of the timeline, resistance can be seen as the most important resilience component, whereby resistance is perceived as the ability of a critical entity to prevent an incident from occurring, whereas the essence of robustness is the absorption of the effects of an incident that has already occurred (Rehak et al., 2022a). The resilience of critical entities is currently determined by several important approaches. These include emergency preparedness (Philpott, 2016), risk management (ISO 31000, 2018), activities taken by an entity to define the hazard environment to which elements of the CI are exposed (Carlson et al., 2012), monitoring (Tracht et al., 2013) or a physical protection system (Kampova et al., 2020). All of these approaches have been successfully applied in practice, but their predictive potential in relation to an

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

https://doi.org/10.1016/j.ssci.2023.106371
Received 19 May 2023; Received in revised form 28 October 2023; Accepted 30 October 2023
Available online 4 November 2023

impending incident is very low. For this purpose, approaches based on the use of indicators in the context of CI resilience are clearly more appropriate (Rehak and Splichalova, 2022).

A number of methods and tools are currently used within the CI systems that use indicators to detect weaknesses, measure and assess resilience, or evaluate its security or vulnerability. The most prominent of these is a method in which individual questions asking about specific resilience-related issues are considered to be indicators (Øien et al., 2017). Through these questions, they try to define whether the system is sufficiently resilient. In contrast, static resilience assessment methods (Rehak et al., 2019; Nan and Sansavini, 2017; Kozine et al., 2018) use indicators to obtain information about the integrated level of resilience and also to model the failure behaviour of infrastructure systems. A different perspective is provided by holistic methods (Mazur et al., 2019; Fu et al., 2021), which identify indicators based on their benefits for enhancing resilience and stakeholder preferences. Another approach is to define indicators based on economic aspects, which are presented in a three-dimensional form, namely functionality, time and cost (Abbasnejadfard et al., 2022).

It is also common practice to use indices, which can then be considered as a specific type of indicator that is also able to identify significant shortcomings and weaknesses that can threaten the functionality of infrastructure systems. The Resilience Measurement Index can be considered as one of the most important indices, which is complementary to other indicators such as the Vulnerability Index (Collins et al., 2011), the Protective Measures Index, the Consequences Measurement Index (Petit et al., 2013), and the Total Resilience Index (Mottahedi et al., 2021).

Therefore, the essence of all the methods and tools presented above is the assessment of the static resilience/vulnerability level (i.e., the level at the time when the element is not exposed to any incident) in order to identify weak points of the assessed CI elements. Such an approach to CI protection has certainly been correct in recent years, but in the context of the new Directive (EU) (2022) it is necessary to shift the focus to critical entities. As a result of this change, it is now possible to view CI resilience in an integral way that links technical and organisational resilience into a single unit. In this context, it is also appropriate to redistribute indicators from the current CI elements to a new position located between threats and critical entities.

On the basis of these newly established conditions, research was launched in 2020 on the indication of CI resilience failures in the energy, transport and ICT sectors. As a result, the CERFI Tool was developed to enable the predictive indication of failure of critical entity's resilience in phases of prevention and absorption of impacts. The essence of this tool is to link the knowledge of threats and the protective part of resilience. Based on this information, entities can detect the most significant threats that could cause a failure in the delivery of their essential services.

2. Perceptions of resilience in relation to the new Directive (EU)

The first professional definition of infrastructure resilience was published in 2009 (NIAC, 2009). However, following the implementation of the new Directive (EU) (2022), the perception of resilience in CI systems is changing. Until now, resilience has been associated mainly with technical elements of CI (Council Directive, 2008; NIAC, 2009; Setola et al., 2016; Rehak et al., 2018b). However, as of the end of 2020, it is starting to be seen primarily in the context of critical entities (Proposal for a Directi, 2020). A fundamental change is the extension of technical resilience to a new dimension that focuses on the resilience of the entity itself. This resilience is referred to as organisational and is explicated as *"the ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions (incidents)"* (Denyer, 2017). Organisational resilience can also be explicated as the ability of an organisation to absorb and adapt to a changing environment (ISO, 2017) or to survive and strengthen in times of crisis (Seville et al., 2008; Gonçalves et al., 2019).

In the context of this change, it is necessary to reclassify the factors that determine resilience. Currently, these factors are defined in two groups of documents. The first group is publications related to resilience assessment of CI elements (Hromada et al., 2021; Rehak et al., 2019; Cai et al., 2018; Kozine et al., 2018; Nan and Sansavini, 2017; Bertocchi et al., 2016; Prior, 2015; Petit et al., 2013). In contrast, the second group of documents relates to organisational resilience (Chen et al., 2021; Annarelli et al., 2020; Rehak, 2020; Patriarca et al., 2018; Rahi, 2018; ISO, 2017; Linnenluecke and Griffiths, 2012; Tillement et al., 2009; ASIS, 2009). By combining these two areas, it is possible to procure a partial overview of the factors determining the resilience of critical entities. Based on the standards, methods and tools presented above, the authors have classified the key factors and developed a structured approach for assessing the resilience of critical entities (see Fig. 1).

The factors shown in Fig. 1 are represented by four components (i.e., resistance, robustness, recoverability, and adaptability) and fourteen variables. The definition of the components is based on the CI Resilience Cycle (Rehak et al., 2019), which consists of four phases focusing on:

- prevention of an incident occurring (this phase is defined by the level of resistance of the critical entity),
- absorption of impacts of an incident that has already occurred (this phase is defined by the level of robustness of the critical entity),
- recovery of damaged elements of CI (this phase is defined by the level of resources and the quality of the organisation's processes),
- adaptation of the critical entity to the incident (this phase is defined by the management of the organisation in question).

From the description of the individual phases of resilience above, it is clear that the components of resilience and robustness are responsible for protecting the critical entity and the essential services it provides in the face of an incident. In contrast, the recoverability and adaptability components are responsible for reconstructing the resilience of the critical entity after an incident. Based on this, it is useful to divide the resilience components into two groups: (1) components of the protective part of resilience, i.e., resilience and robustness, and (2) components of the reconstructive part of resilience, i.e., recoverability and adaptability. In the context of assessing the potential resilience failure of a critical entity at the time of an incident, it is sufficient to pay attention solely to the components of the protective part of resilience. For this reason, it is advisable to pay attention to the description of these two components.

In the context of critical infrastructure, robustness was first defined in 2009: *"the ability to maintain critical operations and functions in the face of crisis."* This can be reflected in physical building and infrastructure design (office buildings, power generation and distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks)" (NIAC, 2009). Although the reactionary nature of this component is evident from this definition, no one has dealt with the area of prevention for a long time. The first comprehensive definition of resistance was published only in 2020: *"the ability of critical infrastructure to prevent the occurrence of an incident"* (Rehak et al., 2020a).

The subsequent sorting of the variables (in Fig. 1) was done based on their nature and relationship to both levels of resilience, i.e., organisational and technical. The variables determining organisational resilience relate mainly to the managerial activities of the organisation. On the other hand, the variables determining technical resilience relate to CI elements. At the same time, however, it is necessary to state that both groups of variables are so interrelated that together they form the comprehensive resilience of critical entities.

3. Threats/incidents affecting the resilience of critical entities

Critical entities and their elements are constantly exposed to a variety of threats. In the event that these threats begin to affect entities or their elements, an incident occurs, which is defined as *"an event which*

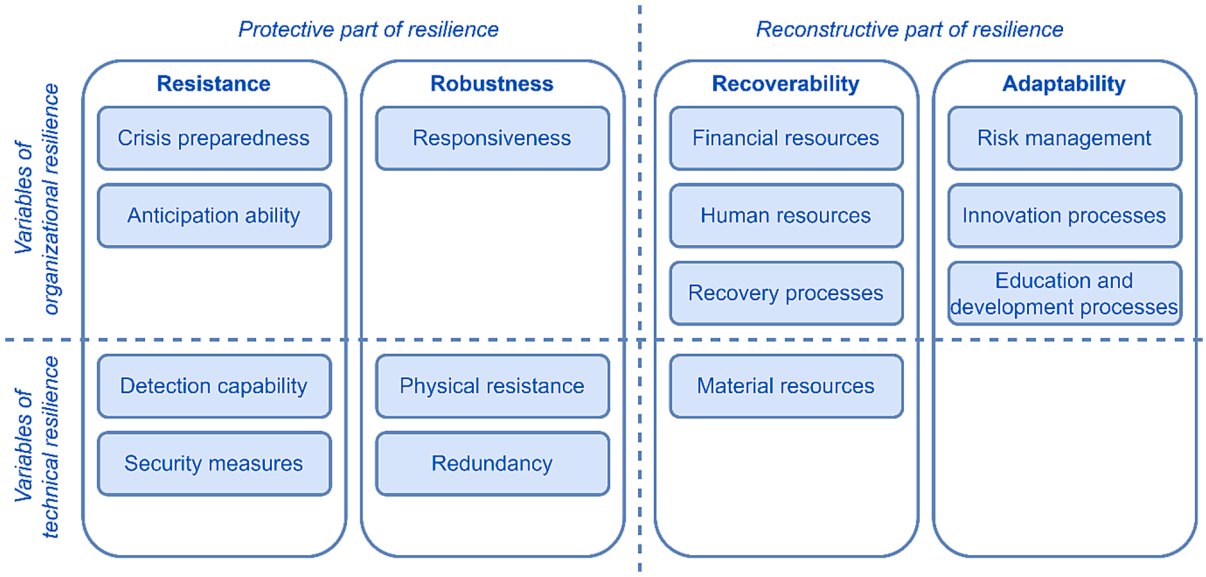

Fig. 1. Factors defining the resilience of critical entities.

has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law" (Directive (EU), 2022). Threats causing incidents can be classified in the context of the issue at hand according to different aspects, such as the area of origin (i.e., external and internal), the area of impact (i.e., organisational and elemental), or the nature of the threat (i.e., naturogenic, technogenic and anthropogenic). This classification then helps to designate the link between the threat/incident and the specific resilience components that may be disrupted. Simplified characterization of the relationship between resistance, robustness, and intensity of the threat causing the incident is presented in Fig. 2.

The essence of the resilience of critical entities is the protection of CI elements and essential services provided by them. Compared to static resilience, dynamic resilience can reach different levels before and during an incident (Rehak et al., 2022b). The initial phase of resilience (i.e., before an incident) is determined by the critical entity's resistance. This phase is responsible for creating or suppressing an incident. If the resistance level is greater than the threat level, it is expected that the incident will not occur. At this phase, the threat effect can only cause a decrease of the element performance. It can be assumed that the critical entity is prepared for this situation and is able to cover performance degradation without major difficulties, without disrupting the provided services continuity. However, if the resistance level is lower (see the orange area in Fig. 2), an incident is expected to occur, i.e., significant disruption to the provision of an essential service (Directive (EU), 2022). This activates robustness which, depending on the level of its variables, can reach a higher but also a lower level of absorptive capacity than was the case with resistance.

As a result of this fact, there may be an increase or decrease in the dynamic level of resilience. Indeed, the resilience level reflects the current state of the measures, that the assessed entity has, and which are expected to be activated. Under this assumption, this is the so-called maximum dispositional resilience level. In the first phase of resilience, the measures determining the subject's resistance (i.e., the green line)

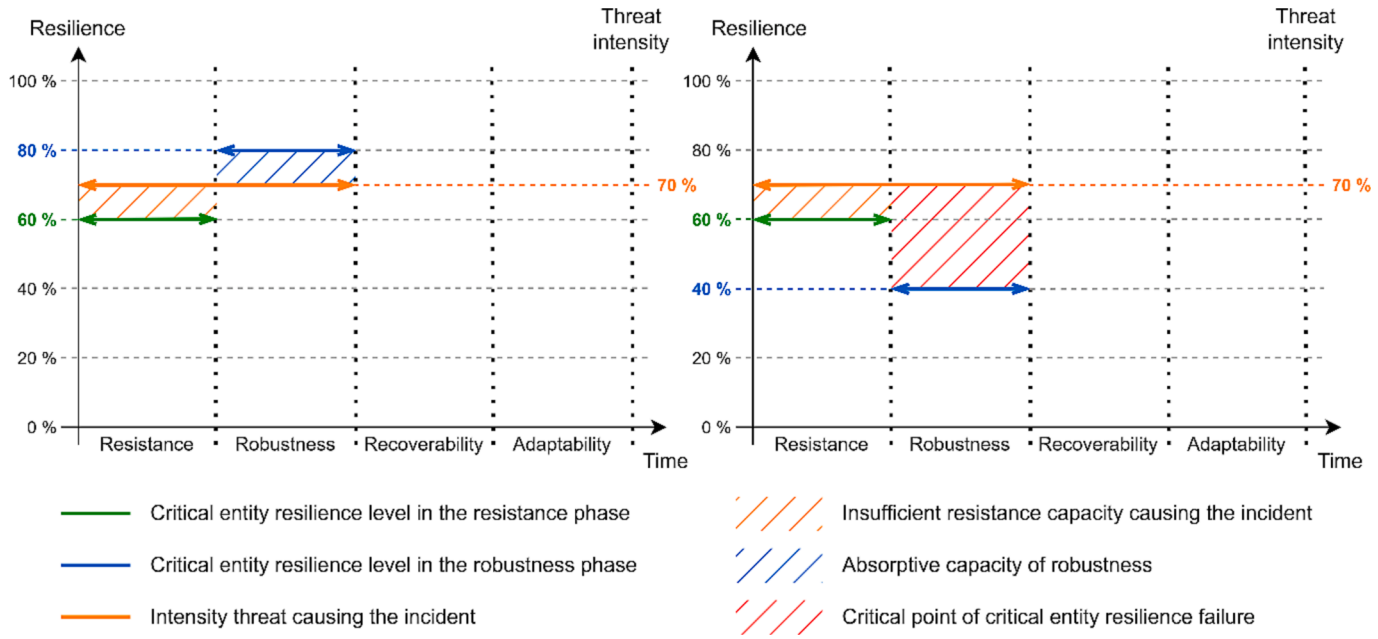

Fig. 2. The relationship between resistance, robustness, and intensity of the threat causing the incident.

are assessed. In the second phase of resilience, the measures determining the subject's robustness are assessed (i.e., the blue line). These two values can therefore reach different levels depending on the available measures, as in Fig. 2. However, if no measures were identified in one of these resilience phases, then in an extreme case the resilience value in a given phase could reach a value of 0. However, such a situation is only hypothetical, as every entity has at least basic security measures in place.

If the robustness level is higher than the threat intensity, the critical entity is able to face the incident effects through absorptive capacity (see the blue area in Fig. 2). However, when the threat intensity reaches a level higher than that of the robustness, a critical point of critical entity resilience failure occurs (see the red area in Fig. 2). Failure of the critical subject resilience in this context refers to a state where the level of resilience is not sufficient to protect the critical subject, as a result of which its functionality is lost. This loss of functionality is manifested in a significant decrease in the performance of critical infrastructure elements, resulting in an immediate failure of the delivery of essential services provided by the critical entity. It is therefore evident from this definition that the essence of protective part of resilience is the protection of a critical entity from the occurrence and impact of incidents that could result in a disruption or failure of the critical entity's performance.

Based on the above, it is evident that a predictive indication of a critical point of failure in the resilience of a critical entity is the result of comparing the intensity of the threat and the security measures (i.e., resistance and robustness) of the critical entity. This predictive indication enables early identification of weaknesses and subsequent strengthening the protective part of its resilience. For this reason, the following section of the paper is devoted to the applicability of indicators in a CI system. At the same time, it is necessary to note that the term resilience in the following parts of the text means only its protective part, which is determined by the resistance and robustness components.

4. Indicators and their use in the critical infrastructure system

Indicators have long been used across a variety of disciplines due to their unique abilities, i.e., to predict or indicate situations that are not directly observable, to present deviations from a desired state in a simple and understandable way, or to describe in a quantitative and transparent way the problems under investigation (Hiete and Merz, 2009; Shavelson et al., 1991). Based on these capabilities, it is clear that indicators can provide vital information about the actual state of CI, e.g., assessing the current level of resilience/vulnerability of CI or providing information about incidents that have already taken place. Provided that these indicators are assessed at regular intervals, they can also be used as a predictive tool to determine deficiencies that may lead to the occurrence of an incident.

Very often, indicators have a specific meaning that is narrowly oriented to a particular area of use, which determines their final form or shape. Indicators are usually presented as a definite variable (Chevalier et al., 1992; Gallopin, 1997), parameter or value (OECD, 2003), measure (McQueen and Noak, 1988; Holling et al., 1978), scale (Joung et al., 2012), but also a statistical measure, index, fact or empirical data. However, if indicators are to be truly usable, they must have clearly defined indicative parameters, which are the merits, determinants or measurable units set for the respective indicators. These are therefore the feature variables of each indicator, which shape its character with expressive power about the indicator itself (Splichalova and Flynnova, 2021).

Indicators can be classified according to their mode of use, indication process and defined purpose. Indicators can be divided into qualitative and quantitative, key and secondary, absolute and proportional, simple and complicated, so-called composite (Gallopin, 1997), or empirical and theoretical (Bunge, 2003). This general division of indicators can be applied in any area, i.e., also in the CI system, but here it is necessary to divide the indicators into more specific categories. Examples include lagging, leading, activity and outcome indicators (Hofmann et al., 2012; Gjerde et al., 2011), which are mainly used to provide information on the vulnerabilities of CI. If these indicators are used before the incident, they are a-priori indicators; if they are used after the incident, they are post-hoc indicators (Prior, 2015). All these indicators can be further subdivided into external and internal environment indicators.

The CI system can be classified into three levels that define the vertical division of the system, i.e., sectoral, sub-sectoral and elemental levels (Rehak et al., 2016). At the sectoral level, indicators tend to be used in the context of forming the integral CI protection policy (Prezelj et al., 2012), assessing the long-term performance of cross-sectoral strategies (Hall, 2014; Giannopoulos et al., 2013; Petit et al., 2013; Fisher and Norman, 2010), or setting up CI in the context of climate change (Wang et al., 2020; Rübbelke and Vögele, 2011). As the different sectors are interlinked and thus influence each other, it can be concluded that, for example, the type of linkage (Galbusera et al., 2020), group (Rinaldi et al., 2001), character or level of dependence of the linkage (Rehak et al., 2020b) are also indicators that are capable of indicating the propagation of faults across sectors.

As at the sectoral level, indicators are used to assess the current state of CI or to assess future developments in individual sub-sectors. In the energy sector, indicators are frequently used in relation to energy security (Kruyt et al., 2009), for monitoring the network status (Löschel et al., 2010), level of commodity provision vulnerabilities (Hofmann et al., 2012), or the sustainability of its featureless operation (ESMAP, 2018). Indicators here most often serve as a measurable, explicable value that indicates faults that affects the safety of the commodity supply.

In transport, indicators are used to measure the performance and quality of the transport network in terms of safety (European Commission, 2020), for the statistical representation of safety, performance and sustainability (ITF, 2019), environmental safety (Ministry of Transport, 2020), measuring the sustainability of transport in the country in question (Dobranskyte-Niskota et al., 2007; Rassafi and Vaziri, 2005), performance monitoring (ITF, 2020) and transport intensity (UNECE, 2018) or indicating the intensity and likelihood of an incident (Titko and Luskova, 2016; Nogal et al., 2016; Dvorak and Chovancikova, 2020). Conversely, in the ICT sub-sector, indicators are used to indicate the current state of system security (ITU, 2017; Øien et al., 2017), address security incidents (Pandey, 2013), and monitor and analyse performance (OECD, 2020; ITU, 2016), mostly in the form of extensive and continuously updated statistics (ITU, 2022).

The final level is the elemental level. At the elemental level, indicators can be considered as information, data or characteristic values by which individual objects can be classified into the CI system. Methods for identifying CI elements often use indicators to determine the basic characteristics of the elements, assess whether they conform to established standards, and then designate the selected entity as critical (Alayande et al., 2020; Ghorani et al., 2015; Lami and Bhattacharya, 2015; NERC, 2009). Indicators also play a role in the inter-linkages between elements, the spread and identification of threats and subsequent damage between sectors (Rehak et al., 2020b; Xian and Jeong, 2018; Halat and Gaitán, 2015; Beccuti et al., 2012).

Based on the above, it can be concluded that indicators are an important part of the whole CI system. They are capable of denoting threats, assessing the current level of resilience or providing information about incidents that have already occurred along with the actual state of CI. However, existing methods do not sufficiently exploit the potential of these indicators. The information provided by these indicators is very often used in isolation and only in the context of CI. However, if the existing indicators are repositioned between threats and critical entities, the newly set indicators can be used as predictors. Through these predictors, it will be possible to prevent incidents from occurring and thus prevent the failure of the resilience of critical entities.

5. Defining a framework and process for critical entities resilience failure indication

From the text presented above, it is clear that the use of predictors to indicate resilience failure offers new possibilities for the protection of critical entities. With the help of these predictors, it is possible to create a tool for the early indication of threats that can negatively disturb the functioning of these entities and their CI. Based on this hypothesis, the authors of this paper developed a tool for Critical Entities Resilience Failure Indication (CERFI Tool). The essence of this tool is a probabilistic algorithm that predicts the relationship between the intensity of the threat and the level of critical entity resilience through indicators (which will be created by the assessors themselves). The result of this prediction is an indication of the critical point of failure of the critical entity's resilience. The following section of the paper defines the framework and procedure for using the CERFI Tool.

5.1. Framework for critical entities resilience failure indication

The essence of the framework is to define the inputs necessary to define the process of critical entities resilience failure indication. These inputs should be divided into four basic environments, which are (1) the critical entity environment, (2) the threat environment, (3) the indication environment, and (4) the methodical environment. A more detailed description of these environments is presented in Fig. 3.

The first important environment of the framework for indicating resilience failure is the characterisation of the critical entity. The essence of this characterisation is the definition of the essential services provided by the critical entity according to the Directive (EU) (2022) and its subsequent classification into the relevant sector, sub-sector, and category. According to this categorisation, it is obligatory to define the structural and performance parameters of its CI. Specifically, this includes knowledge of the topological structure of each element (i.e., whether it is a point, line or area element) and knowledge of the technological structure of these elements (e.g., the number and performance of key technologies).

Another environment of the framework is the definition of the threats. This data is an important input to the downstream indication environment as it defines the area and sub-area of threats against which resilience failure will be indicated. In the context of current threats, resilience failure can be indicated by the impact of threats from three areas, namely naturogenic, technogenic and anthropogenic. These areas can then be further classified into the following sub-areas: geological, meteorological, process-technical, cascading, personnel, cyber and physical (Rehak et al., 2019). Indicators will then be created between the threats of the selected environment and the critical entity, and their indicative parameters will be defined.

The third and central environment of the framework is the definition of the indicator environment, which consists in defining the factors necessary for the creation of indicators. These factors include information on the threats identified in the above environment and their connection to the critical entity being assessed. According to this, it is necessary to define indicative parameters not only for the identified threats (i.e., their expected intensity), but also for the critical entity (i.e., its level of the protective part of resilience, i.e., resistance and robustness). These indicative parameters must be defined on the same measurable scale to enable their subsequent comparison. For this reason, it is recommended to use a probabilistic model, i.e., from 0 to 1. The characteristics of the indicator environment are presented in Fig. 4.

The final environment of the framework is the definition of the methodology necessary for the indication procedure. Specifically, this concerns the methods, procedures, and tools to be used in the indication process which can then be classified into four basic groups: (1) CI element identification methods, (2) threat identification methods, (3) threat intensity assessment methods, and (4) resilience assessment methods. The specific methods, procedures, and tools are defined in another connected section of this article, namely the Critical Entity Resilience Failure Indication Procedure.

5.2. Process for critical entities resilience failure indication

Based on the reference points and assumptions set out in the framework, it is possible to proceed to the actual definition of the process, which consists of four continuous steps. Each step includes an overview of the methods/techniques to be used and the most appropriate one is recommended by the authors. Based on the steps defined in this way, the critical entity is able to assess whether the protective part of the resilience will be exhausted, and the delivery of essential services will be disrupted (i.e., the critical point). By requesting a retrospective review, i.e., a review of the resilience, the critical entity can focus on the

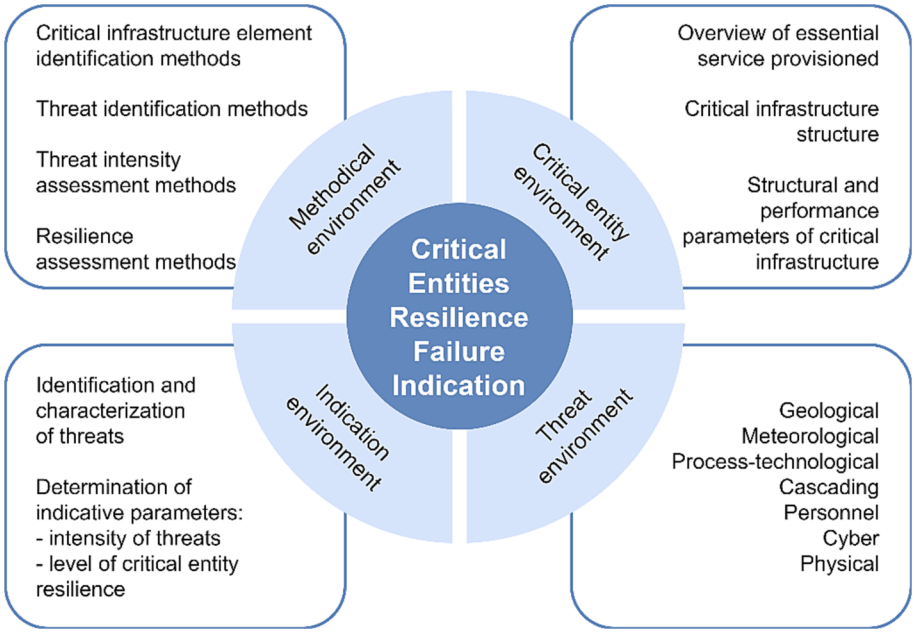

Fig. 3. Framework for critical entities resilience failure indication.

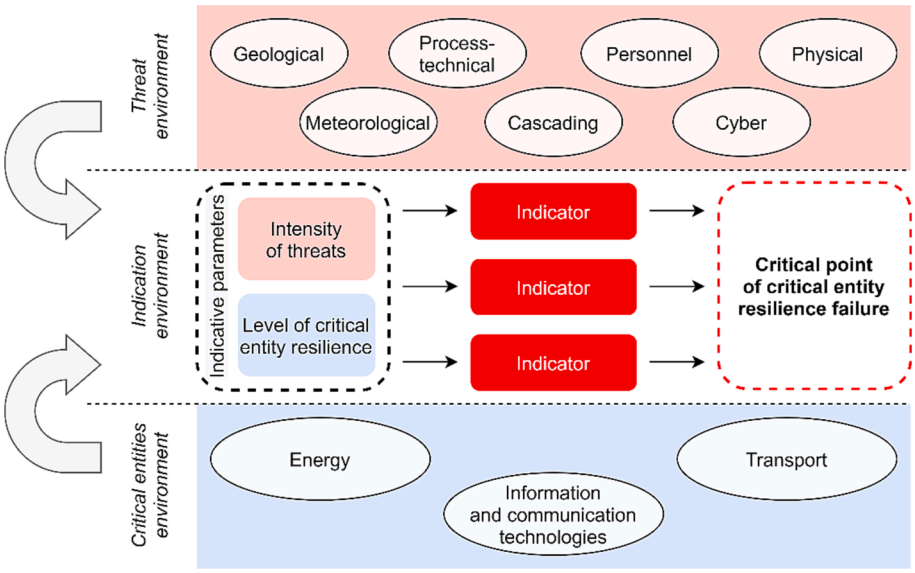

Fig. 4. Characteristics of the CERFI Tool indicator environment.

specific deficiencies that have been identified in the application of the procedure, i.e., identify resilience weaknesses that should subsequently be strengthened. The comprehensive process and its individual steps are shown in Fig. 5.

The procedure presented above is universal, i.e., it can be applied to any part of the CI in any sector. It is therefore a comprehensive procedure that defines the process of using available methods/techniques in order to identify the critical point of resilience failure. This procedure can be described as unique, as it finds and is able to determine the relationship between the intensity of a specific threat and the resilience of a critical entity through the indicators created. The following text presents a detailed elaboration of the individual steps of the procedure for indicating the resilience failure of critical entities.

Step 1: Preparation of the indication process

If an entity is classified as critical in one of the categories (Directive (EU), 2022), it is possible to proceed to collect the information needed to develop indicators. The preparation of the indicator process can be divided into two parts. In the first part, it is necessary to identify the CI, i.e., all CI elements that the critical entity has under its management. Here it is advisable to compile an inventory and to add a brief description of

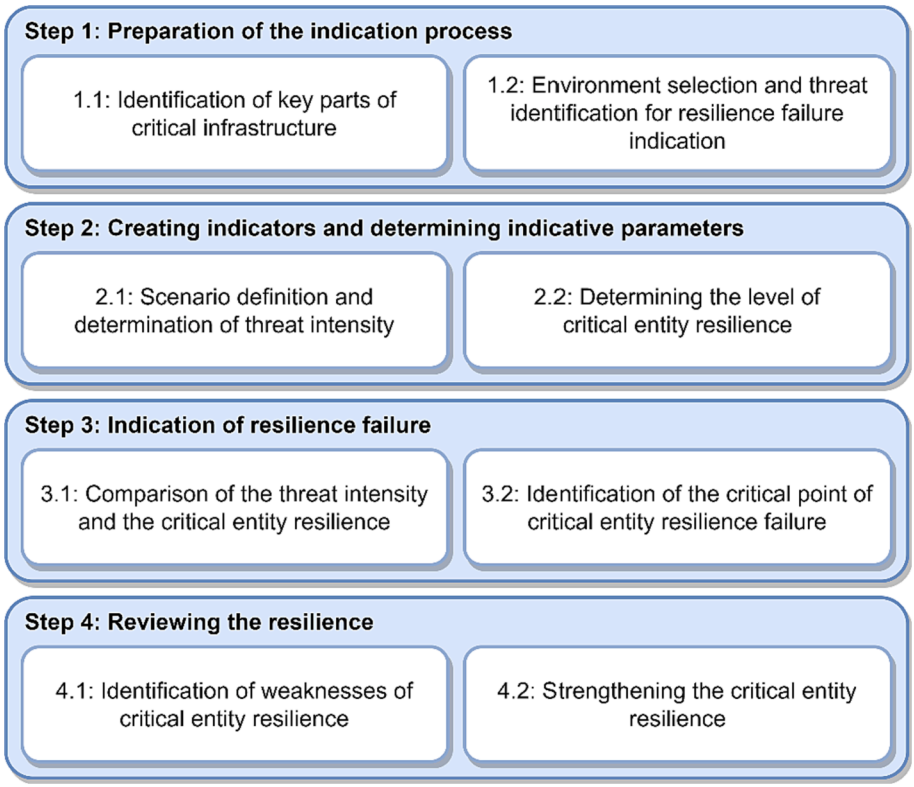

Fig. 5. Process for critical entities resilience failure indication.

each element. This will create a portfolio from which a specific CI element can be selected. In the second part of this step, it is obligatory to select the environment in which the identification of threats will subsequently be carried out.

Sub-step 1.1: Identification of key parts of critical infrastructure

In the past, it was already the case that each Member State of the European Union had to identify and briefly characterise CI elements across sectors, in accordance with Council Directive (2008). A variety of methods have been and continue to be used for this purpose (Alayande et al., 2020; Rehak et al., 2020c; Dvorak et al., 2017; Fekete et al., 2012; NERC, 2009; Council Directive, 2008). Therefore, it can be concluded that each critical entity already has a list of its elements. It is this list that can be used to create the aforementioned CI portfolio. At a minimum, this portfolio should contain an overview of the basic services provided, the structural and performance parameters of the elements and their topological and technological structure. However, it is desirable to revise these elements and, where appropriate, to add additional entities that meet the requirements of the new Directive (EU) (2022).

If a critical entity manages multiple elements of CI, it is necessary to prioritise these entities. For this purpose, a simple ranking can be used, where CI elements are ranked based on their importance or each element is assigned a value from a pre-selected scoring scale, or the prioritisation of elements is done on the basis of pairwise comparisons (Saaty, 1980). However, in this section it is recommended to use more sophisticated methods that are able to prioritise CI elements based on predetermined criteria (preferences) that are key to the critical entity. This condition is fulfilled by methods that work on the basis of a Multi Criteria Analysis (MCA) of multiple variants and at the same time are able to take into account the importance of the set criteria (Saaty, 1996; Brans, 1982; Hwang and Yoon, 1981; Saaty, 1977).

The choice of a specific MCA to identify a piece of CI is entirely up to the preferences of the critical entity. Nevertheless, the basic MCA rules, design principles and proper criteria setting should always be followed (Dodgson et al., 2009; Mendoza et al., 1999). Based on what has been stated so far, the authors of this paper recommend the Analytic Hierarchy Process (AHP method) (Saaty, 1987). It is this method that is appropriate to use when a larger number of criteria are specified by the critical entity or when these criteria are further subdivided. The fact that variations must be identified, evaluation criteria selected, weights assigned to these criteria and a criteria matrix constructed ensures the responsible identification of the key part of the CI, i.e. the identification of a relevant element of the CI.

Sub-step 1.2: Environment selection and threat identification for resilience failure indication

Currently, natural disasters (Panteli and Mancerella, 2017; House of Lords, 2015), cyber threats (Kure and Islam, 2019; Hurst et al., 2014) and especially cascading threats (Lonapalawong et al., 2022; Gjorgiev and Sansavini, 2022; Wang et al., 2018) can be considered to be the most frequently occurring threats disrupting the CI system. However, the threats acting on the CI system are numerous. Therefore, it is important to first determine the specific threat environment that the critical entity will continue to address.

Every critical entity should carry out a risk assessment, i.e., it should have up-to-date and comprehensive knowledge of all the risks to which it is exposed and also make an analysis of these risks (Council Directive, 2008). It is clear that risks are based on possible relevant threats. For the sake of clarity, these threats as well as the whole risk assessment are broken down into relevant environments or areas. For example, threats can be classified into many groups in context of their intent, nature, source of action or impact on the CI system (Osei-Kyei et al., 2021; Bie et al., 2017; Klügel, 2016). The definition of the environment and its subsequent selection is left entirely to the critical entity. However, for the purpose of making an indication of resilience failure of the critical entity, it is important to focus on smaller units, i.e., sub-areas. According to this fact, the authors of this paper recommend dividing the threat environment into six sub-areas, which have been defined by the framework and also shown in Fig. 4. The essence of this part of step 1 is therefore the determination and subsequent selection of the environment and sub-area for the indication of resilience failure. This selection of a specific environment and sub-area becomes an important input to the indication setting and the subsequent Step 2, which focuses on indicator generation. Within this environment, or sub-areas, relevant threats that have the potential to cause an incident are subsequently identified.

The threat identification can again be performed, as in sub-step 1.1, using the MCA method. Again, criteria can be set to prioritise threats using the Risk Priority Number (RPN) value. However, the identification of threats can also be made on the basis of simple decision making. For example, a threat may be selected for which there is a high probability that an incident will occur, i.e. the CI is highly vulnerable to this threat or this threat (according to historical data) occurs very often in the vicinity of the CI and the critical entity wants to be better prepared for the impact of this threat or the critical entity wants to test the readiness of the CI for a specific threat, due to anticipated shortcomings, etc. Therefore, it is entirely up to the preferences of the critical entity whether it is necessary to pay attention to each threat from the selected sub-area, or only a part of it, or whether the critical entity focuses on only one specific threat.

The authors of the article recommend focusing on only one specific threat against which the resilience of the critical entity will be subsequently assessed. For this selection it is advisable to use one of the Risk Assessment Techniques (IEC, 2019). The most suitable ones are tree-based techniques which enable combinations of causes that could lead to an effect. Recommended methods are Event Tree Analysis (IEC, 2010) or Fault Tree Analysis (IEC, 2006). However, the FMECA method (IEC, 2018) is also suitable for this purpose. Threat analyses that the critical entity already has in place can also be used here but need to be updated.

Step 2: Creating indicators and determining indicative parameters

This proposed process is based on an indicator-based approach. Each indicator created must always have defined indicative parameters within a predetermined range against which the indicator can be measured. In relation to the given issue and the fact that the created indicator predicts the relationship between the intensity of the threat and the level of critical entity resilience, it is obligatory to determine the indicative parameters for both the threat environment (i.e., the intensity of the threat) and the critical entity environment (i.e., the resilience of the critical entity). Therefore, it is clear that the range of the assessment scale for the defined indicative parameters must be set identically in both environments in order to compare them.

Sub-step 2.1: Scenario definition and determination of threat intensity

Each threat found has its own specific characteristics by which it can be measured, assessed or evaluated. These specific characteristics are considered to be the nature, degree, intensity, impact and also the intensity of the threat (Splichalova et al., 2020). These specific characteristics of threats, and especially their intensity, are so significant and have a high indicative power in relation to CI that they can be considered to be indicative parameters.

To determine the indicative parameters from the threat environment, it is recommended to first create a scenario of events (i.e., variants of threat action) and impacts that may occur in the CI element. The scenario definition should be as objective as possible. On this basis, the determination should be made using as wide a range of relevant information and data about the threat as possible and should also be preceded

by a specialist discussion or consultation with other experts in the field. To build a scenario, the authors recommend using the Event Tree Analysis (ETA method) (IEC, 2010), which, based on its principle, is able to represent the relationship between the event and the impact, which is strongly influenced by the intensity of the threat. This method can be used to determine the intensity of a threat on existing generally-accepted scales, e.g., the Richter scale (see Fig. 6). However, it can also be used for threats for which no intensity scale has yet been established. An example is the classification of floods according to an index of the potential magnitude of flood flows (NERC, 1975). This classification can range, for example, from flood hazard (Q5–Q10), to widespread (Q20) and extreme (Q50) flooding, up to catastrophic flooding (Q100–Q500).

The determination of the indicative parameters is based on a linear assessment of the probabilistic model, i.e., from 0 to 1. This percentage assessment therefore reflects the intensity, danger, and impact of the threat on the CI element. Based on this fact, each indicative parameter rating scale created becomes a unique representation of each threat. Based on the scenario defined in this way, it is possible to select the most likely variant of the threat and the expected impacts. This provides the assessor with an indicative parameter threat intensity that will subsequently be used in step 3, i.e., an indication of resilience failure.

Sub-step 2.2: Determining the level of critical entity resilience

Over the last decade, several methods have been developed to assess the resilience of CI elements. This assertion is evidenced by review articles summarising the current understanding of resilience along with the correctly setup framework for resilience assessment (Yang et al., 2023; Gasser et al., 2019; Häring et al., 2017), the resilience management process (Curt and Tacnet, 2018) and the development of proposals to improve infrastructure resilience management (Guo et al., 2021). Thus, the critical entity has considerable choice in the application of an appropriate method, the selection of which depends solely on their preferences.

The authors of the paper recommend that the protective part of resilience should be assessed separately, i.e., to set a level for resistance and then for robustness. However, the independent assessment of resilience is currently the subject of research (Rehak et al., 2022a) and it is therefore appropriate to use existing resilience assessment methods that already include some resilience factors (such as crisis preparedness, prediction ability, physical resilience and safety measures) to determine

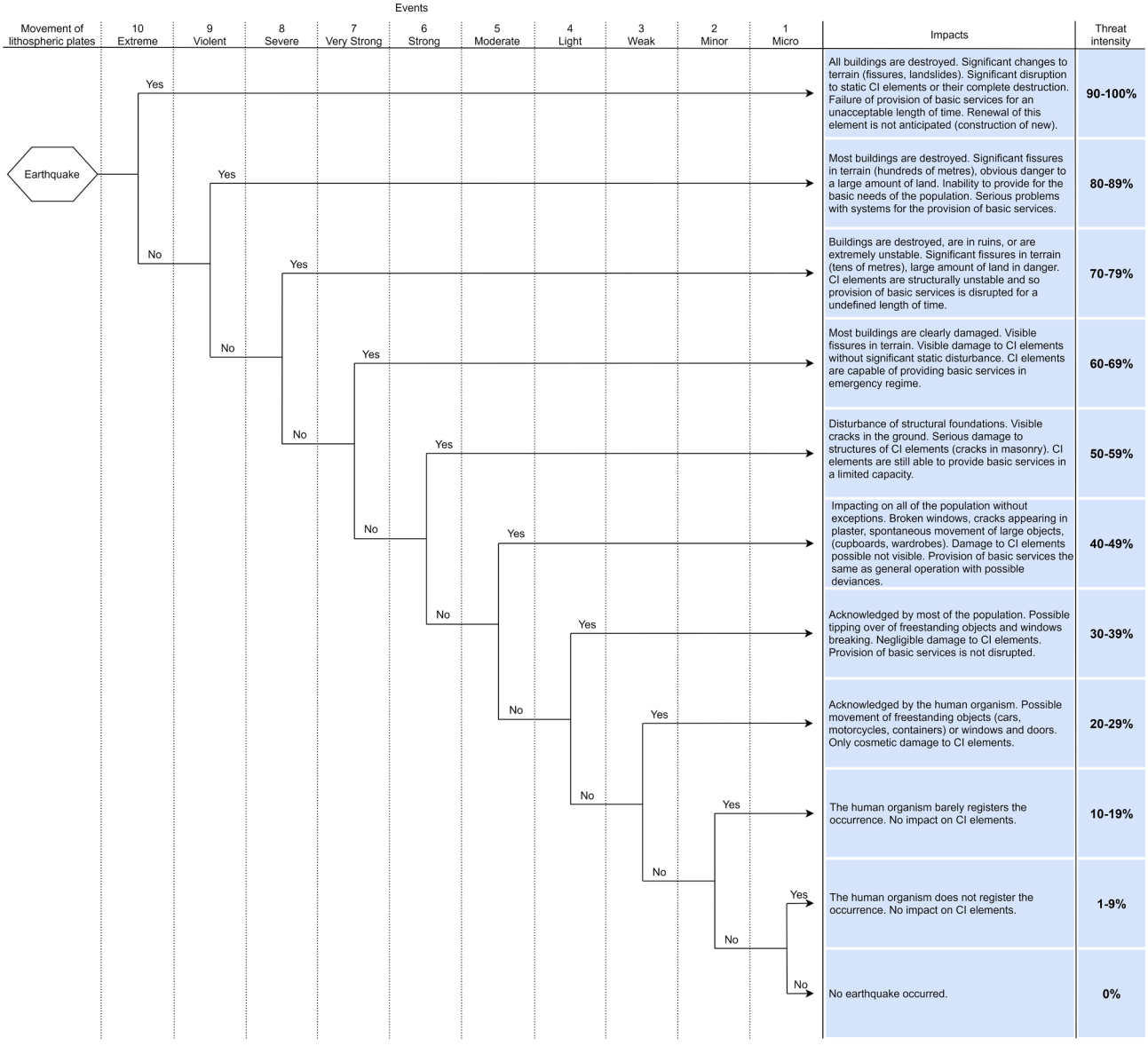

Fig. 6. Threat scenario for the creation of indicative parameters.

resilience. Examples include approaches addressing network infrastructure behaviour during natural hazard events (Reed et al., 2009), resilience based on performance measurement (Avritzer and Bondi, 2012), system resilience with respect to its internal capabilities (Shen and Tang, 2015), or the identification and mapping of interdependency-induced vulnerabilities (Imani and Hajializadeh, 2020). Other methods can also be used to show an overall visualisation of the resilience of a CI element (CISA, 2021; Alheib et al., 2016; Bertocchi et al., 2016; Petit et al., 2013).

As already mentioned, the choice of the method for assessing protective resilience is entirely left to the preferences of the critical entity. However, the authors of the paper recommend the use of methods that assess and subsequently present the resilience level quantitatively (Mottahedi et al., 2021; Raoufi and Vahidinasab, 2021; Argyroudis et al., 2020; Rehak et al., 2019; Moslehi and Reddy, 2018; Nan and Sansavini, 2017; Vugrin and Camphouse, 2011). An example of a possible outcome from a resilience assessment is presented in Fig. 7.

It is significant that the identified level of resilience is displayed in a specific percentage rating scale. Both of these conditions are met by the CIERA method (Rehak et al., 2019), which uses a table to assess the level of the protective part of resilience, with percentages divided into levels that approximate the current state of the critical entity in question. The great advantage of this method is that it provides the results of the assessment as a specific percentage. This percentage value can be considered as an indication of the resilience of the critical entity, which will serve as a second comparative parameter.

Step 3: Indication of resilience failure

This step is central to the whole procedure and involves two successive sub-steps. In the first sub-step, a comparison of indicative parameters is made, through which the critical entity is provided with information to indicate whether or not a resilience failure will occur. In a subsequent sub-step, a critical point of resilience failure of the critical entity is identified.

Sub-step 3.1: Comparison of the threat intensity and the critical entity resilience

In the preceding step 2, the critical entity established the indicative parameters for the threat environment and the critical entity environment. Since these indicative parameters were set on the same rating scale (i.e., percentage), they can now be compared with each other. The comparison of these indicative parameters is suitable to be done in the manner presented in Fig. 2.

The purpose of the comparison of the established indicative parameters is to determine the current state of the critical entity and whether it has a sufficient level of the protective part of resilience to defend against the selected threat, also considering the threat's intensity. According to this comparison, the critical point of failure of the critical entity resilience can be identified in the next part of this step.

Sub-step 3.2: Identification of the critical point of critical entity resilience failure

The results of the comparison of the indicative parameters provide demonstrable data to identify the critical point of failure of the critical entity's resilience. This critical point represents the maximum possible threat intensity that the protective part of the critical entity's resilience is able to absorb. If the comparison has revealed a lower percentage resilience level of the critical entity than the expected threat intensity, then a failure of critical entity resilience and the essential services provided by it is indicated. This is considered a critical point and must be addressed immediately. Each critical entity, upon identification of a critical point, shall endeavour to strengthen the protective part of the resilience as soon as possible through a retrospective review. The abstraction of this review is the weaknesses identification that are deficient, which is the subject of the last step of this process.

If the comparison has not demonstrated a critical point of resilience failure in the critical entity, the application of this process may be discontinued. However, it is still recommended by the authors of the paper to conduct a review of the level of resilience, which may reveal weaknesses and subsequently lead to the identification of new approaches to strengthen them.

Step 4: Reviewing the resilience

The fourth step of the critical entity resilience failure indication procedure is to examine the resilience level of the individual factors. This review can be based on the results of the critical entity resilience level assessment (sub-step 2.2.2) and consists of identifying the critical entity resilience weaknesses and then strengthening them.

Sub-step 4.1: Identification of weaknesses of critical entity resilience

If a critical point has been identified in sub-step 3.2, the process of identifying weaknesses, i.e., dissecting the results of the critical entity resilience assessment, should be initiated immediately. The essence of this process is to find the factors that scored low in the critical entity resilience assessment. The authors of the article recommend, based on logical selection, creating a list of evaluated factors that significantly reduce the resulting level of resilience. It is clear that such factors will exhibit significant deficiencies contributing to the vulnerability of the critical entity, and thus require increased attention. Based on what has

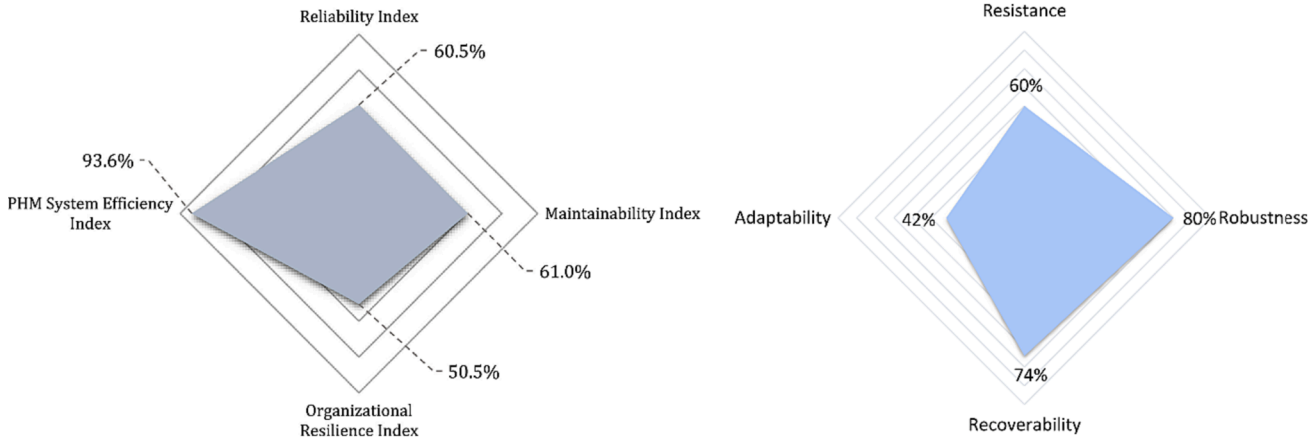

Fig. 7. Example of presentation of results of quantitative resilience assessment of critical infrastructure elements (Mottahedi et al., 2021; Rehak et al., 2019).

been presented so far, it can be concluded that the identification of these weaknesses contributes to the effective and targeted strengthening of the critical entity resilience.

Sub-step 4.2: Strengthening the critical entity resilience

Increasing the resilience of a critical entity can be implemented through a variety of means based on the selection and adoption of appropriate measures. The application of these measures is done primarily for the weaknesses identified in the previous sub-step 4.1. The critical entity should adopt security, technical and/or organisational measures that effectively enhance resilience and prevent incidents from occurring (Directive (EU), 2022). Effective measures can be considered to be those that are targeted, adequate to the expected intensity of the threat and inexpensive in terms of time and money.

The selection of appropriate measures to strengthen the resilience of a critical entity can be implemented using specific approaches that are currently receiving increasing attention. Existing approaches include those that, for example, classify security measures according to time (Shakou et al., 2019), type of resilience (Janeckova, 2023) or their areas of applicability (Rehak et al., 2022c; Kete et al., 2018).

6. Use case of the CERFI Tool in the energy sector

An example of practical application of the developed CERFI Tool is presented using a selected critical entity in the energy sector operating in the Czech Republic, which is a critical entity of particular European significance, but for security reasons remains anonymous. The potential resilience failure of this critical entity will be assessed against a sub-area of physical threats.

The first step in the application of the CERFI Tool is the preparation of the indication process (**step 1**). As part of this step, the assessed energy entity was classified in the Electricity sub-sector, Transmission system operators category (Directive, 2019). It is then possible to start identifying the key part of the CI (**sub-step 1.1**). This identification is based on an existing list of CI elements of the entity. However, as this is an entity with a large number of elements, it is necessary to prioritise them. For this purpose, a group of substation elements with a voltage of at least 110 kV were selected by the Security Liaison Officer. From this group of elements, one specific CI element was then selected to be further subject to the indication process. The selection of this element was carried out through the AHP method (Saaty, 1987) based on the selected criteria (see Fig. 8 presenting the evaluation of only part of the identified elements).

It is then possible to proceed to the selection of the environment and identification of threats to indicate resilience failure (**sub-step 1.2**). In the context of the current security environment, the Security Liaison Officer selected the area of anthropogenic threats, sub-area physical threats. In this sub-area, attention is subsequently paid in particular to threats of a deliberate nature. The identification of these threats is based on a security study that the critical entity regularly commissions (Deloitte Advisory, 2022). Prioritisation was then performed using the FMECA method (IEC, 2018). Based on these results, the two most significant threats (with the highest RPN) were identified and the threat with the higher occurrence rate selected for further evaluation (see Fig. 9).

The next step of the CERFI Tool application is to create an indicator and determine the indicative parameters (step 2). The essence of this step is to create an indicator against each selected threat. In this case, the indicator is "Failure of substation resilience due to physical assault using a motor vehicle". For this indicator, it is then necessary to establish indicative parameters, both on the side of the threat and the critical entity. The essence of establishing the indicative parameter on the threat side is to define the scenario and determine the intensity of the threat (**sub-step 2.1**). In this case, the scenario was built using the ETA method (IEC, 2010) and based on this, the evaluator selected a physical assault scenario using an N3 category motor vehicle (see Fig. 10). The intensity of the threat in this case was set at the middle level of the interval range (90%), as an assault (crash) by a truck (Category N3) weighing more than 12 tonnes, with the use of hazardous substances, is anticipated.

The determination of the indicative parameter on the side of the critical entity consists in assessing the level of its resilience (**sub-step 2.2**). For this purpose, an upgraded version of the CIERA method (Rehak et al., 2019) was selected, which allows for a separate assessment of the protective part of resilience, i.e., the resistance and robustness of the critical entity. The results of the assessment are presented in Figs. 11 and 12.

The third step in the application of the CERFI Tool is the indication of resilience failure (**step 3**). First, it is necessary to compare the intensity of the selected threat and the level of critical entity resilience (**sub-step**

Selection of key critical infrastructure element

Criteria	Status		Type		Criticality		
Local weights	0.166		0.073		0.761		
Subcriteria	**Age of the building**	**The last reconstruction**	**Classification**	**Manner of service**	**Victims**	**Public**	**Economy**
Local weights	0.125	0.875	0.889	0.111	0.775	0.169	0.056
Global weights	0.021	0.145	0.065	0.008	0.589	0.129	0.043

								Evaluation	Order
Transmission station 1	10	-	400/220 kV	Without operator, regularly supervision	140	500,000	0.9	0.141	3
Transmission station 2	25	2015	400/220 kV	Without operator, remote controlled	120	135,000	0.3	0.135	4
Transmission station 3	30	2003	400/220 kV	Permanent operator	200	180,000	0.7	0.189	2
Transmission station 4	35	2022	400/220 kV	Without operator, remote controlled	450	700,000	1.5	0.372	1
Transmission station 5	15	-	400/110 kV	Permanent operator	100	100,000	0.8	0.077	6
Transmission station 6	20	2000	400/110 kV	Permanent operator	55	125,000	0.2	0.086	5

Fig. 8. Prioritisation of critical infrastructure elements through the AHP method.

Element/Function	Threat	Effect(s) of Failure/Threat	Cause(s) of Failure	Severity	Occurrence	Detection	RPN
Transmission station 4 - ensuring a continuous supply of electricity in the required quantity	Forced entry of a stranger into the space	Restriction of operation of the element, loss of functionality of the element.	Deficiently assuring perimeter of the element.	1	4	1	4
	Unauthorized access of a stranger to the space	Theft and misuse of information about the element, the possibility of damage to the functional parts of the element.	Deficiently physical protection system – regime measures.	1	3	1	3
	Breaking in to the space	Disrupt of the integrity of the security agens of the element, with subsequent damage to key parts of the element.	Deficiently assuring perimeter of the element, failure of some safety features.	1	3	1	3
	Theft by a stranger	Theft of agens that can be used, for example, in the repair of an element or for its regular maintenance.	Deficiently assuring perimeter of the element.	1	4	2	8
	Use of a weapon/robbery	Imperilment of employees or damage to functional parts of the element.	Deficiently element security and assuring perimeter of the element.	2	3	1	6
	Destruction of outdoor lines	Interruption of electricity supply for the basic operation of the electric station.	Deficiently backup system.	1	4	1	4
	Unauthorized handling of elements of the physical protection systém	Disrupt of the integrity of the security agens of the element, with subsequent damage to key parts of the element.	Deficiently element security.	1	5	3	15
	Attack with a decoy explosive system	Partial or complete destruction of the element, interruption of the supply of electricity.	Deficiently assuring perimeter of the element.	4	4	5	80
	Assault by motor vehicle	Serious disruption, destruction or complete destruction of equipment, devices or apparatus, ensuring the key functions of the element.	Deficiently assuring perimeter of the element.	3	5	5	75
	Attack with standard technical tools	Disrupt protection of the perimeter, destruction of the agens of the element ensuring transformation of voltage.	Deficiently assuring perimeter of the element.	2	4	4	32
	Impersonation by third-party workers	Theft and misuse of information about the element, the possibility of damage to the functional parts of the element.	Deficiently physical protection system – regime measures.	1	4	2	8

Fig. 9. Threat prioritisation against the selected substation.

3.1). Since these indications have been determined on the same rating scale (i.e., percentage), they can now be compared with each other. The results of the comparison are presented in Fig. 13.

Based on the results of the comparison of the indicative parameters, it is possible to state that the critical entity resistance level (96%) should be sufficient to prevent the incident occurrence, since the threat intensity reaches only 90%. However, this absorptive capacity of resistance is so low that it is advisable to also pay attention to the identification of the critical point of critical entity resilience failure (**sub-step 3.2**). In this case, critical point has been identified as the level of critical entity robustness (80%) is lower than the intensity of the threat (90%). In such a case, potential damage to the CI element is expected, and therefore it is recommended to proceed with the critical entity resilience review (**step 4**). This last step of the CERFI Tool application consists in identifying the weaknesses of the critical entity resilience and then strengthening the level of this resilience. Identifying the weaknesses of resilience (**sub-step 4.1**) consists of identifying factors that score low on the critical entity resilience assessment, i.e., a score of 3 or less. In this case, these were the following measurable items:

– 2.2.2 Seismic resistance (Responsiveness),
– 2.3.1 The probability of intruder elimination (Responsiveness).

For these measurable items, it is recommended to initiate the process of strengthening the critical entity resilience (**sub-step 4.2**). In the case of item 2.2.2, no specific measures need to be taken as the CI element under assessment is located in an area without seismic activity. In the case of item 2.3.1, it is recommended to implement resilience strengthening using currently available approaches to assess and strengthen physical protection systems (e.g., Garcia, 2008; Vidrikova et al., 2017; Kampova et al., 2020).

7. Conclusion

With the adoption of Directive (EU), 2022/2557, the focus on CI has shifted from elements to entities. This change in perception is very positive, as the basis for reliable CI is sufficiently resilient critical entities. However, the adoption of the Directive has raised the question of how to assess the resilience of critical entities in relation to contemporary security threats. Until now, all attention has been devoted exclusively to assessing the resilience of CI elements. An important solution to this problem could be a predictive indication of resilience failure of critical entities. For this purpose, the CERFI Tool was developed by the authors of the paper.

The essence of the CERFI Tool is a probabilistic algorithm that predicts the relationship between the intensity of the threat and the protective part of critical entity resilience through indicators (to be created by the assessors themselves). The result of this prediction is an indication of the critical point of failure of the critical entity's resilience in phases of prevention and absorption of impacts. Failure of the critical entity resilience in this context refers to a situation where the level of the protective part of resilience is not sufficient to protect the critical entity, as a result of which there is an immediate failure of the supply of basic services provided by the critical entity. At the same time, it is necessary to mention some limitations of this approach. The CERFI Tool enables the indication of the failure of resilience of only one critical entity as a result of the action of only one threat and the subsequent occurrence of only one incident. As part of the assessment, it is therefore not possible to consider the interdependencies of critical infrastructures or actually occurring cascading or synergistic effects.

The CERFI Tool thus contributes to improving the security of

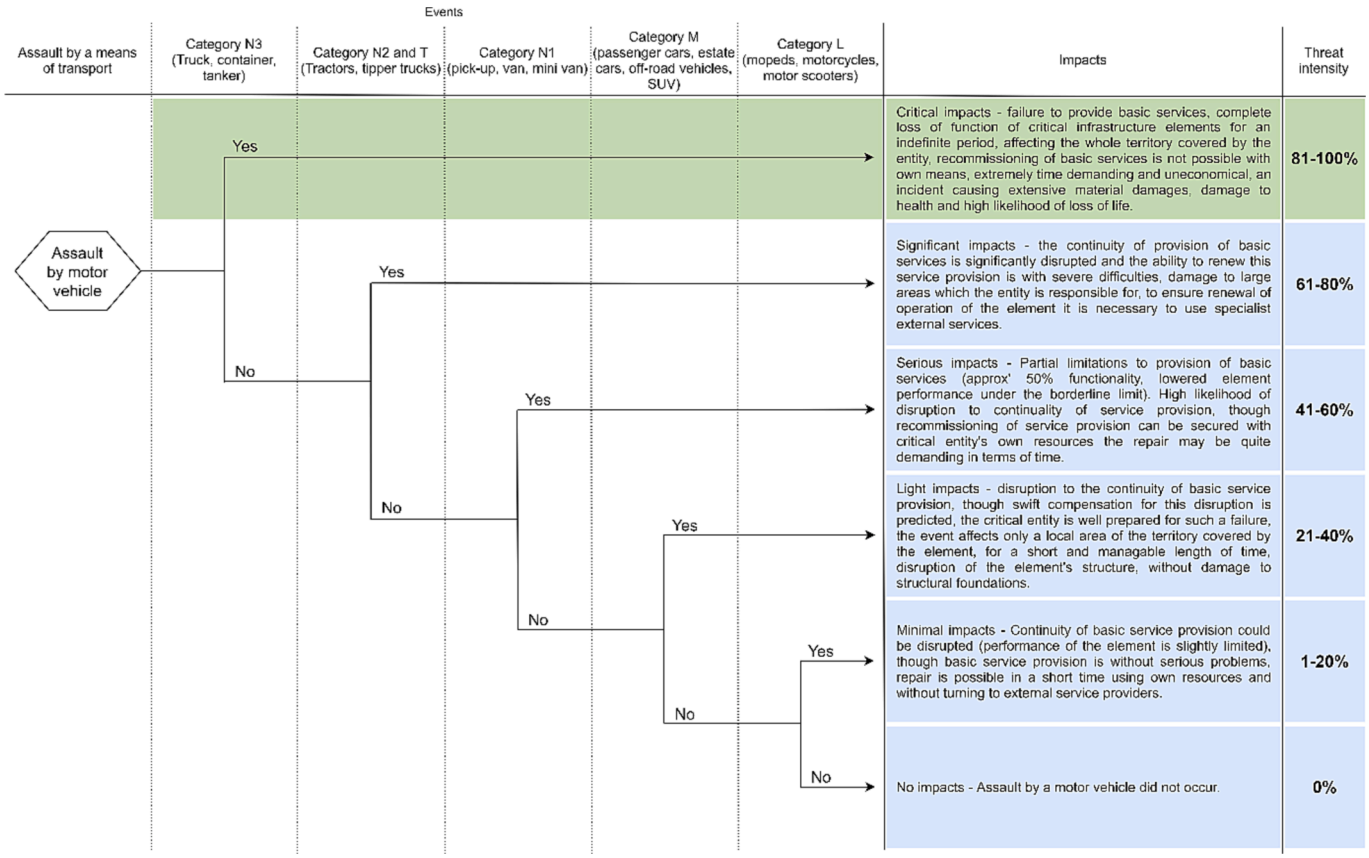

Fig. 10. Scenario of a threat of physical attack using a motor vehicle.

CIERA²
Critical Infrastructure Elements Resilience Assessment

Critical Infrastructure Elements Resilience Assessment

400/220 kV transformation station — *Element name*

Assault by motor vehicle — *Threat name*

2015-2019 RESILIENCE Critical Infrastructure

1. Assessment of Resistance

Number	Variables	Measurable items	Score MI_k [1-5]	Weight w_k	Variable $V_j = 20 \sum MI_k w_k$ [%]	Weight v_j	Resistance $RES = \sum V_j v_j$ [%]
1.1.1	Crisis preparedness	Risk assessment	4	0,4	92	Point = 0,20 Areal = 0,30 Linear = 0,20	96
1.1.2		Safety planning	5	0,6			
1.2.1	Anticipation ability	Procedures indicating disruption of resilience	4	0,4	86	Point = 0,25 Areal = 0,15 Linear = 0,35	
1.2.2		Regular checks and surveys	5	0,3			
1.2.3		Software applications for predicting incidents	4	0,3			
1.3.1	Detection capability	Monitoring	5	0,6	100	Point = 0,25 Areal = 0,20 Linear = 0,30	
1.3.2		Cumulative probability of intruder detection	5	0,4			
1.4.1	Security measures	Monitoring	5	0,4	100	Point = 0,30 Areal = 0,35 Linear = 0,15	
1.4.2		Physical protection system	5	0,6			

Fig. 11. Assessment of resistance of critical entity.

technically oriented infrastructure systems, especially those in the areas of energy and transport. However, in some cases it can also be applied to selected socio-economic infrastructure systems, e.g., in the field of emergency services or healthcare. The CERFI Tool is primarily intended for security liaison officers of individual infrastructure systems. By applying this tool, they can obtain valuable information about the level of the protective part of resilience of a critical entity and its elements. However, this information is only predictive in nature and is essentially

CIERA² Critical Infrastructure Elements Resilience Assessment

Critical Infrastructure Elements Resilience Assessment

400/220 kV transformation station — *Element name*

Assault by motor vehicle — *Threat name*

2015-2019 RESILIENCE Critical Infrastructure

2. Assessment of Robustness

Number	Variables	Measurable items	Score MI_k [1-5]	Weight w_k	Variable $V_j = 20 \sum MI_k w_k$ [%]	Weight v_j	Robustness $ROB = \sum V_j v_j$ [%]
2.1.1	Redundancy	Power supply backup of the technical protection system	5	0,3	86	Point = 0,25 Areal = 0,20 Linear = 0,40	80
2.1.2		Backup of the technical protection system elements	4	0,4			
2.1.3		Redundancy of technological solutions	4	0,3			
2.2.1	Physical resistance	Fire resistance	5	0,4	82	Point = 0,40 Areal = 0,40 Linear = 0,35	
2.2.2		Seismic resistance	3	0,3			
2.2.3		Explosion resistance	4	0,3			
2.3.1	Responsiveness	The probability of intruder elimination	3	0,5	74	Point = 0,35 Areal = 0,40 Linear = 0,25	
2.3.2		Influence of false alarms on reactivity	4	0,3			
2.3.3		Decrease of function	5	0,2			

Fig. 12. Assessment of robustness of critical entity.

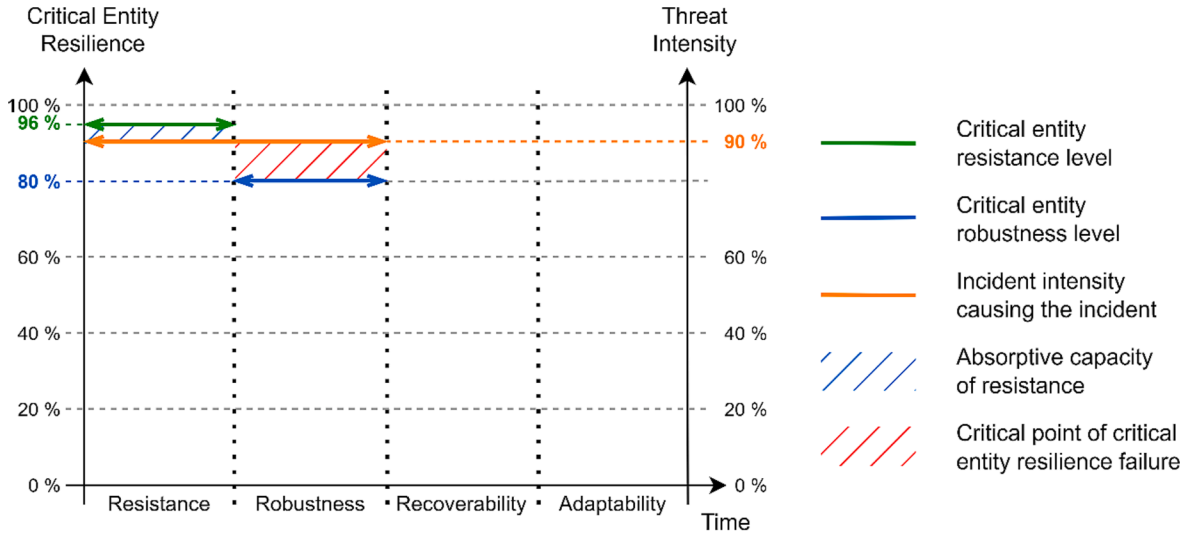

Fig. 13. Comparison of indicative parameters of selected threats and critical entities.

an indication of weaknesses that require subsequent attention.

The CERFI Tool has already been successfully tested in practice on selected critical entities in the energy and transport sectors. This is illustrated by the case study presented at the end of the article. This study focused on the indication of a substation resilience failure due to a physical assault using a motor vehicle. The results of the study show that the CERFI Tool indicated an insufficient level of critical entity resilience in question and identified weaknesses that need increased attention. According to the findings, it is proposed that further research be directed particularly in the area of tools for strengthening the resilience of critical entities and assessing their effectivity. It would also be appropriate to pay attention to research on the critical entities' resilience failure indication in the recovery and adaptation phase.

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 SP2023/086].

CRediT authorship contribution statement

David Rehak: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization. **Alena Splichalova:** Conceptualization, Formal Analysis, Investigation, Methodology, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Martin Hromada:** Writing – review & editing, Writing – original draft, Validation, Methodology, Data curation. **Neil Walker:** Writing – review & editing, Writing – original draft, Validation, Formal analysis. **Heidi**

Janeckova: Data Curation, Formal Analysis, Investigation, Resources, Validation, Writing – original draft, Writing – review & editing. **Josef Ristvej:** Writing – review & editing, Writing – original draft, Validation, Investigation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abbasnejadfard, M., Bastami, M., Abbasnejadfard, M., Borzoo, S., 2022. Novel deterministic and probabilistic resilience assessment measures for engineering and infrastructure systems based on the economic impacts. Int. J. Disaster Risk Reduct. 75, 102956 https://doi.org/10.1016/j.ijdrr.2022.102956.

Advisory, D., 2022. Methodology to Ensure of Critical Infrastructure Protection in the Area of Electricity Generation, Transmission and Distribution. Deloitte Advisory, Prague in Czech.

Alayande, A.S., Jimoh, A.A.G., Yusuff, A.A., 2020. Identification of critical elements in interconnected power networks. Iran. J. Sci. Technol. Trans. Electr. Eng. 44, 197–211. https://doi.org/10.1007/s40998-019-00235-1.

Alheib, M., Baker, G., Bouffier, C., Cadete, G., Carreira, E., Gattinesi, P., Guay, F., Honfi, D., Eriksson, K., Lange, K., Lundin, E., Malm, A., Melkunaite, L., Merad, M., Miradasilva, M., Petersen, L., Rodrigues, J., Salmon, R., Theocharidou, M., Willot, A., 2016. Report of Criteria for Evaluating Resilience, Ref. Ares 2519174 - 31/05/2016. SP Technical Research Institute of Sweden, Vaxjo.

Annarelli, A., Battistella, C., Nonino, F., 2020. A framework to evaluate the effects of organizational resilience on service quality. Sustainability 12 (3), 958. https://doi.org/10.3390/su12030958.

Argyroudis, S.A., Mitoulis, S.A., Hofer, L., Zanini, M.A., Tubaldi, E., Frangopol, D.M., 2020. Resilience assessment framework for critical infrastructure in a multi-hazard environment: case study on transport assets. Sci. Total Environ. 714, 136854 https://doi.org/10.1016/j.scitotenv.2020.136854.

ASIS, 2009. The Organizational Resilience Standard [ASIS SPC.1-2009]. American National Standards Institute, Washington, DC.

Avritzer, A., Bondi, A.B., 2012. Resilience assessment based on performance testing. In: Wolter, K., Avritzer, A., Vieira, M., van Moorsel, A. (Eds.), Resilience Assessment and Evaluation of Computing Systems. Springer, Berlin, Heidelberg, pp. 305–322. https://doi.org/10.1007/978-3-642-29032-9_15.

Beccuti, M., Chiaradonna, S., Giandomenico, F., Donatelli, S., Dondossola, G., Franceschinis, G., 2012. Quantification of dependencies between electrical and information infrastructures. Int. J. Crit. Infrastruct. Prot. 5 (1), 14–27. https://doi.org/10.1016/j.ijcip.2012.01.003.

Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., Oliva, G., Traballesi, A., 2016. Guidelines for Critical Infrastructure Resilience Evaluation. Italian Association of Critical Infrastructures' Experts, Roma.

Bie, Z., Lin, Y., Li, G., Lim, F., 2017. Battling the extreme: a study on the power system resilience. Proc. IEEE 105, 1253–1266. https://doi.org/10.1109/JPROC.2017.2679040.

Brans, J.P., 1982. Lingenierie de la decision. Elaboration dinstruments daide a la decision. Methode PROMETHEE. In: Nadeau, R., Landry, M. (Eds.), Laide a la Decision: Nature, Instrument s et Perspectives Davenir. Presses de Universite Laval, Quebec, pp. 183–214 (in France).

Bunge, M., 2003. Philosophical Dictionary, Enlarged ed. Prometheus Books, New York, NY.

Cai, B., Xie, M., Liu, Y., Liu, Y., Feng, Q., 2018. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab. Eng. Syst. Saf. 172, 216–224. https://doi.org/10.1016/j.ress.2017.12.021.

Carlson, J.L., Haffenden, R.A., Bassett, G.W., Buehring, W.A., Collins, M.J., Folga, S.M., Petit, F.D., Phillips, J.A., Verner, D.R., Whitfield, R.G., 2012. Resilience: Theory and Applications. Argonne National Laboratory, Lemont, IL.

Chen, R., Xie, Y., Liu, Y., 2021. Defining, conceptualizing, and measuring organizational resilience: a multiple case study. Sustainability 13 (5), 2517. https://doi.org/10.3390/su13052517.

Chevalier, S., Choiniere, R., Bernier, L., Sauvageau, Y., Masson, I., Cadieux, E., 1992. User Guide to 40 Community Health Indicators. Health and Welfare Canada, Ottawa.

CISA, 2021. Methodology for assessing regional infrastructure resilience. Cybersecurity and Infrastructure Security Agency Infrastructure Security Division. U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency, Washington, DC.

Collins, M., Petit, F., Buehring, W., Fisher, R., Whitfield, R., 2011. Protective measures and vulnerability indices for the enhanced critical infrastructure protection programme. Int. J. Crit. Infrastruct. 7 (3), 200–2019. https://doi.org/10.1504/IJCIS.2011.042976.

European Commission, 2020. EU Road Safety Policy Framework 2021-2030: Next steps towards 'Vision Zero'. Luxembourg: Publications Office of the European Union. https://doi.org/10.2832/391271.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Curt, C., Tacnet, J.M., 2018. Resilience of critical infrastructures: review and analysis of current approaches. Risk Anal. 38 (11), 2441–2458. https://doi.org/10.1111/risa.13166.

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

Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU.

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.

Dobranskyte-Niskota, A., Perujo, A., Pregl, M., 2007. Indicators to Assess Sustainability of Transport Activities – Part 1: Review of the Existing Transport Sustainability Indicator Initiatives and Development of an Indicator Set to Assess Transport Sustainability Performance. Office for Official Publications of the European Communities, Luxembourg.

Dodgson, J., Spackman, M., Pearman, A., Phillips, L., 2009. Multi-Criteria Analysis: A Manual. Department for Communities and Local Government, London https://eprints.lse.ac.uk/12761/1/Multi-criteria_Analysis.pdf.

Dvorak, Z., Chovancikova, N., 2020. Research of safety management indicators. Tech. Soc. Sci. J. 8 (2020), 552–1545. https://doi.org/10.47577/tssj.v8i1.545.

Dvorak, Z., Sventekova, E., Rehak, D., Cekerevac, Z., 2017. Assessment of critical infrastructure elements in transport. Proc. Eng. 187, 548–555. https://doi.org/10.1016/j.proeng.2017.04.413.

Esmap, 2018. Regulatory Indicators for Sustainable Energy. Energy Sector Management Assistance Program, The World Bank, Washington, DC.

Fekete, A., Lauwe, P., Geier, W., 2012. Risk management goals and identification of critical infrastructures. Int. J. Crit. Infrastruct. 8 (4), 336–353. https://doi.org/10.1504/IJCIS.2012.050108.

Fisher, R., Norman, M., 2010. Developing measurement indices to enhance protection and resilience of critical infrastructure and key resources. J. Bus. Contin. Emer. Plan. 4 (3), 191–206.

Fu, X., Hopton, M.E., Wang, X., 2021. Assessment of green infrastructure performance through an urban resilience lens. J. Clean. Prod. 289, 125146 https://doi.org/10.1016/j.jclepro.2020.125146.

Galbusera, L., Trucco, P., Giannopoulos, G., 2020. Modeling interdependencies in multi-sectoral critical infrastructure systems: evolving the DMCI approach. Reliab. Eng. Syst. Saf. 203, 107072 https://doi.org/10.1016/j.ress.2020.107072.

Gallopin, G.C., 1997. Indicators and their use: information for decision-making. SustAinAbility IndicAtors: A Report on the Project on SustAinAbility IndicAtors of SustAinAble Development. Wiley, New York, NY.

Garcia, M.L., 2008. Design and Evaluation of Physical Protection Systems. 2nd edit. Butterworth-Heinemann, Oxford. https://doi.org/10.1016/C2009-0-25612-1.

Gasser, P., Lustenberger, P., Cinelli, M., Kim, W., Spada, M., Burgherr, P., Hirschberg, S., Božidar, S., Sun, T.Z., 2019. A review on resilience assessment of energy systems. Sust. Resil. Infrastruct. 6 (2), 1–27. https://doi.org/10.1080/23789689.2019.1610600.

Ghorani, R., Fotuhi-Firuzabad, M., Dehghanian, P., Li, W., 2015. Identifying critical components for reliability centred maintenance management of deregulated power systems. IET Gener. Transm. Distrib. 9 (9), 828–837. https://doi.org/10.1049/iet-gtd.2014.0361.

Giannopoulos, G., Dorneanu, B., Jonkeren, O., 2013. Risk assessment methodology for critical infrastructure protection. European Commission, Joint Research Centre, Ispra. https://doi.org/10.2788/78850.

Gjerde, O., Kjølle, G.H., Hernes, J.G., Hestnes, B., Foosnæs, J.A., 2011. Indicators to monitor and manage electricity distribution system vulnerability. In: 21st International Conference on Electricity Distribution (CIRED), p. 0805.

Gjorgiev, B., Sansavini, G., 2022. Identifying and assessing power system vulnerabilities to transmission asset outages via cascading failure analysis. Reliab. Eng. Syst. Saf. 217, 108085 https://doi.org/10.1016/j.ress.2021.108085.

Gonçalves, L., Navarro, J.B., Sala, R., 2019. Spanish validation of the Benchmark Resilience Tool (short-form version) to evaluate organisational resilience. Saf. Sci. 111, 94–101. https://doi.org/10.1016/j.ssci.2018.09.015.

Guo, D., Shan, M., Owusu, E.K., 2021. Resilience assessment frameworks of critical infrastructures: state-of-the-art review. Buildings 11 (10), 464. https://doi.org/10.3390/buildings11100464.

Halat, M., Gaitán, V., 2015. Electrical & Telecom infrastructure description and identification of critical elements and threats. [Project report]. Aplicaciones de Informática Avanzada, Barcelona.

Hall, E., 2014. Indicators to assess the exposure of critical infrastructure in England to current and projected climate hazards. [Final project report]. HR Wallingford, Wallingford.

Häring, I., Sansavini, G., Bellini, E., Martyn, N., Kovalenko, T., Kitsak, M., Vogelbacher, G., Ross, K., Bergerhausen, U., Barker, K., Linkov, I., 2017. Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies. In: Linkov, I., Palma-Oliveira, J. (Eds.), Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-1123-2_2.

Hiete, M., Merz, M., 2009. An indicator framework to assess the vulnerability of industrial sectors against indirect disaster losses. 6th International Conference on Information Systems for Crisis Response and Management – Boundary SpannIng Initiatives and New Perspectives (ISCRAM), Gothenburg.

Hofmann, M., Kjøllea, G.H., Gjerde, O., 2012. Development of indicators to monitor vulnerabilities in power systems. In: 11th International Probabilistic Safety

Assessment and Management Conference and the Annual European Safety and Reliability Conference, pp. 5869–5878.
Holling, C.S., Bazykin, A., Bunnell, P., Clark, C.W., Gallopin, C.G., Hilborn, R., Jones, D. D., Peterman, M.R., Rabinovich, E.J., Steele, H.J., Walters, J.C., 1978. Adaptive Environmental Assessment and Management. International Institute for Applied Systems Analysis, Luxenburg.
House of Lords, 2015. The Resilience of the Electricity System. The Stationery Office Limited, London.
Hromada, M., Rehak, D., Lukas, L., 2021. Resilience assessment in electricity critical infrastructure from the point of view of converged security. Energies 14, 1624. https://doi.org/10.3390/en14061624.
Hurst, W., Merabti, M., Fergus, P., 2014. A survey of critical infrastructure security. IFIP Advances in Information and Communication Technology 441. https://doi.org/10.1007/978-3-662-45355-1_9.
Hwang, C.L., Yoon, K., 1981. Multiple Attribute Decision Making: Methods and Applications. Springer-Verlag, New York, NY.
IEC 61025, 2006. Fault Tree Analysis (FTA). International Electrotechnical Commission, Geneva.
IEC 62502, 2010. Analysis Techniques for Dependability – Event Tree Analysis (ETA). International Electrotechnical Commission, Geneva.
IEC 60812, 2018. Failure modes and effects analysis (FMEA and FMECA). International Electrotechnical Commission, Geneva.
IEC 31010, 2019. Risk Management—Risk Assessment Techniques. International Organization for Standardization, Geneva.
Imani, M., Hajializadeh, D., 2020. A resilience assessment framework for critical infrastructure networks' interdependencies. Water Sci. Technol. 81 (7), 1420–1431. https://doi.org/10.2166/wst.2019.367.
ISO 22316, 2017. Security and Resilience – Organizational Resilience – Principles and Attributes. International Organization for Standardization, Geneva.
ISO 31000, 2018. Risk management – Guidelines. International Organization for Standardization, Geneva.
Itf, 2019. Road Safety Annual Report 2019. International Transport Forum, Paris.
ITF, 2020. ITF Transport Statistics: Transport performance indicators. Organisation for Economic Co-operation and Development, Paris. https://doi.org/10.1787/trsprt-data-en.
Itu, 2016. The Partnership on Measuring ICT for Development: Core List of ICT Indicators: March 2016 version. International Telecommunication Union, Geneva.
Itu, 2017. Measuring the Information Society Report 2017, Vol. 1. International Telecommunication Union, Geneva.
Itu, 2022. World Telecommunication/ICT Indicators Database 2022. International Telecommunication Union, Geneva.
Janeckova, H., 2023. The Basis for Strengthening Organisational Resilience of Critical Transport Infrastructure Entities. In 15th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2023) (article in press).
Joung, B.C., Carrell, J., Sarkar, P., Feng, C.S., 2012. Categorization of indicators for sustainable manufacturing. Ecol. Ind. 24, 148–157. https://doi.org/10.1016/j.ecolind.2012.05.030.
Kampova, K., Lovecek, T., Rehak, D., 2020. Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak Republic. Int. J. Crit. Infrastruct. Prot. 30, 100376 https://doi.org/10.1016/j.ijcip.2020.100376.
Kete, N., Punzo, G., Linkov, I., 2018. Enhancing resilience within and between critical infrastructure systems. Environ. Syst. Decis. 38, 275–277. https://doi.org/10.1007/s10669-018-9706-5.
Klügel, J.U., 2016. Risk and hazard assessment of extreme natural events for critical infrastructures. Int. J. Safety Secur. Eng. 6 (2), 96–103. https://doi.org/10.2495/SAFE-V6-N2-96-103.
Kozine, I., Petrenj, B., Trucco, P., 2018. Resilience capacities assessment for critical infrastructures disruption: the READ framework. Int. J. Crit. Infrastruct. 14 (3), 199–220. https://doi.org/10.1504/IJCIS.2018.10015604.
Kruyt, B., van Vuuren, D.P., de Vries, H.J.M., Groenenberg, H., 2009. Indicators for energy security. Energy Policy 6 (37), 2166–2181. https://doi.org/10.1016/j.enpol.2009.02.006.
Kure, H., Islam, S., 2019. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. J. Univ. Comput. Sci. 25, 1478–1502.
Lami, B., Bhattacharya, K., 2015. Identification of critical components of composite power systems using minimal cut sets. In IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Washington, DC, pp. 1–5. https://doi.org/10.1109/ISGT.2015.7131786.
Linnenluecke, M.K., Griffiths, A., 2012. Assessing organizational resilience to climate and weather extremes: complexities and methodological pathways. Clim. Change 113, 933–947. https://doi.org/10.1007/s10584-011-0380-6.
Lonapalawong, S., Yan, J., Li, J., Ye, D., Chen, W., Tang, Y., Huang, Y., Wang, C., 2022. Reducing power grid cascading failure propagation by minimizing algebraic connectivity in edge addition通过最小化边缘添加中的代数连接度来减少电网级联故障传播. Front. Inform. Technol. Electron. Eng. 23 (3), 382–397.
Löschel, A., Moslener, U., Rübbelke, D.T.G., 2010. Indicators of energy security in industrialised countries. Energy Policy 4 (38), 1665–1671. https://doi.org/10.1016/j.enpol.2009.03.061.
Mazur, C.h., Hoederle, Y., Brucoli, M., Dam, K., Guo, M., Markides, C.N., Shah, N., 2019. A holistic resilience framework development for rural power systems in emerging economies. Appl. Energy 235, 219–232. https://doi.org/10.1016/j.apenergy.2018.10.129.
McQueen, D., Noak, H., 1988. Health Promotion Indicators: current status, issues and problems. Health Promot. Int. 3 (1), 117–125. https://doi.org/10.1093/heapro/3.1.117.
Mendoza, G.A., Macoun, P., Prabhu, R., Sukadri, D., Purnomo, H., Hartanto, H. (Eds.), 1999. Guidelines for Applying Multi-Criteria Analysis to the Assessment of Criteria and Indicators. Center for International Forestry Research (CIFOR).
Ministry of Transport, 2020. Transport Indicators: Healthy and Safe People. Ministry of Transport of New Zealand, Wellington.
Moslehi, S.T., Reddy, A., 2018. Sustainability of integrated energy systems: a performance-based resilience assessment methodology. Appl. Energy 228, 487–498. https://doi.org/10.1016/j.apenergy.2018.06.075.
Mottahedi, A., Sereshki, F., Ataei, M., Qarahasanlou, A.N., Barabadi, A., 2021. Resilience estimation of critical infrastructure systems: application of expert judgment. Reliab. Eng. Syst. Saf. 215, 107849 https://doi.org/10.1016/j.ress.2021.107849.
Nan, C., Sansavini, G., 2017. A quantitative method for assessing resilience of interdependent infrastructures. Reliab. Eng. Syst. Saf. 157, 35–53. https://doi.org/10.1016/j.ress.2016.08.013.
Nerc, 1975. Flood Studies Report, vol. 5. Natural Environment Research Council, London.
Nerc, 2009. Security Guideline for the Electricity Sector: Identifying Critical Assets. North American Electric Reliability Corporation, Washington, DC.
NIAC (National Infrastructure Advisory Council), 2009. Critical Infrastructure Resilience: Final Report and Recommendations. U.S. Department of Homeland Security, Washington, DC.
Nogal, M., O'Connor, A., Caulfield, B., Brazil, W., 2016. A multidisciplinary approach for risk analysis of infrastructure networks in response to extreme weather. Transp. Res. Procedia 14, 78–85. https://doi.org/10.1016/j.trpro.2016.05.043.
Oecd, 2020. Key ICT Indicators. Organisation for Economic Co-operation and Development, Paris https://www.oecd.org/internet/broadband/oecdkeyictindicators.htm.
OECD, 2003. OECD and Development Environmental Indicators Development, Measurement and use. Organisation for Economic Co-operation and Development, Paris.
Øien, K., Jovanovic, A.S., Grøtan, T.O., Choudhary, A., Øren, A., Tetlak, K., Bodsberg, L., Jelic, M., 2017. D3.2 - Assessing Resilience of SCIs based on Indicators. SINTEF, Stuttgart.
Osei-Kyei, R., Tam, V., Ma, M., Mashiri, F., 2021. Critical review of the threats affecting the building of critical infrastructure resilience. Int. J. Disaster Risk Reduct. 60, 102316 https://doi.org/10.1016/j.ijdrr.2021.102316.
Pandey, B.R., 2013. Indicators for ICT Security Incident Management. Norwegian University of Science and Technology, Department of Telematics, Trondheim.
Panteli, M., Mancerella, P., 2017. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Syst. J. 11 (3), 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272.
Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A., Bilotta, F., 2018. An analytic framework to assess organizational resilience. Saf. Health Work 9 (3), 265–276. https://doi.org/10.1016/j.shaw.2017.10.005.
Petit, F., Bassett, G., Black, R., Buehring, W., Collins, M., Dickinson, D., Fisher, R., Haffenden, R., Huttenga, A., Klett, M., Phillips, J., Thomas, M., Veselka, S., Wallace, K., Whitfield, R., Peerenboom, J., 2013. Resilience measurement index: an indicator of critical infrastructure resilience. Argonne National Laboratory, Lemont. https://doi.org/10.2172/1087819.
Philpott, D., 2016. Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity, second ed. Bernan Press, Lanham, MD.
Prezelj, I., Kopac, E., Svete, U., Ziberna, A., 2012. Cross-sectoral scanning of critical infrastructures: from functional differences to policy-relevant similarities. J. Homel. Secur. Emerg. Manage. 9 (1) https://doi.org/10.1515/1547-7355.1901.
Prior, T., 2015. Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9). Eidgenössische Technische Hochschule, Zurich.
Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM/2020/829 final).
Rahi, K., 2018. Indicators to assess organizational resilience: a review of empirical literature. Int. J. Disaster Resil. Built Environ. 10 (2/3), 85–98. https://doi.org/10.1108/IJDRBE-11-2018-0046.
Raoufi, H., Vahidinasab, V., 2021. Power system resilience assessment considering critical infrastructure resilience approaches and government policymaker criteria. IET Gener. Transm. Distrib. 15 (20), 2819–2834. https://doi.org/10.1049/gtd2.12218.
Rassafi, A.A., Vaziri, M., 2005. Sustainable transport indicators: definition and integration. Int. J. Environ. Sci. Technol. 2 (1), 83–96. https://doi.org/10.1007/BF03325861.
Reed, D.A., Kapur, K.C., Christie, R.D., 2009. Methodology for assessing the resilience of networked infrastructure. IEEE Syst. J. 3 (2), 174–180. https://doi.org/10.1109/JSYST.2009.2017396.
Rehak, D., 2020. Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the slovak republic. Saf. Sci. 123, 104573 https://doi.org/10.1016/j.ssci.2019.104573.
Rehak, D., Flynnova, L., Slivkova, S., 2022a. Concept of Resistance in the Railway Infrastructure Elements Protection. In Prentkovskis, O., Yatskiv (Jackiva), I., Skačkauskas, P., Junevičius, R., Maruschak, P. (eds.) TRANSBALTICA XII: Transportation Science and Technology. Lecture Notes in Intelligent Transportation and Infrastructure, pp. 419-428. Springer, Cham. https://doi.org/10.1007/978-3-030-94774-3_41.
Rehak, D., Splichalova, A., 2022. In: Application of Composite indicator in Evaluation of Resilience in Critical Infrastructure System. IEEE, Valec, Czech Republic, pp. 1–6. https://doi.org/10.1109/ICCST52959.2022.9896610.
Rehak, D., Markuci, J., Hromada, M., Barcova, K., 2016. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. Int. J. Crit. Infrastruct. Prot. 14, 3–17. https://doi.org/10.1016/j.ijcip.2016.06.002.

Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., Novotny, P., 2018a. Cascading impact assessment in a critical infrastructure system. Int. J. Crit. Infrastruct. Prot. 22, 125–138. https://doi.org/10.1016/j.ijcip.2018.06.004.
Rehak, D., Senovsky, P., Slivkova, S., 2018b. Resilience of critical infrastructure elements and its main factors. Systems 6 (2), 21. https://doi.org/10.3390/systems6020021.
Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., 2019. Complex approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Prot. 25, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003.
Rehak, D., Hromada, M., Lovecek, T., 2020a. Personnel threats in an electric power critical infrastructure sector and their impacts on dependent sectors. Saf. Sci. 127, 104698 https://doi.org/10.1016/j.ssci.2020.104698.
Rehak, D., Patrman, D., Brabcova, V., Dvorak, Z., 2020b. Identifying critical elements of road infrastructure using cascading impact assessment. Transport 35 (3), 300–314. https://doi.org/10.3846/transport.2020.12414.
Rehak, D., Slivkova, S., Pittner, R., Dvorak, D., 2020c. Integral approach to assessing the criticality of railway infrastructure elements. Int. J. Crit. Infrastruct. 16 (2), 107–129. https://doi.org/10.1504/IJCIS.2020.107256.
Rehak, D., Hromada, M., Onderkova, V., Walker, N., Fuggini, C., 2022b. Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security. Int. J. Electr. Power Energy Syst. 136, 107700 https://doi.org/10.1016/j.ijepes.2021.107700.
Rehak, D., Slivkova, S., Janeckova, H., Stuberova, D., Hromada, M., 2022c. Strengthening resilience in the energy critical infrastructure: methodological overview. Energies 15 (14), 5276. https://doi.org/10.3390/en15145276.
Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21 (6), 11–25. https://doi.org/10.1109/37.969131.
Rübbelke, D., Vögele, S., 2011. Impacts of climate change on European critical infrastructures: the case of the power sector. Environ Sci Policy 14 (1), 53–63. https://doi.org/10.1016/j.envsci.2010.10.007.
Saaty, T.L., 1977. A scaling method for priorities in hierarchical structures. J. Math. Psychol. 15 (3), 234–281. https://doi.org/10.1016/0022-2496(77)90033-5.
Saaty, T.L., 1980. The Analytic Hierarchy Process, Planning, Priority Setting, and Resource Allocation. McGraw-Hill, New York, NY.
Saaty, R.W., 1987. The analytic hierarchy process: what it is and how it is used. Math. Model. 9 (3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8.
Saaty, T.L., 1996. Decision Making with Dependence and Feedback: The Analytic Network Process. RWS Publications, Pittsburgh, PA.
Setola, R., Luiijf, E., Theocharidou, M., 2016. Critical infrastructures, protection and resilience. In: Setola, R., Rosato, V., Kyriakides, E., Rome, E. (Eds.), Managing the Complexity of Critical infrastructures. Studies in Systems, Decision and Control. Springer, Cham. https://doi.org/10.1007/978-3-319-51043-9_1.
Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S., Vargo, J., 2008. Organisational resilience: researching the reality of New Zealand organisations. J. Bus. Contin. Emer. Plan. 2 (3), 258–266.
Shakou, L.M., Wybo, J.L., Reniers, G., Boustras, G., 2019. Developing an innovative framework for enhancing the resilience of critical infrastructure to climate change. Saf. Sci. 118, 364–378. https://doi.org/10.1016/j.ssci.2019.05.019.
Shavelson, R.J., McDonnell, L.M., Jeannie, O., 1991. What are educational indicators and indicator systems? Pract. Assess. Res. Eval. 2, 11. https://doi.org/10.7275/rtkj-a222.
Shen, L., Tang, L., 2015. In: A Resilience Assessment FrAmework for CriticAl InfrAstructure Systems. IEEE, Beijing, China, pp. 1–5. https://doi.org/10.1109/ICRSE.2015.7366435.
Splichalova, A., Flynnova, L., 2021. Indicator approach to the failure of critical road transportation infrastructure elements. Transp. Res. Procedia 55, 1767–1774. https://doi.org/10.1016/j.trpro.2021.07.168.
Splichalova, A., Patrman, D., Kotalova, N., Hromada, M., 2020. Managerial decision-making within indicating disruption of critical infrastructure elements resilience. Admin. Sci. 10 (3), 75. https://doi.org/10.3390/admsci10030075.
The White House, 2013. Presidential Policy Directive – Critical infrastructure security and resilience (PPD-21. 2013). The White House, Washington, DC.
Tillement, S., Cholez, C., Reverdy, T., 2009. Assessing organizational resilience: an interactionist approach. Management 12, 230–264. https://doi.org/10.3917/mana.124.0230.
Titko, M., Luskova, M., 2016. Analysis of risks associated with transport infrastructure elements failure due to extreme weather events. In: 20th International Scientific on Conference Transport Means 2016. Juodkrante, Lithuania, pp. 207–212.
Tracht, K., Goch, G., Schuh, P., Sorg, M., Westerkamp, J.F., 2013. Failure probability prediction based on condition monitoring data of wind energy systems for spare parts supply. CIRP Ann. 62, 127–130. https://doi.org/10.1016/j.cirp.2013.03.130.
Unece, 2018. 2018 Inland Transport Statistics for Europe and North America (Volume LIX). The United Nations, Geneva.
Vichova, K., Hromada, M., 2019. Power outage in the hospitals. In International Conference on Intelligent Medicine and Image Processing (IMIP '19), pp. 15–20. https://doi.org/10.1145/3332340.3332345.
Vidrikova, D., Boc, K., Dvorak, Z., Rehak, D., 2017. Critical Infrastructure and Integrated Protection. The Association of Fire and Safety Engineering, Ostrava.
Vugrin, E.D., Camphouse, R.C., 2011. Infrastructure resilience assessment through control design. Int. J. Crit. Infrastruct. 7 (3), 243–260. https://doi.org/10.1504/IJCIS.2011.042994.
Wang, T., Qu, Z., Yang, Z., Nichol, T., Clarke, G., Ge, Y.-E., 2020. Climate change research on transportation systems: climate risks, adaptation and planning. Transp. Res. Part D: Transp. Environ. 88, 102553.
Wang, W., Yang, S., Hu, F., Stanley, H.E., He, S., Shi, M., 2018. An approach for cascading effects within critical infrastructure systems. Physica A 510, 164–177. https://doi.org/10.1016/j.physa.2018.06.129.
Xian, H.A., Jeong, Ch.E., 2018. Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards. Reliab. Eng. Syst. Safety 177, 162-175. .
Yang, Z., Barroca, B., Weppe, A., Bony-Dandrieux, A., Laffréchine, K., Daclin, N., November, V., Omrane, K., Kamissoko, D., Benaben, F., Dolidon, H., Tixier, J., Chapurlat, V., 2023. Indicator-based resilience assessment for critical infrastructures – a review. Saf. Sci. 160, 106049 https://doi.org/10.1016/j.ssci.2022.106049.