energies

MDPI

Article

Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview

David Rehak [1,*], Simona Slivkova [1], Heidi Janeckova [1], Dominika Stuberova [1] and Martin Hromada [2]

[1] Faculty of Safety Engineering, VSB-Technical University of Ostrava, Lumirova 13/630, 700 30 Ostrava, Czech Republic; simona.slivkova@vsb.cz (S.S.); heidi.janeckova@vsb.cz (H.J.); dominika.stuberova@vsb.cz (D.S.)

[2] Faculty of Applied Informatics, Tomas Bata University in Zlin, Nad Stranemi 4511, 760 05 Zlin, Czech Republic; hromada@utb.cz

* Correspondence: david.rehak@vsb.cz; Tel.: +420-597322816

Abstract: As the number of threats and the severity of their impact increases, an ever greater emphasis is being placed on the protection of critical infrastructure. Thus, the issue of resilience, or its assessment and strengthening, is increasingly coming to the fore. The resilience assessment of critical infrastructure, especially in the energy sector, has received considerable attention due to the high level of interest in this issue. However, the issue of strengthening resilience poses a significant challenge not only in the energy sector but also in the entire critical infrastructure system. Despite the great importance of this area, there is not a large number of authors moving in this direction and paying attention to resilience-strengthening tools. For this reason, the aim of this article is to provide the reader with a comprehensive methodological overview of resilience strengthening in the critical energy infrastructure sector. This article also provides an overview of internal and external tools suitable for strengthening resilience and presents a possible procedure for their application to energy critical infrastructure elements.

Keywords: critical infrastructure; energy; strengthening resilience; resilience assessment; approaches and methods

Citation: Rehak, D.; Slivkova, S.; Janeckova, H.; Stuberova, D.; Hromada, M. Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview. *Energies* **2022**, *15*, 5276. https://doi.org/10.3390/en15145276

Academic Editor: Andrea Mariscotti

Received: 27 June 2022
Accepted: 18 July 2022
Published: 21 July 2022

1. Introduction

The increasing dependence of the human population on infrastructure is mainly due to growing urbanization. Increasing demands on infrastructures also bring with them wider and more serious impacts. Especially in the case of infrastructures that are designated as critical [1], disruptive events can cause serious impacts not only on the population but also on the essential functions of the state. However, the issue of critical infrastructure in the event of disruption or failure is far more complicated, as the interdependence and interconnectedness often result in a cascading effect [2], i.e., the transfer of impacts to dependent sectors. From this perspective, the energy sector can be considered uniquely critical [3], as almost all critical infrastructure sectors depend on energy supplies [4].

Although the energy critical infrastructure sector is currently relatively resilient, disruptive events can occur in both the internal and external environment that can have negative impacts not only on the performance of the energy sector but also on all dependent systems. In this context, volatile renewable energy production [5] and extreme weather [6] can be considered key risk factors. In this regard, it is essential to take steps to protect critical energy infrastructure elements. This protection can be achieved using the principle of resilience, which is defined as "*the ability to reduce the magnitude and/or duration of disruptive events; the effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event*" [7].

Resilience assessment in critical infrastructure systems has received considerable attention in recent years, resulting in a large number of quantitative and semi-quantitative ap-

proaches across different sectors. Currently, available quantitative methods (e.g., Brown et al. [8], Lee et al. [9], and Van der Merwe et al. [10]) are predominantly used to assess organizational and social resilience. Other methodologies (e.g., Zhou and Chen [11] and Wei et al. [12]) approach resilience assessment by measuring and comparing the performance of elements or a system before and after a disruptive event. A quantitative approach based on the assessment of indicators can also be considered innovative [13]. From this perspective, quantitative approaches can be divided into deterministic and probabilistic approaches [14]. The second approach is a semi-quantitative assessment, which evaluates resilience through index values. Semi-quantitative assessments have been used in publications by, for example, Bertocchi et al. [15], Nan and Sansavni [16], Johansen and Tien [17], Rehak et al. [18], and Ciapessoni et al. [19].

Other approaches focus on assessing resilience as a system since the individual subsystems are interconnected by links. Other approaches, on the other hand, assess resilience solely at the elementary level (i.e., assessing the resilience of a specific element of critical infrastructure). Similarly, attention can be paid to static or dynamic resilience, depending on whether the timeline is reflected in the assessment. Simonovic and Arunkumar [20] define static resilience as an abstract property of a system that is useful for assessing vulnerability to disturbances but does not capture the interaction between system behavior and the relationships between components within the system. Dynamic resilience, on the other hand, allows the system to adapt to the impact of a disruptive event disruption and improve the ability of individual parts of the system to function during the disruption. Dynamic resilience assessment is addressed in the reseach by Ouyang et al. [21], Eljaoued et al. [22], Kammouh et al. [23], and Rehak et al. [24].

Labaka et al. [25] took into account the assessment by the type of resilience (technical, organizational, economic, and social) and proposed a holistic framework based on the identification of resilience policies. The goal is to increase the resilience of critical infrastructure by identifying new levels of resilience, vulnerabilities, and potential improvements that need to be implemented.

The energy sector primarily uses the technical resilience assessment approach. Currently, this area is the most important in research, as disruption of energy systems can cause cascading effects and thus disrupt transport systems, information and communication systems, water distribution, etc. Among the authors already mentioned above, this issue has mainly been addressed by Nan and Sansavini [16], Johansen and Tien [17], Rehak et al. [18], Ciapessoni et al. [19], Ouyang et al. [21], Rehak et al. [24], and Zimmerman et al. [26]. In their publications, the authors modeled and assessed resilience through case studies against selected threats.

It is clear from the overview presented above that sufficient attention is paid to resilience assessment. However, in the area of resilience strengthening, the situation is far more complex. Resilience strengthening has been addressed by a small number of authors to date, including Labaka et al. [25], Haines [27], Reeves et al. [28], Walker et al. [29], Tonn et al. [30], Rahman and Ghosh [31], and Silla et al. [32]. In the context of energy issues, we can mention in this regard, for example, the authors Bucci et al. [33].

In the context of resilience strengthening, there is a significant gap in the research, mainly due to the lack of comprehensive methods (tools) that specifically focus on resilience strengthening. At the same time, however, it is clear from the forthcoming European legislation that strengthening resilience is the future of critical infrastructure protection [34]. For this reason, the aim of this article is to provide the reader with a comprehensive methodological overview in the field of resilience strengthening in critical energy infrastructure. Such an overview will be a valuable starting document for further research on specific methods and tools for strengthening resilience not only in the field of critical energy infrastructure.

2. Methodology

Since the entire article is designed as a methodological overview, it is not possible to strictly define the methodology only in this part of the article. For this reason, the

methodology is designed in two units. The first whole, which is presented in this part of the article, is the methodology related to the perception of resilience in the critical infrastructure system and the approaches and methods of strengthening the resilience of the energy critical infrastructure. The second whole, which is presented in the Results section, is the methodology related to tools for strengthening the resilience of energy critical infrastructure elements. Data collection was carried out on the basis of currently available sources dealing with the issue in question. Subsequently, the relevance of these sources and their arrangement in relation to the thematic parts of this article were assessed.

2.1. Perception of Resilience in a Critical Infrastructure System

The term resilience was first defined by Holling [35] in the context of the resistance and stabilization of ecological systems (later also socio-ecological systems). Over time, the concept of resilience began to be reflected in other disciplines such as sociology, psychology, and economics. One relatively young field, in terms of exploring systems resilience, is engineering. In the context of critical infrastructure, resilience represents the internal preparedness of subsystems for disruptive events. Thus, it is the ability of these subsystems to provide and maintain their functions when negatively affected by internal and/or external factors. Resilience can, therefore, be understood to be the opposite of vulnerability, or resilience and vulnerability are inverse to each other. Vulnerable subsystems lack resilience and, conversely, resilient subsystems are not very vulnerable. The importance of the infrastructure network's resilience in the context of increasing urbanization has been pointed out for a long time by a number of prominent authors [36–38].

2.1.1. Factors Determining the Resilience of Critical Infrastructure Elements

The resilience of critical infrastructure elements is determined by factors that can be classified into four groups. The first group is presented by the factors determining the resistance of critical infrastructure elements. Resistance is the ability of an element to prevent the occurrence of a disruptive event. These are preventive measures that determine structural and security resistance. Factors determining resilience are crisis preparedness, anticipation ability, physical resilience, and security measures [39].

The second group is the factors determining the robustness of critical infrastructure elements. Robustness is the ability of an element to absorb the impact of a disruptive event that has already occurred. These impacts can be absorbed through the early recognition and management of a disruptive event. Factors determining robustness are the detection ability, responsiveness, and redundancy [40].

The third group is represented by factors determining the recoverability of critical infrastructure elements. Recoverability is the ability of an element to restore its operation to its original (desired) level of service after the effects of a disruptive event have ceased. Recoverability is understood in the field of critical infrastructure as repairability; therefore, only the repair or replacement of damaged or destroyed components of an element is considered. Factors determining recoverability are material resources, financial resources, human resources, and recovery processes [40].

The last group is factors determining the adaptability of critical infrastructure elements. Adaptability is the ability of a critical infrastructure entity (i.e., an organization) to prepare elements for repeated exposure to a disruptive event that has already occurred. It represents the dynamic (long-term) ability of an organization to adapt to a changing situation. Factors determining adaptability are risk management, innovation processes, and educational and development processes [41].

A summary of the factors determining the resilience of critical infrastructure elements is presented in Table 1. In this context, it is still necessary to note that resistance, robustness, and recoverability are considered as components that determine the technical resilience of critical infrastructure elements while adaptability is considered a component that determines organizational resilience, the essence of which is strengthening the resilience of organizations that manage these critical infrastructure elements [8].

Table 1. Factors determining resilience of critical infrastructure elements.

Components	Factors
Resistance	Crisis preparedness Anticipation ability Physical resistance Security measures
Robustness	Detection ability Responsiveness Redundancy
Recoverability	Material resources Financial resources Human resources Recovery processes
Adaptability	Risk management Innovation processes Educational and development processes

2.1.2. Resilience Strengthening Cycle

Resilience in the context of critical infrastructure was first used in the Critical Infrastructure Resilience Final Report and Recommendations [7], where it is defined as the ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. In the context of this definition, it is necessary to perceive resilience in a critical infrastructure system as a cyclic process of continuous improvement of prevention, absorption, recovery, and adaptation of the individual elements of critical infrastructure. Figure 1 presents one cycle in which resilience is enhanced from the original level (i.e., the black dashed line) to a new level (i.e., the red dashed line). The difference between these levels Δ is seen as resilience strengthening.

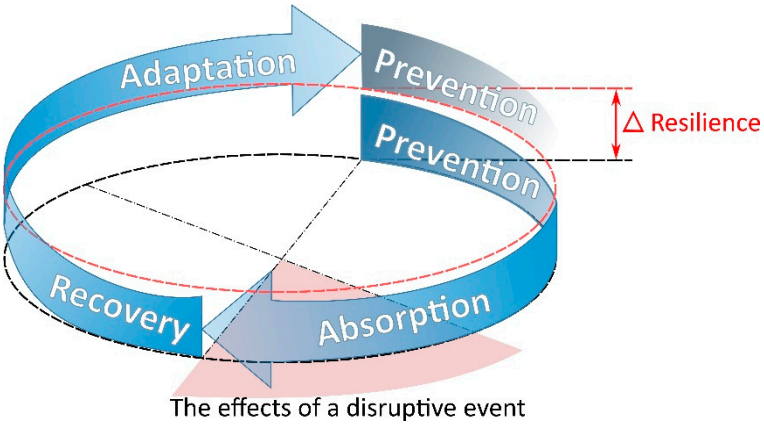

Figure 1. Cycle of strengthening the resilience of energy critical infrastructure elements [40].

The first phase of the resilience cycle is prevention, which is determined by the resilience of critical infrastructure elements. By implementing prevention activities, the critical infrastructure entity (i.e., the owner or operator) prepares the elements for future disruptive events; preparedness is, therefore, the resulting state of prevention. At the moment of exposure to such events, resilience then moves from the prevention phase to the absorption phase.

Absorption is initiated by the impact of a disruptive event and is determined by the robustness of critical infrastructure elements. The essence of robustness is the ability of critical infrastructure elements to absorb the impact of a disruptive event without disrupting the services they provide.

After the disruptive event has ended, the recovery phase occurs. It is characterized by recoverability, i.e., the ability of elements to restore their activity to the original or desired level of performance. The length of the recovery phase is determined by the available resources and the time required for the individual recovery processes.

The final phase of the critical infrastructure resilience cycle is adaptation. It is the ability of the organization to adapt the operational elements to a possible recurrence of a disruptive event that has already occurred, thus learning from disruptive events dealt with in the past. Adaptation thus represents the dynamic, long-acting ability of an organization to adapt to a changed situation. Adaptation is determined by the organization's internal processes related to resilience strengthening, i.e., risk management, innovation processes, and educational and development processes. However, strengthening the resilience of the elements can already take place in the recovery phase, e.g., by replacing components or modifying their functioning processes.

2.2. Approaches and Methods for Strengthening the Resilience of Energy Critical Infrastructure

Once the resilience assessment is completed, steps can be taken to strengthen resilience that has a positive impact on reducing the vulnerability of an energy critical infrastructure element. Approaches and methods addressing this issue can be divided into those that highlight the need for collaboration between entities and external participants and those that focus on approaches and methods for strengthening technical and organizational resilience.

The need for cooperation between entities and external actors is highlighted, for example, in the publication Boosting Resilience through Innovative Risk Governance [42]. This paper encourages private and public sector collaboration, providing a set of possible policy tools for managing critical infrastructure resilience.

The involvement of state and local emergency responders in an exercise related to the energy sector, specifically a nuclear power plant, is mentioned by Bucci et al. [33]. In their documentary After Hurricane Sandy: Time to Learn and Implement the Lessons in Preparedness, Response, and Resilience, they address this issue in the context of the Federal Emergency Planning Act requirements.

The issue of funding is also an essential aspect in the context of resilience strengthening and external cooperation. This issue is highlighted by Tonn et al. [30], who define 20 possible proposals aimed at improving resilience using insurance, economic incentives, and other policy instruments. Other well-known authors who draw attention to the issue of external and internal resilience or the need for cooperation and the possibility of external factors influencing resilience include, for example, Labaka et al. [25], Reeves et al. [28], and the National Infrastructure Commission [43].

In the context of strengthening the resilience of an energy critical infrastructure element, approaches and methods focusing on technical resilience can be used, among others. This area is dealt with, for example, by Silla et al. [32], Haines [27], and the American Association of State Highway and Transportation Officials [44] study. One of the questions that constitutes another gap in resilience strengthening is the question regarding the type of approach to organizational resilience, or which approach is most beneficial for a given subject [45]. Thus, the authors' intentions and their research should not only focus on the area of strengthening technical resilience but also on the area of strengthening organizational resilience in the energy sector.

With time, the area of organizational resilience, which is not only about risk management but also about the strength and success of the organization, is also coming to the fore, assuming learning from its own or other organizations' experiences [46]. The authors Walker et al. [29] divide this area into two interrelated levels (organizational and personnel), within which the organization needs to be strengthened to be more agile and more coordinated. This area, in the context of critical infrastructure, is highlighted, for example, by Rehak [41], who mentions the possibility of identifying weaknesses in organizational resilience and their subsequent strengthening using the ASOR method. Strengthening

organizational resilience is also referred to, for example, in ISO 22316 [47], which sets out principles and attributes that enable an organization to adapt to its circumstances.

A different perspective on resilience strengthening is provided by Rahman and Ghosh [31] using a participatory planning approach, which they illustrate in a study on the vulnerability of Bangladeshi people to natural disasters.

Most of the above-mentioned documents provide only strategies, recommendations, or specific measures that can be used to strengthen resilience; however, they do not provide a comprehensive overview of resilience-strengthening tools.

3. Results

On the basis of the information obtained from the analysis of available resources, it is possible to outline the procedure for strengthening the resilience of the elements of the critical energy infrastructure. This procedure is the authors' research result and consists of five basic steps: identification of the element of interest, risk assessment, scenario definition, resilience assessment, and selection of resilience-strengthening tools (see Figure 2).

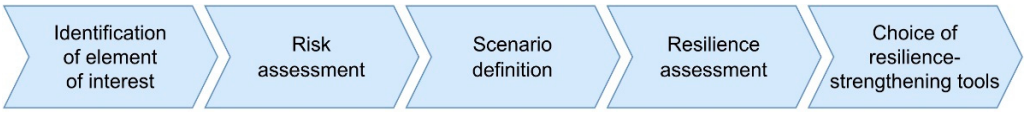

Figure 2. Procedure for strengthening the resilience of energy critical infrastructure elements.

As a first step, it is necessary to identify the element of interest to which the procedure will be applied. The identification of the element can be carried out by the entity using some managerial decision-making methods such as SWOT analyses or brainstorming [48]. The second step consists of risk assessment, i.e., its identification, analysis, and subsequent evaluation. Additionally, in this step, managerial decision-making methods such as a checklist or the Ishiaka diagram can be used [48]. However, it is more appropriate to use risk assessment methods directly, e.g., ETA [49], FTA [50], or HAZOP [51]. These methods can also be used for the third step, which is scenario definition. The essence of this scenario is the identification of vulnerabilities [41], i.e., factors determining resilience, for which a resilience assessment is required. For factors with a low level of resilience, it is necessary to subsequently apply tools suitable for strengthening resilience. The steps involving resilience assessment and choice of resilience-strengthening tools (i.e., steps four and five) are discussed separately in the following text.

3.1. Resilience Assessment

As already mentioned, there are a large number of approaches and methods for assessing resilience in a critical infrastructure system. Therefore, Table 2 illustrates an overview of the authors' recommended publications that can be used to assess resilience in the energy sector.

Table 2. An overview of the selected resilience assessment approaches in the energy sector.

Authors	Title	Year
Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., Oliva, G., Traballesi, A. [15]	Guidelines for Critical Infrastructure Resilience Evaluation	2016
Zimmerman, R., Zhu, Q., de Leon, F., Guo, Z. [26]	Conceptual modelling framework to integrate resilient and interdependent infrastructure in extreme weather	2017
Nan, C., Sansavini, G. [16]	A Quantitative Method for Assessing Resilience of Interdependent Infrastructures	2017
Johansen, C., Tien, I. [17]	Probabilistic multi-scale modelling of interdependencies between critical infrastructure systems for resilience	2018

Table 2. *Cont.*

Authors	Title	Year
Ouyang, M., Liu, C., Xu, M. [21]	Value of resilience-based solutions on critical infrastructure protection: Comparing with robustness-based solutions	2019
Ciapessoni, E., Cirio, D., Pitto, A., Sforna, M. [19]	A risk-based resilience assessment tool to anticipate critical system conditions in case of natural threats	2019
Rehak, D., Senovsky, P., Hromada, M., Lovecek, T. [18]	Complex Approach to Assessing Resilience of Critical Infrastructure Elements	2019
Jovanovic, A.S., Chakravarty, S., Jelic, M. [13]	Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach	2021
Rehak, D., Hromada, M., Onderkova, V., Walker, N., Fuggini, C. [24]	Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security	2022

3.2. Choice of Resilience-Strengthening Tools

In the context of currently available approaches and methods for resilience strengthening, areas of tools suitable for strengthening individual determinants of critical infrastructure resilience were developed (see Figure 3). Based on the literature review, these tools are divided into internal and external tools. Furthermore, they are structured according to their nature into several thematic groups. Internal tools are divided into four groups covering the main functional areas and management processes of the organization. External tools are divided into six groups corresponding to the PESTLE method, the essence of which is the analysis of external factors of the organization.

Figure 3. Tools for strengthening the resilience of critical energy infrastructure elements.

3.2.1. Internal Tools

The first area of internal tools is **personnel tools**. In general, these tools can be described as training and development activities and their main forms include long-term education, study abroad, skills development, and training (both preventive and repressive) [52]. Significant weight can also be given to tools to maintain psychological and occupational well-being, as psychologically balanced people have lower error rates and higher work performance [53].

In the context of resilience strengthening, **substantive tools** are also essential. The primary objective of substantive tools is to provide technical support for the functioning of a given element or system. RAMS, key elements, monitoring, and upgrading are the basic

tools to ensure this goal. RAMS (reliability, availability, maintainability, and safety) is used to characterize a product or system. RAMS is used as a decision-making tool to increase the availability of the system, and thus increase the overall profit and reduce the life cycle costs [54]. The second tool is the approach of the so-called key elements. These are defined as elements that are relevant to the functioning of the system [55]. Monitoring is an effective tool for checking the status of a given element and its function, e.g., Tracht et al. [56]. In contrast, upgrading serves to keep the technical state of an element up to date with current trends and technologies, e.g., Lindenberger et al. [57].

In particular, a physical protection system can be used to protect the element [58]. This system consists of the regime, organizational, and technical measures that prevent physical damage to critical energy infrastructure elements. Regime measures include, for example, the entry and exit regime for persons, goods, means of transport, and information; the method of proving the eligibility for the entry of persons and entry of vehicles; or the method of checking, keeping, and maintaining records of the entry and exit of goods. Physical security includes the guarding of the object and the manner, extent, and procedure of physical security. The technical means of the physical protection system include mechanical barriers (e.g., fences, grilles, roller shutters, and locks) and alarm systems (e.g., alarms, cameras, access control systems, electrical fire alarms).

The core area of **procedural tools** is planning documents, i.e., concepts, strategies, or other internal documents and agreements ensuring crisis preparedness and a timely response to disruptive events. Due to the need to upgrade existing technologies and increase the skills of personnel, there is a need to ensure support for national and international cooperation and the involvement of energy critical infrastructure actors in science and research. An important area of process tools is risk management [59,60]. When applying other international standards, the adoption of an integrated management system should be considered [61].

For the possible implementation of the above-mentioned instruments, the **financial tools** of energy critical infrastructure entities are necessary. The funding should be distributed in such a way that the costs of all areas can be covered. The creation of a reserve fund from which the entity can draw if necessary is essential. It is also advisable to have funds earmarked for investment so that the system can be properly developed [62].

3.2.2. External Tools

The first area of external instruments is **economic tools**. By creating specific subsidy programs or insurance, external participants are able to cover at least part of the costs of critical energy infrastructure entities that may arise from the need for upgrades or repairs in the event of a disruptive event. An example is natural disaster insurance [63].

Political tools can also help in this regard through involvement in international organizations. It is worth mentioning the International Energy Agency (IEA), which works with countries around the world to shape energy policies for a secure and sustainable future [64].

Social tools are an important area through which external participants can influence resilience. These are, for example, demographic or educational factors. Using these tools, it is possible to increase the level of education or awareness of employees and residents [52].

Due to the ever-increasing concern for the environment, **ecological tools** can also be used, which, if used correctly, can mitigate the consequences of disruptive events, and thus increase the resilience of critical energy infrastructure or the surrounding ecosystem. A good example is the use of green infrastructure in the energy sector [65].

Other external instruments include **legislative tools**. This area refers in particular to laws, decrees, and/or standards. With the right adjustment of existing or new legislation, the resilience of a given entity can be increased. A good example is the preparation of a proposal for a directive on the resilience of critical entities [34].

The last group is **technological tools** that can influence the readiness of emergency services to respond to disruptive events affecting critical energy infrastructure elements. This category includes all developments of new technologies or means of ensuring pre-

paredness for emergency services (e.g., vehicles, equipment, devices). An example is a large-scale industrial company alarm receiving center modernization [66].

External tools can be considered as general tools, i.e., they can be used to strengthen the resilience of elements in other technically oriented sectors of critical infrastructure.

3.2.3. Matrix for Selecting Tools Suitable for Resilience Strengthening

The final step in the resilience-strengthening process is the selection of tools suitable for resilience strengthening. This selection can be made based on the matrices presented in Tables 3 and 4, which are based on a combination of resilience determinants (green factors represent resistance, blue factors represent robustness, yellow factors represent recoverability, and grey factors represent adaptability) and tool definition areas. Table 3 focuses on internal instruments and Table 4 on external instruments.

Table 3. Matrix for selecting internal resilience-strengthening tools.

Factors	Internal Tools			
	Personnel	**Substantive**	**Procedural**	**Financial**
Crisis preparedness	Long-term education; Study abroad; Skills development; Psychological and occupational well-being	RAMS	Planning documents	Financial plan
Anticipation ability	Training	RAMS; Monitoring	Planning documents	Financial plan; Innovation
Physical resistance	-	Technical means of the physical protection system	-	-
Security measures	Long-term education; Training; Psychological and occupational well-being	Physical security	Regime measures; Integrated management system	Financial plan
Detection ability	Training	Monitoring	-	Financial plan; Innovation
Responsiveness	Skills development; Training	Monitoring	Planning documents	Financial plan; Reserve fund
Redundancy	Training	Monitoring	Planning documents	Investment
Material resources	-	Key elements	-	-
Financial resources	-	-	-	Reserve fund
Human resources	Psychological and occupational well-being	-	Planning documents	-
Recovery processes	Long-term education; Study abroad; Skills development	-	Planning documents; National and international cooperation	Reserve fund
Risk management	Long-term education; Study abroad	Monitoring	Risk management	Financial plan
Innovation processes	Study abroad	Upgrading	Involvement in science and research; Integrated management system	Innovation
Educational and development processes	Long-term education; Study abroad; Skills development; Training	Upgrading	Involvement in science and research; National and international cooperation; Integrated management system	Innovation

Table 4. Matrix for selecting external resilience-strengthening tools.

Factors	External Tools					
	Economic	**Political**	**Social**	**Ecological**	**Legislative**	**Technological**
Crisis preparedness	Subsidy programs	International organizations	Increase the level of education or awareness	Mitigate the consequences of disruptive events	Legislation creation	Technologies and means of emergency services
Anticipation ability	Subsidy programs	International organizations	Increase the level of education or awareness	-	-	Technologies and means of emergency services
Physical resistance	-	-	-	-	-	-
Security measures	Subsidy programs	International organizations	-	-	Legislation creation	Technologies and means of emergency services
Detection ability	Subsidy programs	International organizations	-	-	-	-
Responsiveness	Subsidy programs	-	Increase the level of education or awareness	-	Legislation creation	Technologies and means of emergency services
Redundancy	Subsidy programs	-	-	-	Legislation creation	-
Material resources	-	-	-	-	-	-
Financial resources	Subsidy programs; Insurance	-	-	-	-	-
Human resources	-	-	Increase the level of education or awareness	-	-	-
Recovery processes	Subsidy programs; Insurance	International organizations	Increase the level of education or awareness	Mitigate the consequences of disruptive events	Legislation creation	Technologies and means of emergency services
Risk management	-	International organizations	-	Mitigate the consequences of disruptive events	Legislation creation	-
Innovation processes	Subsidy programs	International organizations	-	Mitigate the consequences of disruptive events	-	-
Educational and development processes	Subsidy programs	International organizations	Increase the level of education or awareness	Mitigate the consequences of disruptive events	Legislation creation	-

The essence of this matrix is to recommend the most appropriate measures for energy critical infrastructure entities to strengthen factors that have been assessed as having a low level of resilience. The selection and application of specific factors are then implemented according to the preferences and financial, technical, and material capabilities of the subjects. After the application of the selected tools, it is advisable to reassess the level of resilience of the factors determining the vulnerabilities of the assessed critical infrastructure element.

4. Discussion

The energy sector is one of the most important areas because of its importance for the proper functioning not only of other critical infrastructure sectors but also of other essential functions of the state. This importance is primarily on the potential cascading effects on dependent sectors and state functions [2,4]. The importance of the energy sector is also supported by a number of important directives, such as Council Directive 2008/114/EC [1] or the Presidential Policy Directive [3].

The energy sector is not exceptional only in its importance. It is also specific in its layout, individual links between elements, and the technical nature of the creation and transfer of energy. All of these and many other aspects create room for the potential for disruptive events or incidents to occur in the energy sector. Some are manageable within the basic stability and resistance of the system. However, others need to be addressed by the additional application of appropriate safety measures [16,24].

The most appropriate solution for dealing with disruptive events or incidents seems to involve the principle of resilience, which is confirmed by a number of authors who focus on resilience research. The most prominent authors involved in resilience research, and the results of their research, can be found throughout this article.

Resilience is generally seen as the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event [7]. The basic components of resilience are resistance, robustness, recoverability, and adaptability.

The energy critical infrastructure sector already has some of these components and features in some form. These characteristics are either natural or acquired through the technological and technical design of the infrastructure. However, strengthening the comprehensive resilience of energy critical infrastructure elements requires the strengthening of other resilience determinants. This means that the natural or technologically acquired properties of the system are not sufficient. In addition, some of the basic components of resilience are oriented exclusively towards its strengthening (primarily adaptability). Strengthening resilience in critical energy infrastructure thus poses a significant challenge.

Strengthening resilience is always underpinned primarily by resilience assessment or evaluation. Without effective resilience assessment, it is not possible to assess whether resilience strengthening has been effective. There is already a lot of research and applicable methods on the issue of resilience assessment. Table 2 provides an overview of the most cited resilience assessment approaches in the energy sector. It is up to the evaluator or owner of the element to choose which of the proposed methods to use. The choice of the method also depends on the input conditions of the assessment, i.e., the specification of the element to be assessed, the quality of the input data, and the details of the expected results.

Taking into account the results of the resilience assessment, the resilience of the energy critical infrastructure elements can be strengthened. Here, however, a research gap can be detected, with only a few approaches or methods currently available for resilience strengthening in general. Some of these methods are presented in Section 2 of this paper. This methodological overview can be seen as one of the basic needs in increasing the resilience of energy critical infrastructure elements. The authors' research resulted in the definition of a resilience-strengthening process consisting of five basic steps: identification of the element of interest, risk assessment, scenario definition, resilience assessment, and selection of resilience-strengthening tools.

For the first four steps, it is recommended to use existing and used methods or procedures. Critical infrastructure entities use many of these methods as part of their normal security practices. For the fifth and final step, i.e., strengthening resilience, the authors suggest implementing the recommended tools in relation to specific resilience factors. To this end, they developed matrices for selecting internal and external tools suitable for resilience strengthening. In these matrices, the authors summarized all currently available approaches and methods suitable for strengthening the technical and organizational resilience of energy critical infrastructure elements.

5. Conclusions

The energy sector is a key sector of the critical infrastructure system. All other critical infrastructure sectors depend on an energy supply to provide indispensable services to society as a whole. For this reason, it is essential to ensure a high level of protection of the elements of the energy sector, in particular through their resilience to disruptive events. The currently available methods allow assessment of the level of resilience and identification of vulnerabilities. However, resilience strengthening in these weak points is no longer receiving as much attention.

For this reason, the aim of this article was to provide the reader with a comprehensive methodological overview in the field of resilience strengthening in the energy critical infrastructure sector. This review focused mainly on currently available tools suitable for resilience strengthening. Based on the results of the research, these tools were sorted into two matrices based on a combination of resilience determinants and domains for defining the tools, i.e., internal and external domains. The first matrix presents internal resilience-strengthening tools, which are classified into personnel, substantive, procedural, and financial. The second matrix presents the external instruments for resilience strengthening, which are classified into economic, political, social, environmental, legislative, and technological. These tools are part of a proposed approach to strengthening the resilience of critical energy infrastructure elements. These tools are part of the proposed resilience-

strengthening procedure and can be used to strengthen the resilience of the elements of all energy critical infrastructure subsystems, i.e., electricity, oil, gas, and heating.

The developed procedure and identified tools are primarily intended for the security liaison staff of critical energy infrastructure entities and other critical energy infrastructure entities. However, external tools may also be useful for security liaison staff in other technically oriented critical infrastructure sectors. However, the practical application of each tool will always depend on the specification of the board whose resilience is to be strengthened and the approach of the organization. In this context, it can be concluded that individual resilience-strengthening tools require further research and verification applications in practice.

From this perspective, it is appropriate to appeal to other research organizations and entities to show interest in this issue and thus contribute to the development of a more comprehensive and holistic approach to strengthening resilience, not only in the critical energy infrastructure sector. It is also worth noting that the subject of further research should be the quantification of the resilience-level enhancement after the application of the recommended tools. For this purpose, some of the existing methods of assessing the level of energy critical infrastructure elements' static resilience could primarily be used (see Table 2).

Author Contributions: Conceptualization, D.R. and H.J.; methodology, D.R., S.S., H.J. and D.S.; software, D.R. and H.J.; validation, D.R. and S.S.; formal analysis, D.S.; investigation, D.R. and H.J.; resources, H.J., D.S. and M.H.; data curation, D.R.; writing—original draft preparation, D.R., S.S., H.J., D.S. and M.H.; writing—review and editing, D.R., S.S., H.J., D.S. and M.H.; visualization, S.S.; supervision, D.R.; project administration, D.R.; funding acquisition, D.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of the Interior of the Czech Republic, grant number VI20192022151, and the VSB—Technical University of Ostrava, grant number SP2022/70.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. *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*; Council of the European Union: Brussels, Belgium, 2008.
2. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T.; Novotny, P. Cascading Impact Assessment in a Critical Infrastructure System. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 125–138. [CrossRef]
3. *Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21. 2013)*; The White House: Washington, DC, USA, 2013.
4. Lauge, A.; Hernantes, J.; Sarriegi, J.M. Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 16–23. [CrossRef]
5. Xiao, D.; Chen, H.; Wei, C.; Bai, X. Statistical Measure for Risk-Seeking Stochastic Wind Power Offering Strategies in Electricity Markets. *J. Mod. Power Syst. Clean Energy*, 2021, *in press*. [CrossRef]
6. Araújo, K.; Shropshire, D. A Meta-Level Framework for Evaluating Resilience in Net-Zero Carbon Power Systems with Extreme Weather Events in the United States. *Energies* **2021**, *14*, 4243. [CrossRef]
7. *Critical Infrastructure Resilience Final Report and Recommendations*; National Infrastructure Advisory Council, U.S. Department of Homeland Security: Washington, DC, USA, 2009.
8. Brown, C.; Seville, E.; Vargo, J. Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *Int. J. Crit. Infrastruct. Prot.* **2017**, *18*, 37–49. [CrossRef]
9. Lee, A.; Vargo, J.; Seville, E. Developing a tool to measure and compare organizations resilience. *Nat. Hazards Rev.* **2013**, *14*, 29–41. [CrossRef]
10. Van der Merwe, S.E.; Biggs, R.; Preiser, R. Sensemaking as an approach for resilience assessment in an Essential Service Organization. *Environ. Syst. Decis.* **2020**, *40*, 84–106. [CrossRef]

11. Zhou, L.; Chen, Z. Measuring the Performance of Airport Resilience to Severe Weather Events. *Transp. Res. Part D Transp. Environ.* **2020**, *83*, 102362. [CrossRef]
12. Wei, D.; Chen, Z.; Rose, A. Evaluating the role of resilience in reducing economic losses from disasters: A multi-regional analysis of a seaport disruption. *Reg. Sci. Assoc. Int.* **2020**, *99*, 1691–1722. [CrossRef]
13. Jovanovic, A.S.; Chakravarty, S.; Jelic, M. Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach. In *Issues on Risk Analysis for Critical Infrastructure Protection*; Rosato, V., Pietro, A.D., Eds.; IntechOpen: London, UK, 2021. [CrossRef]
14. Hoisieni, S.; Barker, K.; Ramirez-Marquez, J.E. A Review of Definitions and Measures of System Resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]
15. Bertocchi, G.; Bologna, S.; Carducci, G.; Carrozzi, L.; Cavallini, S.; Lazari, A.; Oliva, G.; Traballesi, A. *Guidelines for Critical Infrastructure Resilience Evaluation*; Italian Association of Critical Infrastructures' Experts: Rome, Italy, 2016. [CrossRef]
16. Nan, C.; Sansavini, G.A. Quantitative Method for Assessing Resilience of Interdependent Infrastructures. *Reliab. Eng. Syst. Saf.* **2017**, *157*, 35–53. [CrossRef]
17. Johansen, C.; Tien, I. Probabilistic multi-scale modelling of interdependencies between critical infrastructure systems for resilience. *Sustain. Resilient Infrastruct.* **2018**, *3*, 1–15. [CrossRef]
18. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T. Complex approach to assessing resilience of critical infrastructure elements. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 125–138. [CrossRef]
19. Ciapessoni, E.; Cirio, D.; Pitto, A.; Sforna, M. A risk-based resilience assessment tool to anticipate critical system conditions in case of natural threats. In Proceedings of the Milan PowerTech (IEEE 2019), Milan, Italy, 23–27 June 2019; pp. 1–6. [CrossRef]
20. Simonovic, S.P.; Arunkumar, R. Comparison of static and dynamic resilience for a multipurpose reservoir operation. *Water Resour. Res.* **2016**, *52*, 8630–8649. [CrossRef]
21. Ouyang, M.; Liu, C.; Xu, M. Value of resilience-based solutions on critical infrastructure protection: Comparing with robustness-based solutions. *Reliab. Eng. Syst. Saf.* **2019**, *190*, 106506. [CrossRef]
22. Eljaoued, W.; Yahia, N.B.; Saoud, N.B.B. A Qualitative-Quantitative Resilience Assessment Approach for Socio-technical Systems. *Procedia Comput. Sci.* **2020**, *176*, 2625–2634. [CrossRef]
23. Kammouh, O.; Gardoni, P.; Cimellaro, G.P. Probabilistic Framework to Evaluate the Resilience of Engineering Systems Using Bayesian and Dynamic Bayesian Networks. *Reliab. Eng. Syst. Saf.* **2020**, *198*, 106813. [CrossRef]
24. Rehak, D.; Hromada, M.; Onderkova, V.; Walker, N.; Fuggini, C. Dynamic robustness modelling of electricity critical infrastructure elementsas a part of energy security. *Int. J. Crit. Infrastruct. Prot.* **2022**, *136*, 107700. [CrossRef]
25. Labaka, L.; Hernantes, J.; Sarriegi, J.M. A Framework to Improve the Resilience of Critical Infrastructures. *Int. J. Disaster Resil. Built Environ.* **2015**, *6*, 409–423. [CrossRef]
26. Zimmerman, R.; Zhu, Q.; de Leon, F.; Guo, Z. Conceptual modelling framework to integrate resilient and interdependent infrastructure in extreme weather. *J. Infrastruct. Syst.* **2017**, *23*, 04017034. [CrossRef]
27. Haines, A. *Resilience of Rail Infrastructure: Update Report to the Secretary of State for Transport Following the Derailment at Carmont, near Stonehaven*; Network Rail: London, UK, 2021.
28. Reeves, S.; Winter, M.; Leal, D.; Hewitt, A. *Rail: An Industry Guide to Enhancing Resilience*; The Resilience Shift and TRL: London, UK, 2019.
29. Walker, B.; Nilakant, V.; Heugten, K.; Kuntz, J.; Malinen, S.; Naswall, K. *Becoming Agile: A Guide to Building Adaptive Resilience*; The University of Canterbury: Christchurch, New Zealand, 2019.
30. Tonn, G.; Erwann, M.K.; Kunreuther, H. *Insurance, Economic Incentives and Other Policy Tools for Strengthening Critical Infrastructure Resilience: 20 Proposals for Action*; Wharton School of the University of Pennsylvania: Philadelphia, PA, USA, 2016.
31. Rahman, M.; Ghosh, S. Increasing Resilience by the Participatory Planning Approach. In Proceedings of the Construction Research Congress 2016; Juan, S., Rico, P., Eds.; American Society of Civil Engineers: Reston, VA, USA, 2016; pp. 1538–1545. [CrossRef]
32. Silla, A.; Jaroszweski, D.; Quinn, A.; Baker, C.; Hooper, E.; Kochsiek, J.; Schultz, S.; Sila, A. *Guidebook for Enhancing Resilience of European Railway Transport in Extreme Weather Events*, 1st ed.; European Commission EC: Brussels, Belgium, 2014.
33. Bucci, S.; Inserra, D.; Lesser, J.; Mayer, M.; Spencer, J.; Slattery, B.; Tubb, K. *After Hurricane Sandy: Time to Learn and Implement the Lessons in Preparedness, Response, and Resilience*; The Heritage Foundation Emergency Preparedness Working Group: Washington, DC, USA, 2013.
34. *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*; COM/2020/829 Final; European Commission: Brussels, Belgium, 2020.
35. Holling, C.S. Resilience and Stability of Ecological Systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [CrossRef]
36. Davoudi, S.; Porter, L. Applying the Resilience Perspective to Planning: Critical Thoughts from Theory and Practice. *Plan. Theory Pract.* **2012**, *13*, 299–333. [CrossRef]
37. Graham, S. *Disrupted Cities: When Infrastructure Fails*; Routledge: New York, NY, USA, 2009. [CrossRef]
38. Graham, S.; Marvin, S. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*; Routledge: London, UK, 2001.

39. Rehak, D.; Flynnova, L.; Slivkova, S. Concept of Resistance in the Railway Infrastructure Elements Protection. In *TRANSBALTICA XII: Transportation Science and Technology*; Prentkovskis, O., Yatskiv, I., Skačkauskas, P., Junevičius, R., Maruschak, P., Eds.; Springer: Cham, Switzerland, 2021; pp. 419–428. [CrossRef]
40. Rehak, D.; Senovsky, P.; Slivkova, S. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* **2018**, *6*, 21. [CrossRef]
41. Rehak, D. Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Saf. Sci.* **2020**, *123*, 104573. [CrossRef]
42. *Good Governance for Critical Infrastructure Resilience*; OECD Publishing: Paris, France, 2019. [CrossRef]
43. *Anticipate, React, Recover: Resilient Infrastructure Systems*; National Infrastructure Commission: London, UK, 2020.
44. *Understanding Transportation Resilience: A 2016–2018 Roadmap, for Security, Emergency Management, and Infrastructure Protection in Transportation Resilience*; American Association of State Highway and Transportation Officials: Washington, DC, USA, 2017.
45. Linnenluecke, M.K. Resilience in business and management research: A review of influential publications and a research agenda. *Int. J. Manag. Rev.* **2017**, *19*, 4–30. [CrossRef]
46. Denyer, D. *Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking*; BSI and Cranfield School of Management: Bedford, UK, 2017.
47. *ISO 22316*; Security and Resilience—Organizational Resilience—Principles and Attributes. International Organization for Standardization: Geneva, Switzerland, 2017.
48. Bridge, J.; Dodds, J.C. *Managerial Decision Making*; Routledge: London, UK, 2018. [CrossRef]
49. *IEC 62502*; Analysis Techniques for Dependability—Event Tree Analysis (ETA). International Electrotechnical Commission: Geneva, Switzerland, 2010.
50. *IEC 61025*; Fault Tree Analysis (FTA). International Electrotechnical Commission: Geneva, Switzerland, 2006.
51. *IEC 61882*; Hazard and Operability Studies (HAZOP Studies)—Application Guide. International Electrotechnical Commission: Geneva, Switzerland, 2016.
52. Armstrong, M. *Armstrong's Handbook of Human Resource Management Practice*, 3rd ed.; Kogan Page: London, UK, 2014.
53. Ratnawat, R.G.; Jha, P.C. Impact of Job Related Stress on Employee Performance: A Review and Research Agenda. *IOSR J. Bus. Manag.* **2014**, *16*, 1–6. [CrossRef]
54. *EN 50126-1*; Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)—Part 1: Generic RAMS Process. European Standard: Brussels, Belgium, 2017.
55. Robinson, C.P.; Woodard, J.B.; Varnado, S.G. Critical Infrastructure: Interlinked and Vulnerable. *Issues Sci. Technol.* **1998**, *15*, 61–68.
56. Tracht, K.; Goch, G.; Schuh, P.; Sorg, M.; Westerkamp, J.F. Failure probability prediction based on condition monitoring data of wind energy systems for spare parts supply. *CIRP Ann.* **2013**, *62*, 127–130. [CrossRef]
57. Lindenberger, D.; Bruckner, T.; Morrison, R.; Groscurth, H.M.; Kümmel, R. Modernization of local energy systems. *Energy* **2004**, *29*, 245–256. [CrossRef]
58. Kampova, K.; Lovecek, T.; Rehak, D. Quantitative Approach to Physical Protection Systems Assessment of Critical Infrastructure Elements: Use Case in the Slovak Republic. *Int. J. Crit. Infrastruct. Prot.* **2020**, *30*, 100376. [CrossRef]
59. *ISO 31000*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
60. *IEC 31010*; Risk Management—Risk Assessment Techniques. International Electrotechnical Commission: Geneva, Switzerland, 2019.
61. Bugdol, M.; Jedynak, P. *Integrated Management Systems*; Springer: Cham, Switzerland, 2015. Available online: https://link.springer.com/book/10.1007/978-3-319-10028-9 (accessed on 13 June 2022).
62. Gibbert, M.; Hoegl, M.; Valikangas, L. Financial Resource Constraints and Innovation. *J. Prod. Innov. Manag.* **2014**, *31*, 197–201. [CrossRef]
63. Picard, P. Natural Disaster Insurance and the Equity-Efficiency Trade-Off. *J. Risk Insur.* **2008**, *75*, 17–38. [CrossRef]
64. IEA—International Energy Agency. Available online: https://www.iea.org/ (accessed on 13 June 2022).
65. *Green Infrastructure in the Energy Sector*; European Commission: Brussels, Belgium, 2014.
66. Sevcik, J.; Malus, M.; Svoboda, P. Large-scale industrial company alarm receiving centre modernization design. *WSEAS Trans. Commun.* **2014**, *13*, 587–595.