systems

MDPI

Article

The Importance of Resistance in the Context of Critical Infrastructure Resilience: An Extension of the CIERA Method

David Rehak [1,*], Lucie Flynnova [1], Martin Hromada [2] and Clemente Fuggini [3]

[1] Faculty of Safety Engineering, VSB—Technical University of Ostrava, 700 30 Ostrava, Czech Republic; lucie.flynnova@vsb.cz
[2] Faculty of Applied Informatics, Tomas Bata University in Zlin, 760 05 Zlin, Czech Republic; hromada@utb.cz
[3] Rina Consulting S.p.A., 20123 Milano, Italy; clemente.fuggini@rina.org
* Correspondence: david.rehak@vsb.cz; Tel.: +420-597-322-816

Abstract: Technical sectors compose an inseparable and elementary part of a complex critical infrastructure (CI) system. Their provided services are essential to the functioning of all of the dependent sectors of CI on which society and states depend, especially in areas experiencing high levels of urbanisation. The initial point for effective CI elements' protection is the permanent assessment and strengthening of their capacity for resilience to the negative effects of internal and external threats. The current perceptions of resilience focus primarily on repressive components responsive to incidents (i.e., robustness, recoverability, and adaptability), while minimal attention is paid to the preventative components. The article's contribution to this literature gap is its definition of resistance, which can be considered as a CI element's ability to prevent the occurrence of incidents. To this goal, the current study defines (1) the individual factors (variables and parameters) determining CI resistance and (2) the methodological procedure for infrastructure element resistance assessment in order to identify the weak points throughout a complex CI system and subsequently strengthen them. Moreover, a practical example of resistance assessment for a selected critical energy infrastructure element is presented. The main outcome of this article is the definition of the primary steps for the expansion of the CIERA method, via the enhancement of CI components' resilience capacity in the prevention phase.

Keywords: resistance; physical resistance; crisis preparedness; anticipation ability; security measures; critical infrastructure resilience

Citation: Rehak, D.; Flynnova, L.; Hromada, M.; Fuggini, C. The Importance of Resistance in the Context of Critical Infrastructure Resilience: An Extension of the CIERA Method. *Systems* **2023**, *11*, 506. https://doi.org/10.3390/systems11100506

Academic Editors: Randy Buchanan and Gregory S. Parnell

Received: 3 September 2023
Revised: 27 September 2023
Accepted: 29 September 2023
Published: 8 October 2023

1. Introduction

The term resilience was firstly introduced by Holling [1] in 1973 within an ecology context as "*a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*", and was originally proposed as a formulation for systems which can be characterized as ecological. However, the concept of resilience has started to be reflected over time in other scientific areas, too, such as psychology, economics, and sociology. It was, therefore, a reasonable consequence that resilience as a concept would be recognized for its feasibility and added value in technically oriented social fields as well.

CI resilience was firstly defined in 2009 in the Critical Infrastructure Resilience Final Report and Recommendations [2], and within this context, is perceived as "*the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event*". Based on this definition, three key components (i.e., robustness, recoverability, and adaptability) have been identified in [2] in order to determine resilience. Although these components are key determinants of resilience, a more thorough investigation reveals that they only have a responsive character, as their impact on CI resilience is only apparent at the time of the incident [2]. This observation leads to the assumption that there is no preventative

component in the process of resilience building; therefore, this role could be supported by resistance, which can be perceived as the CI ability to prevent the incident occurring.

The Britannica Dictionary [3] defines resistance as the ability to prevent something from having an effect. The term resistance is used by authors within various and broader scientific fields, e.g., in medicine, to refer to antibacterial resistance to antibiotics [4,5], or in sociology to refer to the manifestation of social resistance [6,7]. The adaptation and integration of the resistance concept into engineering practice were influenced by the ecology field, where the term was firstly introduced in relation to resilience by Sugden [8] and in connection with alpine lake ecosystems. The author defined the main logical differences between resistance and resilience. He sees resistance as a measure of how much an ecosystem is able to withstand a disturbance such as the introduction of an alien species. Resilience was then considered as a response and recovery measure of the ecosystem after eliminating the source of the change.

Over the last decade, CI resilience issues have been analysed by several authors. Some studies deal more generally with the importance of resistance in the context of CI resilience [9–12], while other publications have already defined the preventive factors of resilience and point to the necessity of their separation from robustness [13–16]. However, there are several frameworks which have already defined and evaluated the resistance variables when assessing the level of CI resilience [17–19]. Under this scope, resistance can be perceived as an important component of resilience, which should be defined and determined through basic factors.

Regarding the above presented landscape, the added value of this article is to define CI resistance and to describe its integration and implementation within the established CIERA method [20]. The most crucial part of this article includes the expression of individual CI resistance factors and the methodological procedure for their assessment with the ambition to strengthen the resistance of these CI systems. Therefore, this study contributes significantly to the definition of a comprehensive concept for CI systems resilience.

2. Materials and Methods

The current study attempts to prove the suitability of integrating resistance into resilience, hence the definition of resilience and its meaning for a CI system are required in the initial phase. The origin of the word resilience is rooted in the Latin language, and it is found as *resiliere*, which literally translates as bounce back [21]. Resilience within the context of CI firstly appeared in 2009 [2], but this definition was expanded in 2012 by the US National Academies of Science in order to include preparation and planning and was expressed as "*the system's ability to prepare and plan for, absorb, recover from, and successfully adapt to disruptive events*" [22]. Since then, there has been no essential change in the perception of CI resilience, which is also illustrated by the definitions of CI resilience given in several important publications within this period [11,23–29]. All of the definitions found in these studies are oriented towards the so-called technical resilience, which refers to critical infrastructure elements (CIEs) and is expressed by their absorption capacity and their ability to recover and adapt to incidents that have occurred. However, a slight shift in the consideration of CI system resilience occurred in 2022, when the European Union issued a respective Directive which has focused on the resilience of critical entities [30]. Resilience within this context is considered as "*a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident*". This definition is evidently spotlighting and promoting the organisational resilience, aiming at increasing the resilience of the entities which are responsible for these CIEs [31].

From the summary and collection of the above-mentioned definitions, it can be stated that CI resilience consists of four phases, which together form the so-called CI resilience cycle [32] and its significance is the ever-increasing CIE protection. Even though resilience is enhanced especially in the adaptation phase to an incident that has occurred, the increase in resilience can be noticed even from the recovery phase in some cases (e.g., by adopting and installing a completely new and more resilient technology).

The initial phase of the CI resilience cycle is prevention, and its importance lies in preventing the occurrence of an incident because of its potential threat or impact on a CIE. These measures aim at the early detection of an incident and the element's preparedness for its impact. When an incident occurs, then the resilience cycle moves into the absorption phase. The essence of this phase is to absorb the incident's effects on the CIE. The element's ability to absorb the incident's effects is referred to as robustness. After the completion of the incident, resilience moves into the recovery phase. The significance of this phase is to mitigate the consequences of the incident's impact on the CIE and restore its performance to its initial level. Adaptation is the final stage of the CI resilience cycle and refers to the importance of the CIE's adaptation to the occurred incident, strengthening thereby the element's overall resilience capacity.

CI resilience is currently determined by three components, as also mentioned in the introduction, but these characterise only three of the above phases (i.e., absorption, recovery, and adaptation), since the prevention phase is not yet considered among the components. However, and before moving to the definition of the component in the prevention phase, it is appropriate to present the components in the existing three phases of resilience [2]:

- robustness is "*the ability of the system to absorb the effects of a disruption without significant deviation from normal operating performance*";
- recoverability is "*the ability of the system to recover quickly from potentially disruptive events*";
- adaptability is "*the ability of the system to adapt to a shock to normal operating conditions*".

Research on these three specific components has been conducted in the past by a number of reputable authors [32–39]. After a detailed analysis of these publications, variables determining the CIE resilience components were defined (Figure 1) as part of the CIERA method's development [20].

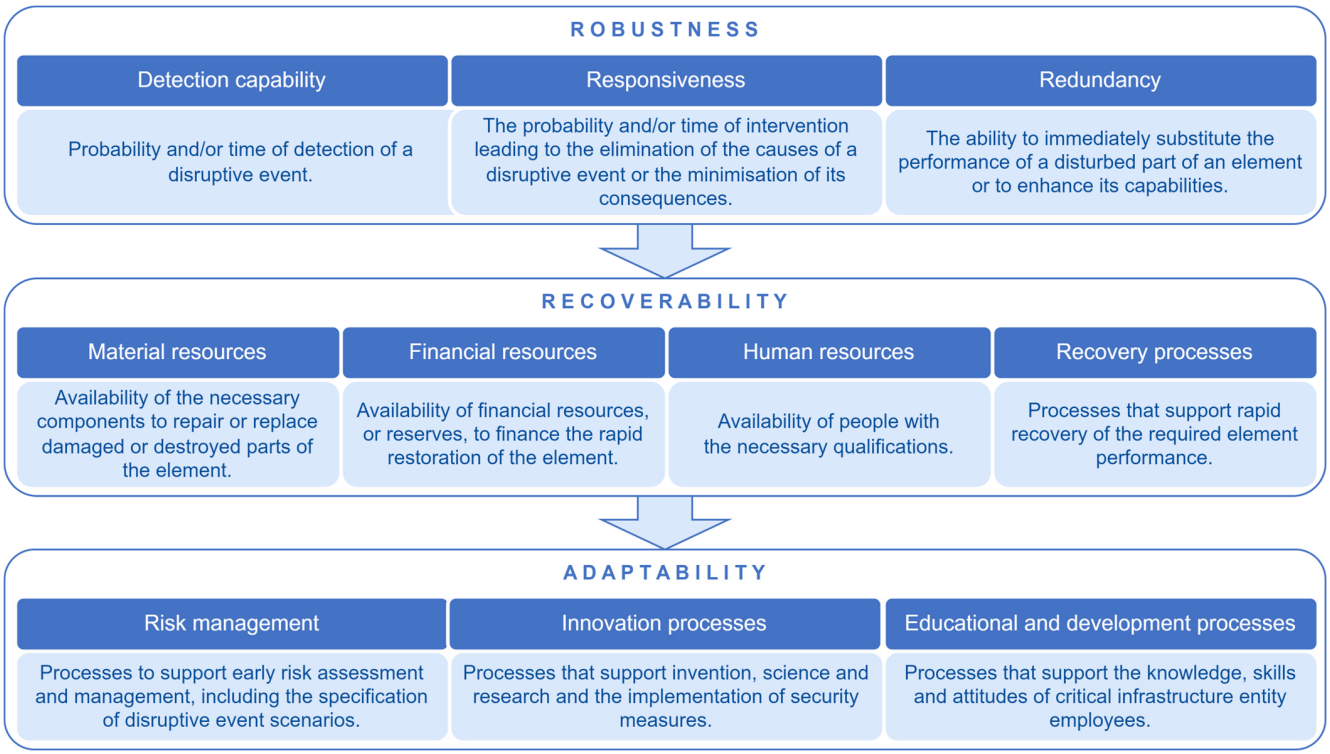

Figure 1. Variables determining CIE resilience components [20].

Based on the above, it can be concluded that there is currently no characteristic component to express the first resilience phase (i.e., prevention). This component could be considered the resistance, which in the context of ecology (from which the whole resilience concept initiated) is found as the ability of an ecosystem to protect itself against a perturbation [8].

3. Results

The following text is a key part of the article, as the authors present here the results of their original research. These results refer mainly to the definitions of (1) CI resistance, (2) the factors determining this resistance, and (3) a methodological procedure for assessing these factors in order to strengthen CIE resistance.

The term resistance was coined by Leonardo da Vinci in The Madrid Codices I–II [40] in order to describe the resistance of water and air to moving solid bodies, as well as of water and fire moving in air. An important definition of resistance was elaborated from Georg Ohm later, in 1827, and it was in relation to the difficulty of passing an electric current through a substance [41]. Another use of the term resistance was recorded in 1862, in the sense of organised opposition to an invader [42]. In the following period, the term was increasingly used in a military-political context to refer to underground resistance movements in any country. Over time, the term resistance has been inserted into the vocabulary and practice of various other scientific fields, such as medicine (e.g., antibiotic or antimicrobial resistance, immune resistance, psychological resistance), ecology (e.g., ecological or environmental resistance, pesticide resistance) or economics (e.g., resistance economy).

In the context of the current study, which is CI systemic resilience, the term resistance has not yet been defined. Some authors consider resistance and resilience as two distinct concepts [43], understanding resistance as being similar to preventing or protecting, while resilience as akin to responding or recovering. Other authors include the two terms in the same context but consider resistance as a component of resilience responsible for reducing the severity or consequences of a hazard [33]. In both cases, it can be stated that this interpretation is inaccurate, as resistance in all of the above mentioned fields is a factor preventing the emergence of an incident. It is thus a fundamental component of resilience that has a clearly preventative but not mitigating character.

Taking into account these considerations, the authors of this article have created a definition where they view resistance as "*the critical infrastructure ability to prevent the occurrence of an incident*". In this context, it is appropriate to draw attention to the fact that this capacity of resistance minimizes the transmission of the incident consequences to dependent CI sectors, thereby preventing the occurrence of cascading and synergistic effects [44]. Based on the above, it is feasible to define resistance within the CI resilience context and, as a consequence, this resistance is to be seen as one of the essential resilience components, especially in its initial phase. Other resilience components are robustness, recoverability, and adaptability. The authors' perceptions of these components regarding an incident are presented in Figure 2.

In the following part of the article and with reference to Figure 1, the definition of the variables determining CIE resistance is feasible (Figure 3). It is evident from the above definition of resistance that the significance of these variables must be their ability to prevent incidents. For this scope, all of these variables must be of a preventative character.

The default variable is crisis preparedness. The essence of crisis preparedness is to increase the readiness of CI entities and their infrastructures against disasters [45]. This preparedness consists in a thorough assessment of risks and the subsequent processing of security planning documentation. Risk assessment is considered a systematic and effective way of identifying, analysing, and evaluating risks and determining the most effective costs and means to minimize these risks [46]. For this purpose, it is advisable to use the recommended risk assessment techniques [47]. Security planning documentation specifically includes emergency plans and a CI entity's crisis preparedness plan [48]. An emergency plan is a document containing a comprehensive set of preventive measures aimed at preparing the CI entity for an accident or other incident, including natural and man-made threats. For example, in the Czech Republic, the crisis preparedness plan serves CI entities to ensure their own functioning during disasters [49].

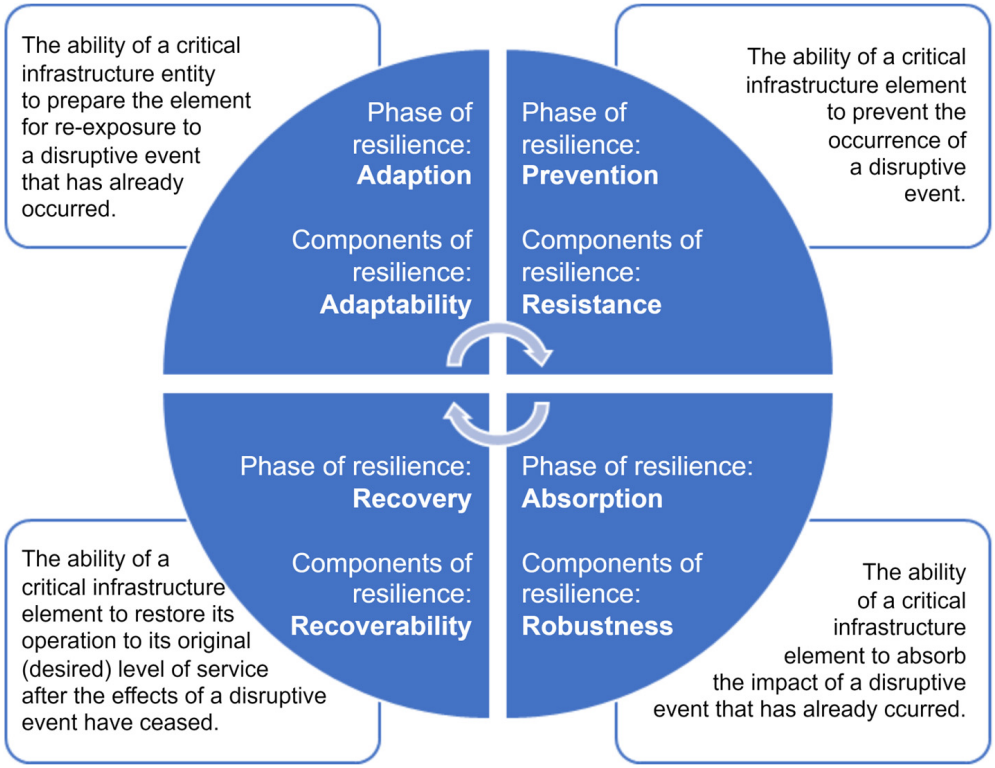

Figure 2. Resistance perceptions in relation to CI resilience.

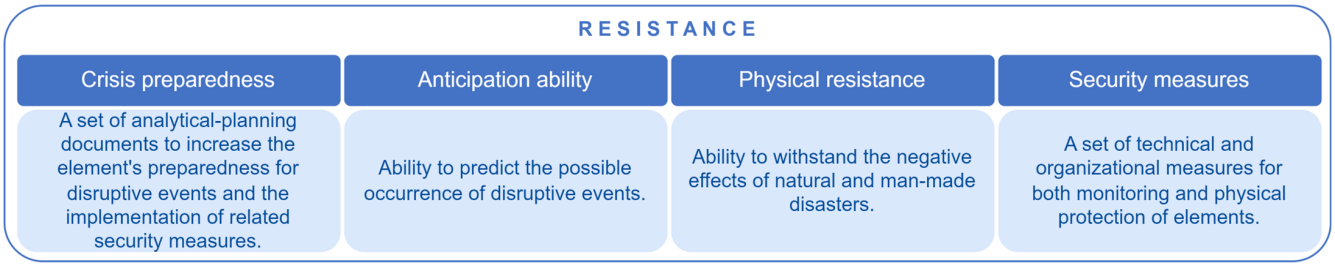

Figure 3. Defining variables determining the CIE's resistance.

The second variable is anticipation ability. The substance of this variable is the ability of the CI entity to predict the possible incident emergence as a result of the threat impact. These are basically the activities of the entity in the context of defining the risk environment that affects the CIE [33]. For this purpose, it is possible to use one of the available methods aimed at indicating the disruption of CIE resilience [29,50,51]. On the basis of the possible element resilience disruption assessment, preventive measures are implemented to prevent the emergence of an incident. Other measures which can be used to predict the emergence of incidents are audits or software applications that enable incident prediction [52,53].

The third variable is physical resistance. The substance of this variable is the CIE's ability to resist the effects of natural and man-made threats (e.g., rockslide or truck attack), through the material and structural resistance of CI buildings [54]. The core areas of physical resistance are fire, seismic and explosion resistance. Fire resistance is the ability of building structures to withstand the effects of a fully developed fire, without their load-bearing capacity and stability, integrity and insulating ability being particularly affected [55]. Seismic resistance is the ability of building structures to withstand the effects of earthquakes through sufficient elasticity or ductility [56]. Explosion resistance is the ability of buildings to prevent explosions (i.e., active explosion protection) or to eliminate the effects of an explosion (i.e., passive explosion protection) through their layout and measures [57].

The last variable is security measures. The usefulness of these measures is in the monitoring and physical protection of CIEs. The goal of monitoring is mainly to check the technical condition of the elements, their functions and the services they provide [58]. If any deficiencies are identified through monitoring, it is advisable to start the process of repairing or modernizing these elements. The essence of modernization is especially in maintaining the technical state of elements with current trends and technologies [59]. A suitable preventive tool for CIE protection is also a physical protection system, which is determined by regime, organizational and technical measures [60].

A comprehensive overview of the variables and their parameters describing CIE resilience is presented graphically in Figure 4. The structure of this figure is designed in the form of a descending classification, where the first level consists of variables, the second level consists of parameters, and the third level recommends some potentially suitable criteria.

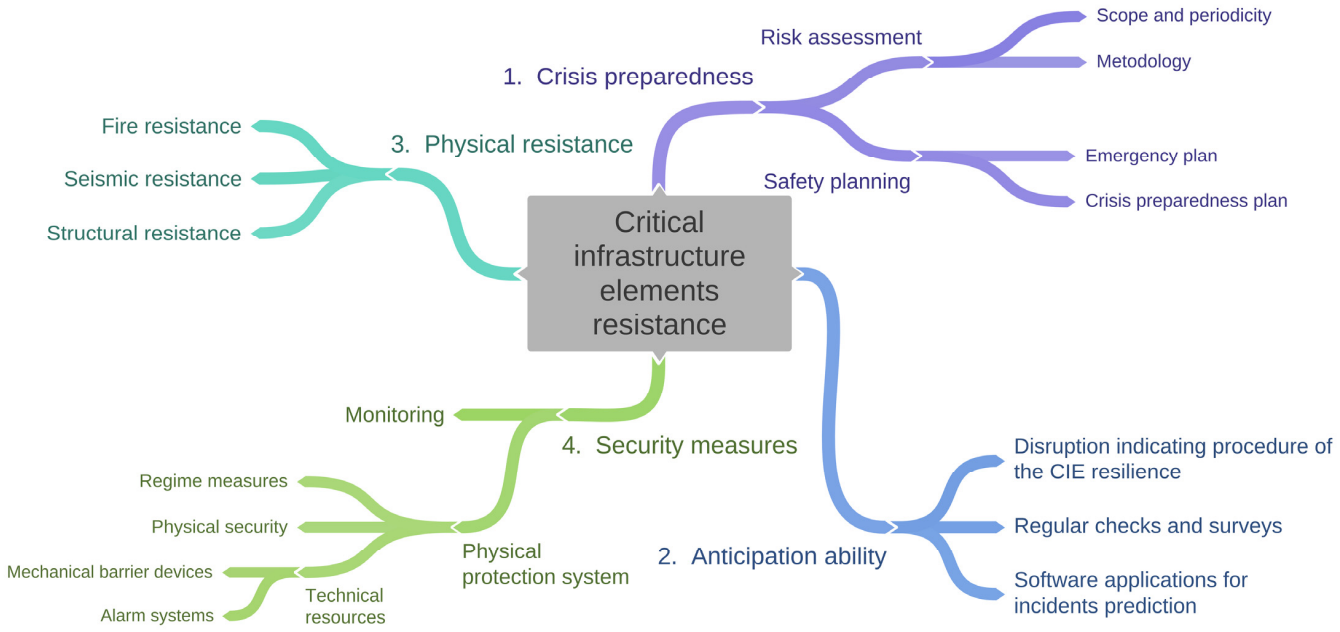

Figure 4. Variables and their parameters describing the CIE's resistance.

The above-defined variables and their parameters can be used in particular to assess CIE resistance, e.g., through the assessment mechanism of the semi-quantitative CIERA method [20]. This method is suitable for assessing the resilience of elements in technical infrastructures, such as energy, transport, communication and information systems or water management. For this purpose, it is necessary to assess all parameters that determine each variable. These parameters must be evaluated against the specific threat, as the level of resistance of the elements cannot be generalised. The assessment can be carried out, similarly to the CIERA method, through point evaluation, where 5 points is the best and 1 point the worst.

The level of each resistance variable is then calculated by a weighted average of the individual parameters (see Equation (1)). Because the parameter level is represented as a score between 1 and 5, the resulting value must be multiplied by 20, which gives a result expressed as a percentage.

$$V_r = 20 \sum_{s=1}^{t} P_s w_s \quad (1)$$

where V_r = the r-th CIE resistance variable [%]; P_s = the s-th CIE resistance parameter [points]; w_s = the s-th standardised weight of the s-th CIE resistance parameter in the interval $\langle 0; 1 \rangle$; t = the number of parameters in the r-th variable. The standardised weights

of the parameters were determined using the pairwise comparison method [61] and are presented in Table 1.

Table 1. Standardised weights for parameters determining resistance variables of CIEs.

Variables	Parameters and Their Standardised Weights			∑
Crisis preparedness (V_1)	Risk assessment ($P_{1.1}$) $w_{1.1}$ = 0.4	Safety planning ($P_{1.2}$) $w_{1.2}$ = 0.6	- -	w_1 = 1.0
Anticipation ability (V_2)	Disruption indicating procedure of CIE resilience ($P_{2.1}$) $w_{2.1}$ = 0.4	Regular checks and surveys ($P_{2.2}$) $w_{2.2}$ = 0.3	Software applications for incident prediction ($P_{2.3}$) $w_{2.3}$ = 0.3	w_2 = 1.0
Physical resistance (V_3)	Fire resistance ($P_{3.1}$) $w_{3.1}$ = 0.4	Seismic resistance ($P_{3.2}$) $w_{3.2}$ = 0.3	Explosion resistance ($P_{3.3}$) $w_{3.3}$ = 0.3	w_3 = 1.0
Security measures (V_4)	Monitoring ($P_{4.1}$) $w_{4.1}$ = 0.4	Physical protection system ($P_{4.2}$) $w_{4.2}$ = 0.6	- -	w_4 = 1.0

In this context, it is worth noting that the current way of calculating individual variables does not take into account the changing nature of a CI element, i.e., whether it is a point, areal or line element [62,63]. The resulting level of CIE resistance is expressed by the weighted average of the individual variables (see Equation (2)):

$$R = \sum_{r=1}^{t} V_r h_r \tag{2}$$

where R = the CIE resistance [%]; V_r = the r-th variable of CIE resistance [%]; h_r = the r-th standardised weight of the r-th variable of CIE resistance [$\langle 0; 1 \rangle$]; t = the number of variables expressing the CIE resistance. The standardised weights of the variables were expressed using the pairwise comparison method [61] and are presented in Table 2.

Table 2. Standardised weights for variables determining the resistance of CIEs.

Variables	Standardised Weights
Crisis preparedness (V_1)	h_1 = 0.2
Anticipation ability (V_2)	h_2 = 0.25
Physical resistance (V_3)	h_3 = 0.25
Security measures (V_4)	h_4 = 0.3
∑	1.00

A potential graphical representation of the resulting level of CIE resistance and its variables is presented in Figure 5.

The resulting level of CIE resistance is expressed as a percentage, which in itself provides only a rough idea of the protection of the element. A more detailed evaluation of this level is necessary by classifying it according to the reference scale (Table 3) which is based on the CIERA method [20].

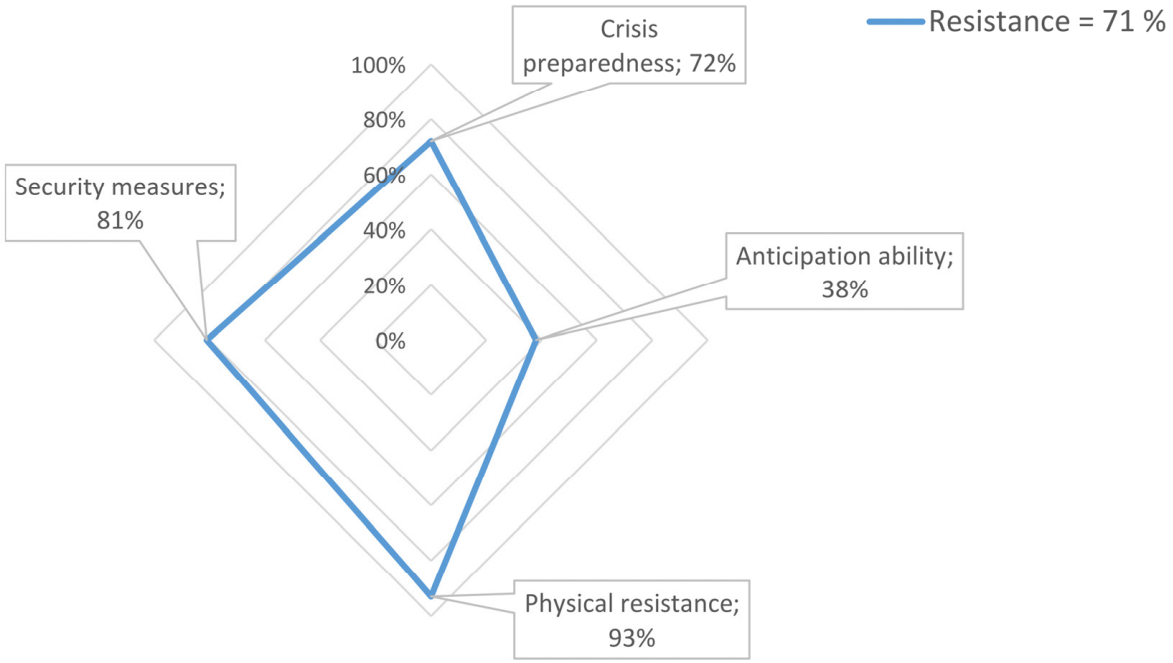

Figure 5. Expression of CIE resistance levels.

Table 3. Reference scale for assessing the CIE resistance level [20].

Resistance Levels of Critical Infrastructure Elements	
High level of resistance	85–100%
Acceptable level of resistance	69–84%
Low level of resistance	53–68%
Insufficient level of resistance	37–52%
Critical level of resistance	≤36%

The acceptability of resistance is diversified into five rating levels, and it is driven by the increased desire, in the interest of the users, to examine the composition of resistance in more detail (i.e., to retrospectively break down resistance into individual variables and parameters). If resistance reaches a level of ≤68%, identification of weaknesses consisting in a breakdown of the resistance assessment results should be carried out at the level of the parameters concerned. For parameters scoring 2 or less, it is necessary to review the affected area of the assessed element and start the process of strengthening its resistance.

To strengthen the resilience of these parameters, it is suitable to use, for example, the tools for strengthening CIE resilience [64]. These tools should be appropriately implemented to strengthen element resistance through the relevant variables. In general, it is feasible to divide these tools into external and internal tools and, due to their nature, into thematic groups. In some cases, these are tools regulating process and functional areas of organization management (i.e., personnel, financial and process tools). In contrary, the tools are focused on external factors (principle of the PESTLE method), considering political, economic, social, legislative, technological, and environmental aspects. Tools suitable for strengthening resistance variables are presented in Figure 6.

Tool areas		Resistance variables of critical infrastructure elements			
		Crisis preparedness	Anticipation ability	Physical resistance	Security measures
Internal tools	Personnel	Long-term education; Study abroad; Skills development; Psychological and occupational well-being	Vocational training; Staff training	-	Long-term education; Vocational training; Staff training; Psychological and occupational well-being
	Substantive	RAMS standard	RAMS standard; Monitoring	Technical means of the physical protection system	Physical security
	Procedural	Planning documents	Planning documents	-	Regime measures; Integrated management system
	Financial	Financial plan	Financial plan; Innovation	-	Financial plan
External tools	Economic	Subsidy programmes	Subsidy programmes	-	Subsidy programmes
	Political	International organisations	International organisations	-	International organisations
	Social	Increase the level of education or awareness	Increase the level of education or awareness	-	-
	Ecological	Mitigate the consequences of disruptive events	-	-	-
	Legislative	Legislation creation	-	-	Legislation creation
	Technological	Technologies and means of emergency services	Technologies and means of emergency services	-	Technologies and means of emergency services

Figure 6. Tools suitable for strengthening CIE resilience variables [64].

4. Practical Example of Resistance Assessment for a Selected Energy CIE

Finally, it is appropriate to demonstrate the applicability of the results obtained in the current study by their implementation to a selected energy CIE. The selected element is an electrical station of a transmission system which is a European CIE. In the Czech Republic, there are a total of 33 electrical stations in operation in the transmission system, of which four stations ensure the connection between the 400 kV and 220 kV systems, 32 stations ensure the connection between TS and DS, 10 stations ensure the output of power from power plants, and eight stations are composed of 400 kV and 220 kV substations. The assessed electrical station is anonymized for security reasons, and only its basic description is provided in Table 4.

In the subsequent section, a semi-quantitative assessment of this selected element's resistance to the selected threat is conducted and presented. This threat is a terrorist attack using an explosive device aimed at physical damage to the control workplace and causing a widespread blackout. The assessment of the resistance of the selected energy CIE is realised in three steps:

- Step 1: Analysis and scoring of each parameter;
- Step 2: Calculation of the level of each variable;
- Step 3: Determination of the resulting energy CIE resistance level.

Step 1: The results of the analysis, including the point rating and its rationale for individual parameters determining the element resistance, are shown in Table 5.

Table 4. Description of selected energy CIE.

Element name	Transmission system electrical station
Sector/subsector	Energy/Electricity/Transmission
Key technologies	1. Transformers 2. Voltage instrument transformers 3. Current instrument transformers 4. Compensation chokes 5. Disconnectors and grounding switches 6. Busbars and branches 7. Circuit breakers
Element performance	400/220 kV

Table 5. Results of analysis and scoring of individual parameters determining element resistance.

Variables	Parameters	Scoring	Justification
Crisis preparedness (V_1)	Risk assessment ($P_{1.1}$)	3	The element risk assessment is only processed for key technologies and does not include detailed scenarios.
	Safety planning ($P_{1.2}$)	4	Emergency plans for all key production technologies are developed for the element.
Anticipation ability (V_2)	Disruption indicating procedure of CIE resilience ($P_{2.1}$)	3	The procedure of indicating a breach of resilience is set only at the strategic-operational level. Elementary levels are absent.
	Regular checks and surveys ($P_{2.2}$)	2	Monitoring of this element is carried out only remotely, and the real arrival time of the intervention unit is set at 1 h.
	Software applications for incident prediction ($P_{2.3}$)	3	The incident prediction is realized using basic software applications that do not allow dynamic modelling.
Physical resistance (V_3)	Fire resistance ($P_{3.1}$)	4	The element's construction can withstand the effects of flame and high temperatures for only 120 min.
	Seismic resistance ($P_{3.2}$)	2	The element's building structure can withstand only the effects of a weak earthquake (magnitude 4.0–4.9).
	Explosion resistance ($P_{3.3}$)	3	The element building's structure has active explosion protection, but passive explosion protection is not sufficient.
Security measures (V_4)	Monitoring ($P_{4.1}$)	4	The element includes security functions to prevent, detect, control, and mitigate an incident.
	Physical protection system ($P_{4.2}$)	4	The physical protection of the element is ensured through modern technical, organizational, and regulatory measures.

Step 2: The results of calculating the level of each variable according to Equation (1) are shown in Table 6.

Table 6. The results of calculating the level of each variable.

Parameters	P_s	w_s	V_r
$P_{1.1}$	3	0.4	72%
$P_{1.2}$	4	0.6	
$P_{2.1}$	3	0.4	54%
$P_{2.2}$	2	0.3	
$P_{2.3}$	3	0.3	
$P_{3.1}$	4	0.4	62%
$P_{3.2}$	2	0.3	
$P_{3.3}$	3	0.3	

Table 6. *Cont.*

Parameters	P_s	w_s	V_r
$P_{4.1}$	4	0.4	80%
$P_{4.2}$	4	0.6	

Step 3: The results of determining the resulting level of resistance of the energy CIE according to Equation (2) are presented in Table 7.

Table 7. The results of determining the resulting level of resistance of the energy CIE.

V_r	h_r	R
72%	0.2	67%
54%	0.25	
62%	0.25	
80%	0.3	

Considering the assessment results presented above, it is possible to state that the element's achieved resistance level is low. For this purpose, it is necessary to determine the weak and vulnerable points, and then to define measures to strengthen the resistance of the selected energy CIE. The identification of weaknesses consists of breaking down the assessment results at the level of the parameters concerned, in doing so identifying all parameters that scored 2 or less. Regarding this case study, these parameters are:

- Regular checks and surveys ($P_{2.2}$),
- Seismic resistance ($P_{3.2}$).

There is subsequently a necessity to identify appropriate tools for enhancing the resistance variables (Table 4) of these parameters and, based on these tools, propose specific security measures at the level of the affected parameters.

The first parameter, regular checks and surveys ($P_{2.2}$), belongs to the variable anticipation ability. In the context of the assessed threat, it is necessary to look for strengthening tools in the field of material tools for this variable. A monitoring tool has been identified in this area. As part of the analysis of existing security measures, it was found that the monitoring of this element is implemented only remotely and the real arrival time of the response unit is set at 1 h. Such measures are insufficient from the element's resistance point of view. A suitable solution is to reduce the arrival time of the response unit, conduct continuous supervision within the given element, or implement irregular physical inspections with a constant frequency per day.

The second parameter, seismic resistance ($P_{3.2}$) belongs to the variable physical resistance. In the context of the assessed threat, it is necessary to look for strengthening tools for this variable also in the field of material tools. In this context, the technical elements of the physical protection tool were identified. As part of the analysis of existing security measures, it was found that the technical means for protecting this element are the least resistant at the level of the materials used. For this reason, a suitable solution is to use more durable materials for strengthening the cooling oil fairing, or to build protective blocks.

Given the presented example, it is evident that the methodical procedure for assessing resistance is particularly suitable for technically oriented infrastructures, such as information and communication technologies or transport buildings. In the case of assessing the resistance of other infrastructure elements, especially those of a socio-economic character, it would be prerequisite to carry out a review of parameters. The current methodological approach is mainly designed and targeted to assess the infrastructure objects' resistance.

5. Conclusions

Technical sectors, especially energy, transport, and information and communication technologies, currently represent a key part of the CI system. Their capacity for resilience is an important factor which ensures and maintains the reliability of services provided not only to the population, but also to dependent sectors of critical infrastructure (e.g., healthcare or emergency services). Potential disruptions to the supply of these basic services would result in extensive impacts on the functioning of the entire company. An important role in ensuring the safety of these deliveries is played by the resistance of infrastructure elements, which the authors of the article define as the critical infrastructure ability to prevent the occurrence of an incident. From this point of view, the critical infrastructure resistance can be considered as an important resilience component which has a preventive character.

Considering the original research results, the authors of this article identified four basic variables responsible for the determination of CI resistance. For each variable, the individual parameters and the principles of their semi-quantitative evaluation were further defined. Subsequently, a methodological procedure for resistance assessment was defined to identify weak points and the subsequent actions in infrastructure element resistance strengthening. The whole process was demonstrated in the conclusion of the article in the form of a practical example using a selected energy CIE. At the same time, it should be noted that the presented methodological approach for resistance assessment has already been successfully applied to and verified on selected European energy CIEs.

The main contribution of this article is to broaden the perception of CI resilience, which has so far been determined only by incident response factors (i.e., robustness, recoverability, and adaptability). The integration of resistance into resilience thus allows CIE protection to be extended and include a preventative component, also. This integration can be practically applied to current or future methods, in the same way it was exploited for the modification of the CIERA method used for CIE resilience assessment. Future research could be focused on the development of the factors that determine infrastructural element resistance and their specification in relation to specific technical, but also selected socio-economic, CI sectors.

Author Contributions: Conceptualization, D.R. and L.F.; methodology, D.R., L.F. and M.H.; validation, L.F. and C.F.; formal analysis, L.F. and M.H.; investigation, D.R.; resources, D.R. and L.F.; data curation, L.F. and C.F.; writing—original draft preparation, D.R., L.F., M.H. and C.F.; writing—review and editing, D.R., L.F., M.H. and C.F.; visualization, D.R.; supervision, D.R.; project administration, D.R.; funding acquisition, M.H. 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 VK01030014.

Data Availability Statement: Restrictions apply to the availability of these data. Data were obtained from a third party and are available only with the permission of that third party.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Holling, C.S. Resilience and Stability of Ecological Systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [CrossRef]
2. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*; U.S. Department of Homeland Security: Washington, DC, USA, 2009.
3. Encyclopædia Britannica. The Britannica Dictionary: Resistance. Available online: https://www.britannica.com/dictionary/resistance (accessed on 21 October 2022).
4. Ddžidić, S.; Šušković, J.; Kos, B. Antibiotic Resistance Mechanisms in Bacteria: Biochemical and Genetic Aspects. *Food Technol. Biotechnol.* **2008**, *46*, 11–21.
5. European Centre for Disease Prevention and Control. Factsheet for Experts. Available online: https://antibiotic.ecdc.europa.eu/en/get-informedfactsheets/factsheet-experts (accessed on 23 October 2022).
6. Baaz, M.; Lilja, M.; Schulz, M.; Vinthagen, S. Defining and Analyzing "Resistance": Possible Entrances to the Study of Subversive Practices. *Altern. Glob. Local Political* **2017**, *41*, 137–153. [CrossRef]

7. Hollander, J.A.; Einwohner, R.L. Conceptualizing Resistance. *Sociol. Forum* **2004**, *19*, 533–554. [CrossRef]
8. Sugden, A.M. Resistance and Resilience. *Science* **2001**, *293*, 1731. [CrossRef]
9. Rogers, C.D.F.; Bouch, C.J.; Williams, S.; Barber, A.R.G.; Baker, C.J.; Bryson, J.R.; Chapman, D.N.; Chapman, L.; Coaffee, J.; Jefferson, I.; et al. Resistance and Resilience—Paradigms for Critical Local Infrastructure. *Munic. Eng.* **2012**, *165*, 73–83. [CrossRef]
10. Dvorak, Z.; Sventekova, E. Evaluation of the Resistance Critical Infrastructure in Slovak Republic. In Proceedings of the 2nd International Symposium Engineering Management and Competitiveness 2012 (EMC 2012), Zrenjanin, Serbia, 22–23 June 2012; pp. 17–22.
11. Curt, C.; Tacnet, J.M. Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Anal.* **2018**, *38*, 2441–2458. [CrossRef]
12. Rehak, D.; Flynnova, L.; Slivkova, S. Concept of Resistance in the Railway Infrastructure Elements Protection. In Proceedings of the 12th International Scientific Conference "Transbaltica 2021: Transportation Science and Technology", Vilnius, Lithuania, 16–17 September 2021; pp. 419–428. [CrossRef]
13. Jovanović, A.; Klimek, P.; Renn, O.; Schneider, R.; Øien, K.; Brown, J.; DiGennaro, M.; Liu, Y.; Pfau, V.; Jelić, M.; et al. Assessing Resilience of Healthcare Infrastructure Exposed to COVID-19: Emerging Risks, Resilience Indicators, Interdependencies and International Standards. *Environ. Syst. Decis.* **2020**, *40*, 252–286. [CrossRef]
14. Braun, M.; Hachmann, C.; Haack, J. Blackouts, Restoration, and Islanding: A System Resilience Perspective. *IEEE Power Energy Mag.* **2020**, *18*, 54–63. [CrossRef]
15. Häring, I.; Sansavini, G.; Bellini, E.; Martyn, N.; Kovalenko, T.; Kitsak, M.; Vogelbacher, G.; Ross, K.; Bergerhausen, U.; Barker, K.; et al. Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies. In *NATO Science for Peace and Security Series C: Environmental Security*; Springer: Dordrecht, The Netherlands, 2017; pp. 21–80. [CrossRef]
16. Fischer, K.; Hiermaier, S.; Riedel, W.; Häring, I. Morphology Dependent Assessment of Resilience for Urban Areas. *Sustainability* **2018**, *10*, 1800. [CrossRef]
17. Labaka, L.; Hernantes, J.; Sarriegi, J.M. A Holistic Framework for Building Critical Infrastructure Resilience. *Technol. Forecast. Soc. Change* **2016**, *103*, 21–33. [CrossRef]
18. Lomba-Fernández, C.; Hernantes, J.; Labaka, L. Guide for Climate-Resilient Cities: An Urban Critical Infrastructures Approach. *Sustainability* **2019**, *11*, 4727. [CrossRef]
19. Adini, B.; Cohen, O.; Eide, A.W.; Nilsson, S.; Aharonson-Daniel, L.; Herrera, I.A. Striving to be Resilient: What Concepts, Approaches and Practices Should be Incorporated in Resilience Management Guidelines? *Technol. Forecast. Soc. Change* **2017**, *121*, 39–49. [CrossRef]
20. 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]
21. Hosseini, 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]
22. US National Academies of Science. *Disaster Resilience: A National Imperative*; National Academies Press: Washington, DC, USA, 2012.
23. Wiseman, E.; McLaughlin, T. *Critical Infrastructure Protection and Resilience Literature Survey: State of the Art*; National Research Council of Canada: Ottawa, ON, Canada, 2014.
24. Setola, R.; Luiijf, E.; Theocharidou, M. Critical Infrastructures, Protection and Resilience. In *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*; Setola, R., Rosato, V., Kyriakides, E., Rome, E., Eds.; Springer: Cham, Switzerland, 2016; pp. 1–18. [CrossRef]
25. Zebrowski, C.; Sage, D. Resilience and Critical Infrastructure: Origins, Theories, and Critiques. In *The Palgrave Handbook of Security, Risk and Intelligence*; Dover, R., Dylan, H., Goodman, M., Eds.; Palgrave Macmillan: London, UK, 2017; pp. 117–135. [CrossRef]
26. Biskupovic, S. *Critical Infrastructure Resilience: Findings from a Systematic Review*; University of Waterloo: Waterloo, ON, Canada, 2021.
27. Cantelmi, R.; Di Gravio, G.; Patriarca, R. Reviewing Qualitative Research Approaches in the Context of Critical Infrastructure Resilience. *Environ. Syst. Decis.* **2021**, *41*, 341–376. [CrossRef]
28. Hromada, M.; Rehak, D.; Lukas, L. Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security. *Energies* **2021**, *14*, 1624. [CrossRef]
29. Sathurshan, M.; Saja, A.; Thamboo, J.; Haraguchi, M.; Navaratnam, S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures* **2022**, *7*, 67. [CrossRef]
30. The European Parliament and The Council of the European Union. *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*; Publications Office of the European Union: Luxembourg, 2022.
31. 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]
32. Rehak, D.; Senovsky, P.; Slivkova, S. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* **2018**, *6*, 21. [CrossRef]

33. 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. *Resilience: Theory and Applications*; Argonne National Laboratory: Lemont, IL, USA, 2012. [CrossRef]
34. Béné, C.; Wood, R.G.; Newsham, A.; Davies, M. Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes. *IDS Work. Pap.* **2012**, *405*, 1–61. [CrossRef]
35. Petit, F.; Bassett, G.; Black, R.; Buehring, W.; Collins, M.; Dickinson, D.; Fisher, R.; Haffenden, R.; Huttenga, A.; Klett, M.; et al. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*; Argonne National Laboratory: Lemont, IL, USA, 2013.
36. Prior, T. *Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9)*; Eidgenössische Technische Hochschule: Zurich, Switzerland, 2015.
37. 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: Roma, Italy, 2016.
38. Nan, C.; Sansavini, G. A Quantitative Method for Assessing Resilience of Interdependent Infrastructures. *Reliab. Eng. Syst. Saf.* **2017**, *157*, 35–53. [CrossRef]
39. Cai, B.; Xie, M.; Liu, Y.; Liu, Y.; Feng, Q. Availability-Based Engineering Resilience Metric and its Corresponding Evaluation Methodology. *Reliab. Eng. Syst. Saf.* **2018**, *172*, 216–224. [CrossRef]
40. Da Vinci, L. *The Madrid Codices I–II*; Biblioteca Nacional of Madrid: Madrid, Spain, 1505.
41. Jenkin, F. Report on the New Unit of Electrical Resistance Proposed and Issued by the Committee on Electrical Standards Appointed in 1861 by the British Association. *Proc. R. Soc. Lond.* **1865**, *14*, 154–164.
42. Simpson, J.A.; Weiner, E.S.C. *The Oxford English Dictionary*; Clarendon Press: Oxford, UK, 1989.
43. Longstaff, P.H.; Armstrong, N.J.; Perrin, K.; Parker, W.M.; Hidek, M.A. Building Resilient Communities: A Preliminary Framework for Assessment. *Homel. Secur. Aff.* **2010**, *6*, 1–23.
44. Rinaldi, S.; Peerenboom, J.; Kelly, T. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control. Syst.* **2001**, *21*, 11–25. [CrossRef]
45. Federal Office for Civil Protection and Disaster Assistance. *Protecting Critical Infrastructures—Risk and Crisis Management*; Federal Ministry of the Interior: Berlin/Heidelberg, Germany, 2008.
46. *ISO 31000*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
47. *IEC 31010*; Risk Management—Risk Assessment Techniques. International Electrotechnical Commission: Geneva, Switzerland, 2019.
48. Philpott, D. *Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity*, 2nd ed.; Bernan Press: Lanham, MD, USA, 2016.
49. The Ministry of the Interior of the Czech Republic. *Act No. 240/2000 Coll. on Crisis Management and on Amendments of Certain Acts (Crisis Act)*; Government of the Czech Republic: Prague, Czech Republic, 2000.
50. Yang, Z.; Barroca, B.; Weppe, A.; Bony-Dandrieux, A.; Laffréchine, K.; Daclin, N.; November, V.; Omrane, K.; Kamissoko, D.; Benaben, F.; et al. Indicator-Based Resilience Assessment for Critical Infrastructures–A Review. *Saf. Sci.* **2023**, *160*, 106049. [CrossRef]
51. Splichalova, A.; Patrman, D.; Kotalova, N.; Hromada, M. Managerial Decision Making in Indicating a Disruption of Critical Infrastructure Element Resilience. *Adm. Sci.* **2020**, *10*, 75. [CrossRef]
52. Kure, H.I.; Islam, S.; Ghazanfar, M.; Raza, A.; Pasha, M. Asset Criticality and Risk Prediction for an Effective Cybersecurity Risk Management of Cyber-Physical System. *Neural Comput. Appl.* **2022**, *34*, 493–514. [CrossRef]
53. Kostopoulos, D.; Tsoulkas, V.; Leventakis, G.; Drogkaris, P.; Politopoulou, V. Real Time Threat Prediction, Identification and Mitigation for Critical Infrastructure Protection Using Semantics, Event Processing and Sequential Analysis. In *Critical Information Infrastructures Security. CRITIS 2013*; Lecture Notes in Computer Science; Luiijf, E., Hartel, P., Eds.; Springer: Cham, Switzerland, 2013; pp. 133–141. [CrossRef]
54. Stochino, F.; Bedon, C.; Sagaseta, J.; Honfi, D. Robustness and Resilience of Structures under Extreme Loads. *Adv. Civ. Eng.* **2019**, *2019*, 4291703. [CrossRef]
55. Chaturvedi, S.; Vedrtnam, A.; Youssef, M.A.; Palou, M.T.; Barluenga, G.; Kalauni, K. Fire-Resistance Testing Procedures for Construction Elements—A Review. *Fire* **2023**, *6*, 5. [CrossRef]
56. Rasulo, A.; Pelle, A.; Briseghella, B.; Nuti, C. A Resilience-Based Model for the Seismic Assessment of the Functionality of Road Networks Affected by Bridge Damage and Restoration. *Infrastructures* **2021**, *6*, 112. [CrossRef]
57. Bangash, M.Y.H.; Bangash, T. *Explosion-Resistant Buildings: Design, Analysis, and Case Studies*; Springer: Berlin/Heidelberg, Germany, 2006. [CrossRef]
58. 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]
59. Lindenberger, D.; Bruckner, T.; Morrison, R.; Groscurth, H.M.; Kümmel, R. Modernization of Local Energy Systems. *Energy* **2004**, *29*, 245–256. [CrossRef]
60. Garcia, M.L. *Design and Evaluation of Physical Protection Systems*, 2nd ed.; Butterworth-Heinemann: Oxford, UK, 2008. [CrossRef]
61. Saaty, T.L. *The Analytic Hierarchy Process, Planning, Priority Setting, and Resource Allocation*; McGraw-Hill: New York, NY, USA, 1980.
62. Rehak, D.; Slivkova, S.; Pittner, R.; Dvorak, Z. Integral Approach to Assessing the Criticality of Railway Infrastructure Elements. *Int. J. Crit. Infrastruct.* **2020**, *16*, 107–129. [CrossRef]

63. Fekete, A. *Urban Disaster Resilience and Critical Infrastructure*; Julius-Maximilians-Universität Würzburg: Würzburg, Germany, 2018.
64. Rehak, D.; Slivkova, S.; Janeckova, H.; Stuberova, D.; Hromada, M. Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview. *Energies* **2022**, *15*, 5276. [CrossRef]