Article

Not peer-reviewed version

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

David Rehak *, Lucie Flynnova, Martin Hromada, Clemente Fuggini

Posted Date: 5 September 2023

doi: 10.20944/preprints202309.0216.v1

Keywords: Resistance; Physical resistance; Crisis preparedness; Anticipation ability; Security measures; Critical infrastructure resilience

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, Czech Republic; lucie.flynnova@vsb.cz
[2] Faculty of Applied Informatics, Tomas Bata University in Zlin, Czech Republic; hromada@utb.cz
[3] Rina Consulting S.p.A., Italy; clemente.fuggini@rina.org
* Correspondence: david.rehak@vsb.cz; Tel.: +420-597-322-816

Abstract: Technical sectors are an inseparable and elementary part of a critical infrastructure (CI) complex system. The services they provide are essential to the functioning of all the dependent sectors of CI on whose services society depends, especially in areas with high levels of urbanisation. The starting point for effective CI elements protection of is permanent assessing and strengthening their resilience to the negative effects of internal and external threats. Current perceptions of resilience focus primarily on repressive components responsive to incident (i.e., robustness, recoverability, and adaptability), while little attention is paid to preventative components. Therefore, the benefit of the article is to define resistance which could be seen as the CI element ability or characteristic to prevent the occurrence of incidents. Based on that, the article defines 1) the individual factors (variables and parameters) determining the CI resistance and 2) the methodological procedure for infrastructure elements resistance assessment in order to identify weak points and subsequently strengthen them. The essence of the article is defining the starting points for extending the CIERA method by a component strengthening the critical infrastructure resilience in the prevention phase. A practical example of resistance assessment for a selected critical energy infrastructure element is presented at the end of the article.

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

1. Introduction

The term resilience in ecology context was first defined by Holling [1] in 1973 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"*. This formulation was originally proposed for systems which can be characterized as ecological. However, over time, the concept of resilience began to be reflected in other scientific areas as psychology, economy, and sociology. It is therefore logical that resilience has found its application and added value in technically oriented social fields as well.

CI resilience was first defined in 2009 in the Critical Infrastructure Resilience Final Report and Recommendations [2]. Resilience is perceived here 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 this document to determine resilience. Although these components are key determinants of resilience, a closer examination reveals that they only have a responsive character. Their impact on the CI resilience is only apparent at the time of the incident [2]. On this basis, it can be concluded that there is no preventative component in the process of resilience building. This role could be played by resistance which could be understood as the CI ability to prevent the incident occurrence.

 doi:10.20944/preprints202309.0216.v1

The Britannica Dictionary [3] defines resistance as the ability to prevent something from having an effect. The term resistance is used by authors from a number of scientific fields, e.g., in medicine to refer to antibacterial resistance to antibiotics [4,5] or in sociology to refer to a manifestation of social resistance [6,7]. An important area from which the resistance concept is taken and transformed into engineering is the ecology field. Here the term was firstly used in relation with resilience by Sugden [8] in connection with Alpine lake ecosystems. The author defined basic logical differences between resistance and resilience to understand resistance as a fact, such as an ecosystem is capable of sustaining a disturbance, such as the introduction of a new genus. Resilience is then a response and recovery measure of the ecosystem after eliminating the source of change.

Over the past decade, the CI resilience issues has been analysed by several authors. Some works deal more generally with the importance of resistance in the context of CI resilience, e.g., [9–13]. Other publications already define preventive factors of resilience and point to the necessity of their separation from robustness, e.g., [14–17]. However, there are also several frameworks that already define and evaluate resistance variables when assessing the level of CI resilience, e.g., [18–20]. From this point of view, resistance can be perceived as an important component of resilience, which should be defined and determined through basic factors.

Based on the above, added value of paper is to define CI resistance and the proposal for its implementation in the CIERA method [21]. The most substantial part of the article also includes the expression of individual the CI resistance factors and the methodological procedure of their assessment with ambition to strengthening the resistance of these infrastructure systems. The paper thus contributes significantly to defining a comprehensive concept of CI system resilience.

2. Materials and Methods

The essence of the article is the effort to prove the suitability of integrating resistance into resilience. For this reason, it is necessary to first define resilience and its meaning in the CI system. Meaning of the word resilience is of Latin origin and means *resiliere* which is literally bounce back [22]. In the context of CI, resilience was first defined in 2009 [2], whereas this definition has been already expanded, in 2012 by the US National Academies of Science, to include preparation and planning: *"the system's ability to prepare and plan for, absorb, recover from, and successfully adapt to disruptive events"* [23].

In the last decade, there has been essentially no change in the perception of CI resilience. This fact is illustrated by the definitions of CI resilience published in several important publications [12,24–30]. All the definitions summarised in these documents are oriented towards so-called technical resilience which refers to the critical infrastructure elements (CIE) and is expressed by their absorption capacity and their ability to recover and adapt to incidents that have occurred.

A slight shift in the understanding of CI system resilience occurred in 2022, when the European Union issued a Directive that focuses on the critical entities resilience [31]. Resilience in this context is seen as *"a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident"*. From this definition, it is evident that it is primarily about organisational resilience, whose main framework is to increase the entities resilience that are responsible for these CIEs [32]. For this reason, the following text continues to focus on CIE technical resilience.

Based on the summary of the conclusions from the definitions presented in the previous text, it can be stated that CI resilience is defined by four phases which together form the so-called CI resilience cycle [33]. The essence of this cycle is the ever-increasing CIEs protection. Resilience is strengthened especially in the phase of adaptation to an incident that has occurred. However, in some cases, the strengthening of resilience can already be noticed in the recovery phase, for example by installing a completely new, more resilient technology.

The initial phase of the CI resilience cycle is prevention. The importance of prevention is preventing the incident occurrence as a result of the threat impact on a CIE. These are measures aimed at early detection of an incident and the element's preparedness for its impact. When an incident

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

occurs, resilience moves into the absorption phase. The essence of this phase is to absorb the incident effects on the CIE. The element ability to absorb the incident effects is referred to as robustness.

After the incident ends, resilience moves into recovery phase. The essence of this phase is to remove the consequences of the incident impact on the CIE and restore its performance to its initial level. The final stage of the CI resilience cycle is adaptation. The importance of this phase is CIE adaptation to the incident that took place and thereby strengthen the overall resilience of this element.

As noted in the introduction to this paper, CI resilience is currently determined by three components, but these components characterise only three of the above phases. Specifically, these are the following components 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 components has been carried out in the past by a number of reputable authors [33–40]. Based on a detailed analysis of these publications, there were defined variables determining individual the CIE resilience components (see Figure 1), as part of the creation of the CIERA method [21].

Components	Variables	Description
Robustness	Detection capability	Probability and/or time of detection of a disruptive event.
	Responsiveness	The probability and/or time of intervention leading to the elimination of the causes of a disruptive event or the minimisation of its consequences.
	Redundancy	The ability to immediately substitute the performance of a disturbed part of an element or to enhance its capabilities.
Recoverability	Material resources	Availability of the necessary components to repair or replace damaged or destroyed parts of the element.
	Financial resources	Availability of financial resources, or reserves, to finance the rapid restoration of the element.
	Human resources	Availability of people with the necessary qualifications.
	Recovery processes	Processes that support rapid recovery of the required element performance.
Adaptability	Risk management	Processes to support early risk assessment and management, including the specification of disruptive event scenarios.
	Innovation processes	Processes that support invention, science and research and the implementation of security measures.
	Educational and development processes	Processes that support the knowledge, skills and attitudes of critical infrastructure entity employees.

Figure 1. Variables determining CIE resilience components [21].

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

3. Results

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

The term resistance was first defined by Georg Ohm in 1827 in relation with 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 come to the fore in other scientific fields, such as medicine

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

(e.g., antibiotic or antimicrobial resistance, immune resistance, psychological resistance), ecology (e.g., ecological or environmental resistance, pesticide resistance) or economy (e.g., resistance economy).

In context of CI, the term resistance has not yet been defined. Some authors consider resistance and resilience as two distinct concepts [43]. They see resistance as being similar to prevent or protect, while resilience is akin to respond or recover. Other authors put the two terms in context but consider resistance as the component of resilience responsible for reducing the severity or consequences of a hazard [34]. In both cases, it can be stated that this interpretation is inaccurate, as resistance in all the above mentioned fields is a factor preventing the emergence of an incident. It is thus a fundamental component of resilience that has clearly preventative but not mitigating character. Based on these facts, the authors of this paper have created a definition where they view resistance as *"the critical infrastructure ability to prevent the occurrence of an incident"*.

Based on the above, it is therefore possible to define resistance in the CI resilience context. It is clear from the previous text that resistance must 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 with regards to an incident are presented in Figure 2.

Phase of resilience	Components of resilience	Definition of components
Prevention	Resistance	The ability of a critical infrastructure element to prevent the occurrence of a disruptive event.
Absorption	Robustness	The ability of a critical infrastructure element to absorb the impact of a disruptive event that has already occurred.
Recovery	Recoverability	The ability of a critical infrastructure element to restore its operation to its original (desired) level of service after the effects of a disruptive event have ceased.
Adaptation	Adaptability	The ability of a critical infrastructure entity to prepare the element for re-exposure to a disruptive event that has already occurred.

Figure 2. Resistance perceptions in relation with CI resilience.

In the following part of the article and with reference to Figure 1, it is possible to define the variables determining the CIEs resistance (see Figure 3). It is clear from the above definition of resistance that the essence of these variables must be their ability to prevent incidents. For this reason, all these variables must be of a preventative character.

Components	Variables	Description
Resistance	Crisis preparedness	A set of analytical-planning documents to increase the element's preparedness for disruptive events and the implementation of related security measures.
	Anticipation ability	Ability to predict the possible occurrence of disruptive events.
	Physical resistance	Ability to withstand the negative effects of natural and man-made disasters.
	Security measures	A set of technical and organizational measures for both monitoring and physical protection of elements.

Figure 3. Defining variables determining the CIEs resistance.

The default variable is crisis preparedness. The essence of crisis preparedness is to increase the CI entities readiness of against threats. This preparedness consists in a thorough assessment of risks and the subsequent processing of security planning documentation. Risk assessment is a systematic

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

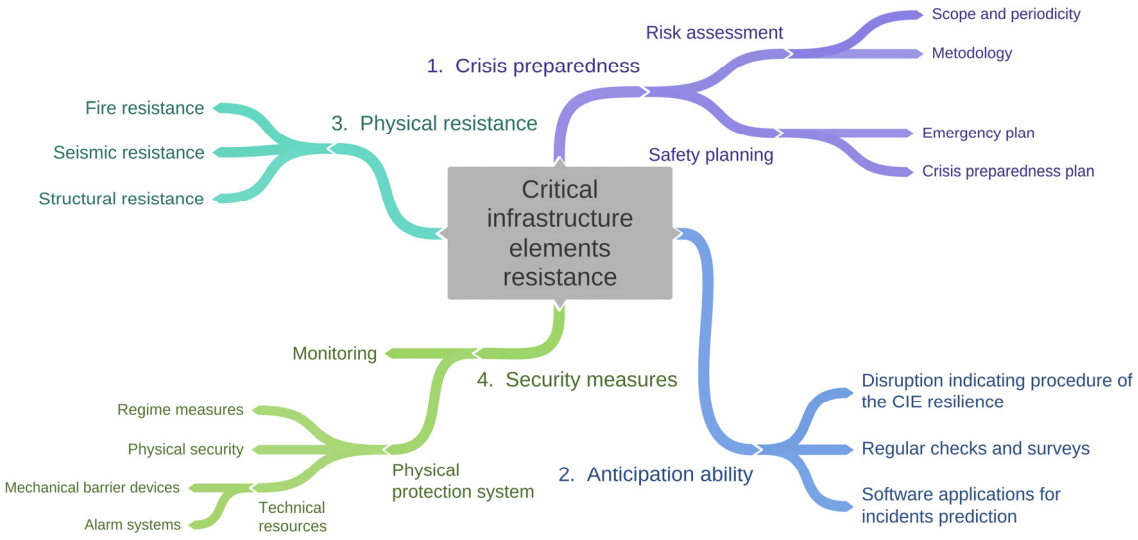
and effective way of identifying, analysing, and evaluating risks and determining the most effective costs and means to minimize these risks [44]. For this purpose, it is advisable to use the recommended risk assessment techniques [45]. Security planning documentation includes especially emergency plans and a CI entity's crisis preparedness plan [46]. 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. The crisis preparedness plan serves CI entities to ensure their own functioning in crisis situations.

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 CIEs [34]. For this purpose, the disruption indicating procedure of the CIE resilience [47] can be used, which assess the elements resilience level and the possibility of their disruption through indicators. On the basis of the possible element resilience disruption assessment, preventive measures are implemented to prevent the emergence of an incident. Other measures that can be used to predict the emergence of incidents are audits or the use of relevant information support enabling the incidents prediction.

The third variable is physical resistance. The substance of this variable is the CIE ability to resist the effects of natural and man-made threats, through the material and structural resistance of these buildings [48]. The core areas of physical resistance are fire, seismic and explosion resistance. Fire resistance is the ability of building structures to sustain the effects of a fully developed fire, without particularly affecting their load-bearing capacity and stability, integrity and insulating ability. Seismic resistance is the ability of building structures to sustain the effects of earthquakes through sufficient elasticity or ductility. 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.

The last variable is security measures. The essence of these measures is monitoring and physical protection of CIEs. The goal of monitoring is mainly to check the technical condition of the elements, their function and the services provided by them [49]. 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 maintaining the technical state of elements with current trends and technologies [50]. A suitable preventive tool for the CIEs protection is also a physical protection system which is determined by regime, organizational and technical measures [51].

A comprehensive overview of the variables and their parameters describing the CIEs 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 of parameters, and the third level recommends some potentially suitable criteria.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

Figure 4. Variables and their parameters describing the CIEs resistance.

The above defined variables and their parameters can be used in particular to assess the CIEs resistance, e.g., through the assessment mechanism of the semi-quantitative CIERA method [21]. This method is suitable for assessing the elements resilience in technical infrastructures, such as energy, transport, communication and information systems or water management. For this purpose, it is necessary to assess all parameters level 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, similar 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 rth CIE resistance variable [%]; P_s = the sth CIE resistance parameter [points]; w_s = the sth standardised weight of the sth CIE resistance parameter in the interval $\langle 0; 1 \rangle$; t = the number of parameters in the rth variable. The standardised weights of the parameters were determined using the pairwise comparison method [52] and are presented in Table 1.

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

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

The resulting level of CIE resistance is expressed by the weighted average of the individual variables (see Equation (2)):

$$R = \sum_{r=1}^{t} V_r h_r \quad (2)$$

where R = the CIE resistance [%]; V_r = the rth variable of CIE resistance [%]; h_r = the rth standardised weight of the rth 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 [52] and are presented in Table 2.

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

Variables	Standardised weights
Crisis preparedness ($\boldsymbol{V_1}$)	h_1 = 0.2
Anticipation ability ($\boldsymbol{V_2}$)	h_2 = 0.25
Physical resistance ($\boldsymbol{V_3}$)	h_3 = 0.25
Security measures ($\boldsymbol{V_4}$)	h_4 = 0.3
∑	1.00

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

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

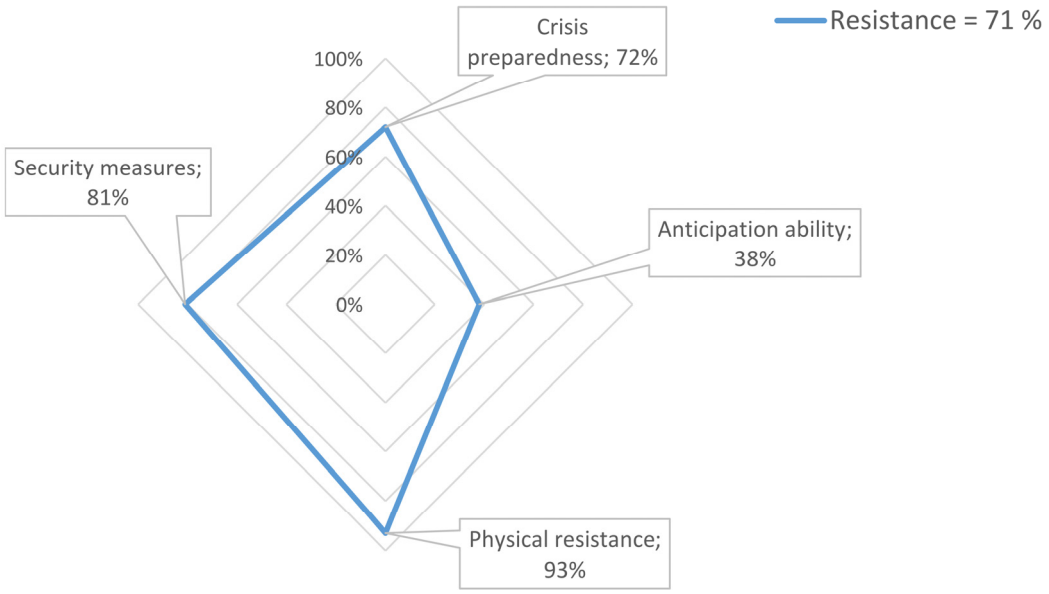


Figure 5. Expression of the CIE resistance level.

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 (see Figure 6) which is based on the CIERA method [21].

Resistance level 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%

Figure 6. Reference scale for assessing the CIE resistance level [21].

The acceptability of resistance is diversified into five rating levels is driven by the desire increase the interest of 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 appropriate to use, for example, resilience strengthening tools for CIEs [53] which would be suitable for implementation to strengthen the resistance of elements through relevant variables. In general, it is possible 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. On the other hand, the tools are focused on external factors (principle of the PESTLE method), considering political, economic, social, legislative, technological, and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

environmental aspects. Tools suitable for strengthening resistance variables are presented in Figure 7.

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 7. Tools suitable for strengthening the CIE resilience variables [53].

4. Practical example of resistance assessment for a selected energy CIE

Finally, it is appropriate to demonstrate the practical applicability of the results obtained in the paper by their application to a selected energy CIE. The selected element is the electrical station of the 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 4 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 8 stations it is 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 3.

Table 3. 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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

In the subsequent section, there is carried out a semi-quantitative assessment of this selected element's resistance to the selected threat. 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 the three steps:

- Step 1: Analysis and scoring of each parameter;
- Step 2: Calculation of the level of each variable;
- Step 3: Determine 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 showed in Table 4.

Table 4. Results of analysis and scoring of individual parameters determining element resistance.

Variables	Parameters	Scoring	Justification
Crisis preparedness ($\boldsymbol{V_1}$)	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 ($\boldsymbol{V_2}$)	Disruption indicating procedure of the 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 one hour.
	Software applications for incidents prediction ($P_{2.3}$)	3	The incidents prediction is realized using basic software applications that do not allow dynamic modelling.
Physical resistance ($\boldsymbol{V_3}$)	Fire resistance ($P_{3.1}$)	4	The element construction can sustain the effects of flame and high temperatures for only 120 minutes.
	Seismic resistance ($P_{3.2}$)	2	The element building structure can sustain only the effects of a weak earthquake (magnitude 4.0–4.9).
	Explosion resistance ($P_{3.3}$)	3	The element building structure has active explosion protection, but passive explosion protection is not sufficient.
Security measures ($\boldsymbol{V_4}$)	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 showed in Table 5.

Table 5. The results of calculating the level of each variable.

Parameters	$\boldsymbol{P_s}$	$\boldsymbol{w_s}$	$\boldsymbol{V_r}$
$\boldsymbol{P_{1.1}}$	3	0.4	72%
$\boldsymbol{P_{1.2}}$	4	0.6	
$\boldsymbol{P_{2.1}}$	3	0.4	54%
$\boldsymbol{P_{2.2}}$	2	0.3	
$\boldsymbol{P_{2.3}}$	3	0.3	
$\boldsymbol{P_{3.1}}$	4	0.4	62%
$\boldsymbol{P_{3.2}}$	2	0.3	
$\boldsymbol{P_{3.3}}$	3	0.3	
$\boldsymbol{P_{4.1}}$	4	0.4	80%
$\boldsymbol{P_{4.2}}$	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 6.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2023 doi:10.20944/preprints202309.0216.v1

Table 6. 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 assessment results presented above, it is possible to state that the element's resistance level achieved is low. For this purpose, it is necessary to determine weak and vulnerable points and 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 important to identify appropriate tools for strengthening the resistance variables (see Table 3) of these parameters. And based on these tools, propose specific security measures at the level of the affected parameters.

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 one hour. 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 or continuous supervision within the given element and the implementation of 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.

From the example presented above, it is clear that the methodical procedure for assessing resistance is particularly suitable for technically oriented infrastructures, such as information and communication technologies or transport structures. For the needs of assessing the of other infrastructures elements resistance, especially of a socio-economic character, it would first be necessary to carry out a review of parameters. These are currently mainly set up to assess the infrastructure objects resistance.

5. Conclusion

Technical sectors are currently essential part in the CI system. The premise that resilience is an important factor having a positive impact on provided services reliability is respected not only to households, but especially to dependent sectors of CI. Disruption to these supplies would result in widespread impacts on the functioning of society as a whole. The elementary starting point for ensuring the security of these supplies is increasing the CIEs resistance. This resistance is defined by the authors of the article as the ability of a CIE to prevent the emergence of an incident. A pragmatic conclusion can therefore be that the CIE resistance is an integral part of resilience, also due to its preventive character.

Considering the original research results, the authors of the paper identified four basic variables that determine the CI resistance. For each variable, the individual parameters and the principle of

their semi-quantitative evaluation were further defined. Subsequently, a methodological procedure for resistance assessment was defined to identify weak points and the subsequent infrastructure elements 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 and verified on selected European energy CIEs.

The main contribution of the 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 the CIEs protection to be extended to include a preventative component. This integration can be practically used e.g., for modification of the CIERA method used for CIEs resilience assessment. Continuing research could be focused on the developing factors determining the infrastructure elements 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.

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

References

1. Holling, C.S. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics* **1973**, *4*, 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245
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 Technology and Biotechnology* **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. *Alternatives: Global, Local, Political* **2017**, *41*, 137-153. https://doi.org/10.1177/0304375417700170
7. Hollander, J.A.; Einwohner, R.L. Conceptualizing Resistance. *Sociological Forum* **2004**, *19*, 533-554. https://doi.org/10.1007/s11206-004-0694-5
8. Sugden, A.M. Resistance and Resilience. *Science* **2001**, *293*, 1731. https://doi.org/10.1126/science.293.5536.1731b
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.; Quinn, A.D. Resistance and Resilience—Paradigms for Critical Local Infrastructure. *Municipal Engineer* **2012**, *165*, 73-83. https://doi.org/10.1680/muen.11.00030
10. Dvorak, Z.; Sventekova, E. Evaluation of the Resistance Critical Infrastructure in Slovak RepublicIn Proceedings of the 2nd International Symposium Engineering Management and Competitiveness 2012 (EMC 2012), Zrenjanin, Serbia, 22-23 June 2012; pp. 17-22.
11. Lovecek, T.; Rehak, D.; Siser, A.; Hromada, M. Resistance of Passive Security Elements as a Quantitative Parameter Influencing the Overall Resistance and Resilience of a Critical Infrastructure Element. In Proceedings of the 10th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), Nice, France, 24-28 July 2016; pp. 200-205.
12. Curt, C.; Tacnet, J.M. Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Analysis* **2018**, *38*, 2441-2458. https://doi.org/10.1111/risa.13166

13. 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. https://doi.org/10.1007/978-3-030-94774-3_41
14. Jovanović, A.; Klimek, P.; Renn, O.; Schneider, R.; Øien, K.; Brown, J.; DiGennaro, M.; Liu, Y.; Pfau, V.; Jelić, M.; Rosen, T.; Caillard, B.; Chakravarty, S.; Chhantyal, P. Assessing Resilience of Healthcare Infrastructure Exposed to COVID-19: Emerging Risks, Resilience Indicators, Interdependencies and International Standards. *Environment Systems and Decisions* **2020**, *40*, 1–35. https://doi.org/10.1007/s10669-020-09779-8
15. Braun, M.; Hachmann, C.; Haack, J. Blackouts, Restoration, and Islanding: A System Resilience Perspective. *IEEE Power and Energy Magazine* **2020**, *18*, 54–63. https://doi.org/10.1109/MPE.2020.2986659
16. Häring, I.; Sansavini, G.; Bellini, E.; Martyn, N.; Kovalenko, T.; Kitsak, M.; Vogelbacher, G.; Ross, K.; Bergerhausen, U.; Barker, K.; Linkov, I. 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, Netherlands, 2017; pp. 21–80. https://doi.org/10.1007/978-94-024-1123-2_2
17. Fischer, K.; Hiermaier, S.; Riedel, W.; Häring, I. Morphology Dependent Assessment of Resilience for Urban Areas. *Sustainability* **2018**, *10*, 1800. https://doi.org/10.3390/su10061800
18. Labaka, L.; Hernantes, J.; Sarriegi, J.M. A Holistic Framework for Building Critical Infrastructure Resilience. *Technological Forecasting and Social Change* **2016**, *103*, 21-33. https://doi.org/10.1016/j.techfore.2015.11.005
19. Lomba-Fernández, C.; Hernantes, J.; Labaka, L. Guide for Climate-Resilient Cities: An Urban Critical Infrastructures Approach. *Sustainability* **2019**, *11*, 4727. https://doi.org/10.3390/su11174727
20. 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? *Technological Forecasting and Social Change* **2017**, *121*, 39-49. https://doi.org/10.1016/j.techfore.2017.01.020
21. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection* **2019**, *25*, 125-138. https://doi.org/10.1016/j.ijcip.2019.03.003
22. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A Review of Definitions and Measures of System Resilience. *Reliability Engineering & System Safety* **2016**, *145*, 47-61. https://doi.org/10.1016/j.ress.2015.08.006
23. US National Academies of Science. *Disaster Resilience: A National Imperative*; National Academies Press: Washington, DC, USA, 2012.
24. Wiseman, E.; McLaughlin, T. *Critical Infrastructure Protection and Resilience Literature Survey: State of the Art*; National Research Council of Canada: Ottawa, Ontario, Canada, 2014.
25. 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. https://doi.org/10.1007/978-3-319-51043-9_1
26. 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, United Kingdom, 2017; pp. 117-135. https://doi.org/10.1057/978-1-137-53675-4_7
27. Biskupovic, S. *Critical Infrastructure Resilience: Findings from a Systematic Review*; University of Waterloo: Waterloo, Ontario, Canada, 2021.
28. Cantelmi, R.; Di Gravio, G.; Patriarca, R. Reviewing Qualitative Research Approaches in the Context of Critical Infrastructure Resilience. *Environment Systems and Decisions* **2021**, *41*, 341-376. https://doi.org/10.1007/s10669-020-09795-8
29. Hromada, M.; Rehak, D.; Lukas, L. Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security. *Energies* **2021**, *14*, 1624. https://doi.org/10.3390/en14061624
30. 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. https://doi.org/10.3390/infrastructures7050067
31. 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.

32. Brown, C.; Seville, E.; Vargo, J. Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection* **2017**, *18*, 37-49. https://doi.org/10.1016/j.ijcip.2017.05.002
33. Rehak, D.; Senovsky, P.; Slivkova, S. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* **2018**, *6*, 21. https://doi.org/10.3390/systems6020021
34. 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. https://doi.org/10.2172/1044521
35. 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 Working Papers* **2012**, *405*, 1-61. https://doi.org/10.1111/j.2040-0209.2012.00405.x
36. Petit, F.; Bassett, G.; Black, R.; Buehring, W.; Collins, M.; Dickinson, D.; Fisher, R.; Haffenden, R.; Huttenga, A.; Klett, M.; Phillips, J.; Thomas, M.; Veselka, S.; Wallace, K.; Whitfield, R.; Peerenboom, J. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*; Argonne National Laboratory: Lemont, IL, USA, 2013.
37. Prior, T. *Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9)*; Eidgenössische Technische Hochschule: Zurich, Switzerland, 2015.
38. 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.
39. Nan, C.; Sansavini, G. A Quantitative Method for Assessing Resilience of Interdependent Infrastructures. *Reliability Engineering & System Safety* **2017**, *157*, 35-53. https://doi.org/10.1016/j.ress.2016.08.013
40. Cai, B.; Xie, M.; Liu, Y.; Liu, Y.; Feng, Q. Availability-Based Engineering Resilience Metric and its Corresponding Evaluation Methodology. *Reliability Engineering & System Safety* **2018**, *172*, 216-224. https://doi.org/10.1016/j.ress.2017.12.021
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. *Proceedings of the Royal Society of London* **1865**, *14*, 154-164.
42. Simpson, J.A.; Weiner, E.S.C. *The Oxford English Dictionary*; Clarendon Press: Oxford, United Kingdom, 1989.
43. Longstaff, P.H.; Armstrong, N.J.; Perrin, K.; Parker, W.M.; Hidek, M.A. Building Resilient Communities: A Preliminary Framework for Assessment. *Homeland Security Affairs* **2010**, *6*, 1-23.
44. ISO 31000. *Risk management—Guidelines*; International Organization for Standardization: Geneva, Switzerland, 2018.
45. IEC 31010. *Risk management—Risk assessment techniques*; International Electrotechnical Commission: Geneva, Switzerland, 2019.
46. Philpott, D. *Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity*, 2nd edition; Bernan Press: Lanham, MD, USA, 2016.
47. Splichalova, A.; Patrman, D.; Kotalova, N.; Hromada, M. Managerial Decision Making in Indicating a Disruption of Critical Infrastructure Element Resilience. *Administrative Sciences* **2020**, *10*, 75. https://doi.org/10.3390/admsci10030075
48. Hromada, M.; Lukas, L. The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation. In Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12-14 November 2013; pp. 589-594. https://doi.org/10.1109/THS.2013.6699070
49. 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 Annals* **2013**, *62*, 127-130. https://doi.org/10.1016/j.cirp.2013.03.130
50. Lindenberger, D.; Bruckner, T.; Morrison, R.; Groscurth, H.M.; Kümmel, R. Modernization of Local Energy Systems. *Energy* **2004**, *29*, 245-256. https://doi.org/10.1016/S0360-5442(03)00063-X
51. Kampova, K.; Lovecek, T.; Rehak, D. Quantitative Approach to Physical Protection Systems Assessment of Critical Infrastructure Elements: Use Case in the Slovak Republic. *International Journal of Critical Infrastructure Protection* **2020**, *30*, 100376. https://doi.org/10.1016/j.ijcip.2020.100376

52. Saaty, T.L. *The Analytic Hierarchy Process, Planning, Priority Setting, and Resource Allocation*; McGraw-Hill: New York, NY, USA, 1980.
53. 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