Article

Managerial Decision Making in Indicating a Disruption of Critical Infrastructure Element Resilience

Alena Splichalova [1,*] **, David Patrman** [1,*] **, Nikol Kotalova** [1] **and Martin Hromada** [2]

[1] Faculty of Safety Engineering, VSB—Technical University of Ostrava, 700 30 Ostrava, Czech Republic; nikol.kotalova@vsb.cz

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

* Correspondence: alena.splichalova@vsb.cz (A.S.); david.patrman@vsb.cz (D.P.)

Abstract: Managerial decision making is an integral process used in public and private organizations. Critical infrastructure entities are a strategically significant group dependent on the quality of decision-making processes. They aim to provide services necessary to ensure state security and to satisfy basic human needs. The quality of decision making is an important factor in the management of these entities. The quality level is determined by many factors, the key of which is risk management. For this reason, it is necessary for the operators to minimize risks affecting the elements of the critical infrastructure through which these services are provided. Risk management is commonly used for this purpose, making it possible to assess and manage these risks. However, there is a specific group of threats that affects the resilience of these elements. The indication of these threats is not possible through common risk management. Therefore, it is necessary to develop specific scenarios of negative impacts and procedures for assessing their impact on the resilience of elements of the critical infrastructure. To this end, this conceptual article introduces an entirely new managerial decision-making process for indicating the resilience of critical infrastructure elements.

Keywords: managerial process; decision making; critical infrastructure elements; resilience; disruption; indication

1. Introduction

As infrastructures are crucial for the functioning of the state and are irreplaceable or difficult to replace, they are referred to as systems of critical infrastructure. Currently, systems of critical infrastructure are being widely discussed due to growing threats. In terms of maintaining the operability and continuity of this system, it is important to focus on their protection. Therefore, it is necessary to create measures which secure the functionality, the continuity of operation and also such measures which minimize the risks of disrupting the function of individual infrastructures (Rehak et al. 2019; Ristvej et al. 2013).

Infrastructures that are highly interconnected with dependent systems are considered especially important. The disruption or failure of these infrastructures would have far-reaching consequences for the security and economy of the state and basic human needs (European Council 2008). This is why it is necessary to especially protect these infrastructures by way of preventive measures in combination with the subsequent strengthening of their resilience towards specific threats. Resilience in the context of critical infrastructure can be perceived as the ability to reduce the magnitude, impact, or duration of a disruption. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event (NIAC 2009). In the context of this

definition, the disruption of resilience can be understood as a degradation in the above-mentioned capabilities of critical infrastructure.

Managerial decision making plays an important role in the protection of critical infrastructure from the very beginning of solving the problem (Zimmerman 2004). Management is an integral part of economic, social and also technical solutions that help increase the resilience of critical infrastructure (Imani et al. 2020). The current critical infrastructure elements are managed by both the public and private sectors. As a result, the decision-making processes of public and private managers are also different (Nutt 2005). For this reason, the problem is focused only on managers of public operators of critical infrastructure (Bozeman and Pandey 2004), with whom the authors have been cooperating for a long time.

Risk management (ISO 2018) is commonly used for critical infrastructure element protection, making it possible to assess and manage these risks. This complex methodological overview was created as part of the publication Risk Assessment Methodologies for Critical Infrastructure Protection-Part I: A State of the Art (Giannopoulos et al. 2012) and Part II: A New Approach (Theocharidou and Giannopoulos 2015). The presented risk assessment methods are an effective preventive tool of a general nature, as they allow early identification of the risk, thus preventing the occurrence of adverse events (ISO 2018). However, these methods lack a link to the specifics related to resilience in a critical infrastructure system. By linking risk management and strengthening resilience, the protection of critical infrastructure is extended by the repressive part, i.e., the response to already-occurring adverse events (NIAC 2009).

For this reason, in recent years, particular attention has been paid to research into methods for assessing and strengthening critical infrastructure resilience, as resilience goes beyond traditional risk management (Petersen et al. 2020). This fact is evidenced, in particular, by articles dealing with resilience in the context of entire cities or urban areas (Chen et al. 2020; Li et al. 2020; Lu et al. 2020; Rehak et al. 2019) of their transport systems (Argyroudis et al. 2020; Machado-León and Goodchild 2017; Dvorak et al. 2017) or individual urban networks (Alizadeh and Sharifi 2020; Liu and Song 2020; Quitana et al. 2020; Shandiz et al. 2020). These approaches are realistically applicable and contribute to strengthening the resilience of critical infrastructure, but do not allow for the early indication of resilience disruption.

It can therefore be stated that there is currently no appropriate managerial tool that would explicitly deal with preventive measures for the protection of critical infrastructure elements. For this reason, the authors of this article have designed an entirely new process of managerial decision making for indicating a disruption in the resilience of critical infrastructure elements, which allows for the early identification of a potential disruption of the resilience of these elements. The added value of this proposal can be seen on two levels. At a theoretical level, it is an interdisciplinary integration of managerial decision making in the field of preventive protection of critical infrastructure elements. At a practical level, it is a matter of creating a new tool that will enable security managers to increase the preventive protection of critical infrastructure elements.

In conclusion, it is necessary to note that the presented article has the character of a conceptual document, which brings a possible solution forming the basic building blocks of the issue. This is a methodological procedure suitable for managerial decision making, the aim of which is to proactively increase the protection of critical infrastructure. Based on this fact, the authors defined the following research question: "Is it possible to preventively indicate a potential disruption of the critical infrastructure elements' resilience before the actual occurrence of the adverse event?"

Based on the above, the article is designed into four consecutive sections. The first section presents the critical infrastructure system and its resilience in the context of threats and the occurrence of adverse events that disrupt this resilience. Subsequently, attention is paid to the application of managerial decision making in the critical infrastructure system. The main part of the article is the third section, which presents the created process for indicating the disruption of the resilience of critical infrastructure elements. The last section then demonstrates the practical use of this process in the form of a case study.

2. Perception of Critical Infrastructure and Its Resilience

Critical infrastructure (CI) means an asset, system or part thereof located within Member States that is essential for the maintenance of vital societal functions and the health, safety, security, economic or social wellbeing of people, the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions (European Council 2008). Critical infrastructure entities are understood to be owners/operators of CI elements responsible for investments in, and/or day-to-day operation of, a particular asset, system or part (European Council 2008).

The elements of critical infrastructure are, in particular, the buildings, facilities, resources or public infrastructure, which are designated according to cross-cutting and sectoral criteria.

2.1. Critical Infrastructure System

The purpose of the critical infrastructure system is to protect the critical infrastructure elements and to ensure the continuity of their operation, i.e., the provision of critically important services. To this end, an infrastructure element protection management process was created (see Figure 1), which shows the principles of the continual management cycle, e.g., the Plan–Do–Check–Act Cycle—PDCA (Tague 2005)—adapted to the conditions of the critical infrastructure system.
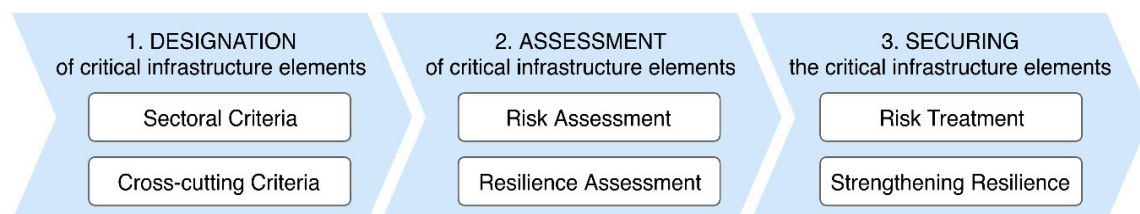

Figure 1. Critical infrastructure element protection management process (Rehak et al. 2018a).

The first sub-process of protection management is the designation of critical infrastructure elements. This sub-process consists of correctly setting criteria for the identification of elements on the European, national, but also regional level. Within this process phase, it is also necessary to consider the suitability of the corresponding method for the identification of elements, which can be based on either the top-down or bottom-up principle (Twidale and Floyd 2008).

The second sub-process of protection management consists of the assessment of critical infrastructure elements. This sub-process consists of the risk assessment of relevant disruptive events (ISO 2018; IEC 2019; Bernatik et al. 2013) and the resilience assessment of an element of interest, its robustness, recoverability and adaptability (NIAC 2009).

The securing of critical infrastructure elements is the last sub-process in protection management and consists of managing risks and strengthening resilience. Risk management consists of the selection and implementation of one or more options in order to minimize risks, i.e., risk retention, risk transfer, risk reduction and/or risk avoidance (see e.g., ISO/IEC 2013). Strengthening resilience (e.g., Government of Canada 2014; Labaka et al. 2015) minimizes the vulnerability of subsystems, which in turn minimizes the occurrence, intensity and spread of failures and their impact on the critical infrastructure system and on society.

2.2. Resilience in a Critical Infrastructure System

The protection of critical infrastructure elements from the impacts of disruptive events is achieved through resilience. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive event (NIAC 2009).

Resilience in a critical infrastructure system that must necessarily be understood as a cyclical process of continual improvement of the prevention, absorption, recovery and adaptation of the system. Figure 2 presents a cycle showing the strengthening of resilience from the original level (i.e., the black

dashed line) to a new level (i.e., the red dashed line). The difference between these levels Δ is the degree of resilience strengthening.
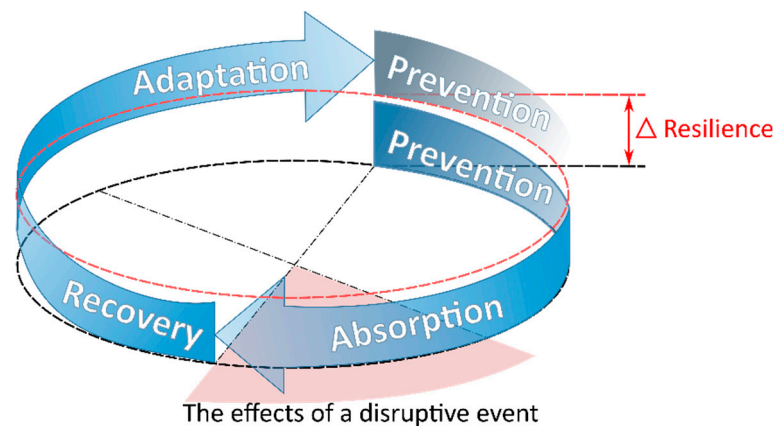

Figure 2. Critical Infrastructure Resilience Cycle (Rehak et al. 2018a).

In reference to the above, it can be noted that the resilience of critical infrastructure elements is determined by four components, which are resistance, robustness, recoverability and adaptability (NIAC 2009). Resistance is the ability of an element to protect itself from the occurrence of a disruptive event, i.e., prevention (Sugden 2001). Robustness is the ability of an element to absorb the impacts of a disruptive event without experiencing fluctuations in the provision of services, i.e., absorption (Stochino et al. 2019). Recoverability is the ability of an element to recover its activity to its original state or required operation level, i.e., recovery (Slivkova et al. 2017). Adaptability is the ability of an organization to adapt its element to the recurrence of an already occurred disruptive event-to learn from the past addressed disruptive events, i.e., adaptation (Denyer 2017). These components are further determined by individual variables, which are presented in Table 1.

Table 1. Components and variables determining the resilience of critical infrastructure elements (adjusted according to Rehak et al. 2018a).

Areas	Technical Resilience			Organizational Resilience
Components	Resistance	Robustness	Recoverability	Adaptability
Variables	Crisis preparedness Physical robustness	Redundancy Detection ability Responsiveness	Material resources Financial resources Human Resources Recovery processes	Risk management Innovation processes Educational and development processes

Resistance, robustness and recoverability are the foundation blocks of the technical resilience of critical infrastructure elements. These three components are determined in each element by three basic factors, which are the technological structure of the element, the element security measures and disruptive events, which are affected by resilience (Rehak et al. 2019).

Aside from technical resilience, the protection of critical infrastructure elements is also ensured by organizational resilience, which is created uniformly for all elements of the given operating organization (Rehak 2020). The organization's management assesses and strengthens this type of resilience from the prevention phase onward, and uses previous experience from dealing with elimination and recovery work processes to adjust the level of internal processes that are necessary in the critical infrastructure element adaptation phase.

2.3. Disruption of Resilience of Critical Infrastructure Elements

The technical organizational level of resilience of critical infrastructure elements can be disrupted by the impact of a disruptive event. Disruptive events are the harmful effects of forces and phenomena

caused by human activity and natural events, but also technical accidents that can endanger an element of the critical infrastructure. Within the context of the critical infrastructure, these disruptive events are caused by the negative impacts of threats, which can be classified into six basic categories (see Table 2).

Table 2. Classification of categories of threats to critical infrastructure elements (Rehak et al. 2019).

	Naturogenic	Technogenic	Anthropogenic
Internal threats	-	Technological	Personal
External threats	Geological, Meteorological	Cascading	Cybernetic, Physical

These threats are divided into internal and external, depending on the environment. Further division is then made based on the type of impact, naturogenic, technogenic or anthropogenic. This threat classification is based primarily on the Peril Classification and Hazard Glossary (IRDR 2014). The cascading threats category was added to the existing list due to the possibility of tracking the spread of failures across the critical infrastructure system due to cascading effects (Rinaldi et al. 2001; Rehak et al. 2018b).

During the course of an ongoing threat, the purpose of resilience is to protect the critical infrastructure element from the disruption of its function and to aid it in its recovery and adaptation to this event. During the threat's impact, however, it is being gradually weakened, which may lead to the disruption of the resilience itself. This state occurs mainly in the prevention phase, when the resistance of an element protects it from the occurrence of a disruptive event, and in the absorption phase, when the robustness of an element absorbs the impacts of an ongoing disruptive event.

3. Managerial Decision Making in the Critical Infrastructure System

The same rules for managerial decision making in critical infrastructure entities apply as in other organizations. Managerial decision making is a process which consists of six basic steps, namely setting managerial objectives, searching for alternatives, comparing and evaluating alternatives, the act of choice, implementing decisions and follow-up and control (Harrison 1999; Cifuentes 1972). This process is used for both general and specific activities. The general activities particularly include the decision making associated with the everyday management of the organization, planning or problem-solving. On the other hand, specific activities are those associated with the organization's specific focus.

The critical infrastructure entities' main activity is to provide services necessary for ensuring the security of the state and satisfying basic human needs (European Council 2008). Managerial decision making is implemented primarily in the phase of the identification and determination of critical infrastructure elements and their subsequent protection. For example, in the Czech Republic, critical infrastructure protection falls within the domain of crisis management (Rehak et al. 2016; Bartosikova et al. 2014). The main goal of critical infrastructure element protection is the management of such risks that can cause the disruption or failure of the function of these elements.

Risk management, within critical infrastructure protection, is based on general risk management principles (ISO 2018). The basic activities within risk management are the assessment and management of risks affecting the functioning of the critical infrastructure element (Rehak et al. 2016). Important work is continuously being published about this area, e.g., Risk assessment methodologies for critical infrastructure protection (Giannopoulos et al. 2012; Theocharidou and Giannopoulos 2015), Risk management goals and identification of critical infrastructures (Fekete et al. 2012), Risk management in critical infrastructure—Foundation for its sustainable work (Bialas 2016) and Applying risk management process in critical infrastructure protection (Luskova and Dvorak 2019). These publications focus primarily on the risk management process and the methodology of risk assessment and management.

However, the development of security engineering is accompanied by the identification of new possible approaches to protecting critical infrastructure elements, e.g., in the area of Indication of critical infrastructure resilience failures (Rehak et al. 2017). The disruption of resilience causes the weakening

of the protection of the critical infrastructure elements, due to which they are more vulnerable, leading to the possibility of their disruption or failure of their function. Due to this, the predictive identification process is a very beneficial approach, but has not yet been properly defined. At the same time, it is worth noting that the implementation of risk management in decision-making processes leads to the timely identification of potential risks, which can then be taken into account in individual phases of the decision-making process, especially in finding, comparing and evaluating alternatives to security measures (ISO 2018).

4. The Process of Indicating the Disruption of the Resilience of Critical Infrastructure Elements

The indication process consists of eight interconnected steps (see Figure 3), which provide the assessor with comprehensive instructions for assessing a possible disruption of the resilience of critical infrastructure elements. At the same time, it enables the assessment of the element's current level of resilience to disruptive elements and forms the basis for the decision to implement a security measure, which will make it possible to mitigate the impacts of the disruptive events weakening the resilience of the element. The resilience disruption indication process, among other things, sets the limit of exhaustion of the resilience absorption capacity, i.e., the limit beyond which the function of the element fails or is disrupted.
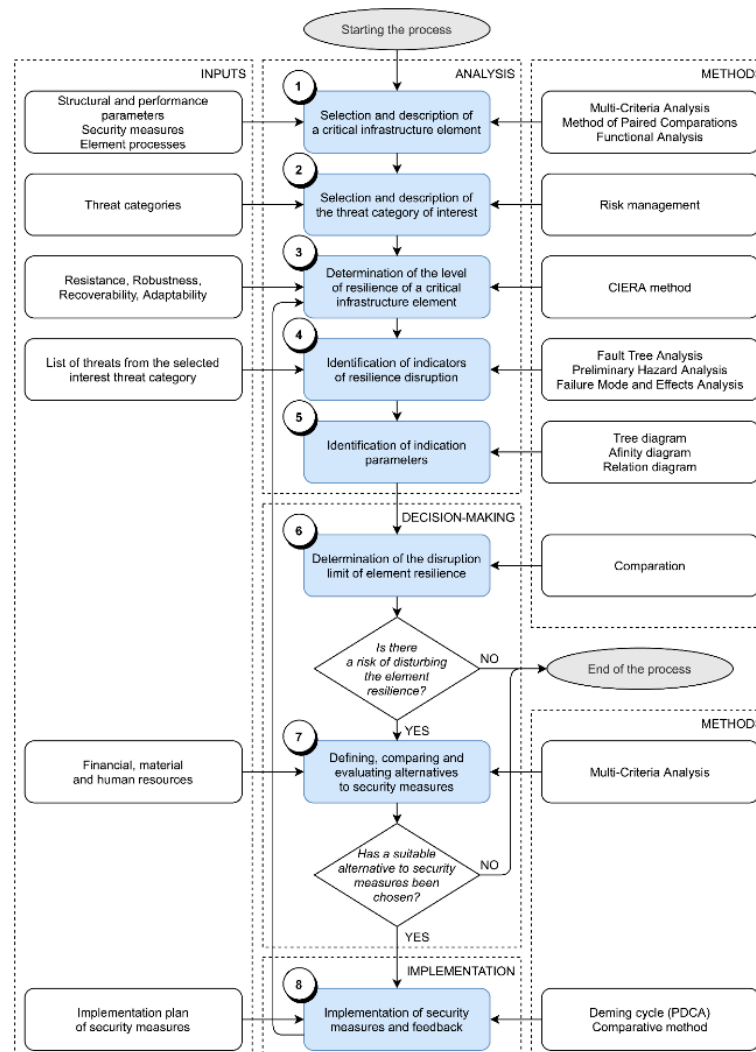

Figure 3. The process of indicating the disruption of the resilience of critical infrastructure elements.

The starting point for the creation of this process was to identify the absence of an approach suitable for indicating the disruption of the critical infrastructure elements' resilience. The current approaches are focused only on the assessing and strengthening of critical infrastructure resilience. Based on this fact, the authors created the process presented below, the essence of which is the analysis of the current state of interest of critical infrastructure and the subsequent introduction of optimal security measures contributing to good governance and cost-effective use of institutional funds. The methodological basis of this process is mainly the managerial and engineering methods presented in Figure 3.

4.1. Step 1: Selection and Description of a Critical Infrastructure Element

The first step of the process of indicating the disruption of the resilience of a critical infrastructure element is selection and subsequent description. The selection of the element is based on the participative decision making of interested parties, i.e., owners and operators of the critical infrastructure. In this step, it is appropriate to use methods which consist in the identification, assessment, assignment of weight and determination of the best possible option out of the selection. For this purpose can be used e.g., Multi-Criteria Analysis (Figueira et al. 2005), Method of Paired Comparations (David 1969) or methods of data mining and machine learning (Zagorecki et al. 2013). These methods take into account the type of element, its strategic significance, substitutability, security or its main vulnerability.

The aim of multi-criteria decision making is to determine one specific critical infrastructure element of the same type, which will be analyzed in detail. To this end, there are decision criteria made, i.e., properties of the element (quantitative or qualitative), according to which the individual or team will assess the element. The portfolio of criteria is based on the preferences of the assessor. Each criterion is assigned a weighting factor which expresses the importance of the individual criteria in comparison to others.

After selecting an element, it is necessary to characterize it, for example, with the help of functional analysis (Kantorovich and Akilov 1982), to provide a comprehensive identification of the element, define and describe its individual functions that are key to the operation of the element. The analysis must be made with regard to the element's ability to absorb the impact of disruptive events. It is important to focus on the selected element's structural and performance parameters, i.e., its topological structure (point, linear or planar element) and key technologies (number and performance of the element's crucial processes and technologies).

4.2. Step 2: Selection and Description of the Threat Category of Interest

The threats which negatively impact the element can be grouped into a number of categories depending on the environment in which they occur and their nature (see Table 2). Within this step, it is necessary to select and then describe the specific threat category. It is appropriate to apply risk management in this selection process (ISO 2018), which will help to identify the threat category to which the examined element is most vulnerable.

4.3. Step 3: Determination of the Level of Resilience of a Critical Infrastructure Element

Determining the level of resilience of a critical infrastructure element is a crucial step in the process. This step provides information about the realistic level of resilience to a specific threat and is the basis for setting security measures. The resulting element resilience level is used as a basis for selecting indicators and setting the limit of the exhaustion of the absorption abilities of resilience.

The level of resilience of the selected element is determined with the help of specific methods (Rehak et al. 2019; Alheib et al. 2016; Bertocchi et al. 2016; Petit et al. 2013). It is appropriate to use the Critical Infrastructure Elements' Resilience Assessment (CIERA) method (Rehak et al. 2019), which provides an overall picture of the element's resilience, its components and variables. This method systematically assesses individual measurable variable items with respect to the threat category. One of the outputs of the CIERA method is data sheets of measurable items which are divided into sections

according to their resilience level. These data sheets can be used as a basis for creating a proposal for measures for strengthening the resilience of the element. The resulting resilience levels are subdivided according to the CIERA methodology (Rehak et al. 2019) into five levels (see Table 3).

Table 3. Comparative table for the assessment of the element's resilience level (Rehak et al. 2019).

Element Resilience Level	Percentage
High level of resilience	85–100%
Acceptable level of resilience	69–84%
Low level of resilience	53–68%
Insufficient level of resilience	37–52%
Critical level of resilience	≤36%

4.4. Step 4: Identification of Indicators of Resilience Disruption

The fourth step of the process is the identification of indicators, i.e., indicators signalizing the disruption of resilience, most likely causing the degradation or failure of the element's key functions. These indicators are the individual security threats that are classified on the basis of Table 2. The threats may be identified using specially designed methods (IEC 2019). Examples of these include Fault Tree Analysis—FTA (IEC 2006a), Preliminary Hazard Analysis—PHA (Ericson 2005), Failure Mode and Effects Analysis—FMEA (IEC 2006b) or a combination thereof.

In the first phase of this step, the FTA method can be used, which finds the possible causes of the degradation of the element's resilience by gradually dividing and analyzing the peak event. Subsequently, it is appropriate to use PHA or FMEA methods, which provide information on the severity or consequences of the threat. Among other things, they provide the possibility of assigning possible measures to individual threats. The assessor will thus have a summary document on security threats.

4.5. Step 5: Identification of Indication Parameters

Indicators must be functional, meet certain conditions and, above all, must provide informative values. So-called indication parameters of individual threats are set to meet these conditions. In the fifth step, in the process of indication of the disruption of an element's resilience, a detailed analysis of individual threats must be performed. Each identified threat has specific properties, such as its character, degree or level of danger, according to which they can be measured, assessed and compared or their level of danger to the element. These values, i.e., indicative threat parameters, are compared with the element's resilience level in Step 6. For example, extreme wind, which falls into the group of meteorological threats, is measured using the Beaufort scale (RMetS 2018). The individual values of this scale determine the indication parameters of this threat. An example of the classification of indication parameters for the threat of "extreme wind" is presented in Table 4.

Table 4. Example of classification of indication parameters for the threat of "extreme wind".

Threat Indication Parameters	Impacts of the Threat on the Critical Infrastructure Element	Percentage Expression of Indication Parameters
Hurricane (118 and more km/h)	Absolute failure of the element's basic functions, high probability of its destruction.	81–100%
Violent Storm (103–117 km/h)	Disruption or failure of basic functions, extensive damage to property, significant disruption of the statics of the element.	61–8%
Storm (89–102 km/h)	Limitations of basic functions, great damage to property, violation of statics of the whole element.	41–60%
Strong Gale (75–88 km/h)	Violation of support functions, damage to property, violation of statics of part of the element.	21–40%
Gale (62–74 km/h)	Element is inaccessible, minor damage to property.	≤20%

The percentage expression of threat indication parameters is organized into five levels based on the impacts of these threats on the critical infrastructure element. While the 0% level of the indication parameter represents no threat to the element, 100% is critical for the element and the failure of the function of the element is assumed with fatal consequences. The example presented above shows that the indication parameters are defined only for those threat levels which can potentially disrupt the function of the critical infrastructure element. For this reason, levels below 62 km/h on Beaufort's scale are not included in the extreme wind indication parameters (RMetS 2018).

Indication parameters can be identified through a graphical–analytical technique known as a Tree Diagram (Salkind 2007). This is a systematic tool which determines detailed information characterizing a threat (e.g., its intensity, danger level, frequency of occurrence) by gradual linear processing. Subsequently, it is possible to set specific values for the indication parameters in the context of the expected impacts with the use of an Affinity Diagram or Relation Diagram (Graham and Cleary 2000).

4.6. Step 6: Determination of the Disruption Limit of Element Resilience

The threat indication parameters themselves can only tell us about threats. Therefore, it is necessary to compare these threat parameters with the corresponding resilience of the element and to set a certain limit. The limit is the maximum threat level that the element's resilience is able to absorb (Rehak et al. 2019). If this limit is exceeded, it is assumed that the element's resilience is disrupted, which may result in the failure of its function. This limit is determined based on a comparison of the already-calculated level of resilience (Step 3) and the indication parameters of the threats (Step 5), i.e., their value, nature, degree or level of danger.

The resulting limit varies depending on the level of resilience of the critical infrastructure element. The higher the element resilience level, the higher this limit is (Rehak et al. 2019). This means that the element is able to withstand a higher impact of a given threat, up to the level of the corresponding relevant indication parameter (Rehak et al. 2018a). For example, an element with an acceptable level of resilience (i.e., 69–84%) is able to withstand the effects of a violent storm (i.e., 61–80%). Exceeding the set limit indicates an insufficient level of resilience and the subsequent disruption or failure of the critical infrastructure element.

4.7. Step 7: Defining, Comparing and Evaluating Alternatives to Security Measures

If there is a risk of disrupting the element's resilience, it is necessary to perform this next step, which is the definition, comparison and evaluation of security measures. The first phase of this step is to clearly define security measures, i.e., define their character (suitability of a measure, acceptability feasibility, does the element have the necessary requirements for implementing the security measure, etc.). Subsequently, it is necessary to compare and evaluate the identified alternatives. The most suitable method for this phase is Multi-Criteria Analysis (Figueira et al. 2005) where, provided with a set of decision criteria and the linkages between them, it is possible to find the option which scores the highest in each criterion (see Figure 4). It is important to set security measures after consulting critical infrastructure operators and other competent persons who have the exclusive decision making right over the entire element. For this purpose, it is appropriate to use the Brainstorming method (Curedale 2013).

Investment Low effect Solution in days (immediately)	Investment Low effect Solutions in weeks	Investment Low effect Solutions in months (years)
Current operating costs Medium effect Solution in days (immediately)	Current operating costs Medium effect Solutions in weeks	Current operating costs Medium effect Solutions in months (years)
Minimum costs (current) High effect Solution in days (immediately)	Minimum costs (current) High effect Solutions in weeks	Minimum costs (current) High effect Solutions in months (years)

Cost and efficiency (vertical axis) — Time (horizontal axis)

Figure 4. Comparison and evaluation of security measures on decision-making criteria (IEC 2005).

The comparison and evaluation of possible alternatives to security measures are carried out on the basis of the three key decision criteria listed in Figure 4. The cells in red represent those measures that are unsuitable to implement due to the excessive financial costs for the critical infrastructure entity and due to the time needed to implement these security measures being disproportionate to their effectivity. The orange cells represent those types of security measures whose effectiveness is acceptable in terms of the time needed for implementation, and the financial costs are comparable with current operational costs. The green cells represent the security measures that can be implemented immediately or within a few days with high effect and minimum costs.

4.8. Step 8: Implementation of Security Measures and Feedback

If a suitable security measure option is chosen, it is possible to continue to the last step of the process of indicating a disruption of resilience. The implementation of measures, i.e., the process of preparation of the implementation of security measures set out in Step 7, will be carried out with the help of a so-called implementation plan (see Figure 5). This plan consists of a set of activities with the aim of effectively and systematically implementing measures in a pre-determined time.
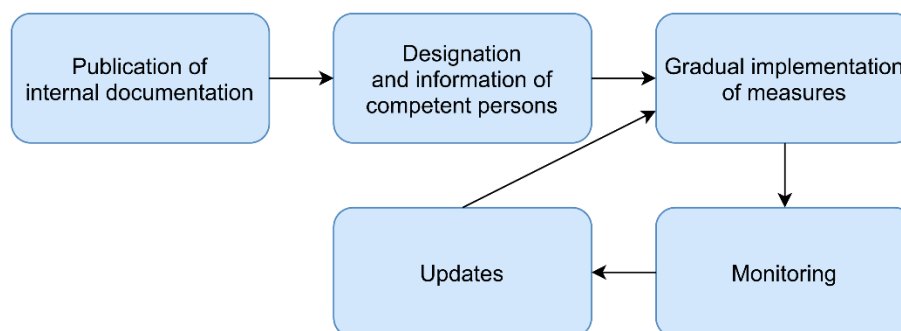

Figure 5. Sub-process of implementation of security measures (Blumenthal and Stoddard 1999).

The first step of the implementation sub-process is the publication of internal documentation (policy, regulation, rule). Then, it is necessary to designate and inform competent persons about the changes which are to be carried out. Then, the implementation of the measure itself can begin. It shall be continuously monitored, and in the event of deficiencies, this step will be adapted to the current conditions (updated). This update step retroactively adjusts the gradual implementation of the measures.

The process of indicating a disruption of a critical infrastructure element is based on the PDCA method (Tague 2005). It is precisely the principle of this method which makes it possible to review the effectiveness of the implemented security measures. Their effectiveness can be evaluated on the basis of an internal audit (Institute of Internal Auditors 2020) of the critical infrastructure element and on a subsequent Comparative Method (Collier 1993), the purpose of which is to compare the

assumed requirements of the security measure with the actual state. The result is a table that provides an overall picture of fulfilled expectations. If these expectations are not fulfilled, this implementation process becomes insufficient. This is why it is suitable to reevaluate the element's resilience level by re-performing Step 3, in which specific deficiencies of the security measures and associated risks can be identified. This step completes the entire process of the indication of the critical infrastructure element's resilience.

5. Case Study

The pilot verification of the proposed process was performed by analyzing the results of case studies that were prepared for the electricity sector (transmission and distribution system), transport (road and railway network) and emergency services (fire stations). The results were then discussed with the operators of the evaluated elements and used to calibrate the method. The anonymized result of one of the evaluations (i.e., fire rescue service station) is presented in the following text to help explain how the proposed process works. This assessment was carried out by the security manager of the Fire and Rescue Service of the territorially relevant region in cooperation with the crisis manager of the same fire and rescue service. The crisis manager then developed recommended solutions, the implementation of which in the final phase of the process was decided by the director of the Fire and Rescue Service of the territorially relevant region.

An anonymized fire rescue service (FRS) station was selected for the process of indicating a disruption of the critical infrastructure element's resilience (Step 1). The station belongs to the emergency service sector and is located in an unnamed region of the Czech Republic. Subsequently, a description of this station was made, which consisted in determining its position in the critical infrastructure structure and the definition of its structural and performance parameters. The structural parameters of this station are specified by its topological structure and in the case of planar elements, by a list of key technologies. The fire station's performance parameter is the number of protected inhabitants (Vichova et al. 2017). These data are presented in Table 5.

Table 5. Description of the assessed element of emergency services of critical infrastructure.

Element Name:	Fire and Rescue Service Station of the Czech Republic
Sector/sub-sector:	Emergency services/integrated rescue system
Topological structure:	Planar element
List of key technologies:	Firefighting means; activation system of firefighting means; information reception dispatch
Number of protected inhabitants:	290 thousand

The indication of resilience disruption of the selected element was carried out as part of the risk management (ISO 2018) against three threat categories (Step 2). However, due to the extent of the results, this article will only present the result of one of the assessed categories of impacts, cascading threats. Cascading threats are threats that cause a disruption of the critical infrastructure element, the effects of which further spread across the critical infrastructure and cause the failure of dependent elements (Rehak et al. 2018b).

Next, the selected critical infrastructure element resilience level was determined (Step 3). The assessment of the fire station's resilience was carried out using the CIERA method (Rehak et al. 2019) and it consisted of the measurement of its levels of robustness, recoverability and adaptability in terms of the selected threat. The assessment of the resilience of this station was done in cooperation with the commander and the security manager of the FRS of the given region. The results of the assessment are presented in Figure 6.
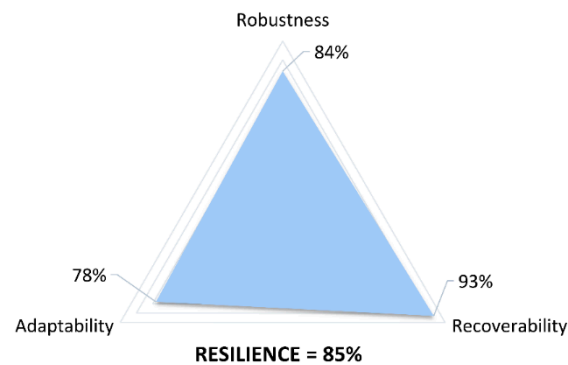
Figure 6. The fire station's level of resilience to the impacts of cascading threats.

The resulting resilience of the fire station to the impact of cascade threats reached the level of 85%, which represents the lower end of high-level resilience.

The next step in indicating a disruption of the resilience of the selected element was the identification of resilience disruption indicators (Step 4). The identification of indicators was carried out using the Fault Tree Analysis method (IEC 2006a) and the results of the identification are presented in Figure 7.
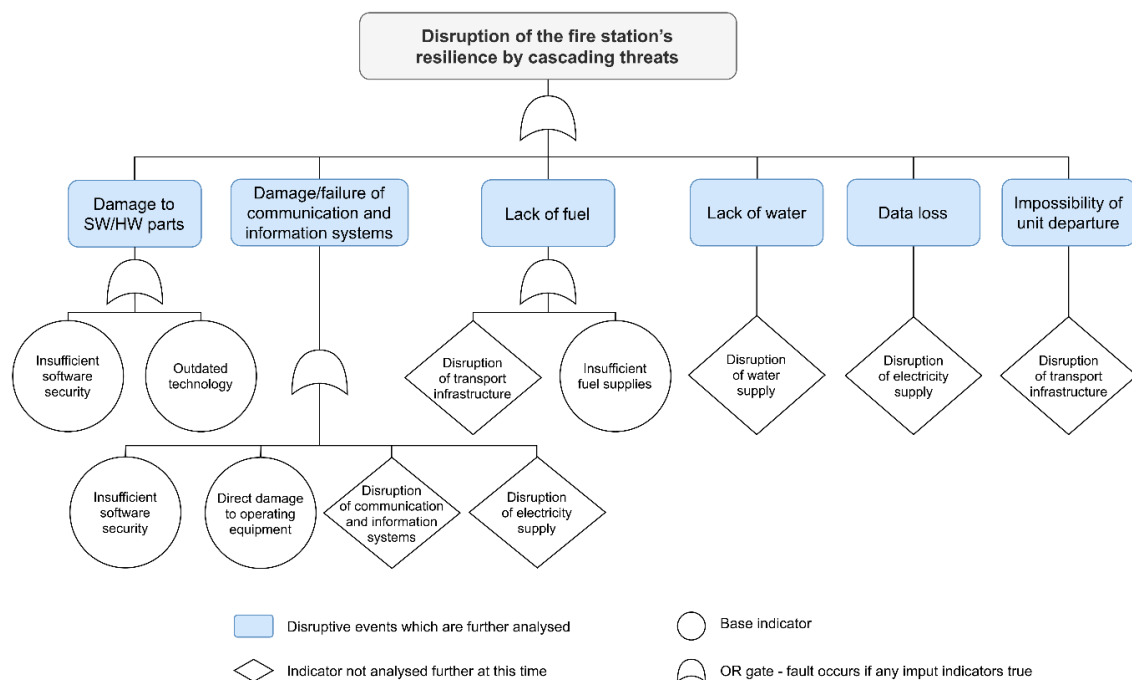

Figure 7. Identification of indicators of disruption of resilience.

The threat of the disruption of the electric energy supply was selected for further analysis based on the results of the identification of the indicators in Figure 7. The reason for this selection is that it was proven that the fire station depends heavily on a supply of electricity. The description of this threat is present in Table 6.

Table 6. Description of the selected threat.

Threat category:	Cascading threats
Threat Name:	Disruption of electricity supply
Threat specification:	Disruption of electricity supply to the fire station

Next, it is possible to proceed to the identification of indication parameters of the selected threat (Step 5). The identification of indication parameters is based on the National Energy Resistance Program of the Czech Republic (MIT 2019) and was performed using graphical–analytical methods, e.g., the Tree Diagram (Salkind 2007). An overview of the indication parameters of the threat of interest is presented in Table 7.

Table 7. Classification of indication parameters for the threat of "disruption of electricity supply".

Threat Indication Parameters	Impacts of the Threat on the Critical Infrastructure Element	Percentage Expression of Indication Parameters
Critical disruption of electricity supply (over 36 h)	Failure of all key technologies	81–100%
Long-term disruption of electricity supply (up to 36 h)	Failure of some key technologies (i.e., firefighting means, firefighting activation system)	61–80%
Medium-term disruption of electricity supply (up to 24 h)	Failure of some non-key technologies (e.g., air conditioning, heating, lighting)	41–60%
Short-term disruption of electricity supply (up to 12 h)	Minor impact on non-key technologies (e.g., air conditioning, heating, lighting)	21–40%
Very short-term disruption of electricity supply (up to 1 h)	No impact on key and non-key technologies.	≤20%

The next step in the process of indicating a disruption of the resilience of critical infrastructure elements is the determination of the limit of disruption of the element's resilience (Step 6). This limit is based on a comparison of the already-calculated level of resilience (Step 3) and the indication parameters of threats (Step 5). In this case, the resilience level of the fire station was set at 85%, which is the lower limit of high-level resilience. In this case, the fire station would be able to operate in a limited mode even in the event of a power failure lasting over 36 h. The reason is mainly its high recoverability level, especially due to redundant capacities. Specifically, the station is equipped with a spare stationary electricity source (i.e., diesel generator) and has spare mobile sources of electricity available and a high area coverage of the Fire and Rescue Service units in the region.

The next step is to define, compare and evaluate alternatives to security measures (Step 7). Weak points in the fire station's resilience were identified using the CIERA method (Rehak et al. 2019). These are the (1) low level of indication of power failure, (2) low physical resilience of technical equipment to the effects of power failure, and (3) lack of funds for security measure innovation. Within the context of these results, it is possible to define adequate security measures and evaluate the suitability of their implementation based on comparison. A Multi-Criteria Analysis (Figueira et al. 2005) was used for this purpose where provided with a set of decision criteria and the linkages between them, it is possible to find the option which scores the highest in each criterion (see Figure 4). Security measures and individual criteria were consulted with the commander of the fire station and the security manager of the FRS of the region. The results of the evaluation of safety measures to increase the physical resistance of technical devices to the effects of power failure (i.e., weakness of resilience No. 2) are presented in Table 8.

Table 8. Evaluation of the suitability of the implementation of security measures to increase the physical resistance of technical means on the impact of power outages.

Security Measure Options	Evaluation Criteria			Evaluation Results
	Financial Costs	Effectiveness	Time Required for Implementation	
Creation of a second replacement stationary source of electricity	Investment	Medium effect	Solution in days	2.
Creating a connection point for a mobile power source	Current operating costs	High effect	Solution in days	1.
Use of renewable electricity sources (e.g., installation of solar panels or wind turbines)	Investment	Low effect	Solution in days	3.

Based on the results of the evaluation, the second option was selected (i.e., the creation of a connection point for a mobile source of electricity), for which the process of implementation and feedback had subsequently been started (Step 8). The implementation process was carried out in accordance with the implementation plan (see Figure 5), which includes a set of activities aimed at the effective and systematic implementation of measures at a pre-determined time. Feedback was provided at the end of the process of indicating the disruption of the resilience of critical infrastructure elements, which allowed us to review the effectiveness of the implemented security measures. For this purpose, the level of resilience of the critical infrastructure element was reassessed (Step 3), reaching the level of 93% after the implementation of the selected security measure. This step finalizes the entire process of indication of the critical infrastructure element's resilience.

6. Discussion and Conclusions

This article offers a contribution to the debate on the need to address the predictive disruption of critical infrastructure elements' resilience. Throughout the work, the authors asked themselves the following question: is the current managerial decision making in the area of the researched problem, i.e., critical infrastructure protection, sufficient? A literature search has shown that in such a specific area as the disruption of critical infrastructure elements' resilience, common decision-making methods are used, lacking a systematic arrangement. For this purpose, a special procedure was created to indicate the violation of the resilience of critical infrastructure elements. The work and the proposed procedure was limited to the area of critical infrastructure in the electricity, transport and emergency services sectors. However, with the elaboration and light transformation, this approach can be used in other areas of critical infrastructure; however, this option is a matter for future research and detailed analysis of other areas.

Risk management is currently being used in most cases of the preventive protection of critical infrastructure elements, making it possible to assess and manage risks (ISO 2018). The current risk assessment methods are an effective general preventive tool (Giannopoulos et al. 2012; Theocharidou and Giannopoulos 2015); however, they lack linkages to the specifics associated with the resilience of the critical infrastructure systems. By linking risk management and strengthening resilience, the protection of critical infrastructure is extended by the repressive part, i.e., the reaction to already occurring adverse events (NIAC 2009). However, current approaches in various areas focus only on assessing and strengthening critical infrastructure resilience (Alizadeh and Sharifi 2020; Argyroudis et al. 2020; Quitana et al. 2020; Li et al. 2020; Shandiz et al. 2020) even though resilience goes beyond traditional risk management (Petersen et al. 2020). Therefore, it can be stated that there is currently no appropriate managerial tool that would explicitly deal with preventive measures for the protection of critical infrastructure elements. For this reason, the authors of this article have designed an entirely new process of managerial decision making for indicating the disruption of the resilience of critical infrastructure elements, which allows for the early identification of a potential resilience disruption of these elements and subsequent setting of the framework for improving the elements' resilience (Labaka et al. 2015).

The indication process consists of eight interconnected steps, which provide the assessor with comprehensive instructions for the indication of a possible disruption of the resilience of critical infrastructure elements. This enables the assessment of the current level of the element's resilience to disruptive events evaluated according to available methods (ISO 2018; IEC 2019; Bernatik et al. 2013) and serves as a basis for the decision to implement security measures and mitigate the impacts of the disruptive events weakening the resilience of the element (Blumenthal and Stoddard 1999). The resilience disruption indication process, among other things, sets the limit of exhaustion of the resilience absorption capacity, i.e., the limit beyond which the function of the element fails or is disrupted.

This information is valuable to security managers of critical infrastructure entities, as it enables them to rapidly indicate disruptions of the resilience of critical infrastructure elements. With this information, managers can make adequate security measures to strengthen the resilience of these elements. The pilot verification of the proposed process was performed by analyzing the results of

case studies, which were prepared for the electricity sector (transmission and distribution system), transport (road and railway network) and emergency services (fire stations). The results were then discussed with the operators of the evaluated elements and used to calibrate the method. Currently, the method can be used for the predictive indication of the resilience of elements of all technical sectors (i.e., energy, transport, information and communication systems and water management) and selected socio-economic sectors (i.e., emergency services and health) of the critical infrastructure.

The process of indicating the disruption of the critical infrastructure elements' resilience was designed from a managerial point of view, so its use in the top management of state institutions is very likely. In particular, it is suitable as a support tool when deciding on investments in strategic public infrastructures and their development. It is also expected that the proposed process will be used in the modernization of public infrastructures to increase their resilience to predicted threats. The proposed process is a comprehensive procedure that supports decision making in the implementation of optimal security measures, and in the context of step seven (i.e., defining, comparing and evaluating alternatives to security measures), contribution to good governance and the economical drawing of institutional funds.

The process of indicating disruption of resilience was created as a support tool for managerial decision making in the critical infrastructure elements protection management. The theoretical benefit of this tool is the interdisciplinary integration of managerial decision making in the field of preventive protection of critical infrastructure elements. This expands the portfolio of the currently available literature dealing with the use of managerial decision making in the field of critical infrastructure protection. At a practical level, it is a matter of creating a new tool that will enable security managers to increase the preventive protection of critical infrastructure elements. This also answers the research question, as the created tool allows us to preventively indicate the potential disruption of the critical infrastructure elements' resilience before the actual occurrence of the adverse event. In the context of practical use, this tool was created primarily for managers of public critical infrastructure operators, with whom the authors have been cooperating for a long time. The tool can also be used in the private sector, but without the possibility of considering the market environment.

The future development of this instrument could therefore not only consider the needs of the private sector, but could also include economic factors to minimize costs. Furthermore, it is appropriate to pay attention to the research of the indicators themselves, which could be structured in more detail, based on functional parameters (i.e., indicators considering structural and performance parameters of critical infrastructure elements) and indication parameters (i.e., indicators of changes in internal but also external environment of critical infrastructure elements).

References

Alheib, M., G. Baker, C. Bouffier, G. Cadete, E. Carreira, P. Gattinesi, F. Guay, D. Honfi, K. Eriksson, K. Lange, and et al. 2016. *Report of Criteria for Evaluating Resilience*. Göteborg: SP Technical Research Institute of Sweden.

Alizadeh, Hadi, and Ayyoob Sharifi. 2020. Assessing Resilience of Urban Critical Infrastructure Networks: A Case Study of Ahvaz, Iran. *Sustainability* 12: 3691. [CrossRef]

Argyroudis, A. Sotirios, Stergios A. Mitoulis, Lorenzo Hofer, Mariano Angelo Zanini, Enrico Tubaldi, and Dan M. Frangopol. 2020. Resilience assessment framework for critical infrastructure in a multi-hazard

environment: Case study on transport assets. *Science of the Total Environment* 714: 136854. [CrossRef] [PubMed]

Bartosikova, Romana, Jana Bilikova, Jan Strohmandl, and Vladimir Sefcik. 2014. Modelling of Decision-making in Crisis Management. Paper presented at the 24th International-Business-Information-Management-Association Conference, Milan, Italy, November 6–7; pp. 1479–83.

Bernatik, Ales, Pavel Senovsky, Michail Senovsky, and David Rehak. 2013. Territorial Risk Analysis and Mapping. *Chemical Engineering Transactions* 31: 79–84. [CrossRef]

Bertocchi, Glauco, Sandro Bologna, Giulio Carducci, Luigi Carrozzi, Simona Cavallini, Alessandro Lazari, Gabriele Oliva, and Alberto Traballesi. 2016. *Guidelines for Critical Infrastructure Resilience Evaluation*. Roma: Italian Association of Critical Infrastructures' Experts.

Bialas, Andrzej. 2016. Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work. *Sustainability* 8: 240. [CrossRef]

Blumenthal, David, and Ray Stoddard. 1999. Implementation Planning: The Critical Step. *PM Network* 13: 80–86.

Bozeman, Barry, and Sanjay K. Pandey. 2004. Public Management Decision Making: Effects of Decision Content. *Public Administration Review* 64: 553–65. [CrossRef]

Cifuentes, Carlos Llano. 1972. Fundamentals of the Managerial Decision-Making Process. *International Studies of Management & Organization* 2: 213–21. [CrossRef]

Collier, David. 1993. The Comparative Method. In *Political Science: The State of the Discipline II*. Washington: American Political Science Association, pp. 105–19.

Curedale, A. Robert. 2013. *50 Brainstorming Methods: For Team and Individual Ideation*. Topanga: Design Community College Inc.

David, H. A. 1969. *Method of Paired Comparisons*, 2nd ed. Port Jervis: Griffin & Company.

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

Dvorak, Zdenek, Eva Sventekova, David Rehak, and Zoran Cekerevac. 2017. Assessment of Critical Infrastructure Elements in Transport. *Procedia Engineering* 187: 548–55. [CrossRef]

Ericson, A. Clifton. 2005. *Hazard Analysis Techniques for System Safety*. Fredericksburg: John & Wiley Sons. [CrossRef]

European Council. 2008. *Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*. Brussels: European Union.

Fekete, Alexander, Peter Lauwe, and Walfram Geier. 2012. Risk Management Goals and Identification of Critical Infrastructures. *International Journal of Critical Infrastructures* 8: 336–53. [CrossRef]

Figueira, Jose, Salvatore Greco, and Matthias Ehrgott. 2005. *Multiple Criteria Decision Analysis: State of the Art Surveys*. New York: Springer. [CrossRef]

Giannopoulos, Giorgios, Roberto Filippini, and Muriel Schimmer. 2012. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A state of the Art*. Ispra: European Commission, Joint Research Centre.

Government of Canada. 2014. *Action Plan for Critical Infrastructure (2014–2017)*; Ottawa: Public Safety Canada.

Graham, D. Jackie, and Michael J. Cleary. 2000. *Practical Tools for Continuous Improvement: Problem-Solving and Planning Tools*. Dayton: PQ Systems, vol. 2.

Harrison, E. Frank. 1999. *The Managerial Decision-Making Process*. Boston, MA: Houghton Mifflin.

Chen, Changkun, Lili Xu, Dongyue Zhao, Tong Xu, and Peng Lei. 2020. A new model for describing the urban resilience considering adaptability, resistance and recovery. *Safety Science* 128: 104756. [CrossRef]

IEC 17799. 2005. *Information Technology—Security Techniques—Code of Practice for Information Security Management*. Geneva: ISO/IEC.

IEC 31010. 2019. *Risk Management—Risk Assessment Techniques*. Geneva: International Organization for Standardization.

IEC 61025. 2006a. *Fault Tree Analysis (FTA)*. Geneva: International Electrotechnical Commission.

IEC 60812. 2006b. *Procedure for Failure Mode and Effects Analysis (FMEA)*. Geneva: International Electrotechnical Commission.

Imani, Maryam, Donya Hajializadeh, and Vasos Christodoulides. 2020. Towards Resilience-Informed Decision-Making in Critical Infrastructure Networks. In *Frontiers in Water-Energy-Nexus—Nature-Based*

Solutions, Advanced Technologies and Best Practices for Environmental Sustainability. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Edited by Naddeo V. M. Balakrishnan and K. H. Choo. Cham: Springer. [CrossRef]

Institute of Internal Auditors. 2020. *What is Internal Audit?* Available online: https://www.iia.org.uk/about-us/what-is-internal-audit/ (accessed on 9 July 2020).

IRDR. 2014. *Peril Classification and Hazard Glossary*. Beijing: Integrated Research on Disaster Risk IPO.

ISO/IEC 27001. 2013. *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. Geneva: International Organization for Standardization.

ISO 31000. 2018. *Risk Management–Guidelines*. Geneva: International Organization for Standardization.

Kantorovich, Leonard V., and G. P. Akilov. 1982. *Functional Analysis*. Amsterdam: Elsevier.

Labaka, Leire, Josune Hernantes, and Jose Mari Sarriegi. 2015. A framework to improve the resilience of critical infrastructures. *International Journal of Disaster Resilience in the Built Environment* 6: 409–23. [CrossRef]

Li, Guijun, Chenhuan Kou, Yongsheng Wang, and Hongtao Yang. 2020. System dynamics modelling for improving urban resilience in Beijing, China. *Resources Conservation and Recycling* 161: 104954. [CrossRef]

Liu, Wei, and Zhaoyang Song. 2020. Review of studies on the resilience of urban critical infrastructure networks. *Reliability Engineering and System Safety* 193: 106617. [CrossRef]

Lu, Xinzheng, Liao Wenkie, Fang Dongping, Lin Kaiqi, Tian Yuan, Zhang Chi, Zheng Zhe, and Zhao Pengju. 2020. Quantification of disaster resilience in civil engineering: A review. *Journal of Safety Science and Resilience* 1: 19–30. [CrossRef]

Luskova, Maria, and Zdenek Dvorak. 2019. Applying Risk Management Process in Critical Infrastructure Protection. *Interdisciplinary Description of Complex Systems* 17: 7–12. [CrossRef]

Machado-León, Jose Luis, and Anne Goodchild. 2017. Review of Performance Metrics for Community-Based Planning for Resilience of the Transportation System. *Transportation Research Record* 2604: 44–53. [CrossRef]

MIT. 2019. *National Energy Resilience Program of the Czech Republic*; Prague: Ministry of Industry and Trade.

NIAC (National Infrastructure Advisory Council). 2009. *Critical Infrastructure Resilience: Final Report and Recommendations*. Washington: U.S. Department of Homeland Security.

Nutt, Paul C. 2005. Comparing Public and Private Sector Decision-Making Practices. *Journal of Public Administration Research and Theory* 16: 289–318. [CrossRef]

Petersen, Laura, David Lange, and M. Theocharidou. 2020. Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. *Reliability Engineering and System Safety* 199: 106872. [CrossRef]

Petit, Frederic, Gilbert Bassett, R. Black, W. Buehring, M. Collins, D. Dickinson, R. Fisher, R. Haffenden, A. Huttenga, M. Klett, and et al. 2013. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Chicago: Argonne National Laboratory.

Quitana, Gabriela, Maria Molinos-Senante, and Alondra Chamorro. 2020. Resilience of critical infrastructure to natural hazards: A review focused on drinking water systems. *International Journal of Disaster Risk Reduction* 48: 101575. [CrossRef]

Rehak, David. 2020. Assessing and Strengthening Organisational Resilience in a Critical Infrastructure System: Case Study of the Slovak Republic. *Safety Science* 123: 104573. [CrossRef]

Rehak, David, Martin Hromada, and Petr Novotny. 2016. European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice. *Chemical Engineering Transactions* 48: 943–48. [CrossRef]

Rehak, David, Martin Hromada, and Jozef Ristvej. 2017. Indication of Critical Infrastructure Resilience Failure. In *Safety and Reliability–Theory and Application (ESREL)*. Edited by M. Čepin and R. Briš. Cleveland: CRC Press, pp. 963–70.

Rehak, David, Pavel Senovsky, Martin Hromada, and T. Lovecek. 2019. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection* 25: 125–38. [CrossRef]

Rehak, David, Pavel Senovsky, and Simona Slivkova. 2018a. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* 6: 21. [CrossRef]

Rehak, David, Pavel Senovsky, Martin Hromada, Tomas Lovecek, and Petr Novotny. 2018b. Cascading Impact Assessment in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection* 22: 125–38. [CrossRef]

Rinaldi, S. M., James P. Peerenboom, and T. K. Kelly. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine* 21: 11–25. [CrossRef]

Ristvej, Jozef, A. Zagorecki, Katarina Holla, Ladislav Simak, and Michal Titko. 2013. Modelling, Simulation and Information Systems as a Tool to Support Decision-Making Process in Crisis Management. Paper presented at the 27th European Simulation and Modelling Conference (ESM 2013), Lancaster, UK, October 23–25; pp. 71–76.

RMetS. 2018. *The Beaufort Scale: How is Wind Speed Measured?* Available online: https://www.rmets.org/resource/beaufort-scale (accessed on 19 June 2020).

Salkind, J. Neil. 2007. *Encyclopedia of Measurement and Statistics*. California: Sage Publications.

Shandiz, Saeid Charani, Greg Foliente, Behzad Rismanchi, Amanda Wachtel, and Robert F. Jeffers. 2020. Resilience framework and metrics for energy master planning of communities. *Energy* 203: 117856. [CrossRef]

Slivkova, Simona, David Rehak, Veronika Nesporova, and Michaela Dopaterova. 2017. Correlation of Core Areas Determining the Resilience of Critical Infrastructure. Paper presented at the 12th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2017). Procedia Engineering, High Tatras, Slovakia, May 31–June 2; vol. 192, pp. 812–17. [CrossRef]

Stochino, Flavio, Chiara Bedon, Juan Sagaseta, and Daniel Honfi. 2019. Robustness and Resilience of Structures under Extreme Loads. *Advances in Civil Engineering* 2019: 4291703. [CrossRef]

Sugden, M. Andrew. 2001. Resistance and Resilience. *Science* 293: 1731. [CrossRef]

Tague, R. Nancy. 2005. *Quality Toolbox*, 2nd ed. Milwaukee: ASQ Quality Press.

Theocharidou, Marianthi, and Georgios Giannopoulos. 2015. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part II: A New Approach*. Ispra: European Commission, Joint Research Centre.

Twidale, B. Michael, and Ingbert R. Floyd. 2008. Infrastructures from the bottom-up and the top-down: Can they meet in the middle? Paper presented at the Tenth Anniversary Conference on Participatory Design (PDC '08), Bloomington, IN, USA, October 1–4; pp. 238–41.

Vichova, Katerina, Martin Hromada, and David Rehak. 2017. The Use of Crisis Management Information Systems in Rescue Operations of Fire and rescue system in the Czech Republic. Paper presented at the 12th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2017). Procedia Engineering, High Tatras, Słowacja, May 31–June 2; vol. 192, pp. 947–52. [CrossRef]

Zagorecki, Adam T., David E. A. Johnson, and Jozef Ristvej. 2013. Data Mining and Machine Learning in the Context of Disaster and Crisis Management. *International Journal of Emergency Management* 9: 351–65. [CrossRef]

Zimmerman, Rae. 2004. Decision-making and the vulnerability of interdependent critical infrastructure. Paper presented at the 2004 IEEE International Conference on Systems, Man and Cybernetics, The Hague, The Netherlands, October 10–13; pp. 4059–63. [CrossRef]