systems

MDPI

Article

Resilience of Critical Infrastructure Elements and Its Main Factors

David Rehak *, Pavel Senovsky and Simona Slivkova

Faculty of Safety Engineering, VSB—Technical University of Ostrava, 700 30 Ostrava, Czech Republic; pavel.senovsky@vsb.cz (P.S.); simona.slivkova@vsb.cz (S.S.)

* Correspondence: david.rehak@vsb.cz; Tel.: +420-597-322-816

Received: 12 April 2018; Accepted: 30 May 2018; Published: 4 June 2018

Abstract: Resilience in a critical infrastructure system can be viewed as a quality that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event. In this context, comprehensive knowledge of the environment and of the main factors whereby resilience is determined, limited, and affected can be said to represent the fundamental precondition for strengthening the resilience of critical infrastructure elements. Based on this idea, the article defines the initial and functional conditions for building and strengthening the resilience of critical infrastructure elements, i.e., the resilience concept in a critical infrastructure system. Subsequently, factors determining the resilience of these elements are identified, both in terms of technical resilience (i.e., robustness and recoverability) and organizational resilience (i.e., adaptability). In the final part of the article, these factors are presented in greater detail in the context of case studies focused on the electricity, gas, information and communications technology, and road transport sectors. Determination of these factors is examined with regard to the intensity of a disruptive event and the performance of the respective critical infrastructure element.

Keywords: critical infrastructure; elements; resilience; determining factors

1. Introduction

Critical infrastructure (CI) represents an intricate and complex system [1] designed to facilitate the permanent provision of services essential to the functioning of society. The uniqueness of this system lies primarily in the required high reliability and availability of services, especially in highly urbanized regions (concentrated utilization). At the same time, this system is composed of extensive systems of infrastructure networks, which are inherently decentralized and extend over vast areas. Individual critical infrastructure subsystems are therefore constantly exposed to the effects of various threats that lead to the occurrence of disruptive events. In turn, these may, depending on their intensity, cause the disruption or even failure of services provided by individual critical infrastructure subsystems.

That is why the issue of critical infrastructure protection, and its relation to the long-term sustainable development of society, has long been the subject of research in a variety of scientific fields. Accordingly, an improved understanding of the linkages between individual CI subsystems [2], as well as between the CI system and society as such, forms the basis for the proposed system of protection of CI and its elements. For this reason, considerable attention is given to the processes and instruments of critical infrastructure protection, while the strengthening of the resilience of these subsystems may be regarded as the initial solution.

The term resilience was first defined by Holling [3] in connection with the resistance and stability of ecological systems (later also socio-ecological systems). Over time, the term began to appear in other scientific fields, including sociology, psychology, and economics. The relatively youngest field, with respect to system resilience research, is engineering. In the context of critical infrastructure,

resilience represents the intrinsic preparedness of subsystems for a disruptive event. It is the ability of these subsystems to perform and maintain their functions when negatively affected by internal and/or external factors. Resilience can thus be perceived as the polar opposite of vulnerability, or, in other words, resilience and vulnerability have an inverse character with respect to each other. Vulnerable subsystems lack resilience and, conversely, resilient subsystems are not particularly vulnerable.

Critical infrastructure resilience was first defined in detail in a document entitled Critical Infrastructure Resilience Final Report and Recommendations [4], although the debate over the need to ensure critical infrastructure protection goes further back in time. The Presidential Decision Directive PDD-63[1] [5] was issued as early as 1998, but it was not until the publication of the Presidential Decision Directive PPD-21 [6] that resilience began to be addressed more extensively in addition to critical infrastructure security.

This article describes the relevant experience gained in implementing the project "RESILIENCE 2015 Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems". The project focuses on the dynamic evaluation of correlation and cascading and synergic effects with respect to major European sectors, namely energy, transport, and information and communications technology. The project is partly based on extensive bibliographic research carried out with a view to identifying methods and indicators that would better describe the level of resilience of critical infrastructure elements [7].

At present, resilience is viewed as the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event [4]. The first comprehensive study defining the components of critical infrastructure resilience was published in 2013 under the title "Resilience Measurement Index" [8]. The study classifies these components into four basic groups, which include Preparedness, Mitigation Measures, Response Capabilities, and Recovery Mechanisms. This classification is not complete, however, in that it fails to reflect on another fundamental component of resilience, which is the adaptability of critical infrastructure subsystems to previous disruptive events. Another major study, looking at indicators for measuring critical infrastructure resilience, was published in 2015 [9], but adaptability is not given due regard here, either. Additional significant studies published in the following years (e.g., references [10,11]) also fail to address the adaptability of critical infrastructure subsystems to adverse events. More recently[2], the EU-VRi (European Virtual Institute for Integrated Risk Management) analysis [12] has identified over 450 potential indicators of resilience as part of the Smart Resilience project, and the study authored by Cai et al. [13] has explored the potential for employing an availability-based engineering resilience metric from the perspective of reliability engineering.

The above-mentioned literary review has demonstrated that, although the general concept of resilience as such is usually shared, notions as to the grouping of individual measurable items and their content vary widely with respect to both the subject being addressed (e.g., the theory of reliability, ecology, management, etc.) and the depth to which the research into the CI (Critical Infrastructure) systems goes (i.e., sectors, subsectors, elements, components). However, these discrepancies should be reconciled for the sake of evaluation.

From the data collected, the broader[3] RESILIENCE 2015 research team selected the three core components of resilience, i.e., robustness and recoverability with regard to technical resilience and

---

1 In 2003, PDD-63 was replaced by HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection, and subsequently, in 2013, this directive was replaced by PPD-21 Critical Infrastructure Security and Resilience.

2 As the studies by Jovanović et al. [12] and Cai et al. [13] were not available at the time of implementing the RESILIENCE 2015 project, they were not taken into account.

3 Institutions involved in the project include Toma Bata University in Zlin/Faculty of Applied Informatics; Centre for Transport Research, public research institution; Ministry of Defence/University of Defence; Technical University of Liberec/Faculty of Mechatronics, Informatics and Interdisciplinary Studies; Technology Platform Energy Security; VSB—Technical University of Ostrava/Faculty of Safety Engineering; and Brno University of Technology/Faculty of Civil Engineering.

adaptability in terms of organizational resilience. Subsequently, variables (12 in total) for these components and measurable items (167 in total) for each variable were derived.

The objective of the selection was to compile the components and variables in a way that would facilitate the evaluation of the resilience of individual critical infrastructure elements. The limiting factors in the selection were the need to focus on individual elements (instead of on the sector as a whole) and the requirement for the selected items to be applicable as the basis for the management of element resilience over the long term. The issue is thus addressed primarily from the perspective of management.

The basic structure of the components and variables was finalized and discussed with the representatives of stakeholders at the project team workshop, held at the beginning of 2017. This was followed by a process whereby individual measurable items were derived and the manner of their application to the evaluation of element resilience was defined. This groundwork became the basis for the CIERA (Critical Infrastructure Elements Resilience Assessment) methodology [14]. The proposed procedures were verified through the analysis of the results of case studies of implementation previously processed for the sectors of electricity (the Control Room of a distribution system operator), transport (a railway station on an international track), and public health (a university hospital).

The CIERA methodology is currently (IV 2018) undergoing a formal certification process, meaning that it has yet to be officially published. This article addresses primarily the basic principles, philosophy, and correlation of the components of resilience for the purposes of evaluation, but it does not include either individual measurable items or the evaluation procedure as such. This is a presentation of the basics required for evaluating the resilience of critical infrastructure elements.

2. The Concept of Resilience in Critical Infrastructure Systems

The development and subsequent strengthening of the resilience of any set of critical infrastructure subsystems is a painstaking process in terms of design, time, and resources, and one that requires clearly defined initial as well as functional conditions. Defining such conditions can be understood as the overall concept of resilience for these subsystems in a critical infrastructure system. The setting of the management process for protecting critical infrastructure elements, comprising the framework for strengthening resilience, can be regarded as the principal initial condition. Conversely, the fundamental functional condition is the unambiguous specification and perception of factors determining critical infrastructure resilience. The management process for protecting critical infrastructure elements, as illustrated in Figure 1, represents an adaptation of principles based on a continual management cycle, e.g., PDCA (Plan-Do-Check-Act) Cycle [15], to fit the critical infrastructure system.

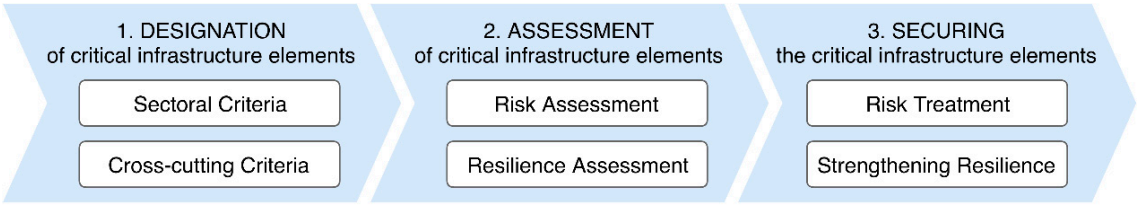

Figure 1. Management process for protecting critical infrastructure elements.

Designation of critical infrastructure elements is the initial sub-process of protection management. This sub-process hinges on the correct setting of criteria for designation of critical infrastructure elements on the European, national, and regional levels. In this phase of the process, it is equally important to consider the suitability of implementing an appropriate approach to element designation, which can be based on either the top-down or the bottom-up principle [16].

The second sub-process of protection management is the assessment of critical infrastructure elements. The key objective of this sub-process is risk evaluation, consisting of the assessment of

relevant disruptive event scenarios [17,18], and the evaluation of the respective element resilience, which involves the assessment of its robustness, recoverability, and adaptability [4].

Securing the critical infrastructure elements is the final protection management sub-process, consisting of risk management and resilience strengthening. Risk treatment involves the selection and implementation of one or more risk minimization options, i.e., risk retention, risk transfer, and/or risk avoidance (e.g., ISO/IEC 27001 [19]). Strengthening resilience (e.g., Action Plan [20] or Labaka et al. [21]) minimizes the vulnerability of subsystems, which in turn curtails the occurrence, intensity and propagation of failures and their impacts on a critical infrastructure system and society.

As mentioned above, the fundamental functional condition for strengthening the resilience of critical infrastructure subsystems is the unambiguous specification and perception of factors that determine it. In this context, the resilience of a critical infrastructure system must be understood as a cyclic process of continual improvement of prevention, absorption, recovery, and adaptation. Figure 2 shows one cycle within which resilience is strengthened from its original level (i.e., the black dashed line) to a new one (i.e., the red dashed line). The difference between these two levels, Δ, is understood as the degree to which resilience has been strengthened.

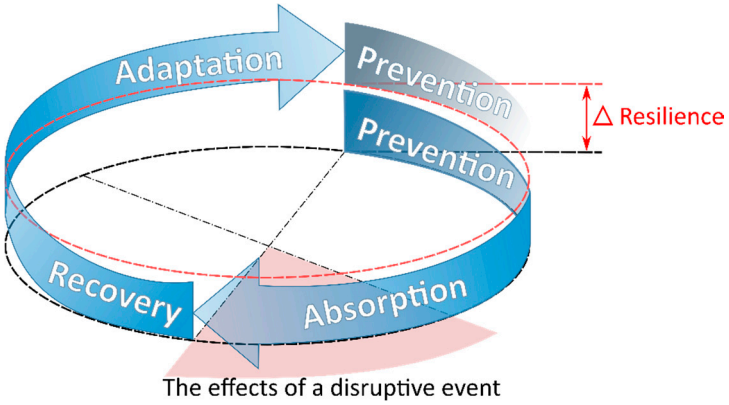

Figure 2. Critical infrastructure resilience cycle [22].

The first phase of the critical infrastructure resilience cycle is prevention. By adopting preventive measures, the owner/operator ensures the subsystem is less vulnerable to future disruptive events; preparedness is thus the resulting condition of prevention. Once a disruption occurs, such a system will switch from prevention to absorption.

Absorption is initiated if a subsystem is impaired due to a disruptive event, and is determined by the robustness of the critical infrastructure subsystem. Robustness is determined by the ability of a critical infrastructure element to absorb the effects of a disruptive event without the occurrence of any fluctuations in the services it provides.

The recovery phase starts after the effects of a disruptive event have worn off. This phase is characterized by recoverability, which is the capacity of a subsystem to recover its function to the original and/or required level of performance. The duration of the recovery phase is determined by the available resources and the time required to complete individual recovery processes.

The final phase of the critical infrastructure resilience cycle is adaptation, which is essentially the ability of an organization to adapt an operated subsystem to the potential recurrence of a disruptive event—i.e., to learn from previous disruptive events. Accordingly, it represents the dynamic long-lasting ability of an organization to adapt to changes in circumstances. Adaptation is determined by the internal processes of an organization focused on the strengthening of resilience, i.e., risk management, innovation processes, and education/development processes. However, strengthening of the resilience of a subsystem already occurs in the phase of recovery, for example in the form of component replacement or adjustments to its functioning processes.

3. Factors Determining Critical Infrastructure Resilience

Critical infrastructure subsystem resilience can be understood as a condition formed by three types of factors: (1) Factors determining resilience (i.e., components and variables of technical and organizational resilience); (2) factors limiting resilience (i.e., statutory regulation of the operation of infrastructure or the level of available financial resources); and (3) factors affecting resilience (i.e., threats or resilience strengthening instruments). The following part focuses exclusively on determining factors.

The resilience of elements in a critical infrastructure system is determined in two basic areas, namely the technological and physical protection of elements and organization management. As mentioned, the first area involves the technological and physical protection of individual elements. This type of resilience, known as technical resilience, is determined by the robustness and recoverability of system elements. The enhancement of technical resilience is invariably achieved exclusively in relation to a particular element or group of identical or very similar elements. A good example is the electricity sector, where robustness and recoverability will be secured in different ways and by different means depending on whether we are dealing with systems for the production of electricity or systems employed for its transmission and distribution.

The second area is organization management. This type of resilience, known as organizational resilience [23], is determined by the level of an organization's internal processes whose core purpose is to create optimum conditions for the adaptation of critical infrastructure elements to disruptive events. For the components of resilience and their variables see Figure 3.

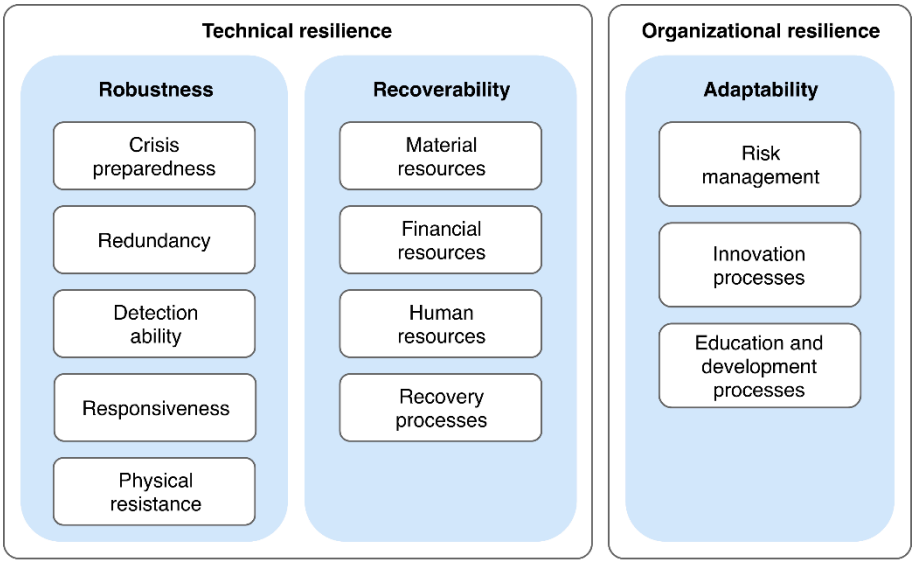

Figure 3. Components and variables determining the resilience of critical infrastructure elements.

Technical resilience is determined by the robustness and recoverability of critical infrastructure elements. For each element, these two components are determined or influenced by three basic factors: The technological structure of the element, the security measures of the element, and the disruptive events that affect element resilience.

Organizational resilience is formed simultaneously for all critical infrastructure elements operated by an organization. This type of resilience is formed, assessed, and strengthened by organization management as early as the prevention phase and factors in the level of internal processes necessary for the phase of adaptation of critical infrastructure elements, relying on the experience gained from previous response and recovery operations.

3.1. Factors Determining Robustness

Robustness is the ability of an element to absorb the impacts of a disruptive event. These impacts may be absorbed via the structural qualities of buildings or the technologies used (i.e., structural robustness) and/or via security measures (i.e., security robustness). Robustness is determined by the following variables:

- Crisis preparedness (a set of measures designed to improve the preparedness of a critical infrastructure element for a disruptive event).
- Redundancy (the ability to promptly substitute the performance of the disrupted part of the element or to enhance its capacity).
- Detection ability (the probability and/or time of recognition of a disruptive event).
- Responsiveness (the probability and/or time of response leading to the elimination of causes of a disruptive event or the minimization of their impacts).
- Physical resistance (a set of technical means and organizational or system measures designed to enhance the physical resistance of a critical infrastructure element to disruptive events [24]).

Where the level of robustness reaches 100%, the element concerned becomes resistant to the impacts of the given disruptive event. This means that it is able to fully resist its effects without perceptible negative impacts on the element of the service provided.

3.2. Factors Determining Recoverability

Recoverability is the capacity of an element to recover its function to the original (required) level of performance after the effects of a disruptive event have ended. With respect to critical infrastructure, recoverability is understood as reparability, in which case, only the damaged or destroyed components of an element are repaired or replaced. Recoverability is determined by the following variables:

- Material resources (the availability of components required for the repair or replacement of damaged or destroyed parts of the element).
- Financial resources (the availability of financial resources or reserves to finance the rapid recovery of the element).
- Human resources (the availability of human resources with the required level of qualifications).
- Recovery processes (processes facilitating the rapid recovery of the required performance of the element).

Provided the above-mentioned resources are adequate, resilience can already be strengthened at this stage. The implementation of more modern technologies, meeting higher security standards and ensuring greater element robustness, can be used as an example.

3.3. Factors Determining Adaptability

Adaptability is the ability of a critical infrastructure operator (i.e., an organization) to prepare an element for the recurring effects of a previous disruptive event. It represents the dynamic (long-term) ability of an organization to adapt to changes in circumstances. Adaptability is determined by the internal processes of an organization focused on creating optimal conditions for the strengthening of resilience. The basic processes that improve the adaptability of critical infrastructure elements to disruptive events are risk management, innovation processes, and education/development processes.

Risk management is a significant internal process of an organization that is essential to ensuring security/safety and strengthening resilience at the prevention stage. Risk management consists of coordinated activities to direct and control an organization with regard to risk [17], and its level in relation to organizational resilience is determined by the following four criteria:

- The level of risk management.

- The level of the applied risk assessment methodology.
- The level of implementation of security/safety standards.
- The level of specification of emergency scenarios, which form the very basis for developing contingency plans.

Additional internal processes that materially contribute to strengthening the resilience of critical infrastructure elements at the stage of prevention are organization innovation processes. From a strictly practical point of view, innovation is categorized into product, process, marketing, and organizational innovation [25]. With regard to resilience enhancement, process, and organizational innovations are especially important, as they focus on the reliability and external security of the technologies used. The innovation process itself consists of three basic phases, which are invention, science and research, and implementation. The level of the innovation process is determined by the following eight criteria:

- Flexibility of the organizational structure.
- Level of implementation of a management system.
- Organizational process management methods.
- Level of innovation of the management process.
- Extent of implementation of technological innovations.
- Level of innovation in security measures.
- Level of involvement in science and research.
- Level of investment in innovation by the organization.

Education and development processes constitute the last group of processes, which form and strengthen the organizational resilience of critical infrastructure elements, thereby improving the ability of the organization to adapt these elements to the effects resulting from disruptive events. Education and development processes can be divided into three basic categories [26], which are: Knowledge (both explicit and tacit); skills (e.g., professional-technical, managerial, analytical and conceptual); and attitudes (reflecting the values held by an individual). Key forms of education and development activities include long-term education, foreign study programs, skills development (soft skills), professional training (both preventive and repressive in nature), and staff training. The level of education and development processes is determined by three criteria:

- Level of education provided to the organization's workers.
- Level of training and maintenance of the practical skills of workers,
- Method of evaluating the effectiveness of training.

4. Graphical Representation of Resilience-Determining Factors

Element resilience affects the dynamics of the performance of the services provided by an element in response to a disruptive event (see Figure 4). This dynamic can vary depending on the type of infrastructure and disruptive event and the manner of its management.

As soon as an element begins to be affected by a disruptive event, the absorption capacity of the element can be broken down into two phases. In the first phase, the system is able to absorb the impacts of a disruptive event without the need to employ redundant capacities, up to the boundary of the element's ability to absorb fully the impacts of the respective disruptive event (see point A in Figure 4). In the second phase of absorption, the redundant capacities available to the element are employed and the element is still capable of delivering its full performance as required. At this point, there is still an opportunity to detect adverse events and subsequently initiate a response.

Only after the redundant capacities of the element have been exhausted, i.e., the limit of its ability to absorb the impacts of a disruptive event has been reached (see point B in Figure 4), do the negative consequences of the event begin to manifest in a decline of functions performed by the element. The nature of this decline is determined by the capabilities of the element to defend against the effects

of the event. Where such capabilities exist, the decline in performance of the element may be gradual; however, if these capabilities are overcome by the intensity of the disruptive event, the decline is likely to be abrupt or even immediate.

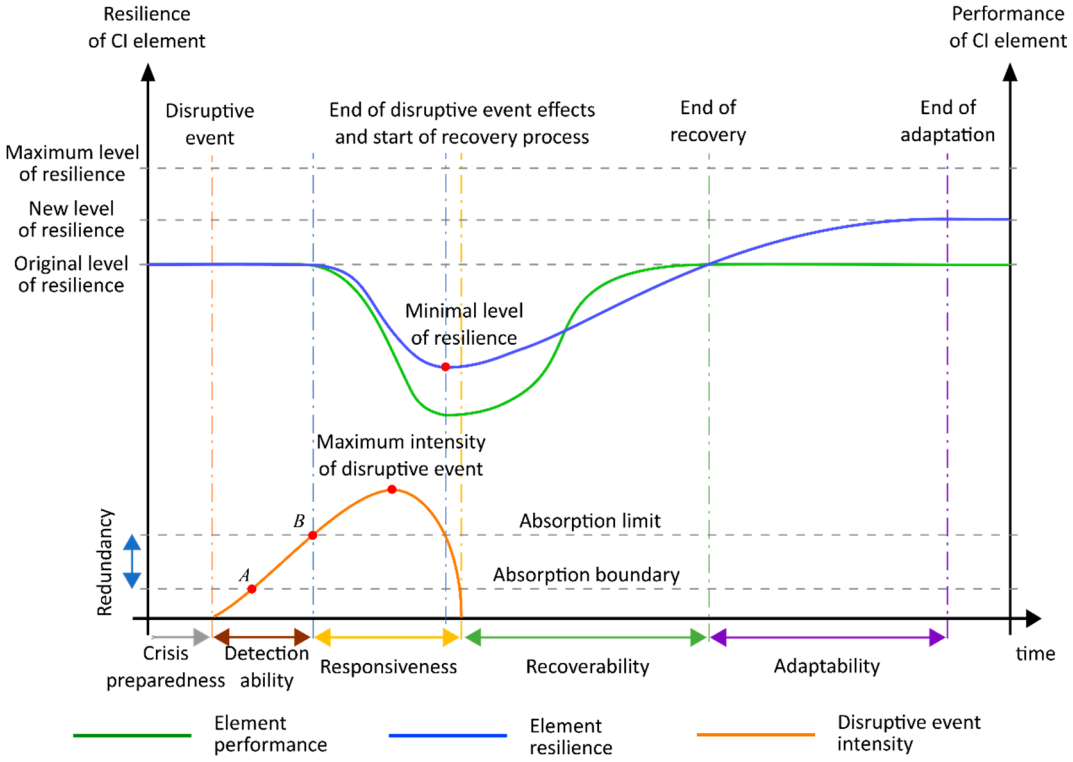

Figure 4. General representation of components and variables determining technical resilience.

4.1. Technical Resilience in the Electricity Sector

Figure 5 shows two possible scenarios for the disruption in electricity production at a power plant. The power plant in the scenario operates four generators to generate electric power and has two backup generators with the same capacity which can be deployed in the case of failure of any of the main units.

Redundancy, as opposed to the situation presented in Figure 4, is characterized differently here—the event causes a failure of the generator, after which the system detects a decrease in generation volume and activates a backup generator to offset the decrease. The element thus experiences a temporary decline in performance, which is, however, quickly compensated for by the use of a backup generator. Only after the failure of the second generator the element's backup capacities will be exhausted—each additional decrease in generator performance will fully manifest in the level of services the element provides. Failures of other generators will thus cause a step-down decline in performance.

In the scenario indicated by the solid line, the system is able to respond with sufficient flexibility to manage the situation. There is a gradual decline in the intensity of the event accompanied by a gradual recovery of the power plant performance up until the original (required) level of performance is achieved. However, at this point the recovery process is not over yet, as the system is able to meet the requirements imposed on it, but at the same time it lacks redundant capacity and its ability to resist the adverse effects of another disruptive event is, therefore, inhibited. This situation is clearly shown by the redundancy graph (blue line in Figure 5). The recovery process does not end until the backup generators have fully recovered.

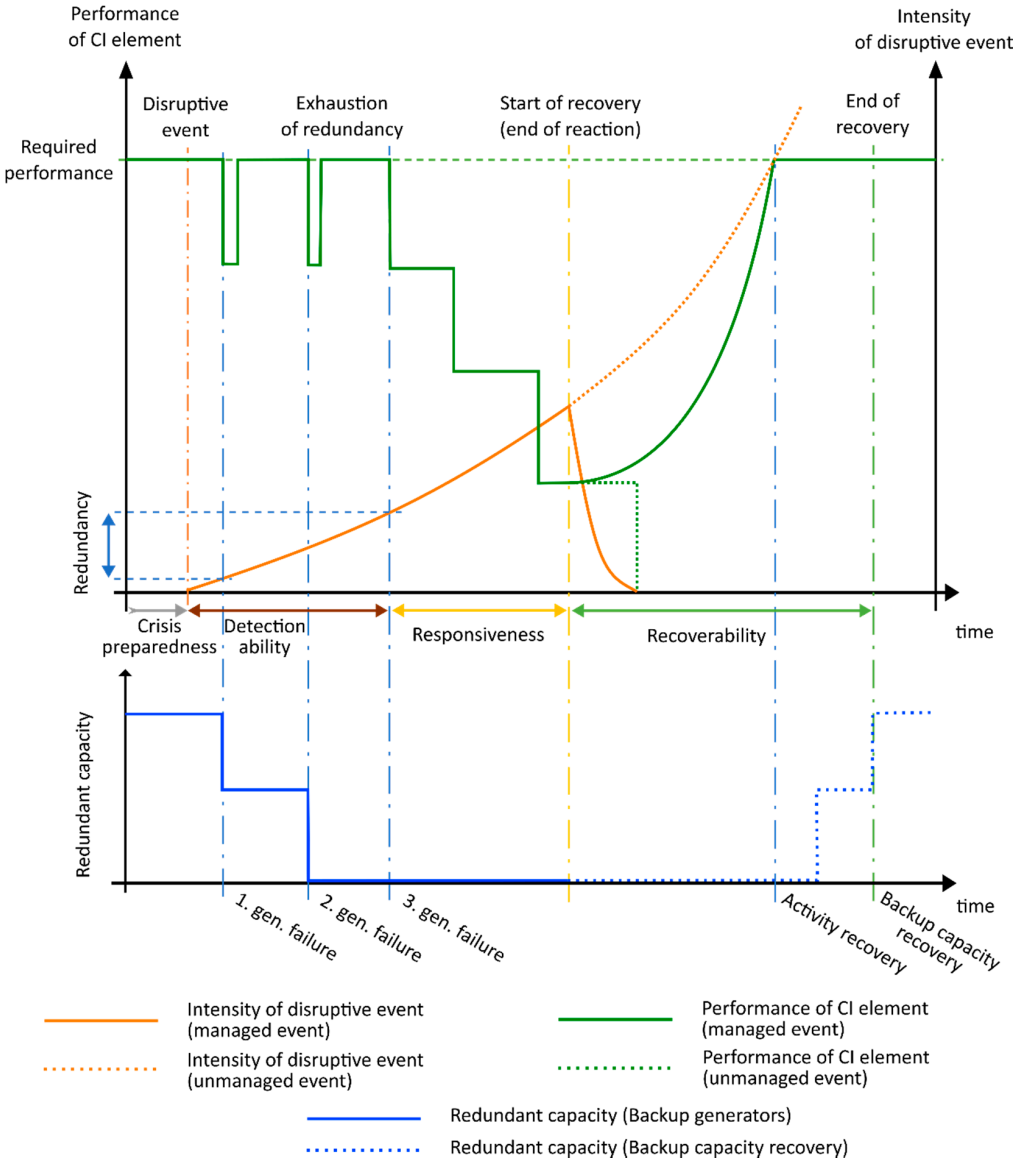

Figure 5. Electric power generation system—the effect of the intensity of a disruptive event on power generation.

4.2. Technical Resilience in the Gas Sector

The scenario in Figure 6 shows a potential loss of control over the gas distribution system with respect to a section of the gas pipeline. In normal circumstances, gas is transported under operating pressure. However, the gas pipeline is designed to withstand even greater pressure. In terms of safety, the difference between the maximum technically possible pressure and the operating pressure represents the redundant capacity of the pipeline.

In the event that the maximum pressure is exceeded, it will be reasonable to expect the occurrence of a pipeline rupture and, consequently, the immediate interruption of services until the damaged section is repaired and the pipeline pressurized.

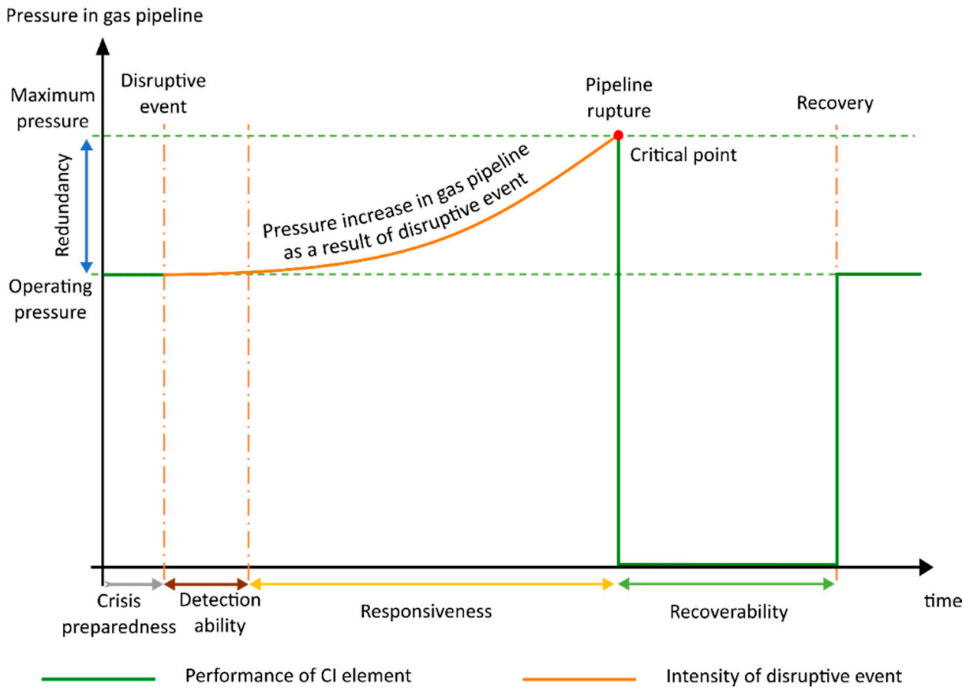

Figure 6. Redundancy and gas pipeline failure due to a disruptive event.

4.3. Technical Resilience in the Information and Communications Technology Sector

Figure 7 presents a scenario involving a DDoS attack (distributed denial-of-service) on an isolated, network-connected system. The attacker floods the system with illegitimate requests that the system must process alongside the requests of legitimate system users.

The system can initially utilize its capacity reserves to process all requests, but if the intensity of new requests sent to the system continues to increase, the proportion of illegitimate requests to legitimate ones will increase accordingly. As a result, the number of processed legitimate requests will keep decreasing until the system is no longer able to respond. However, once the intensity of the attack is diminished, the system will gradually start to recover.

4.4. Technical Resilience in the Road Transport Sector

Figure 8 shows a simplified form of a fundamental chart which conveys the relationship between the intensity and density of road traffic.

The initial state of equilibrium, i.e., a free flow of vehicles, is characterized by low density (large distances between vehicles) and at the same time low intensity. The vehicles, despite large distances between them (and therefore higher speed), pass the reference section in low quantities per unit of time.

An increasing density caused by negative events affecting the critical element, such as other vehicles arriving at the reference section from different directions, will initially manifest only in decreased vehicle spacing, while their speed remains the same. As individual vehicles are not restricted enough to reduce their speed, the traffic intensity begins to increase sharply.

Once traffic density reaches a critical point, the limit of available performance and thus the robustness of the element are also reached. This will lead to an abrupt change in the condition of the traffic flow and a rapid decrease in the average speed of vehicles. Traffic intensity sharply decreases despite the still-increasing density. This leads to congestion, which is characterized by maximum density and minimum speed, and thus very low traffic intensity. This condition is also very stable, and system recovery will normally occur only after the traffic density has dropped substantially below the critical point which initially led to the system collapse.

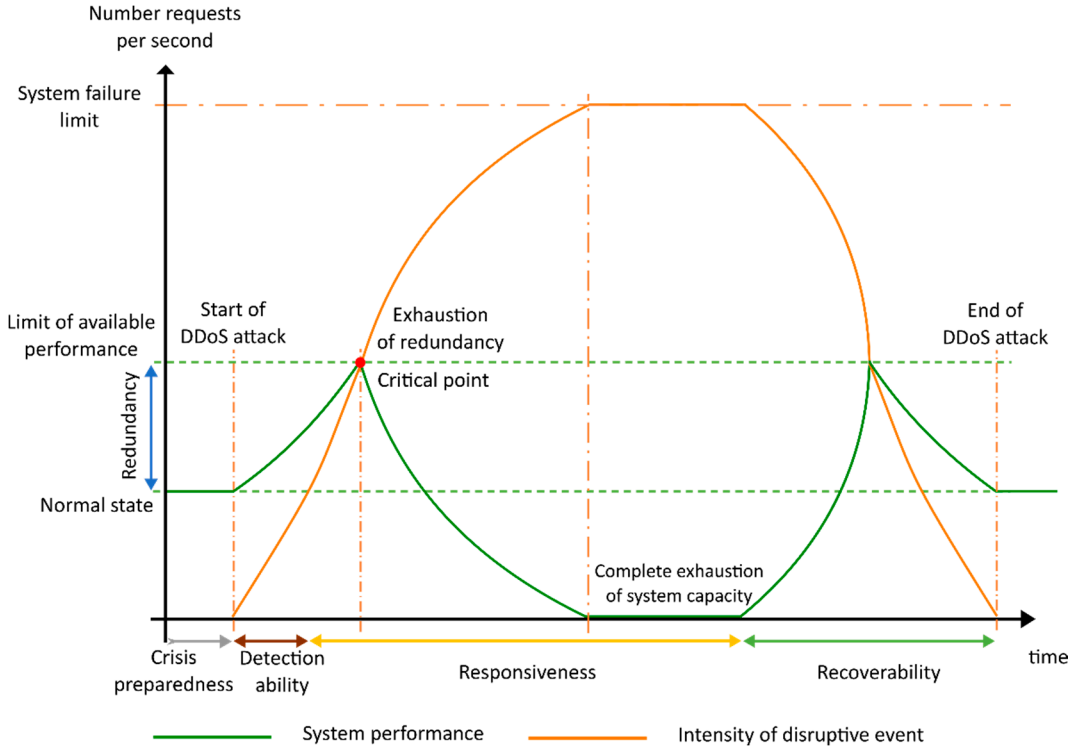

Figure 7. DDoS attack and its impact on system performance.

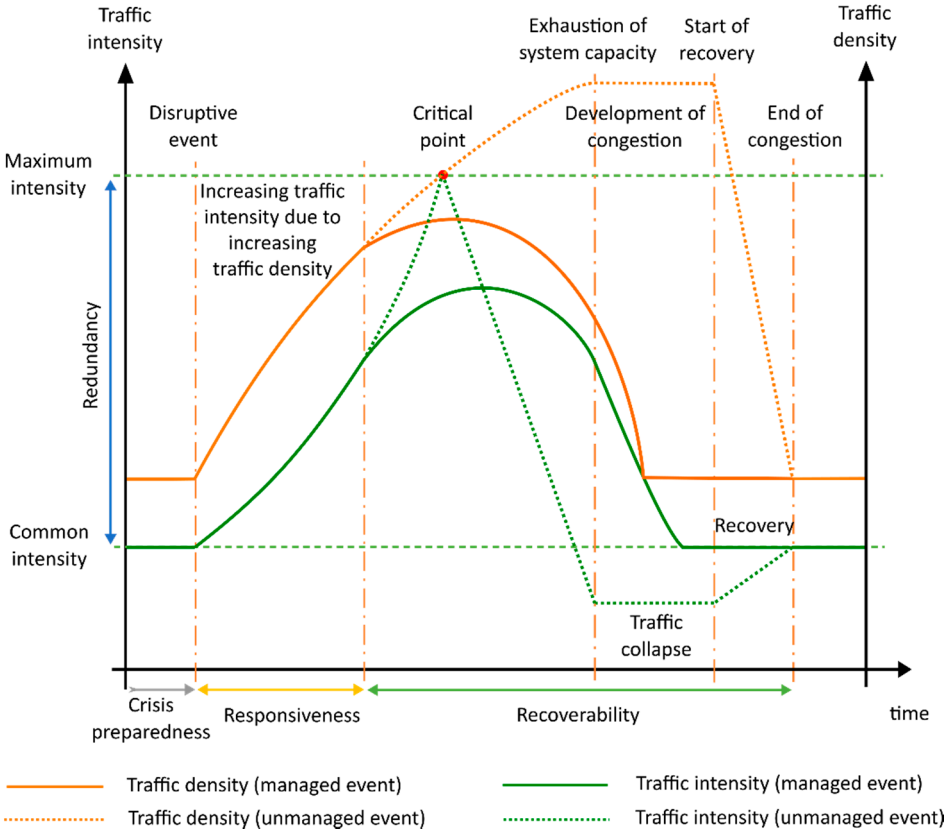

Figure 8. Impacts of high density traffic flow on intensity of traffic within a length of roadway.

In the recovery phase, traffic density continues to decrease significantly, which leads to a steady increase in traffic intensity, the recovery of the performance of the CI element and a return to the optimum condition.

5. Conclusions

Critical infrastructure system resilience is defined as the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event. In this context, it can be understood as a condition closely related to the performance function of individual subsystems. During disruptive events, resilient subsystems show a smaller decrease in performance, and the time needed for them to return to their required level is measurably shorter. The initial factor contributing to the development and strengthening of resilience is the establishment of functional conditions, which in turn enables the unambiguous formulation of the resilience concept with respect to these subsystems within a critical infrastructure system.

The strengthening of resilience is based on the continual enhancement of the level of factors which determine it. Sustained attention should be devoted to these factors in the areas of both technical resilience (i.e., robustness and recoverability) and organizational resilience (i.e., adaptability). At the same time, it is equally important also to reflect on factors hindering resilience (i.e., statutory regulation of the infrastructure's operation or the availability of financial resources) and factors that affect it (i.e., threats or resilience strengthening instruments).

These principles are usually acceptable across individual sectors of critical infrastructure. However, in order to implement the evaluation system effectively, it is essential that this accord also manifests at deeper levels, such as the level of individual resilience factors, the action of which varies significantly in different critical infrastructure sectors. This article has presented one way in which to harmonize the perception of these factors while maintaining sector specifics, especially with regard to the electricity, gas, information and communications technology, and transport sectors.

Author Contributions: Conceptualization, D.R. and P.S.; Methodology, D.R., P.S. and S.S.; Validation, D.R. and S.S.; Investigation, D.R., P.S. and S.S.; Writing-Original Draft Preparation, D.R., P.S. and S.S.; Visualization, D.R., P.S. and S.S.; Supervision, D.R. and P.S.; Project Administration, D.R.; Funding Acquisition, D.R.

Funding: The article was elaborated within a Ministry of the Interior of the Czech Republic Project, filed under: VI20152019049, entitled 'Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems' and within a VSB—Technical University of Ostrava Project, filet under: SP2018/116, entitled 'Dynamic Modelling of Resilience of Critical Infrastructure Elements'.

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

References

1. Van der Lei, T.E.; Bekebrede, G.; Nikolic, I. Critical infrastructures: A review from a complex adaptive systems perspective. *Int. J. Crit. Infrastruct.* **2010**, *6*, 380–401.
2. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25. [CrossRef]
3. Holling, C.S. Resilience and Stability of Ecological Systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [CrossRef]
4. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*; U.S. Department of Homeland Security: Washington, DC, USA, 2009.
5. PPD-63. *Presidential Decision Directive: Critical Infrastructure Protection*; The White House: Washington, DC, USA, 1998.
6. PPD-21. *Presidential Decision Directive: Critical Infrastructure Security and Resilience*; The White House: Washington, DC, USA, 2013.
7. Slivkova, S.; Rehak, D.; Brabcova, V.; Dopaterova, M.; Nesporova, V.; Novotny, P.; Markuci, J.; Taslova, J. *Defining the Resilience of Critical Infrastructure System*; VSB–Technical University of Ostrava: Ostrava, Czech Republic, 2017. (In Czech)

8. Petit, F.; Bassett, G.; Black, R.; Buehring, W.; Collins, M.; Dickinson, D.; Fisher, R.; Haffenden, R.; Huttenga, A.; Klett, M.; et al. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*; Argonne National Laboratory: Chicago, IL, USA, 2013.
9. Prior, T. *Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9)*; Eidgenössische Technische Hochschule Zürich: Zurich, Switzerland, 2015.
10. Bologna, S. *Guidelines for Critical Infrastructure Resilience Evaluation*; Italian Association of Critical Infrastructures' Experts: Roma, Italy, 2016.
11. Nan, C.; Sansavini, G. A quantitative method for assessing resilience of interdependent infrastructures. *Reliab. Eng. Syst. Saf.* **2017**, *157*, 35–53. [CrossRef]
12. Jovanović, A.; Klimek, P.; Choudhary, A.; Schmid, N.; Linkov, I.; Øien, K.; Vollmer, M.; Sanne, J.; Andersson, S.L.; Székely, Z.; et al. *D1.2-Analysis of Existing Assessment Resilience Approaches, Indicators and Data Sources*; EU-VRi: Stuttgart, Germany, 2018.
13. Cai, B.; Xie, M.; Liu, Y.; Liu, Y.; Feng, Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. *Reliab. Eng. Syst. Saf.* **2018**, *172*, 216–224. [CrossRef]
14. Rehak, D.; Senovsky, P.; Hromada, M.; Pidhaniuk, L.; Dvorak, Z.; Lovecek, T.; Ristvej, J.; Leitner, B.; Sventekova, E.; Maris, L. *Methodology of the Critical Infrastructure Elements Resilience Assessment*; VSB–Technical University of Ostrava: Ostrava, Czech Republic, 2018. (In Czech)
15. Tague, N.R. *Quality Toolbox*, 2nd ed.; ASQ Quality Press: Milwaukee, WI, USA, 2005.
16. Twidale, M.B.; Floyd, I. Infrastructures from the bottom-up and the top-down: Can they meet in the middle? In *Proceedings of the Tenth Anniversary Conference on Participatory Design (PDC '08)*; Indiana University Indianapolis: Bloomington, IN, USA, 2008; pp. 238–241.
17. ISO 31000. *Risk Management–Guidelines*; ISO: Geneva, Switzerland, 2018.
18. IEC 31010. *Risk Management–Risk Assessment Techniques*; IEC: Geneva, Switzerland, 2009.
19. ISO/IEC 27001. *Information Technology—Security Techniques—Information Security Management Systems—Requirements*; ISO/IEC: Geneva, Switzerland, 2013.
20. Government of Canada. *Action Plan for Critical Infrastructure (2014–2017)*; Public Safety Canada: Ottawa, ON, Canada, 2014.
21. Labaka, L.; Hernantes, J.; Sarriegi, J.M. A framework to improve the resilience of critical infrastructures. *Int. J. Disaster Resil. Built Environ.* **2015**, *6*, 409–423. [CrossRef]
22. Rehak, D.; Senovsky, P.; Hromada, M. Analysis of Critical Infrastructure Network. In *Modern and Interdisciplinary Problems in Network Science: A Translation Research Perspective*; Chen, Z., Dehmer, M., Emmert-Streib, F., Shi, Y., Eds.; CRC Press: Boca Raton, FL, USA, 2018; pp. 143–171.
23. Denyer, D. *Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking*, 1st ed.; BSI and Cranfield School of Management: Cranfield, UK, 2017.
24. Lovecek, T.; Ristvej, J.; Simak, L. Critical Infrastructure Protection Systems Effectiveness Evaluation. *J. Homel. Secur. Emerg. Manag.* **2010**, *7*, 34. [CrossRef]
25. OECD/Eurostat. *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data*, 3rd ed.; OECD Publishing: Paris, France, 2005.
26. Armstrong, M. *Armstrong's Handbook of Human Resource Management Practice*, 3rd ed.; Kogan Page: London, UK, 2014.