# Failures in a Critical Infrastructure System

David Rehak and Martin Hromada

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70446

**Abstract**

The purpose of this chapter is to provide a comprehensive overview of a critical infrastructure system, of failures and impacts that occur within it and of the resilience, which effectively reduces the risk of these impacts spreading on to dependent subsystems. The chapter presents a basic description of a critical infrastructure system and of the hierarchic arrangement of its subsystems and linkages between them. Critical infrastructure system failures, including their causes and impacts on dependent subsystems and on society as a whole, are presented in the following section. Particular focus is given to the propagation of impacts in a critical infrastructure system and the current approaches to their modeling. The chapter concludes by expounding on the resilience of critical infrastructure subsystems and its impact on the minimization of failures in critical infrastructure subsystems in circumstances involving emergencies.

**Keywords:** critical infrastructure, system, disruption, failure, impacts, resilience

## 1. Introduction

Society has traditionally depended on a broad variety of services as much as on the infrastructures providing them. Over time, some of these infrastructures, or rather their elements considered to be of vital importance to society, began to be regarded as critical. At present, these infrastructures constitute the critical infrastructure system [1], which consists of individual subsystems, i.e., sectors, subsectors, and elements. There are dependencies between critical infrastructure subsystems which can, due to a disruption in the functionality of one subsystem, spread to dependent subsystems, and thereby escalate the impacts from emergencies on society.

## 2. Critical infrastructure system description

The issue of critical infrastructure protection began to be addressed in the United States in response to a terrorist bombing on a federal building in Oklahoma City in 1995 [2]. Over the following years, other countries also started tackling these problems, e.g., from 1998 in Canada and from 1999 in the United Kingdom, Germany, Sweden, and Switzerland. Following the September 11, 2001 attacks, the majority of European countries proceeded to define "Critical Infrastructure" and began to take actions aimed at its protection [3].

The US Department of Homeland Security (DHS) currently defines a critical infrastructure as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" [4]. A critical infrastructure at the European Union level is specified in a Council Directive [1], defining a critical infrastructure as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*"

The hierarchic arrangement of a critical infrastructure system has three levels that constitute a vertical classification [3]: system level, sector level, and element level (see **Figure 1**). The system level is the basic classification of a critical infrastructure according to its functions. This level comprises two areas, namely the technical infrastructure and the socioeconomic infrastructure. The technical infrastructure includes sectors producing and providing specific

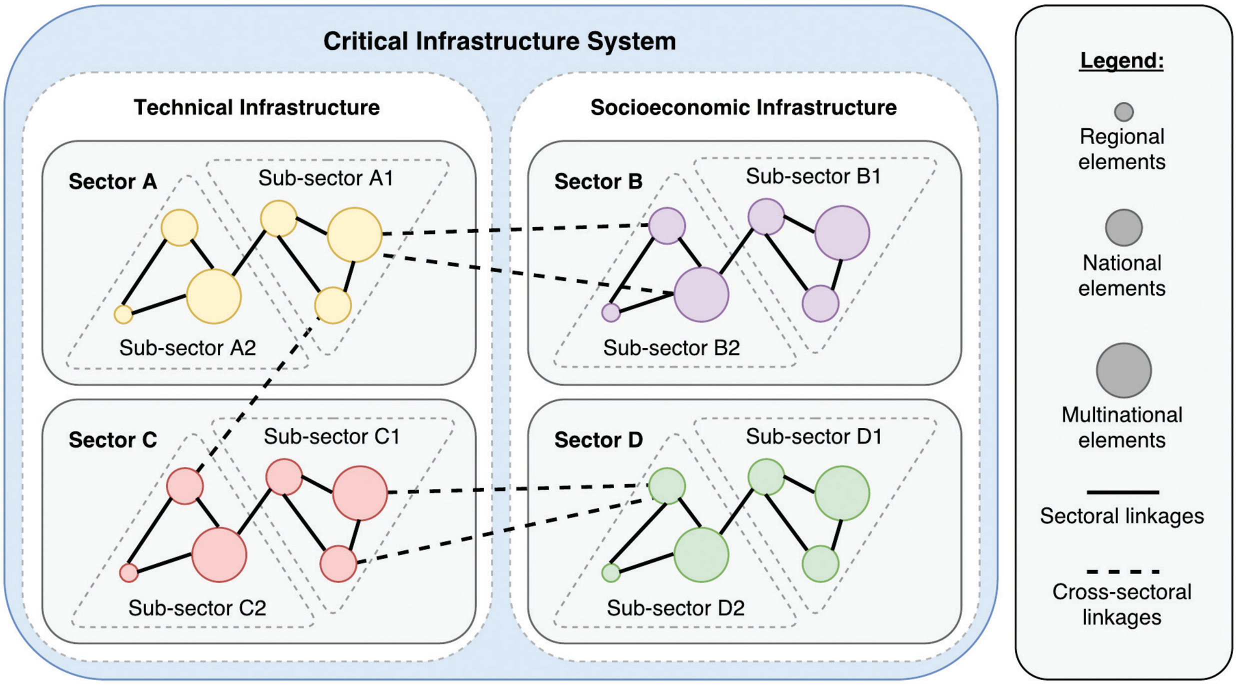

**Figure 1.** Hierarchic arrangement in a critical infrastructure system.

commodities (e.g., energy and water supply) or sectors providing technical services (e.g., transport or ICT systems). The socioeconomic infrastructure is composed of sectors that provide social or economic services (e.g., health care, financial and currency markets, emergency services, and public administration). There are significant dependencies between two types of critical infrastructure [5]. For instance, all of the socioeconomic sectors require the unrestricted availability of commodities produced by the technical infrastructure sectors, whereas the technical infrastructure, by contrast, fully depends on the socioeconomic sectors, especially in crisis situations.

The sector level is composed of the individual sectors and subsectors of a critical infrastructure. This level represents the classification of specific sectors and their mutual linkages. The transportation sector, for example, is made up of five subsectors, namely road transport, rail transport, air transport, inland waterways transport, and ocean and short-sea shipping and ports [1]. The individual elements that form the element level are the basic building blocks of the critical infrastructure system. These elements reach different degrees of relevance within the system, depending on the extent of the impact that their disruption or failure can potentially produce.

It is imperative that a critical infrastructure system be viewed in a comprehensive manner, taking into account its networked arrangement where individual subsystems are interlinked via various types of linkages. The basic structure of these linkages arises from their character and includes one-way linkages, which represent an influence or dependency, and two-way linkages involving interdependency. Rinaldi et al. [6] have classified interdependencies in more detail as physical, cybernetic, geographic, and logical in nature and noted that interdependencies increase the risk of failures or disruptions in multiple infrastructures. Pederson et al. [5] have subsequently further classified these linkages for lower levels of detail.

## 3. Impacts of critical infrastructure system failures on dependent subsystems and society

Like any other complex system, a critical infrastructure system includes a multitude of elements with different levels of importance, categorized into several levels and interconnected by linkages of various types and intensity. Such a structural arrangement leads to a broad correlation between individual subsystems, which determines the manner and intensity of propagation of impacts from critical infrastructure system failures on dependent subsystems and society.

### 3.1. Critical infrastructure system failures

The functioning of a critical infrastructure system is constantly being threatened by a wide range of security threats. These threats can be generally categorized into five basic groups [7]:

- climatological threats (including natural disasters such as floods, tornadoes, heavy snowfall, or extensive fires);

- geological threats (e.g., earthquakes, volcanic activity, landslides);
- biological threats (e.g., pandemics);
- technological threats (including technological emergencies such as radiation emergencies, hazardous chemical spills, flooding caused by damage to hydraulic structures, widespread disruptions to engineering networks, public water supply emergencies or major road, rail, or air traffic accidents); and
- criminal threats (e.g., terrorism, criminal activity, armed conflicts).

The effects produced by these threats on a critical infrastructure system or its subsystems can cause adverse events, which can in turn lead to disruptions or in extreme cases, failures of different subsystems. This involves, in particular, disruptions to functional parameters causing a decline in the performance of specific elements (see **Figure 2**) where the decline is directly proportional to the intensity of the emergency and the degree of resilience of the respective critical infrastructure element.

Depending on the category of threats, three types of emergencies, that subsequently generate individual failures, can occur in a critical infrastructure system. These include intentional anthropogenic events (i.e., terrorism and criminal activity), unintentional anthropogenic events (i.e., technological emergencies), and natural events (i.e., climatological, geological, and biological threats). Once generated, the failures can propagate further within a critical infrastructure system and produce negative impacts of different character, intensity, and effect. Rinaldi et al. [6] were the first to define the basic types of failure propagation in a critical infrastructure system:

- A cascading failure occurs when a disruption in one infrastructure causes the failure of element in a second infrastructure, which subsequently causes a disruption in the second infrastructure (e.g., electric power failure could create disruption in other infrastructures).
- An escalating failure occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity or the time for recovery of the second failure (e.g., disruption in ICT network may escalate to disruption in a road transport network).
- A common cause occurs when two or more infrastructure networks are disrupted at the same time: elements within each network fail because of some common cause (e.g., action of natural disaster to all local infrastructures).

Over the following years, numerous scholarly papers and studies attempting to elaborate on and tackle the issue of failure propagation within a critical infrastructure system from different viewpoints were published based on the work of Rinaldi et al. [6]. These include Visualization of Critical Infrastructure Failure [8], Cascading Effects of Common-Cause Failures in Critical Infrastructures [9], Analyzing Critical Infrastructure Failure with a Resilience Inoperability Input–Output Model [10], or Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures [11] to name a few.

### 3.2. Impacts of critical infrastructure system failures

Critical infrastructure system failures subsequently produce negative impacts. These impacts can propagate further not only within the critical infrastructure system (between dependent subsystems), but also outside the system where they can specifically affect society, including national interests such as state security, the economy, and basic human needs [1].

The intensity and propagation of the impacts from critical infrastructure system failures is affected by several external and internal factors of the system concerned. While the external factors include, in particular, resilience of society and the character, and the scope and duration of an emergency; the principal internal factors include the type and scope of the failure inside the system [6], subsystem linkages, and subsystem resilience. The nature of the impacts is characterized by the scope, structure, intensity, duration, and effect of the emergency (see **Figure 3**) [3].

In the event of a disruption to a critical infrastructure system, the impacts spread into two basic areas. The first instance involves impacts within the system where the failure of one critical infrastructure subsystem causes a failure of another subsystem in what is known as a cascading effect [6]. In the second instance, the impacts exert influence outside the system, specifically, on society, producing negative effects on national interests such as security, the economy, and basic human needs [3].

In both of the above-mentioned cases, the impacts may be classified as direct or indirect from a structural point of view. The immediate effect of a disrupted subsystem on another subsystem or directly on society is considered to be a direct or primary action. In contrast, indirect effects of impacts occur vicariously through any critical infrastructure subsystem, regardless of whether or not they affect another subsystem or society as a result. Indirect effects of impacts may be secondary (through one subsystem) or multi-structural (through several subsystems) in character [3].

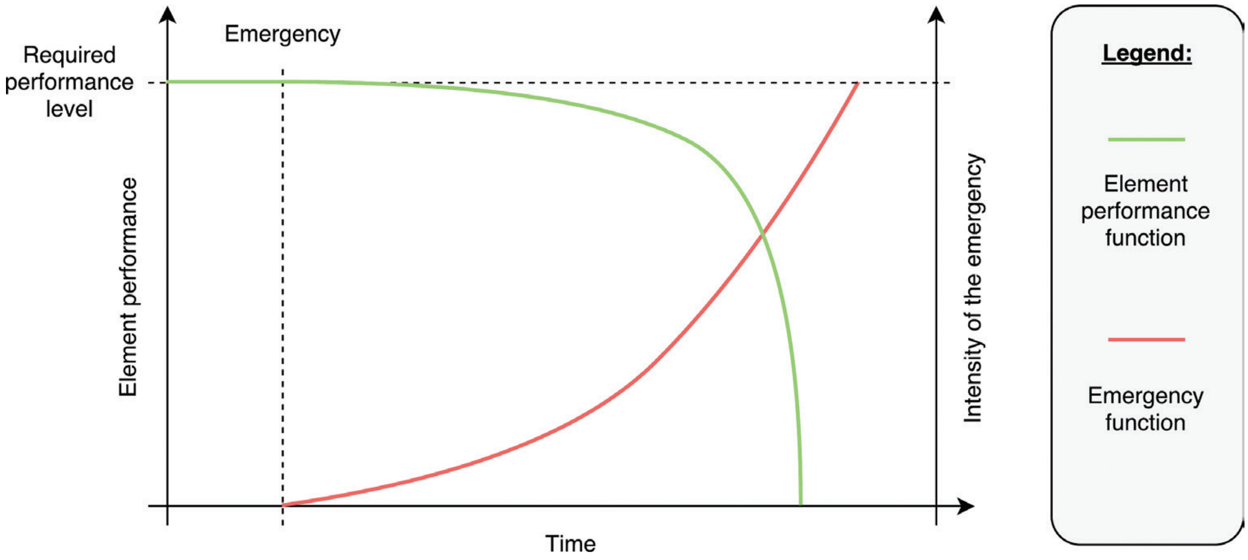

**Figure 2.** Disruption to an element in a critical infrastructure system.

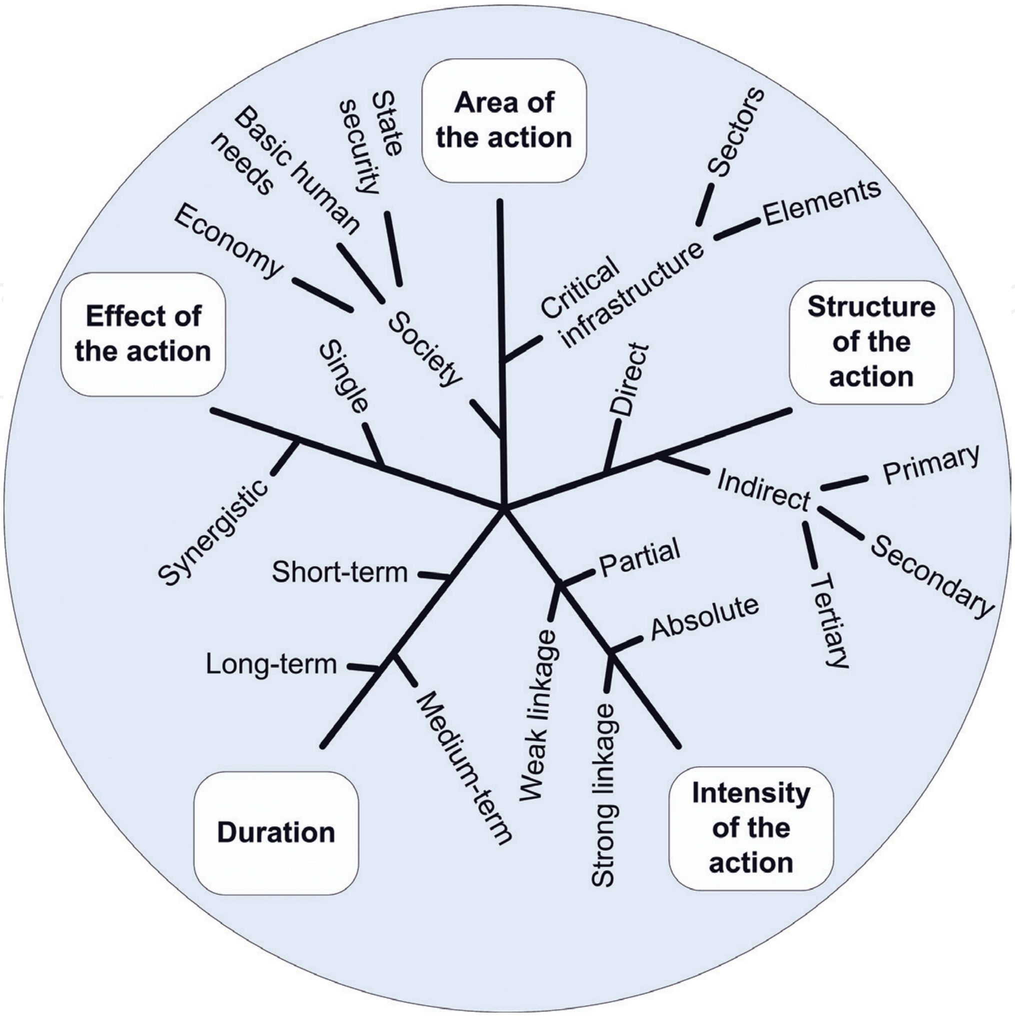

**Figure 3.** Aspects that create the character of impacts in a critical infrastructure system [3].

Other important factors determining the character of impacts are their intensity and duration. The impact intensity depends on the extent of a failure in a subsystem, that in turn affects another critical infrastructure subsystem, as well as on the level of their linkage. If the linkage is weak, the impact intensity is low and the subsequent impact on the affected subsystem is limited. However, if this linkage is strong, the impact intensity is high and the impact on the affected subsystem can be devastating or absolute. The impact duration, which may be short-term, medium-term, or long-term, represents an important variable with respect to the impact intensity. Ouyang et al. [12] present the typical time progression of a critical infrastructure disruption, dividing it into prevention, propagation, damage, assessment, and recovery periods [3].

Another key factor determining the character of impacts is the effect of their action. If the impacts of a disrupted subsystems act on another subsystem or society in one way only, the impact effect can be regarded as a single impact. However, if the impact effects are multi-way (e.g., through the combination of direct and indirect impacts) and occur concurrently in real-time, then the effects are considered to be synergistic [3].

### 3.3. Propagation of impacts in a critical infrastructure system

The above-mentioned aspects, shaping the character of impacts, also significantly contribute to the propagation of these impacts in a critical infrastructure system. At the core of their propagation lie critical infrastructure system failures caused by the negative effects of security risks (i.e., causes of disruptions or failures of a critical infrastructure), which can be either external or internal in nature. Such impacts can then exert a direct influence on society (i.e., direct impacts), spread further across the critical infrastructure, and cause other failures, which lead to additional impacts (i.e., cascading impacts) or they can, due to a cascading effect, act jointly on a single target (i.e., synergistic impacts). See **Figure 4** for a graphical representation of all the potential ways in which impacts can propagate within a critical infrastructure system.

Direct impacts are impacts caused by the disruption or failure of a critical infrastructure subsystem, which act directly on society. The effects of a security threat (e.g., a terror attack) to a component of a critical road infrastructure of international importance (e.g., a major freeway bridge) can be used as an example. These negative effects result in the disruption to the functional parameters of the freeway, which has a direct impact on society (in this instance on passengers and freeway network operators).

Cascading impacts are impacts caused by the disruption or failure of a critical infrastructure subsystem, which spread further across the critical infrastructure, resulting in failures in dependent subsystems that in turn lead to an escalation in other impacts. The effects of a security threat (e.g., a gale) to a component of a critical electric energy infrastructure of national importance (e.g., 110 kV distribution system) can be used as an example. These negative effects result in the disruption to functional parameters of the distribution system, which cascades into dependent subsystems (e.g., a railroad signaling system). The disruption to a distribution system then results in a cascading impact on society due to nonfunctioning railroad transport.

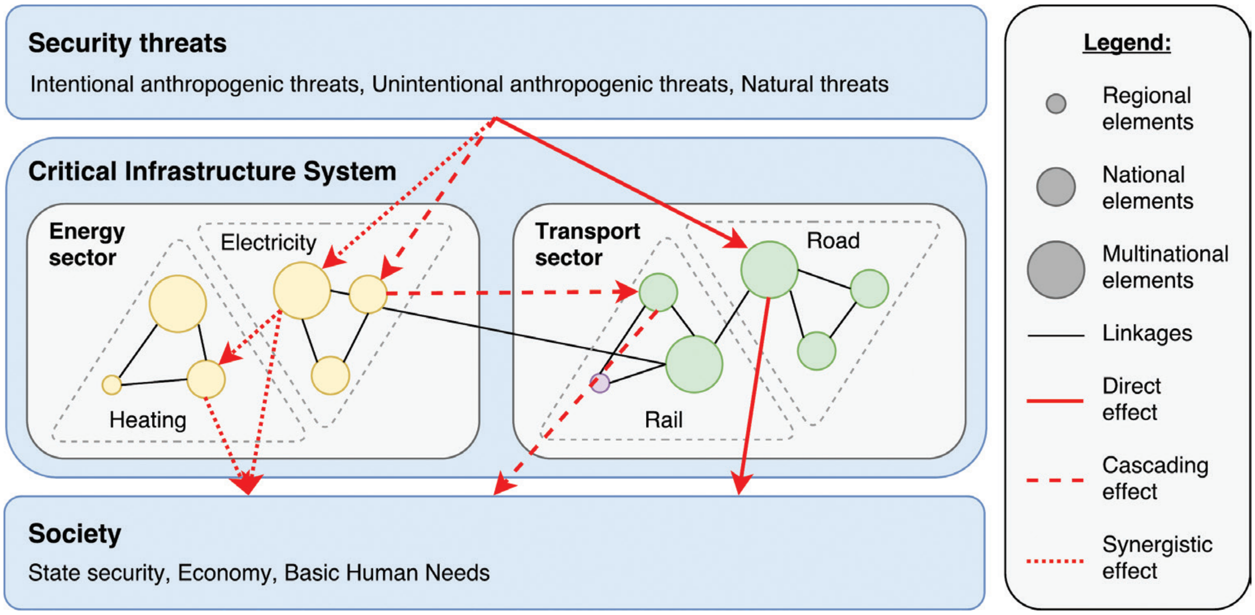

**Figure 4.** Ways of impact propagation in a critical infrastructure system.

Synergistic impacts are impacts caused by the disruption or failure of two or more critical infrastructure subsystems which occur concurrently, thereby exacerbating their impacts on society [3, 9]. The effects of a security threat (e.g., a technological accident) to element of a critical electric energy infrastructure of international importance (e.g., a nuclear power plant) can be used as an example. These negative effects result not only in direct impacts on society (i.e., large-scale power outages), but also in the impacts cascading to dependent subsystems (e.g., heat production and distribution), the disruption of which produces additional impacts on society. This situation brings about a synergistic effect, consisting of the added effect of joint impacts on society, and increasing their mere sum [3].

### 3.4. Modeling of impacts of critical infrastructure system failures

Modeling the anticipated propagation of impacts constitutes an important approach contributing to their minimization in a critical infrastructure system. However, it involves a complex process which should be based on mathematical modeling as well as on the integration of innovative approaches to analyze the critical infrastructure system. The basis for this process should include, in particular [13]:

- early indication of impacts using a bottom-up approach;
- harmonization and transformation of cross-cutting criteria at the regional level;
- European critical infrastructure risk and safety/security management; and
- implementation of a preferential critical infrastructure risk assessment.

An early indication of impacts through the application of a bottom-up approach should be based on the determination of resilience disruption indicators in interconnected critical infrastructure subsystems. It is a holistic approach to assess the resilience of a critical infrastructure based on a comprehensive perception of specific political, economic, social, technological, legislative, and ecological environments. The essence of this approach is a systematic approach consisting of a cross-sectoral evaluation based on a research into the mutual linkages between individual critical infrastructure subsystems. It factors in the propagation of cascading impacts and synergistic effects in a critical infrastructure system. The referenced system solution should be applied using a progressive bottom-up approach, which is based on a critical infrastructure evaluation from the lowest level (city, region) upwards and has already been implemented in a number of developed countries (e.g., Switzerland and the Netherlands). This approach can be viewed as the logical continuation of the ongoing research into critical infrastructure security in terms of integrating the research results, via identifiers describing the critical infrastructure status, into a composite resilience indicator (see **Figure 5**) [13].

The application of the bottom-up approach is closely related to the need to harmonize and transform cross-cutting criteria at the regional level. Individual Member States of the European Union have already set the cross-cutting criteria values for national critical infrastructure elements. However, the vast majority of states have failed to disclose these values, making the follow-up research into the modeling of the impacts on society particularly

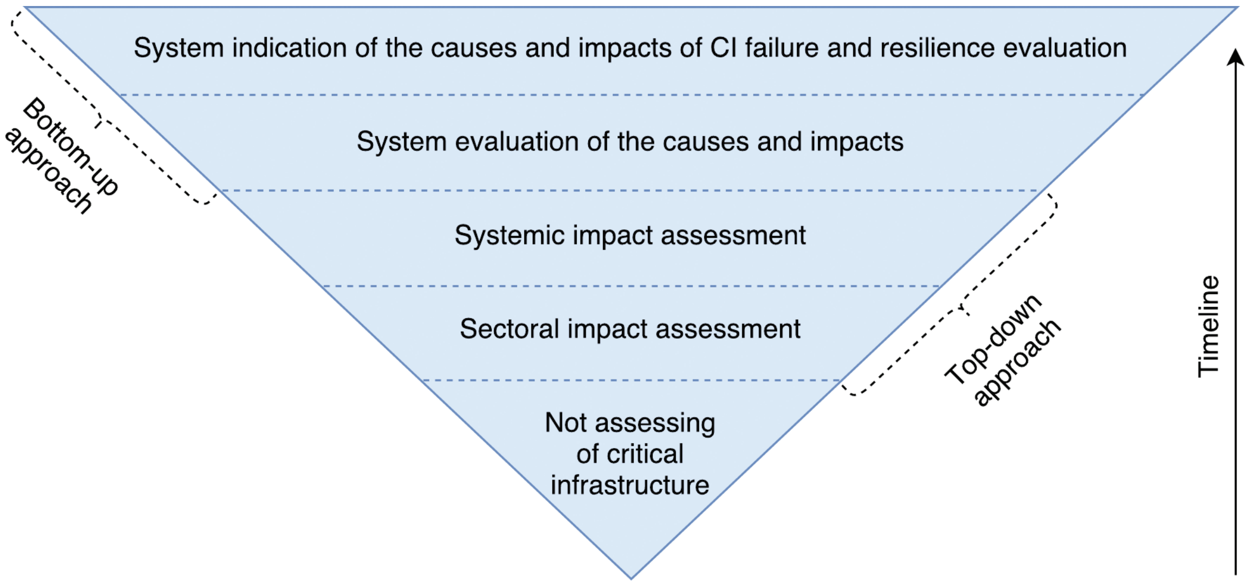
System indication of the causes and impacts of CI failure and resilience evaluation
System evaluation of the causes and impacts
Systemic impact assessment
Sectoral impact assessment
Not assessing of critical infrastructure
Bottom-up approach
Top-down approach
Timeline

**Figure 5.** Development of the approach to a critical infrastructure research [14].

challenging. For this purpose, it is possible to use the results of the international RAIN project [15] undertaken as part of the EU's 7th Framework Programme. Based on recommendations arising from a European Union directive [1] and a regulation on the criteria for determining critical infrastructure elements adopted by the government of the Czech Republic [16], the following cross-cutting criteria were defined for a wider international debate within the RAIN project [15]:

- health impacts—the number of victims with a threshold value of more than 25 fatalities or more than 250 individuals hospitalized for a period exceeding 24 hours per 1 million inhabitants within the region under review;
- economic impacts with an economic loss threshold value of over 0.5% of gross domestic product; and
- impacts on the public with a threshold value of more than 12,500 individuals per 1 million inhabitants within the region under review affected by extensive restrictions in the provision of essential services or by other major disruptions to everyday life.

A provisional transformation of national criteria could form the basis for the setting of cross-cutting criteria values at the regional level (note: however, this method of setting regional values is not ideal in terms of applying the bottom-up approach as it is more akin to the top-down approach due to the transformation of national criteria). The transformation involves the dynamic conversion of threshold values for national cross-cutting criteria to regional criteria. This ratio is mainly applied as a proportion of the population of a given state to the population of the region concerned, and of the threshold values of national cross-cutting criteria to those of regional cross-cutting criteria. In principal, static threshold values are converted to dynamic values not only due to the varying population sizes in different regions, but also due to the different levels of gross domestic product generated in these regions [17].

European critical infrastructure risk and safety/security management comprises an important aspect of modeling the impacts of critical infrastructure failures. In adopting this approach, risks are recognized at an early stage, allowing for a timely indication of impacts on independent critical infrastructure subsystems. The following methodologies should be employed with a view to optimize the risk and safety/security management system and comply with the requirements for crisis preparedness plans applicable to critical infrastructures entities, as an equivalent to the Operator Security Plan:

- Methodology for selected CIs system resilience element evaluation [18]; and
- Methodology for ensuring the protection of CIs in the production, transmission, and distribution of electricity [19].

Implementation of a preferential critical infrastructure risk assessment provides another important basis for the modeling of impacts produced by critical infrastructure failures [20]. This allows the assessor to introduce subjective conditions into an otherwise objective process of risk assessment, providing the assessor with an option to partially influence the assessment process by preferring certain factors over others. The significance of this phase of the assessment process lies in the fact that different entities perceive certain risks from different points of view, which creates a conducive environment for discussion of all stakeholders, ensuring the most appropriate safety/security actions are taken. Moreover, a preferential critical infrastructure risk assessment also provides an important basis for the modeling of impacts of critical infrastructure failures as its results determine vulnerabilities enabling the propagation of impacts throughout the critical infrastructure system [13].

## 4. Resilience of critical infrastructure subsystems

The purpose of each critical infrastructure subsystem is to deliver services to recipients. It is therefore essential to ensure that each subsystem is fully functional and that appropriate steps are taken to minimize its failures and curtail the propagation of any potential impacts on society or any other dependent critical infrastructure subsystems. According to existing scientific knowledge, the best and most effective way of minimizing the impacts of critical infrastructure system failures is to reach the highest possible level of resilience with respect to all of its subsystems.

### 4.1. Definition of resilience

The term resilience was first defined in connection with the resistance and stability of ecological systems where two types of system behavior were identified [21]. The first type, stability, is the ability of a system to return to an equilibrium state after a temporary disturbance and the more rapidly it returns, the more stable it is. The second type of system behavior, known as resilience, is a measure of the ability of a system to absorb impacts without significant changes to the system status. Over time, this perspective was expanded to include the sphere of sociology, which then led to resilience being explored in socio-ecological systems. Based on the achieved results, the research into resilience gradually spread to other disciplines such as psychology, economy, and engineering.

In 2001, Holling shed light on understanding the complexity of economic, ecological, and social systems with the publication of a definition based on two fundamental components of each system, namely hierarchy and adaptive cycles [22]. Together they form panarchy according to Holling. Panarchy can be defined as a structure in which systems of nature and humans are interlinked in never-ending adaptive cycles of growth, accumulation, restructuring, and renewal.

The research into the resilience of socio-ecological systems also sparked an interest in research focused on resilience in society. The resilience of a society is dependent on its ability to respond to a stress factor and can be defined as *"The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management"* [23].

Resilience gradually began to be defined in general terms for any system, including engineering. Resilience was first described in connection with a critical infrastructure in a document entitled Critical Infrastructure Resilience Final Report and Recommendations [24], where it is defined as the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event. By contrast, the critical infrastructure resilience strategy [25] defines critical infrastructure resilience as the ability to reduce the magnitude and/or duration of a disruptive event. These definitions clearly show what constitutes resilience, or rather what characteristics enhance the resilience of a system. For example, Chandra [26], based on his study of socio-ecological systems, includes the following attributes in engineering systems resilience: redundancy, adaptability, flexibility, interoperability, and diversity.

As research into the resilience of critical infrastructures has since been pursued by numerous leading research workers and institutions, the definition of resilience has been repeated over and over again without any added value. However, the different approaches to determining their attributes/aspects/components/properties/characteristics/capacities/abilities/assets/parameters may be worth mentioning. Below are some examples of the different approaches:

- Ehlen et al. [27]—absorption, adaptation, and recovery.
- Keeping the country running [28]—the ability to anticipate, absorb, adapt, and/or rapidly recover. For the system to function as a whole, it must incorporate four assets or elements: resistance, reliability, redundancy, response, and recovery.
- Carlson et al. [29]—the form of linkages between six aspects (anticipation, resistance, absorption, ability to respond, adaptability, and recovery), which according to the author define resilience, and four parameters (preparedness, mitigation, response, and recovery), which characterize the process of enhancing the resilience capacity of a system.
- Béné et al. [30]—three basic aspects: absorptive capacity (the ability to cope with the impacts of adverse changes and shocks), adaptive capacity (the ability of a system to adapt to changes), and transformative capacity (the ability to create a fundamentally new system).

- Presidential Policy Directive—Critical Infrastructure Security and Resilience [31]—the ability to prepare, resist, and rapidly recover.
- Hromada et al. [32]—preparedness and adaptability as the basis for the fulfillment of the resilience function. Key indicators: robustness, preparedness, ability to respond, recoverability.
- Eid et al. [33]—the ability to anticipate, resist, absorb, respond, adapt, and rapidly recover from a disruption.
- Ortiz De La Torre et al. [34]—prepare, prevent, and protect (before the disruption), mitigate, absorb and adapt (during the disruption), and respond, recover and learn (after the disruption).
- Bologna et al. [35]—the overall activities of modeling, and analysis of critical infrastructure system aimed to evaluate the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made.
- Nan and Sansavini [36]—ability of the system to withstand a change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability), and by recovering from them (restorative capability).

Some experts consider critical infrastructure resilience to be the primary national policy framework and a vital criterion for the future sustainability of cities or infrastructures as such, and argue that, from a broader perspective, resilience is indispensable in terms of population protection and crisis management [33, 37].

### 4.2. Concept of critical infrastructure resilience

Based on the accepted definitions, resilience can be said to represent the level of internal preparedness of critical infrastructure subsystems for emergencies or the ability of these subsystems to perform and maintain their functions when negatively affected by internal and/or external factors. Strengthening resilience (e.g., Action Plan for Critical Infrastructure [38] or Labaka et al. [39]) minimizes the vulnerability of subsystems, which in turn curtails the occurrence, intensity, and propagation of failures and their impacts in a critical infrastructure system and society.

Understanding and clear definition of resilience represent the cornerstone of resilience assessment and strengthen with respect to critical infrastructure subsystems. In fact, critical infrastructure system resilience must be understood as a cyclic process based on continual strengthening of resilience of individual subsystems (see **Figure 6**). The crucial phases of this process are prevention, absorption, recovery, and adaptation.

The first phase of the critical infrastructure resilience cycle is prevention. In individual critical infrastructure subsystems, this is determined by permanent preparedness and protection of each subsystem. Prevention is provided on a continuous basis until a subsystem disruption occurs, at which time it is suspended, and for the duration of the emergency, replaced by absorption.

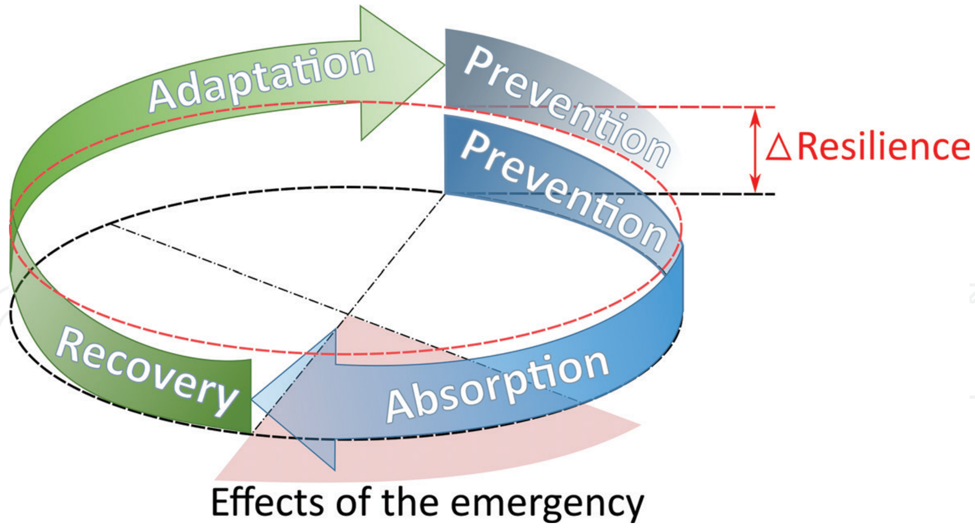

**Figure 6.** Cycle of critical infrastructure resilience.

Absorption, the second phase of the resilience cycle, is initiated if a subsystem is disrupted due to an emergency and is determined by the critical infrastructure subsystem robustness. Accordingly, robustness is determined by the ability of a critical infrastructure element to absorb the effects of an emergency. In a critical infrastructure system, two types of robustness are recognized, namely structural and security robustness. Structural robustness is determined by the progress in the decline of a function and the level of redundancy, while security robustness is based on the level of protective measures, detection, and ability to respond.

The recovery phase starts after the effects of an emergency have worn off. This phase is characterized by recoverability, which is the capacity of a subsystem to recover its function to the required level of performance after the effects of an emergency no longer exist. The success of recovery is determined by the available resources and the time required to complete the recovery process.

The final phase of the critical infrastructure resilience cycle is adaptation, which is essentially the ability of an organization to adapt a subsystem to subsequent effects of an emergency. It represents the dynamic long-acting 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 and innovation/education processes. However, strengthening of the resilience of a subsystem already occurs during the recovery phase of its performance.

### 4.3. Resilience assessment in a critical infrastructure system

The Resilience Assessment and Evaluation of Computing Systems compilation monograph [40] was the first comprehensive overview study exploring critical infrastructure resilience assessment in the field of information and communication technology. Another important monograph, Critical Infrastructure System Security and Resiliency [41], introducing a practical methodology for the development of an efficient system of critical infrastructure protection, was published a year later. This methodology focuses both on the prevention of emergencies and the mitigation of its consequences. The same year saw the publication of the Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience study [42], whose main objective is to measure the ability of a critical infrastructure to reduce the magnitude and/or duration of impacts from disruptive events.

In 2013, the European Commission published a working document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure [43]. This document clearly emphasized the importance of resilience and interdependencies in a critical infrastructure as well as the need to develop tools and methods for their assessment.

In addition, the issue of measuring critical infrastructure resilience has long been explored by the Swiss Federal Institute of Technology in Zurich (Eidgenössische Technische Hochschule Zürich). The institute presents the results of its risk and resilience research in the form of scientific reports, with the issue of resilience measurement addressed in detail in the SKI Focus Report 8: Measuring Resilience [44] and the SKI Focus Report 9: Measuring Critical Infrastructure Resilience [45].

There are also several major international projects dealing with critical infrastructure resilience assessment at present, including SMART RESILIENCE: Smart Resilience Indicators for Smart Critical Infrastructures, IMPROVER: Improved Risk Evaluation and Implementation of Resilience Concepts to Critical Infrastructure, RESILIENS: Realizing European Resilience for Critical Infrastructure, or RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems.

In 2016, a comprehensive approach based on the results of leading research projects was published in the Guidelines for Critical Infrastructures Resilience Evaluation document [35]. This approach has its basis in the evaluation of individual indicators constituting resilience, the resulting composite indicator being a function of indicators in technical (i.e., prevention, absorption, adaptation, and recovery), personal, organizational, and cooperative dimensions.

Additional significant approaches to evaluate resilience have been presented, for example, in an interim report of the project RESILIENS D2.2: Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement [34]. The second part of the document presents a critical infrastructure resilience assessment tool (CI-RAT), which has been developed as part of this project and is based on a semi-quantitative methodology for CI resilience assessment, and on a CI resilience management concept.

## 5. Conclusion

The chapter entitled "Failures in a Critical Infrastructure System" presents a comprehensive overview of a critical infrastructure system, which may be regarded as the basis for ensuring the functional continuity of society from both the economic and social perspectives. The introductory part of the chapter is designed as a historical framework, defining critical infrastructures in relation to legislative, normative, and institutional processes involved in addressing the issues concerned. The described framework formulates the basis, approaches, and logic of a hierarchical system arrangement in connection to interdependencies and linkages between elementary elements. Infrastructure failures have been classified in terms of their sources and causes because the potential impacts of failures in selected dependent systems can have profound effects on the functioning of society as a whole. It was argued that the impacts of failures in dependent systems increase the occurrence of cascading and synergistic effects, which fundamentally affect the resilience of individual elements and the general function of the system. This led to establishing the relationship between system resilience and failures with respect to critical infrastructure network elements.

Based on these facts, the impacts of failures and their propagation were described in the context of the necessity to model such impacts. In this regard, the significance and applicability of top-down and bottom-up approaches in relation to the exploration of mutual linkages was further compared as one of the identifiers describing the critical infrastructure status. The significance of identifying and labeling critical infrastructure elements is, therefore, also viewed from the perspective of the need for a more objective setting of cross-cutting criteria values, equally applicable at the regional level. As already mentioned, element resilience exerts a substantial effect on the overall impacts of potential failures. That is why a resilience framework for critical infrastructure subsystems was established with a view to defining resilience, formulating a resilience concept, and setting up a resilience evaluation process in a critical infrastructure system. The presented facts are based on the Ministry of the Interior of the Czech Republic Security Research project—RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems and form a resilience knowledge base as the ability of a system, community, or society exposed to adverse events to resist, absorb, accommodate, adapt to, transform, and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and recovery of its essential basic structures and functions through risk management.

## Acknowledgements

The chapter has been elaborated within the project of the Ministry of the Interior of the Czech Republic filed under VI20152019049 and entitled "Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems."

## Author details

David Rehak[1] and Martin Hromada[2]*

*Address all correspondence to: hromada@fai.utb.cz

1 Faculty of Safety Engineering, VŠB - Technical University of Ostrava, Czech Republic

2 Faculty of Applied Informatics, Tomas Bata University in Zlín, Czech Republic

## References

[1] European Union. 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

[2] Pesch-Cronin KA, Marion NE. Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective. London, United Kingdom: Taylor & Francis Group; 2017. p. 366

[3] Rehak D, Markuci J, Hromada M, Barcova, K. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. International Journal of Critical Infrastructure Protection. 2016;**14**:3-17. DOI: 10.1016/j.ijcip.2016.06.002

[4] The Department of Homeland Security. The National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, DC, USA: U.S. Department of Homeland Security; 2013. p. 50

[5] Pederson P, Dudenhoeffer D, Hartley S, Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Idaho Falls, ID, USA: Idaho National Laboratory; 2006. p. 116

[6] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine. 2001;**21**(6):11-25. DOI: 10.1109/37.969131

[7] Rehak D, Martinek B, Ruzickova P. Population Protection in the Context of Current Security Threats. Ostrava, Czech Republic: SPBI; 2015. p. 131

[8] Wilde WD, Warren MJ. Visualisation of critical infrastructure failure. In: Australian Information Warfare and Security Conference. Perth, Western Australia: Edith Cowan University; 2008. pp. 48-63. DOI: 10.4225/75/57a82a75aa0de

[9] Kotzanikolaou P, Theoharidou M, Gritzalis D. Cascading effects of common-cause failures in critical infrastructures. In: Butts J, Shenoi S, editors. Critical Infrastructure Protection VII. Berlin, Germany: Springer; 2013. pp. 171-182. DOI: 10.1007/978-3-642-45330-4_12

[10] Jonkeren O, Giannopoulos G. Analysing critical infrastructure failure with a resilience inoperability input–output model. Economic Systems Research. 2014;**26**(1):39-59. DOI: 10.1080/09535314.2013.872604

[11] Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Lykou G, Gritzalis D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. International Journal of Critical Infrastructure Protection. 2016;**12**:46-60. DOI: 10.1016/j.ijcip.2015.12.002

[12] Ouyang M, Dueñas-Osorio L, Min X. A tree-stage resilience analysis framework for urban infrastructure systems. Structural Safety. 2012;**36-37**:23-31. DOI: 10.1016/j.strusafe.2011.12.004

[13] Rehak D, Novotny P. Bases for modelling the impacts of the critical infrastructure failure. Chemical Engineering Transactions. 2016;**53**:91-96. DOI: 10.3303/CET1653016

[14] Rehak D, Hromada M, Ristvej J. Indication of critical infrastructure resilience failure. In: Čepin M, Briš R, editors. Safety and Reliability—Theory and Application (ESREL). Florida, London, United Kingdom: CRC Press; 2017. pp. 963-970

[15] RAIN Project [Internet]. 2015. Available from: http://rain-project.eu/about/the-scope-of-the-project/ [Accessed: 2017-07-01]

[16] Government Decree 432/2010 of 22 December 2010 on Criteria for Determination of the Critical Infrastructure Element

[17] Novotny P, Markuci J, Rehak D. Determination of the critical infrastructure elements at regional level. Spektrum. 2014;**14**(1):54-59

[18] Hromada M. Information support system development in relation to critical infrastructure element resilience evaluation. In: International Conference on Emerging Security Information, System and Technologies (SECURWARE); 24-28 July 2016; Nice, France. Wilmington, DE, USA: IARIA; 2016. pp. 174-184

[19] Methodology to Ensure of Critical Infrastructure Protection in the Area of Electricity Generation, Transmission and Distribution. Prague, Czech Republic: Deloitte Advisory; 2012. p. 55

[20] Rehak D, Senovsky P. Preference risk assessment of electric power critical infrastructure. Chemical Engineering Transactions. 2014;**36**:469-474. DOI: 10.3303/CET1436079

[21] Holling CS. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics. 1973;**4**:1-23. DOI: 10.1146/annurev.es.04.110173.000245

[22] Holling CS. Understanding the complexity of economic, ecological, and social systems. Ecosystems. 2001;**4**(5):390-405. DOI: 10.1007/s10021-001-0101-5

[23] United Nations Office for Disaster Risk Reduction. Terminology on Disaster Risk Reduction [Internet]. 2007. Available from: https://www.unisdr.org/we/inform/terminology [Accessed: 2017-07-15]

[24] Critical Infrastructure Resilience Final Report and Recommendations. Washington, DC, USA: National Infrastructure Advisory Council; 2009. p. 54

[25] Critical Infrastructure Resilience Strategy. Sydney, Australia: Commonwealth of Australia; 2010. p. 34

[26] Chandra A. Synergy between biology and systems resilience [thesis]. Rolla, MO, USA: Missouri University of Science and Technology; 2010. p. 134. Available from: http://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=7727&context=masters_theses

[27] Ehlen MA, Vugrin ED, Warren DE. Overcoming challenges in critical infrastructure resilience analysis: A new framework for resilience assessments. In: Workshop on Grand Challenges in Modeling, Simulation, and Analysis for Homeland Security (MSAHS-2010); 17-18 March 2010; Washington, DC, USA: U.S. Department of Homeland Security; 2010

[28] Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. London, United Kingdom: Cabinet Office; 2011. p. 98

[29] Carlson L, Bassett G, Buehring W, Collins M, Folga S, Haffenden B, Petit F, Phillips J, Verner D, Whitfield R. Resilience: Theory and Application. Argonne, IL, USA: Argonne National Laboratory; 2012. p. 60. DOI: 10.2172/1044521

[30] Béné C, Wood RG, Newsham A, Davies M. Resilience: New Utopia or New Tyranny? Reflection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes. IDS Working Papers. 2012;**2012**(405):1-61. DOI: 10.1111/j.2040-0209.2012.00405.x

[31] The White House. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. Washington, DC, USA: The White House; 2013

[32] Hromada M, Lukas L, Matejdes M, Valouch J, Necesal L, Richter R, Kovarik F. The System and Approach to Critical Infrastructure Resilience Evaluation. Ostrava, Czech Republic: SPBI; 2014. p. 177

[33] Eid M, Serafin D, Barbarin Y, Kuligowska E, Soszyńska-Budny J, Kolowrocki K. A resilience model based on Stochastic Poison Process. In: Summer Safety and Reliability Seminars (SSARS); 21-27 June 2015; Gdansk, Poland. 2015. DOI: 10.13140/RG.2.1.2418.3766

[34] Ortiz De La Torre P, et al. Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement (Project Report). Dublin, Ireland: Future Analytics; 2016. p. 138

[35] Bologna S, Carducci G, Bertocchi G, Oliva G, Traballesi A, Carrozzi L, Cavallini S, Lazari A. Guidelines for Critical Infrastructures Resilience Evaluation. Roma, Italy: Italian Association of Critical Infrastructures' Experts; 2016. p. 101

[36] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety. 2017;**157**:35-53. DOI: 10.1016/j.ress.2016.08.013

[37] Gross B, Weichselgartner J. Modernes Risikomanagement: Zwischen Robustheit und Resilienz. Bevölkerungsschutzmagazin. 2015;**1**:12-17

[38] Public Safety Canada. Action Plan for Critical Infrastructure (2014-2017). Ottawa, Canada: Public Safety Canada; 2014. p. 14

[39] Labaka L, Hernantes J, Sarriegi JM. A framework to improve the resilience of critical infrastructures. International Journal of Disaster Resilience in the Built Environment. 2015;**6**(4):409-423. DOI: 10.1108/IJDRBE-07-2014-0048

[40] Wolter K, Avritzer A, Vieira M, van Moorsel A, editors. Resilience Assessment and Evaluation of Computing Systems. Berlin, Germany: Springer Heidelberg; 2012. p. 490. DOI: 10.1007/978-3-642-29032-9

[41] Biringer B, Vugrin E, Warren D. Critical Infrastructure System Security and Resiliency. London, United Kingdom: CRC Press; 2013. p. 229. DOI: 10.1201/b14566

[42] Petit F, Bassett G, Black R, Buehring W, Collins M, Dickinson D, Fisher R, Haffenden R, Huttenga A, Klett M, Phillips J, Thomas M, Veselka S, Wallace K, Whitfield R, Peerenboom J. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Argonne, IL, USA: Argonne National Laboratory; 2013. p. 56

[43] European Union. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. Brussels, Belgium: European Commission; 2013. p. 17

[44] Prior T, Hagmann J. SKI Focus Report 8: Measuring Resilience. Zurich, Switzerland: Eidgenössische Technische Hochschule Zürich; 2012. p. 25

[45] Prior T. SKI Focus Report 9: Measuring Critical Infrastructure Resilience. Zurich, Switzerland: Eidgenössische Technische Hochschule Zürich; 2015. p. 13