Methodology for quantitative assessment of critical infrastructure resilience

Oleg Tretyakov[1,†], Batyr Khalmuradov[1,*,†], Maksym Pukha[2,†], Viktoriia Sydorenko[1,3,†], Larysa Chubko[1,†] and Vitaliy Nechiporuk[1,†]

[1] *National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine*

[2] *State Service for Special Communications and Information Protection of Ukraine, Solomianska St., 13, Kyiv, 03110, Ukraine*

[3] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zalizniak Str., 3/6, Kyiv, 03142, Ukraine*

Abstract

A methodological approach is proposed to quantify the level of resilience of critical infrastructure facilities, regardless of the critical infrastructure sector to which they belong and all types of project threats. The proposed approach makes it possible to conduct a resilience analysis for all elements of a critical infrastructure facility, conduct a comparable analysis of the vulnerability and resilience of sector facilities, assess the amount of additional investment required to reduce the vulnerability and increase the resilience of facility elements, develop sectoral programmes to improve the resilience of sector facilities, and determine the necessary territorial reserve resources and their volumes.

Keywords

resilience, critical infrastructure, quantitative assessment

1. Problem statement

According to the Law of Ukraine "On Critical Infrastructure" [1], critical infrastructure is defined as infrastructure, systems, their parts and their aggregate, which are important for the economy, national security and defence, and whose disruption may harm vital national interests.

The resilience of critical infrastructure is defined as the state of critical infrastructure that ensures its ability to function normally, adapt to constantly changing conditions, withstand and quickly recover from threats of any kind. The concept of resilience has been developed and applied in a variety of fields (psychology, psychiatry, ecology, social sciences, economics and engineering) for several decades [2, 3], and has recently gained increasing attention in the risk management field. In particular, the critical infrastructure community has evolved from a primary focus on security protection in the 1990s to a broader emphasis on safety and resilience [4, 5].

In the field of national security, to define national policies to strengthen and maintain safe, functional and resilient critical infrastructure in sectors that are important for national security, public health and safety, economic viability and overall quality of life. Resilience is defined as the ability to prepare for and adapt to changing conditions, as well as to withstand disruptions and recover quickly from them, including deliberate attacks, accidents or natural hazards [6].

The resilience of a community or region is a function of the resilience of its subsystems, including critical infrastructure, economy, civil society and governance. As noted in the Community Resilience

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

mega_ovtr@ukr.net (O. Tretyakov); batyrk@ukr.net (B. Khalmuradov); mspuha@gmail.com (M. Pukha); viktoriia.sydorenko@npp.nau.edu.ua (V. Sydorenko); larysa.chubko@npp.nau.edu.ua (L. Chubko); vitalij.nechyporuk@kitu.nau.edu.ua (V. Nechiporuk)

0000-0002-0457-9553 (O. Tretyakov); 0000-0003-2225-6528 (B. Khalmuradov); 0009-0009-4794-9436 (M. Pukha); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-4647-3156 (L. Chubko); 0000-0003-3580-9953 (V. Nechiporuk)

Planning Guide published by the National Institute of Standards and Technology, buildings and infrastructure play an important role in ensuring the health and vitality of a community's social and economic fabric [7]. Achieving resilience can be challenging because of the highly complex dependencies and interdependencies that exist in infrastructure systems, the geographic scope and jurisdictional boundaries within which infrastructure systems operate, the distributed ownership of infrastructure, the distributed responsibility for risk management, and the potential for failures to cascade across systems [8].

Infrastructure resilience depends on both the physical characteristics of the engineered infrastructure systems and the capabilities of the organisations that influence the operation and management of these systems (e.g. infrastructure owners and operators, regulators, suppliers and contractors). Infrastructure resilience can be assessed at the asset, system or system of systems level. Resilience is also influenced by organisational factors such as the existence of business continuity and contingency plans, the level of staff training, the frequency of exercises to test plans, the flexibility of staff working hours, and internal and external communication capabilities. All of this requires a unified approach to quantify the resilience of critical infrastructure, especially when the country recognises 24 sectors of critical infrastructure.

2. Analysis of recent research and publications

Definitions of resilience vary considerably by author and discipline. Some of these differences are related to the focus of the definition on a specific entity (e.g., enterprise resilience; system resilience; community resilience). Other definitions of resilience emphasise different time periods (e.g. resilience focusing on measures taken before and after a disaster). To understand infrastructure resilience from a regional perspective, the definition of resilience is a logical and widely used option.

The main elements of this definition - the ability to prepare for and adapt to changing conditions, as well as to withstand and recover quickly from disruptions - can be described by four building blocks: preparedness, mitigation measures, response capacity, and recovery mechanisms.

Together, these four pillars can help practitioners break down the concept of resilience into practical steps and ultimately measure progress in improving resilience over time. Table 1 describes these pillars and provides examples for consideration [9, 10].

This approach does help experts to break down the concept of resilience into practical steps and to conduct a qualitative assessment of the resilience of critical infrastructure. However, it does not allow for a comparative analysis of the resilience of critical infrastructure, especially if they belong to different sectors of critical infrastructure.

The purpose of the research is to develop a methodological approach to quantify the level of resilience of critical infrastructure facilities, regardless of the critical infrastructure sector to which they belong and all types of project threats.

3. Results of the research

To overcome the difficulties in considering the components of resilience and concentrating them in the context of infrastructure operations from a time perspective, it is possible to consider the operation of a critical infrastructure facility as a function of the volume of service provision over time under different conditions, especially under the influence of a hazard (natural, man-made, terrorist, military), as shown in Figure 1.

Until a hazardous event occurs, the critical infrastructure facility operates in a steady state and provides services in the design scope. From the moment a hazardous event occurs: a natural disaster (earthquake, landslide, flood, etc.), man-made accidents, unauthorised interference, cyberattack, terrorist act, military attack, etc., the volume of services provided by the critical infrastructure facility is sharply reduced or stopped altogether (t_1). This is followed by a period of preparation for the restoration of the facility's functioning (design work, concentration of the necessary material resources, engagement of contractors, etc.), which precedes the restoration work, after which the facility's capacity is restored with a gradual return to a sustainable mode of service provision in the design volume.

Table 1
Components of Resilience

Components	Description	Examples
Readiness	Activities aimed at anticipating relevant threats/hazards and possible consequences of their occurrence, including prevention and protection measures; indicates the adaptability of infrastructure systems and the process of integrating and incorporating lessons learned	• Maintenance of security forces • Establishing/monitoring physical access control • Develop continuity plans, contingency plans and cyber security plans • Train staff on the plans • Conduct regular drills to test the plans • Establish information sharing mechanisms
Mitigating the consequences	Activities aimed at countering and/or absorbing the negative effects of an event, reducing the severity or consequences of a threat; indicates the reliability of the infrastructure.	• Modernisation of facilities to mitigate the effects of various natural hazards (e.g. flood control equipment, flood barriers) • Modernisation of equipment to withstand foreseeable hazards • Improving the reliability/redundancy of infrastructure support systems • Establishment of an alternative backup site that can continue operations after an incident and facilitate recovery • Understanding cross-sectoral dependencies on key external resources (e.g., electricity, fuel, water, communications) • Prepare additional supplies (e.g. fuel, backup generators, backup communications) in advance
Response	Measures and programmes implemented or developed to respond to and adapt to the negative consequences of an event; indicates the resourcefulness of infrastructure owners and operators in managing crisis situations	• Maintaining on-site response capabilities to key hazards (e.g. chemical spills, fires, explosives, armed attacks, medical emergencies) • Building relationships with local first responders and cross-sector partners • Have the capacity to manage contingencies on site, including trained staff, a functional operations centre and an understanding of cross-cutting issues
Recovery	Activities and programmes to help organisations return to an acceptable level of working conditions and recover from an event; demonstrates the ability to resume service delivery quickly	• Establish priority recovery agreements with key service providers • Estimating the time and activities required to restore full organisational operations after a disruption • Strategies for rapid replacement/repair of critical components (e.g., certified vendors, maintaining emergency stocks)

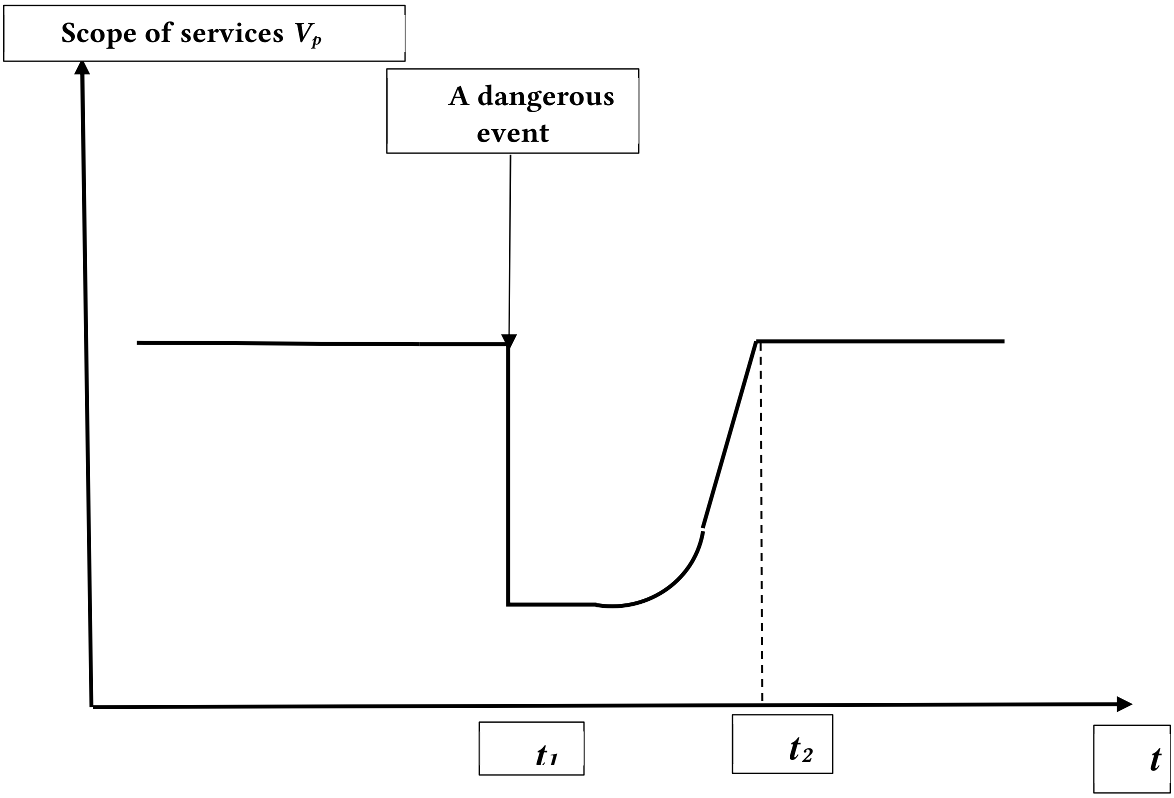

Figure 1: Dependence of the volume of service provided by a critical infrastructure facility on time under the influence of a hazardous factor.

The initial stage after a hazardous event is a type of disaster manifestation in the theory of disasters [11]. A "fold" type disaster $(x^3 + ax)$– is one of the simplest disasters. In this case, the standard deformation (drop in the level of services) is given by the formula:

$$V_p(t) = \frac{t^3}{3} + at, \tag{1}$$

where V_p is the scope of the service; t is time.

The numerical coefficient is introduced to simplify further calculations. The multivariety M of such a catastrophe is defined by equation:

$$0 = \frac{d}{dt} V_t(t) = t^2 + a, \tag{2}$$

The loss of service provision by a critical infrastructure facility as a result of a hazardous event will be determined:

$$W = \int_{t_1}^{t_2} V_p\, f(t), \tag{3}$$

and will characterise the vulnerability of the critical infrastructure facility.

The resilience of a critical infrastructure facility (or its part, subdivision, etc.) can be defined as the product of the time to full recovery and the costs associated with restoring the volume of services to the baseline:

$$S_i = \Delta t \cdot \sum E_i, \tag{4}$$

where Δt is time to fully restore the critical infrastructure facility (or its part, subdivision, etc.); $\sum E_i$ – all recovery costs (financial, material, energy, human, transport, etc.).

For convenience, the costs of restoring a critical infrastructure facility (or its part, subdivision, etc.) can be taken not as an absolute value, but as a share of the facility's design cost.

If the quantitative assessment of the risk of hazardous events is carried out on the basis of a simulation model to assess the threat of cascading effects for different scenarios in the area of the critical infrastructure facility, which provides for the following procedures:

- Determination of events in the scenario of the situation development (constituent elements of the scenario that have a potential impact on the realisation of the threat).
- Determining the set of possible states of events that affect the threat level.
- Formation of threat development scenarios (identification of links consisting of pairs: "event - transition to a given state") that lead to the realisation of the threat, presentation of a structural and logical model of the development of a crisis situation that has a complex structure according to different scenario options at a critical infrastructure facility.
- Formation of a threat scenario organisation chart (a structural and logical model that includes all threat scenarios).
- Estimation of probabilities of event states and their transitions.
- Assessing the likelihood of threat scenarios being realized.

The use of such a simulation model for cascading effects makes it possible to obtain probabilistic assessments of the development of events under certain scenarios and allows for the assessment of threats to a critical infrastructure facility by the probability of events and transitions between them.

Based on the obtained values of the probability of occurrence of hazardous events for all elements of the critical infrastructure facility, we identify the most vulnerable ones and conduct a quantitative assessment of their resilience. This makes it possible to assess the necessary resources (financial, material, energy, human, transport, etc.) to increase resilience. Identify the necessary backup elements to avoid cascading effects and undesirable consequences.

This approach is appropriate for a critical infrastructure facility:

- Conduct a sustainability analysis for all elements of the facility.
- To determine the vulnerability and resilience of each in the event of any threats in quantitative terms.
- Identify the most vulnerable and least resilient elements of the facility.
- Estimate the amount of additional investment required to reduce vulnerability and increase the resilience of facility elements.
- Determine the necessary reserve resources and their volume.

For a sectoral body in the field of critical infrastructure protection:

- Conduct comparable analyses of the vulnerability and resilience of sector facilities.
- Identify the most vulnerable and least resilient.
- Develop a sectoral programme to improve the resilience of sector facilities.
- Identify investment priorities to improve the resilience of sector facilities.

For territorial communities:

- Conduct a resilience analysis for all critical infrastructure facilities.
- Identify the most vulnerable and least resilient in the community.
- Develop a territorial programme to improve the resilience of critical infrastructure facilities.
- Identify the necessary territorial reserve resources and their volume.
- Estimate the amount of additional investment required to reduce vulnerability and increase the resilience of critical infrastructure in the community.

The proposed approach can be used to develop Methodological Recommendations for assessing the resilience of critical infrastructure facilities for the development of sectoral programmes to improve their resilience.

4. Conclusions

Based on the theory of catastrophes, a unified methodological approach has been developed to quantify the level of resilience of critical infrastructure facilities, regardless of the critical infrastructure sector to which they belong.

The proposed approach makes it possible to conduct a resilience analysis for all elements of a critical infrastructure facility, conduct a comparative analysis of the vulnerability and resilience of sector facilities, assess the amount of additional investment required to reduce the vulnerability and increase the resilience of facility elements, develop sectoral programmes to improve the resilience of sector facilities, and determine the necessary territorial reserve resources and their volumes.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Law of Ukraine "On Critical Infrastructure" of 16.11.2021 No. 1882-IX as amended on 01.01.2024 (1909-IX). URL: https://zakon.rada.gov.ua/laws/show/1882-20.

[2] C. S. Renshler, A. E. Fraser, L. A. Arendt, G. P. Cimellaro, A. M. Reinhorn, M. Bruno, A framework for defining and measuring community-based resilience: the people-based resilience framework, National Institute of Standards and Technology, 2010. URL: https://hsdl.org/?view&did=790013.

[3] A. Rose, Economic resilience to disasters, CARRI Research Report 8 (2009).

[4] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings 2255 (2018) 193–204. URL: https://ceur-ws.org/Vol-2255/paper18.pdf.

[5] J. S. Al-Azzeh, M. Al Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10(5) (2017) 328–336. doi: 10.15866/iremos.v10i5.12009.

[6] APCBI, "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience". 2013. URL: https://cisa.gov/national-infrastructure-protection-plan.

[7] NIST (National Institute of Standards and Technology), Community Disaster Resilience Planning Guide for Buildings and Infrastructure Systems: Volume 1, May 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.119 0v1.pdf.

[8] N. S. Kuzmenko, I. V. Ostroumov, K. Marais, An accuracy and availability estimation of aircraft positioning by navigational aids, in: Proceedings of 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), IEEE, Kiev, Ukraine, 2018, pp. 36–40. doi: 10.1109/MSNMC.2018.8576276.

[9] J. L., Carlson, R. A. Huffenden, G. W. Bassett, W. A. Behring, M. D. Collins, III, S. M. Folga, F. Petit, J. A. Phillips, D. R. Werner, R. Whitfield. Resilience: Theory and Applications, USA, 2012. doi: 10.2172/1044521.

[10] D. Mi et al., Demonstrating immersive media delivery on 5G broadcast and multicast testing networks, IEEE Transactions on Broadcasting 66(2) (2020) 555–570. doi: 10.1109/TBC.2020.2977546.

[11] J. Thompson, T. Michael, Instabilities and Catastrophes in Science and Engineering, New York, Wiley, 1982.