

CRITICAL INFRASTRUCTURE RESILIENCE ASSESSMENT AS A SOURCE OF REQUIREMENTS FOR THE SECURITY SYSTEMS DEVELOPMENT

Valeri Panevski

Received on November 15, 2024

Presented by Ch. Roumenin, Member of BAS, on November 26, 2024

Abstract

Critical infrastructure can be affected by, or cause, disruptive events and incidents. Some of these events are internally system-manageable, but others must be addressed by additional implementation of appropriate security measures.

One of the appropriate solutions to deal with disruptive events or incidents involves improving the organizational resilience of critical infrastructure. Consideration of the possibility of the results of the resilience assessment being used as input data for the development of CI security systems, including physical security, is the content of this publication.

Key words: organizational resilience, security systems

Introduction. Critical infrastructure (CI) is of particular importance to national security because of the potential for cascading effects on other essential state functions. CI is exceptional not only in its meaning, but it is also specific

This paper is the result of implementation of the scientific work of the author, as a part of the IMSETHC-BAS team, participating in Work package 2 “Intelligent security systems”, Project BG05M2OP001-1.002-0006 Competence Center “Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)”, funded by the European Regional Development Fund through the Operational Programme “Science and education for smart growth”, co-financed by the European Union through the European Structural and Investment Funds.

<https://doi.org/10.7546/CRABS.2024.12.08>

in its structuring, the established and developing cross-sectoral connections, as well as the specificity of the elements and the technical nature of the creation and provision of goods and services. All these, as well as many other aspects, imply the possibility that the CI will be exposed to risk events or will itself cause them. One of the appropriate solutions to deal with disruptive events or incidents is the CI resilience principle, which is confirmed by a number of authors who focus on resilience research. Resilience is generally seen as the ability to reduce the magnitude and duration of the impact of disruptive events. The effectiveness of resilient CI depends on its ability to anticipate, absorb, adapt and rapidly recover from a potentially disruptive event. The main components of resilience are durability, strength, recoverability and adaptability.

The built CI, according to the specifics of its mission, already has some of these components and characteristics in some form, which are natural or acquired through technological and technical design. However, strengthening the resilience of CI elements requires strengthening other determinants of resilience. This means that the natural or technologically acquired properties of the system are not sufficient. Moreover, some of the main components of resilience, such as adaptability, are exclusively aimed at strengthening it. Strengthening CI resilience therefore represents a significant challenge.

At its core, CI resilience building is based on a resilience assessment, the findings of which provide inputs for the development of security systems. Without effective resilience assessment, it is not possible to assess whether resilience strengthening has been effective.

This publication does not address the different approaches and methodologies for resilience assessment, but only the possibility that the conclusions of the assessment can be applied to formulate requirements for the development of security systems of CI or its critical elements.

Security management and resilience. *Security management.* Defining clear functional conditions for building and strengthening the resilience of critical infrastructure subsystems related to design, time and resources can be understood as the overall concept of resilience of these CI subsystems. Also, the establishment of the security management process of the CI elements, including the resilience strengthening framework, can be seen as a key initial condition. Rather, the main functional condition is the unambiguous specification and perception of the factors determining the resilience of CI.

The security management process for CI elements is an adaptation of principles based on a continuous management cycle based on the Deming cycle [1].

The correct structuring of the criteria for identifying a CI (including the designation as European or national) and its *critical infrastructure elements* is the initial step of security management. In this phase of the process, it is important to consider the appropriateness of applying an appropriate approach to identifying critical elements, which can be based on a top-down or bottom-up approach.

The logical next step is the evaluation of the CI critical element. The main objective of this activity being the risk assessment, consisting of the assessment of the relevant scenarios of disruptive events and the resilience assessment of the relevant element (assessment of its robustness, recoverability and adaptability).

Ensuring the required security levels of CI elements is the final step of the security management process, consisting of *risk management* and *resilience improvement*. Risk management involves the selection and implementation of one or more risk minimization options – risk retention, risk transfer and/or risk avoidance (ISO/IEC 27001 – Information security management). Resilience improvement minimizes the vulnerability of subsystems, which in turn limits the occurrence, intensity and spread of failures and their impact on CI and society. The main functional condition for improving the resilience of CI subsystems is the categorical specification and perception of the factors that determine it. In this context, CI resilience should be understood as a cyclical process of continuous improvement of prevention, absorption, recovery and adaptation.

Resilience. CI resilience is determined by two main areas, namely technological and physical element protection and organizational management.

The resilience of technological and physical protection of individual elements, known as *technical resilience*, is determined by the strength and the ability to restore the elements of the system. The increase in technical stability is achieved exclusively in relation to a specific element or a group of identical or very similar elements. A good example is the electricity sector, where resilience and recovery will be ensured in different ways and by different means depending on whether it concerns electricity generation systems or electricity transmission and distribution systems.

Technical resilience is influenced by the following main factors: technological structure of the element; security measures of the item and destructive events that affect the durability of the element.

The resilience of the organization's management, known as *organizational resilience*, is determined by the level of the organization's internal processes, the main purpose of which is to create optimal conditions for adapting critical infrastructural elements to disruptive events.

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

Organizational resilience is of primary importance for the development of security systems, since technical resilience is embedded in the design and technological documentation of both CI equipment and the products and systems that are manufactured and delivered to stakeholders. Therefore, the *adaptability* of the organization to the dynamics of the risk factors that may affect the resilience are

of fundamental importance for the structure, functionality and integration of the necessary security systems.

Adaptability represents the long-term and dynamic ability of CI to adapt to changes in circumstances and is determined by internal processes aimed at creating optimal conditions for strengthening resilience. The main processes that improve the adaptability of CI elements to disruptive events are *risk management*, innovation processes and process of learning.

Risk Management (RM) is an important internal process of the organization that is essential to ensure security and strengthen resilience in the prevention phase. RM consists of coordinated activities to guide and control an organization in terms of risk, and its level in terms of organizational resilience is determined by the criteria, shown in Fig. 1.

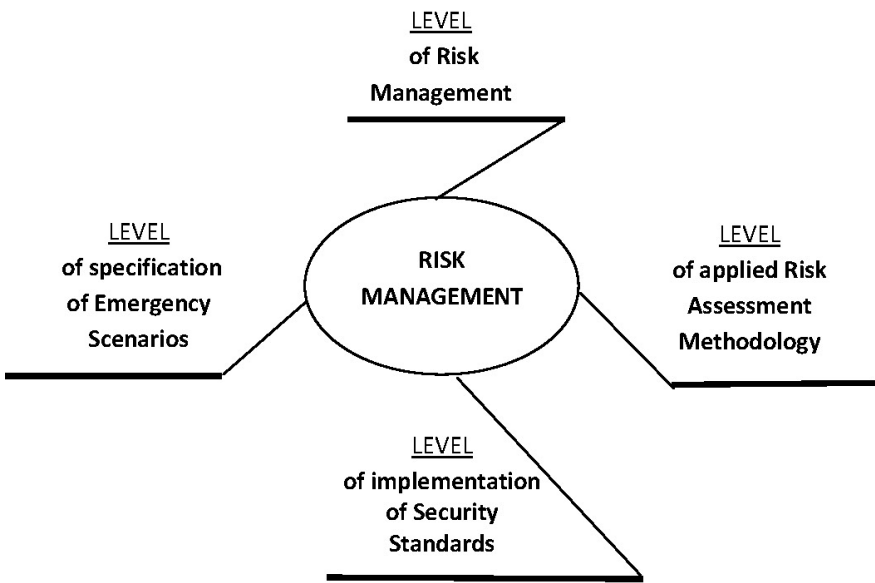


Fig. 1. RM criteria in the scope of the organization's resilience

The *organization's innovation processes* are additional internal processes that significantly contribute to strengthening the resilience of CI elements at the prevention stage. From a strictly practical point of view, innovations are categorized as product innovations, process innovations, marketing innovations and organizational innovations. In terms of increasing resilience, organizational innovation is particularly important as it focuses on the reliability and security, external and internal, of the organization. The innovation process itself consists of three main phases, which are: invention, science and research, and application.

Education and development processes form the last group of processes that build and strengthen organizational CI resilience, thus improving the organization's ability to adapt these elements to the effects resulting from disruptive events.

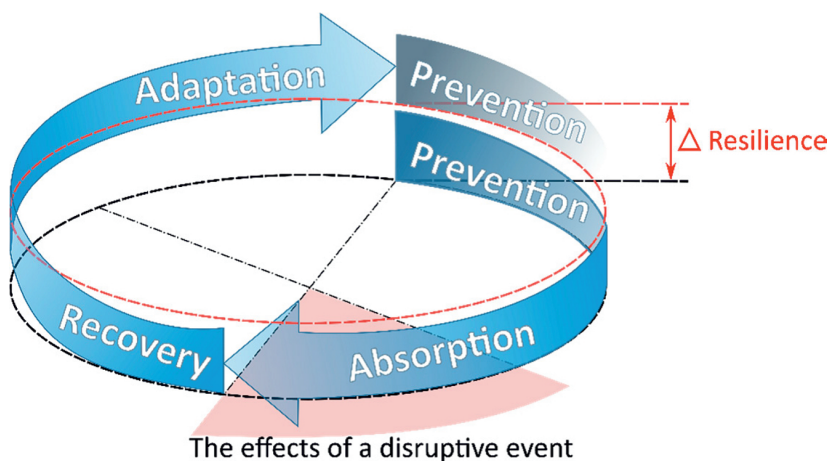


Fig. 2. Critical infrastructure resilience cycle improvement [2]

Resilience improvement. Good international practice shows that the right approach is to consider the improvement of CI resilience as the result of realizing the cyclical process of continuous improvement of prevention, absorption, recovery and adaptation. A good example in this direction is the cycle presented in Fig. 2 [2], within which the resistance improves from its initial level, limited by the black dashed line, to the new red dashed line. The difference between these two levels, “ Δ ”, is understood as the extent to which resilience is improved.

At the same time, the design, development and coordination of management disciplines and their alignment with the strategic objectives of CI are fundamental to the level of improvement of organizational resilience.

Management disciplines and CI resilience. According to item “4.1 General” of ISO 22316:2017 [3], the general principles that provide the basis for improving the organizational resilience and are closely related to the process of developing security systems state that resilience “is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise” and “relies upon effectively managing risk”.

Also, the design, development and coordination of management disciplines and their alignment with the organization’s strategic goals are fundamental to improving organizational resilience, which gives complex importance to the development of security systems. In “Annex A” to item “5.8 Development and coordination of management disciplines” [3], an example list of 20 management disciplines is given, of which I can point out as directly related to the development of security systems: “... business continuity management”; “... risk management” and “... physical security management”.

The international experience, communicating good practices in the field of management disciplines, finds its communication and acceptance in the standards of the International Organization for Standardization (ISO) (see Table 1).

T a b l e 1

Management disciplines [3] closely related to the development of security systems

Management disciplines	ISO standards
Business Continuity Management	– ISO 22300 – Security and resilience – Vocabulary; – ISO 22301 – Security and resilience – Business continuity management systems – Requirements; – ISO 22313 – Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301; – ISO 22317 – Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA);
Physical Security Management	ISO 27001 – Annex A.11: Physical & Environmental Security;
Risk Management	– ISO 31000 – Risk management – Guidelines – ISO/IEC 31010 – Risk management – Risk assessment techniques; – ISO/TS 31050 – Risk management – Guidelines for managing an emerging risk to enhance resilience

Resilience assessment as a source of requirements for the development of CI security systems. Organizational resilience assessment “... helps to identify the signs of an emerging issue or an opportunity that requires attention ...” [3] as well as to propose ways to overcome them, including and by building security systems. The CI management is responsible to “... monitor the effectiveness of initiatives established for the management of risk, including those managed by established management disciplines” [3].

As a result of the resilience assessment, it is expected to receive objective information about:

- the possible risk events, external and internal, that would affect the CI or its structural elements;
- critical structural elements of CI, the impact on which would disrupt mission performance;
- the ways to prevent, accept or recover from possible risk events impact;
- the functional characteristics of the security systems, including physical security systems.

As a result of the sustainability assessment, regardless of the applied methodology according to the specifics of CI, input data are obtained for the type, structure, and integration of the elements of the security system in the general CI management system, as well as the business model for their development [4].

The application of the approach of using the results of the CI resilience assessment as a source of data for the development of security systems was closely related

to the implementation of the activities of WP2 “Intelligent security systems” of the QUASAR project and its development continues, through the implementation of tasks in the field of the mechatronic security systems modelling, study of acoustic and surface seismic waves created by anthropogenic sources and, last but not least, nuclear security [5, 6], in accordance with the Plan for scientific research activity in 2023–2025 of the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A. Balevski” at the Bulgarian Academy of Sciences.

Conclusions. CI, as a provider of essential services, plays an important role in maintaining vital social functions or market economic activities in an increasingly interconnected economy. Therefore, it is extremely important to improve the CI resilience by establishing harmonized rules through guidance documents at international and national level, including through ISO standards. An essential part of strengthening CI resilience is risk assessment of the likely impact of natural and anthropogenic risks, including those of a cross-sector or transboundary nature, accidents, natural disasters, public health emergencies and hybrid or other hostile threats, including terrorist crimes. The findings of the risk assessment, closely related with the resilience assessment, provide the necessary data for the development of a CI security system, as well as the related business model development activities.

REFERENCES

- [1] <https://deming.org/explore/pdsa/>.
- [2] REHAK D., P. SENOVSKY, S. SLIVKOVA (2018) Resilience of critical infrastructure elements and its main factors, *Systems* 2018, **6**(2), 21, <https://doi.org/10.3390/systems6020021>, www.mdpi.com/journal/systems.
- [3] ISO 22316:2017(en) Security and resilience – Organizational resilience – Principles and attributes.
- [4] PANEVSKI V. (2024) Possible interaction of the security systems development business model with the organization’s vulnerability management, *Danish Sci. J.*, **83**, 63–66, <https://doi.org/10.5281/zenodo.11097923>.
- [5] DIMITROV D., N. RANDELOVA (2024) Management systems for nuclear security, *International Scientific Journal “Security&Future”*, STUME, **8**(1), 7–10.
- [6] DIMITROV D., N. RANDELOVA (2024) Introduction in the management system at Kozloduy NPP supporting Process 8 “Training and qualification”, *International Scientific Journal “Security&Future”*, STUME, **8**(1), 15–17.

Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A. Balevski”, Bulgarian Academy of Sciences, 67 Shipchenski Prohod St, 1574 Sofia, Bulgaria
e-mail: panevski@ims.bas.bg