

APPLICABLE INTERNATIONAL STANDARDIZED BASIS
IN DEFINING DATA FOR SECURITY SYSTEMS
DEVELOPMENT

Valeri Panevski

Received on May 29, 2024

Presented by Ch. Roumenin, Member of BAS, on June 25, 2024

Abstract

Creating an intelligent security environment is one of the main trends in the activity of scientific organizations, where security technologies are a significant part of the product range. Organizations using these technologies, including critical infrastructure with built-in security systems, provide increased operational efficiency, guaranteeing readiness for action in emergency situations. For this purpose, standardized approaches are applied to determine the requirements for the development of security systems, according to the specifics of the organization, ensuring the prevention of any level of potential consequences of possible risk events, both in the structural objects of the organization and for the population in the adjacent territories.

The author's intention is through this publication to present his experience in the application of modern standardized approaches ensuring the construction and operation of critical infrastructure security systems developed by scientific organizations in the conditions of key partnerships of the Competence Center.

Key words: standardized basis, security systems

This paper is the result of implementation of the scientific work of the author as a part of the IMSETCH-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.2024.08.10>

Introduction. Currently, modern international standards have been developed, summarizing good international practices, for determining the goals and/or security requirements, in accordance with the characteristics of the critical infrastructure (CI). The formulation of requirements for physical security systems, as an element of security systems of CIs, has a significant impact on the functioning of CIs with advantages that include greater resilience and mobility of systems, and accessibility to users.

An essential aspect in the development of the security systems is the security regime of the organization. Threat information is used to define the CI security regime as a basis for developing common requirements and performance objectives, as well as criteria for assessing the compliance or effectiveness of security.

CI operators with an innovative vision realize large-scale innovations related to making demanding decisions that can help them keep up with the technological pace of security. They are looking for simplified, standardized processes and enhanced visibility to create a security environment, streamlined operations and a dynamic, accurate understanding of the organization's security posture. The goal is to gain insight into possible operational risks occurring now and those that could occur later so they can make better decisions to maintain the safety and productivity of manufacturing operations.

To properly define the appropriate inputs, it is useful to pay attention to good international practice in the field of business continuity development. Also, this publication does not address the responsibilities of national operators for the implementation of different approaches to physical protection (including systems), according to the specifics of the respective CIs and the requirements of the leading international organizations, as they are assumed to be predefined and are implemented and updated periodically.

Last but not least, the implementation of international standards in the field of security and resilience is the basis of the good results achieved as a result of the scientific and applied activity of the author, as a member of the team of IMSETCH-BAS, participating in Work package 2 "Intelligent security systems" under the QUASAR project.

Business impact analysis as a data source for security systems. The main source of data for development of the security systems are the "Business Impact Analysis" (BIA) and "Risk Analysis" stages of the development of business continuity management systems (ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements).

To be able to understand the essence of BIA, it is important to know the definition of BIA, namely – "business impact analysis – process of analyzing the impact over time of a disruption on the organization" [1].

The analysis of the impact on the activity is carried out in accordance with ISO/TS 22317:2021 Security and resilience – Business continuity management systems – Guidelines for business impact analysis, essentially BIA is a functional anal-

ysis that is implemented as part of the continuity of the activity (ISO 22301:2019), in which the assessment and calculation of the qualitative and quantitative impacts on the CI's activity as a result of a probable risk event (natural disaster or man-made destruction).

Qualitative impacts relate to operational aspects such as the ability to perform, while quantitative impacts relate to financial losses and have a numerical monetary value. CIs should conduct a detailed and in-depth BIA to help their business and operational units understand the impact of a potential risk event. The BIA should list the critical and necessary business functions, their resource dependencies, and the level of criticality to the entire organization. The development of the Business Continuity Management Plan is based on BIA which helps the organization understand the impact of a devastating event on the organization.

BIA is a management-level analysis that identifies the impact of the loss of resources on the organization, involving four main steps: identification of critical processes and resources; identifying the impact of the disruption and assessing the disruption; identifying resource requirements and identification of recovery priorities.

As a result of the BIA, it is determined for which risk assets a security system should be provided, the requirements for it are formulated (according to the specifics of the risk asset) and its integration into an existing security system of CI.

Risk analysis. Due to the dynamic nature of the CI security function, it is strongly recommended that the risk analysis process be reviewed systematically, resulting in the identification of areas for improvement.

In support of what has been said is the definition of risks analysis – “risk analysis – process to comprehend the nature of risk and to determine the level of risk” [1].

CI's senior management must implement and manage all aspects of operational security, including risk analysis, security policies and procedures, incident response training, and awareness of emerging technologies. The risk analysis process plays an important role in risk management and assessment. The threats that may occur, the potential impact of the threats, the frequency of the threats, and the level of confidence in the information collected must be identified and analyzed.

According to clause “8.2.3 Risk assessment” of ISO 22301: 2019 [2], the risk analysis must be carried out in accordance with ISO 31000: Risk management – Guidelines. The main activities related to risk analysis can be mentioned, but not limited to: gathering information using automated risk assessment tools, questionnaires, interviews and reviews of policy-making documents in this area; identification of the organization's assets and their values; identification of threats and vulnerabilities; determining the probability of threatening events and determining their impact and identifying risk as a combination of probability and impact.

Good international practice and theory identifies two types of risk analysis – quantitative and qualitative:

- **Quantitative risk analysis** includes numerical values for every aspect of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, security cost, etc.
- **Qualitative risk analysis** involves intuition, experience and best practices such as brainstorming, focus groups, surveys, questionnaires, interviews, the “Delphi method” and meetings.

The advantages and disadvantages of the two risk analyses are presented in Table 1.

T a b l e 1
Advantages and disadvantages of types of risk analysis

Type of risk analysis	Advantages	Disadvantages
Quantitative	– using fewer assumptions	– requires time – requires data collection efforts – requires the use of mathematical equations, which can be difficult and time-consuming
Qualitative	– prioritization of risks – identifying areas for immediate improvement	– results are subjective

Based on the advantages and disadvantages of both risk analyses, most organizations jointly apply quantitative risk analysis for tangible assets and qualitative risk analysis for intangible assets. Thus, one of the important outcomes of CI is increasing resilience.

Resilience of the organization. According to the ISO 22316 standard [3], organizational resilience is the ability of an organization to accept the impact and adapt in a changing environment. Therefore, resilience in CI can be seen as a quality state that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event. In this context, a comprehensive knowledge of the CI operating conditions (operating environment, environment and security environment) and of the main factors by which resilience is defined, limited and affected is the main prerequisite for strengthening the resilience of critical infrastructure elements.

It should not be forgotten that CI is a complicated and complex system designed to facilitate the continuous 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 areas. At the same time, this system consists of extensive subsystems of infrastructure networks that are inherently decentralized and spread over vast areas. Therefore, individual critical infrastructure subsystems are constantly exposed to the impact of various threats that lead to the occurrence of destructive events. Depending on their intensity, these events can cause disruption or even denial of services provided by individual critical infrastructure subsystems.

Because of this reason, the question of the security and protection of CI and the relationship with the long-term sustainable development of society has long been the subject of research in various scientific fields. Accordingly, a better understanding of the relationships between individual CI subsystems, as well as between CI and society as such forms the basis for the proposed CI security and protection system and its elements. For this reason, significant attention is being paid to CI security processes and tools, and improving the resilience of these subsystems can be seen as an initial solution.

In the CI context, resilience represents the inherent readiness of subsystems to be affected by 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. Therefore, resilience can be seen as the polar opposite of vulnerability or, in other words, resilience and vulnerability are opposite in nature to each other. Vulnerable subsystems lack resilience, and conversely, resilient subsystems are not particularly vulnerable.

Risk analysis and vulnerability of the organization. The risk and vulnerability attributed to the CI should be analyzed and assessed to address them through design, operation and management, including security systems.

Risk analysis. Risk analysis, as an accepted and evolving theory and practice, has been around for several decades and has reached a wide range of applications in order to uncover and identify potential failure states and hazards in various CIs and their systems so that they can be corrected before they occur. Broadly speaking, risk includes two dimensions to describe the possible consequences potentially arising from the operation of CI systems and from the activities of management and staff, and the associated uncertainty.

Consequences are usually viewed in negative, undesired terms in relation to intended goals. Their characterization is uncertain due to imperfect knowledge of the conditions under which they actually develop during an accident.

Incident scenarios are an important part of risk because they are those combinations of events that potentially lead to undesirable consequences. Their uncertainty is expressed quantitatively through frequencies and probabilities of occurrence of the corresponding events. Although the concept of risk is quite mature, the concept of vulnerability is still evolving and not yet fully established. The term vulnerability has been introduced as a hazard-oriented perception of disas-

ters for which the risk representation appears too limited. A low-intensity hazard may have severe consequences for CIs, while a high-intensity hazard may have minor consequences: the CI's level of vulnerability makes the difference.

Vulnerability of the organization. The concept of vulnerability, considered as a global system property, includes three other concepts: degree of losses and damages from the impact of hazards; degree of exposure to hazards – probability of exposure to hazards and the ability to bear losses and damages and degree of resilience – a measure of the system's ability to predict, absorb; to withstand and recover from the impact of hazards.

In order to be able to understand the essence of the concept of vulnerability, it is vital to know the definition of vulnerability analysis – “vulnerability analysis – process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence” [1].

In the context of the present development, vulnerability is considered a global technical property and is interpreted as a flaw or weakness in the design, development, operation and/or management of the CI or its elements that makes them susceptible to destruction or inoperability when exposed to danger or threat, or reduces the ability to recover under new stable conditions.

The objectives of vulnerability and risk analysis can be [4]: identification of the likely events and the sequence of possible realization of these events that may cause damage and loss effects in relation to the intended objectives; identification of the set of “initiating events” and assessing their cascading impact on a group of elements or the CI as a whole; identification of the set of events and/or sequences of those events that would cause damage and loss effects in relation to the intended objectives. For any real-world situation, the set of possible sequences of events can be very large. In practice, the challenges are related to the completeness of the set and the management of its dimension, by organizing and structuring it so that the important sequences of events are explicitly identified and the less important are grouped into a finite number of categories and defining dependencies and connecting them in a different sequence.

It is directly related to the accepted set of output events, probable sequences of events and expected observable results, which contributes to the definition of input data in the development of security systems of the organization and is closely related to the content of the required technical specifications.

Applicability of standardized approaches to CI security systems development. The ISO standards, developed and maintained by the technical committee ISO/TC 292 – “Security and resilience”, with a focus on business continuity and organizational resilience, provide access to good international practices to support CI management to build security systems, to respond to risk events and create conditions for effective recovery from disruptions associated with reduced costs, less impact on business performance and customer respect.

By implementing a standardized approach based on ISO/TC 292 standards, security creation and management actions will be consistent throughout the organization, which will create and develop the confidence of customers, suppliers, regulators and other stakeholders that CI has the sustainable security system and business continuity processes.

A driving force for good business continuity and resilience is the application of a multidisciplinary approach that is strategically positioned in CI, which is a key to integrating business continuity management and operational resilience into the organization's business and risk strategies.

A variant of a standardized approach, based on ISO/TC 292 standards, was applied in the implementation of stage "Development of conceptual design for ISS (models of security systems)" of the work plan of Work package 2 "Intelligent security systems" of the QUASAR project. Here, the basis for the parameters of the security system model was the result of the Risk Analysis, BIA and vulnerability analysis to ensure the resilience and business continuity of the CI.

Conclusions. With a sufficient level of conviction, it can be argued that the security of CI has become a national and international priority. For security systems to be effective, vulnerability analysis and risk analysis must be performed based on new, expanded paradigms formulated in ISO/TC 292 standards in the area of societal security and resilience.

Also, the high degree of connectivity achieved by CIs can make them vulnerable to global disruptions when exposed to hazards of various natures, from accidental mechanical/physical/material damage to natural events, software failures, intentional malicious impacts, human and organizational errors. This wider range of hazards and threats requires an all-hazards approach to understanding the behaviour of CIs when exposed to a risk event to ensure effective security.

Therefore, a possible way to address this challenge is to conceptualize the control framework for risk and vulnerability analysis, which applies the multivariate approach to the occurrence of incidents that are outside the design and operational safety constraints of CIs, including its structural objects. In this way, completeness of the necessary information is achieved for the preparation of technical specifications for the development of a security system. This approach was applied in the development of Work package 2 "Intelligent security systems" from the QUASAR project.

REFERENCES

- [1] ISO 22300:2021 – Security and resilience – Vocabulary.
- [2] ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements.
- [3] ISO 22316:2017 – Security and resilience – Organizational resilience – Principles and attributes.

- [4] ZIO E. (2016) Critical infrastructures vulnerability and risk analysis, Eur. J. Secur. Res., **1**, 97–114, <https://doi.org/10.1007/s41125-016-0004-2>.

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