Possible approach for developing a model of intelligent security system applicable in its design in the quasar center of competence

Valeri Panevski
Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *Through the development and operation of intelligent security systems, with a focus on critical infrastructure, it is expected to improve the security of the population in our country. This process finds real dimensions in the goals and tasks of the centers of competence, which are in the process of construction during the current period. A key element contributing to the proper functioning of intelligent security systems is its design, in accordance with the specifics of the security environment.*
Precisely the synergy of the efforts of the scientific, educational and industrial communities for the development of contemporary models of security systems, structured within the functional scope of the QUASAR competence center, is the basis of this article.
Keywords*: INTELLIGENT SECURITY SYSTEMS, DESIGN*

1. Introduction

Business Continuity Management (BCM) is the way which can solve the challenges facing critical infrastructure (CI), related to the diversity of critical risks to the security environment. The essential part of the BCM is the correct identification of CI-critical risks, the related management strategies to be planned and how to respond to probable risk events.

At the same time, physical security is one of the most basic security aspects of the organization providing BCM. The application of physical security is the process of using layers of physical security measures to prevent unauthorized access or damage.The crucial element that contributes to the smooth improvement of the organization's security is technology.

An intelligent solution is the basis of the operation of the entire technology of the security system, in which the common security is built and managed by the security policy. As the security situation changes, the security policy must be dynamically defined and adjusted in order to achieve the necessary adequate levels of compliance with the type and extent of the likely risks.

In earlier security systems, decision-making and the adjustment of security and protection policies relied mainly on people, leading to an ineffective security response. For highly dynamic and complex network systems, this traditional way of making security decisions and policy adjustments does not meet security requirements **[1,2,3]**.

With the development of technology, it has become possible to automate decision-making with the help of intelligent systems (mechatronic and those with artificial intelligence). In this way the awareness of the situation is improved and through the automated response technology the adaptive protection against the threats to the security of the CI is realized and the speed of reaction is significantly increased.

All this requires a rethinking of the approach to the development of modern CI security systems that meet both the dynamics of the risks of the security environment and be in line with the innovations and innovative processes of applied science and industrial technologies globally.

Therefore, the emphasis of this publication is aimed at presenting the current results of the activities and stages developed by the Institute of Metallurgy, Equipment and Technologies with a Center for Hydro- and Aerodynamics „Academician Angel Balevski" at BAS in the implementation of the Working Package 2 „Intelligent Security Systems" from Project BG05M2OP001-1.002-0006 „Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar), funded by the Operational Program „Science and Education for Smart Growth", co-financed by the European Union through European Structural and Investment Funds.

2. Possible model of the Intelligent Security System

The organization's Intelligent Security System Model (ISSM) schematically describes the purpose and activities of security (and, if necessary, protection), the personnel who perform them, and the interrelationships and consequences of these activities.

Functions of the organization's ISSM:

- Detection of probable risk impact, identification and response;
- Maintaining a constant readiness for reaction;
- Ensuring continuous and normal operation of CI.

The purpose of the ISSM is through technical, organizational and other measures and actions to: identify threats; propose response and reaction to prevent unauthorized access to / unauthorized impact on the protected area / protected areas of the organization / facility of the organization.

The model consists of two parts:

- Organizational part – analyzes and evaluations, policies, strategies, plans and procedures.
- Technical part.

An important moment in the implementation of the ISSM model is the risk analysis and risk assessment, which in the most general framework includes the following elements:

- Risk factors assessment;

- Vulnerability assessment of CI components;

- Staff's resilience assessment against the impact of risk factors.

Based on proper risk assessment, the implementation of preventive protection activities is determined, including works such as:

- Analysis and identification of the risks against which the critical processes are determined, the interdependence between them and the resources necessary for the functioning of the organization. Based on the results, a vulnerability analysis is prepared for all components;

- Analysis of these risks, in terms of their potential to induce long-term cessation of the manufacturing process as well as the probability of their realization and determine their impact level;

- Comparative assessment of the risks level. The aim is to establish, implement and maintain an officially documented risk assessment process that systematically identifies, analyzes and assesses the risk of the impact of the identified risk factors on the components of the CI.

3. *Design of a physical protection system model for critical infrastructure*

Definition of physical protection system

physical protection system: *An integrated set of physical protection measures intended to prevent the completion of a malicious act.* **[4]**

The design of the physical protection system (PPS), as part of its life cycle, is best achieved through a systematic approach, which consists of three phases (Figure 1), namely:

Phase 1: Identification of the objectives and requirements for PPS;

Phase 2: Design of the PPS to meet the objectives and requirements set out in Phase 1;

Phase 3: Performing an analysis and assessment of the PPS, designed in Phase 2, to achieve the objectives and requirements set during Phase 1.

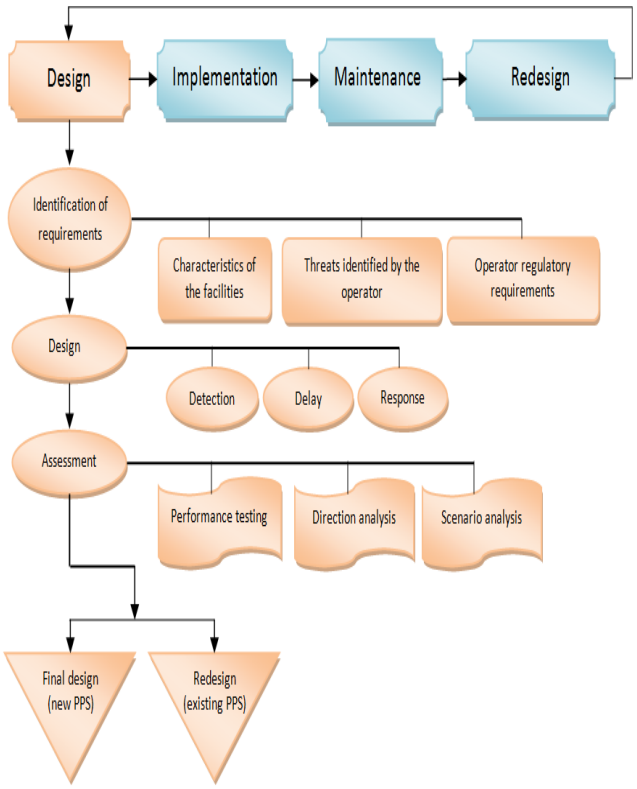

Figure 1: *PPS model design process.*

In Phase 1 of the PPS project design, the key asset management needs to determine how the state's requirements for physical protection of critical infrastructures are included **[4]**.

Several consecutive and interrelated steps need to be taken to identify these requirements:

➢ Characterization of activity and operating conditions of critical infrastructure;

➢ Analysis of the information on the threat provided by the state bodies and organizations, which will serve as a basis for the design]

➢ Defining targets, as well as their location on the object, that must be protected against possible impact.

In Phase 2, a new physical protection system is designed or the existing system is redesigned to ensure the implementation of new or updated physical protection measures, with regard to the timely detection of a probable risk event, delay its implementation and provide an adequate response to its neutralization.

Once the SPS has been designed and characterized, it must be analyzed and evaluated to ensure that it meets the requirements for physical protection.

In Phase 3, an assessment shall be made to determine whether the system meets the requirements set out in Phase 1,

➢ Confirmation of the functioning of the PPS in accordance with the requirements set in the process of its design and development;

➢ Identification of possible shortcomings of the system in the design or its implementation, which must be considered in order to provide adequate corrective actions;

➢ Analysis of possible improvements that may be needed to overcome the deficiencies and improve the functionality of the system;

➢ Re-evaluate the effectiveness of the PPS on an annual basis to take into account any changes in the objectives, functionalities of the system or the requirements to it.

All this should provide the PPS with the ability to ensure timely detection, maximum delay in implementation and adequate response to possible risk events through structural, technical and personnel measures.

Methods for assessing the effectiveness of PPS, based on results from the operation of this system, could include: analysis of dependencies between many variables; simulation and exercises.

4. *General ISSM, applicable in their design*

The ISSM schematically describes the purpose and activities of the security, the personnel who perform them, and the interrelationships and consequences of these activities. It could possess a structure set forth in the following.

Functions of the ISSM of the organization:

➢ Detection of probable risk impact, identification and response;

➢ Maintaining a constant readiness for reaction;

➢ Ensuring continuous and normal operation of CI.

The purpose of ISSM is through different and interconnected measures and activities to be identified threats and proposed response and to prevent unauthorized access to the protected area / protected areas of the organization.

The model consists of two parts:

➢ Organizational part - analyzes, evaluations, policies, strategies, plans, procedures;

➢ Technical part.

The organizational part consists of:

➢ Identification of threats;

➢ Risk analysis and assessment;

➢ Development of security and protection policy;

➢ Development of security and protection strategies;

➢ Development of a security and protection plan;

➢ Development of corrective preventive activities;

➢ Development of training programs.

Actions to prevent / repel unauthorized access to security areas must be planned in advance on the basis of scenarios that must correspond to the depth of penetration, location of the breach, separation of the region to prevent adverse effects from random people and taking measures to neutralize intruders and ensure the security and protection of security components. The extent of different levels of protection is determined by the level of risk, the response time, the technical means available and the characteristics of the area.

An important point in the risk assessment is the *vulnerability and criticality assessment* and based on that, determination of the structure of the *technical part* of the model of CI security and protection system.

Vulnerability and criticality assessment process

This process examines the review and analysis of the CI mission in relation to a probable threat (s). The review should assess the value of countermeasures with regard to lost or reduced mission effectiveness. It is then necessary to assess the level of acceptable risk for CIs and personnel, taking into account the level of expected failure in the effectiveness of the mission.

The data obtained from the vulnerability and criticality assessments process provide the CI management with a picture of the overall vulnerability to a likely critical risk impact. As a result, management organizes the development of a security and protection plan that covers all levels of probable threats, regardless of the current level.

The assessment includes:

- identification of key assets of CI;
- determining the possibility of duplicating critical functions in identifying different impact scenarios;
- determining the time needed to duplicate key assets or CI efforts if the key assets are temporarily or permanently lost;
- determining the vulnerability of key CI assets to probable risk events;
- prioritizing the response to the impact of probable risk events on key CI assets.

An important point in assessing the vulnerability and criticality of CI is the conduct of training. Multivariate games are the best test, apart from the actual risk event, to analyze the CI reaction. Trainings and exercises test suspected vulnerabilities and countermeasures. They also train CI management and personnel, as well as the leadership of the response forces, and help maintain a valid threat assessment by identifying and adapting to changing threats.

Given what has been said here, for the purposes of this article in the following lines will be discussed briefly a model of technical part of the ISSM.

Technical part of MISS

According to Directive 2008/114 / EC, security measures are subdivided into **[5]**:

- *permanent security measures* - for their implementation the necessary security investments and the funds to be used at any time are determined. These include a set of passive and active measures to prevent leakage of operational information on: general measures, such as technical measures (including installation of detectors, access control devices, protective and precautionary measures); organizational measures (including signaling and crisis management procedures); control and inspection measures; communication; awareness raising and training; and security of information systems.
- *graded security measures* - are implemented depending on the degree of various risks and threats. They are mainly related to protection against the effects of sudden risk events. These measures are achieved through a set of active safety measures and are applied in combination with permanent security measures. The graded security measures and procedures are regulated in the security plan of the organization / site, developed by the operator.

The combination of security measures defined by the Directive applies to structure the technical part of the MISS. The technical part of MISS outlines three models: a model of the territory on which the organization / object of the organization is located; a model of risks and threats and a model of security and protection equipment. The models determine the parameters determined by the probable means of impact by risk factors and natural disasters, the characteristics of the technical equipment for monitoring and warning of the reaction forces - transport, CIS, armament, assessment of the territory and determination of time to reach critical points, etc.

The generalized model of the technical part reproduces schematically, reduced by the structure and properties of the target by:

- model on the territory of the location of the CI;
- model of risks and threats for CI;
- model of the equipment for security and protection of CI.

Model of the territory on which the organization / object of the organization is located

It includes the development of a model on the territory of a key asset of the organization / object of the organization, considering in detail the peripheral security zone. The model covers all elements of the territory, assessment of risks and threats, and equipment of security components (including protection, if necessary). Areas with different levels of security are defined, and their size is in accordance with the importance of the asset for the functioning of the organization; the level of risk; reaction time; the constructed technical facilities; the terrain of the area, etc.

Actions to prevent/reflect unauthorized access to security and protection areas should be planned in advance on the basis of scenarios that should correspond to the depth of penetration, localization of passability, separation of the area in order to prevent adverse effects from random people and taking measures to neutralize violators and protect the components of the asset. These activities are part of the activities carried out within the organizational part of the model by the security force planning authorities and the specific objective.

The modeling of complex location of an object is done in order to present the security and protection of the object (in each area and segment) through a digital analogue of mathematical modeling and data processing. To solve this problem, the model of the territory on which the organization / object of the organization is located is described by zones, regions and segments.

Risk and threat model

The development of the model aims to analyze the possibilities for impact on the critical goal / critical asset on the basis of developed scenarios and risk assessment.

The model solves the following problems:

- identification of the most probable directions / lines for impact of a probable risk event;
- determination the personnel and equipment that will be used to carry out the impact on the CI/CI object.

The object of modeling is the most probable means of influence with which the probable violators are able to realize influences on the target.

Model of the equipment on the CI/CI object

The model of the equipment is built in order to specify the types of equipment, depending on the possibilities of the probable intruders to have an impact on the CI.

Anticipating the impact on equipment involves solving two types of challenges:

- assessment of the importance of the risk assets of the CI for ensuring the continuity of the activity of the organization in case of the expected impact of a terrorist attack;
- identification of potential means of influencing the risk assets of the CI, which may cause a suspension of operation for a certain period of time.

The development of the technical part of MISS must allow the combination of security features and procedures that work together to ensure the complexity of security and protection of CIs **[6,7]**. MISS functionality must relate to the systematic, integrated, ex-ante protection of CI assets, and not to provide a response to probable risk events after their occurrence. The technical part of MISS and in particular the model of the equipment (in particular the physical protection system) works better if the detection is as far as possible from the CI **[8,9]**, in the presence of a close link between the detection and evaluation processes or a combination of detection, delay and response activities.

5. Conclusion

The presented approach for developing a model of an intelligent security system, in the aspect of its technical part, is only a separate step in the development of a complete model. The main direction of determining the structure of the technical part of the model is based on the process of risk identification and assessment of the possible threat to CI and the consequences caused by the impact of a certain risk factor / certain risk factors. The essential point is the treatment of the act of threat as a set of risk factors, each of which is able to change the system of security and protection of elements of CI. The correct choice of the structure and the appropriate technical level of the elements of the physical protection system also play an important role here.

Also, the formal division of the technical part into three models allows for the exact distribution of functions between the management and the staff of the CI, with responsibilities in the field of security and protection. This means timely planning of the necessary funds for establishment and development of capabilities, for training and coaching, with a focus on prevention and counteraction of possible risk events that may affect CI.

Acknowledgement

This paper is the result of implementation of the scientific work 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.

Literature:

[1] Dimitar Dimitrov, "Comperatve evaluation of modeling and simulation techniques for interdependent critical infrastructure", International Scientific Journal "Security & Future", Issue 4/2019, Scientific Technical Union of Mechanical Engineering, 2019, ISSN:ISSN: 2535-0668 (print), 2535- 082X (online), p.p. 128-132;

[2] Dimitar Dimitrov, "Comparative assessment of techniques for modeling and simulation of interconnected critical infrastructure", Proceedings of the annual university conference, "Vasil Levski" National Military University Publishing complex, ISSN 1314-1937, p. 231 -241, 2020;

[3] Ventsislav Ivanov Pehlivanski, "Tests in the process of designing protection systems", Sofia 2020, IMSTCH-BAS; ISBN: 978-619-188-359-2;

[4] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, Vienna (2011);

[5] 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;

[6] A. Tumbarska, "Trends in the development of non-lethal technologies and protection systems", Monograph. IMSTCH-BAS, 2020, ISBN: 978-619-7466-07-2, 402 ps.;

[7] Nikolay Gueorguiev, Yavor Boichev, Konstantina Belotelova, Ivan Ivanov, "Frequency characteristics of seismic piezoelectric sensors under one-dimensional mechanical action", Journal of Theoretical and Applied Mechanics, Sofia, Vol.49 (2019), ISSN: 0861-6663 (Print), 1314-8710 (Online) pp. 130-141. Bulgarian Academy of sciences, National committee of theoretical and applied mechanics, 50, 2, 2020, ISSN:0861-6663 (Print), 1314-8710 (Online), 130-141. SJR (Scopus):0.28;

[8] Georgiev, N.L. "Analysis of one class of specialized sensors for protection of objects from critical infrastructures", 2015, ISBN:978-619-90310-4-9, 170, monograph;

[9] Georgiev, N.L, "Summary description of the state of sensors by object protection systems", "Collection of scientific papers - Days of non-destructive control", 2015, ISSN: 1310-3946, p.p. 118-120.