INTEGRATED CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Chief Assistant Dr. Eng. Panevski V.S.
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: *Integrated management should be seen as synonymous with good management, which means that it is necessary to manage the organization's activities, resources, personnel, impact on its functioning and countless risks that can cause a lot of problems if it is allowed to be happen than if they being avoided.*

The best way to define the parameters of integrated security implies the use of a simple, clear and comprehensive approach and format that allows the senior management of the organization to focus on the key elements that need to be planned, implemented and managed to fulfill the mission of the organization.

Keywords*: INTEGRATED SECURITY; CRITICAL INFRASTRUCTURE; MANAGEMENT*

1. Introduction

Critical Infrastructures (CI) are organizational units whose functionality if compromised could have led to unpredictable breaches in security, economy, public health and lifestyle of the population not only of one, but also in neighboring countries. While it is unlikely disruptions can be prevented completely, an effective analysis of CI can minimize their impact by improving assessments of vulnerability and protection planning strategies for response and recovery. The analysis aims to give an idea of the CI behavior in terms of occurrence and impact of possible risk events, which will increase the efficiency of protection plans and operations for response and recovery. The end result of the analysis is the presentation of a decision to ensure the Business Continuity of the CI, namely the establishment of an Integrated Security.

It is necessary to understand that "…we should not perceive critical infrastructure protection as an isolated and independently-functioning structure, because security aspects penetrate all, even seemingly irrelevant spheres of the operation of the organization". **[1]**

In the most general case, in modern theory and practice, under the integrated security of CIs is meant the deployment of intelligent protection, including both the identification of specific threats and vulnerabilities and the inclusion of the best adapted solutions, namely:

- External perimeter solutions, including radars, motion detectors, microwave, infrared, acoustic, vibration and CCTV;
- Inside perimeter technologies and solutions ranging from access control to video analysis;
- Integration Platforms (command centers of business management solutions for security of outer and inner perimeters).

But is this integrated security?

Presented in this way, Integrated CI Security provides a partial picture of the nature of the challenge. It should be pointed out that the creation of integrated security covers all the elements (systems and subsystems) of the CI management as a business organization: external and internal security; staff; finance; environment; quality; information security, business continuity management; corporate social responsibility and etc. Precisely in this direction, the following text will present the views and practical results of the activity to ensure integrated CI security.

2. Interactions between Business Continuity Management System and Business Organization Management System

In order to identify these interrelations, it is necessary to point out the *similarities* and *differences* with regard to the requirements for the establishment of the Business Continuity Management (BCM) System and the management systems for: quality assurance, environmental protection, health and safety at work, finance, human resources, information technologies and data protection, corporate social responsibility, risk management. **[2]**

Similarities

The construction of the above-mentioned systems requires the creation of documents specific to the individual area of activity of the business organization or the carrying out of actions such as: policy; a strategy for the implementation of key policy directions for development; risk analysis; a detailed plan for the implementation of the strategic objectives and objectives; updating, maintaining and testing the plan; training of the personnel for the implementation of the individual modules and tasks of the plan; conducting preventive and corrective actions, regular monitoring of changes in the business environment and audit of activities, related to achieving the objectives of the policy and strategy.

The methodology used is either the same (quality, environment, health and safety at work), or similar and very similar (finance, human resources), which creates conditions for understanding the general and specific problems of the organization by most of its employees and employees.

Differences

The significant difference between them is the conduct of *Business Impact Analysis* (BIA) in the course of building a Business Continuity Management System.

The purpose of BIA for each action, process, product, or service is to:

- document the impacts that may arise as a result of loss or interruption of the organization / system activity;
- determine the time required for recovery of the function;
- determine the conditions (internal and external) needed to operate the system / organization effectively.

This is the *basis of the difference* between BIA and Risk Analysis, namely that first explores the events that led to major disruptions of operations, while the second examines all potential events that may affect the business of the organization. **[2]** Considering the fact that BCM is in close relation with all other subsystems of the

Organization Management System, and that it only lays down specific requirements for all of them we can, with a sufficient degree of conviction, declare that it is the connecting link in the management of the organization.

3. Integrated model for security and protection of critical infrastructure protection

In the period 2011 ÷ 2013, under the leadership of the Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Center "Academician Angel Balevski",Bulgarian Academy of Sciences, an Integrated Model for Security and Protection of CI was developed and successfully tested. This result was achieved during the implementation of the European project "Development of tools needed to coordinate inter-sectoral power and transport cip activities at a situation of multilateral terrorist threat. Increase of the capacity of key CIP objects in Bulgaria", reg. № HOME / 2010 / CIPS / AG / 019. The model outlined and described the characteristics of the integrated security and protection management of the CI and, on the other hand, gave the specialists in this field a starting point for discussion and improvement of the system characteristics.

Essence of the model

Good practice so far has shown that the starting point for the development of the security and protection models (CPM) of CI is the adopted uniform terminology. For example, the following definition was used to describe the content of the term "*Security and Defense System*": "The Security and Protection System is a set of elements operating under a unified security concept, purposefully managed in a common information environment to provide the processes , aimed at timely detection of threats and a preventive response to prevent side effects".**[3]** As far as the term "Critical Infrastructure" is concerned, the natural definition of Council Directive 2008/114 / EC, namely: "means 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".

On the other hand, the creation of CPM was taken to apply the methodology of the schematic description of the site and the activities of security and defense, who perform them and what are the interrelationships and consequences of these activities.

The Functions of the Model:

- Detection of terrorist attacks, recognition and reaction;
- Standby keeping for reaction;
- Provide continuous and normal operation of CI.

The purpose of CPM is to identify threats, to provide an answer and a response to prevent unauthorized access to the protected area of CI **[3]** through organizational and technical activities, offering the following characteristics:

- Organizational part;
- Technical part;
- Procedures for the implementation of policies, strategies and plans.

Organizational part

The organizational part can be composed of multiple elements, in this case, their structures consist of risk analysis and risk assessment and develop: security and protection policy; security and protection strategy; security and protection plan; corrective and preventive activities and training programs.

Of course, risks analysis and risks assessment can be done using different methodologies. The essential point is to link the results of this process with follow-up by the authorities involved, aimed at enhancing the security and protection of the CI. Thus, without claiming completeness, the process may include the following elements **[4]**:

- Evaluating risk factors, such as the following groups of threats: natural; against machinery, equipment and buildings; against staff; against technology; against operations and social.
- Vulnerability assessment of the elements of CI;
- Sustainability Assessment of personnel and population.

In turn, vulnerability assessment of the structural elements of CI can be done in terms of the effect of external influences, the result of which is a map of vulnerabilities and their interconnections. It involves evaluating each item with the following parameters:

- Constructive reliability - measures the extent and ability of site elements to protect technology, machines, and those working with them from the actions of terrorists;
- Accessibility for external impact - measured under conditions of relative ease, serenity, or difficulty in moving terrorists to or within the protected object;
- Recognition of an external observer - characterizes the difficulty in determining the functions and significance of the object or machines and the technological lines located therein.

On the basis of this assessment and in order to identify the responsiveness to a particular threat, the level of the most effective implementation of the security and protection activities of the CI should be determined.

The assessment of the sustainability of personnel and the population with the impact of risk factors can be done by using the numerous human resource management methodologies.

Based on the analysis and risk assessment, it is necessary to develop the conceptual framework that will direct our efforts in the right direction, i.e. to formulate a security and protection policy for the CI.

Security policy is a set of documented solutions adopted by the organization's management and aimed at ensuring security and protection of the object of CI. **[5]**

The policy defines the principles and responsibilities for interrupting technical processes as a result of a terrorist threat in a way that ensures the maintenance or timely recovery of critical functions (processes), while minimizing the impact on critical functions and equipment. It should be directed to:

- ensuring the continuity of the critical functions (processes) of the CI;
- allocation, between management and response forces, of the roles and responsibilities of management in the event of a terrorist threat;
- ensuring a consistent approach to building security and protection in line with international and national standards;
- integration of the system to ensure the security and protection within and processes for risk management of the CI.

Meanwhile, Security and Protection Strategy defines the basic framework of rules and instructions for operation of the Security and Defense System. It regulates the determination of the means and procedures as well as the responsibilities of all participants in the process. The result of the implementation of the Strategy is to

achieve support from senior management to overall Security and Protection System.

The development of the Security and Protection Plan describes the processes and resources needed to achieve the objective - ensuring the continuity of the CI work. It should contain, but is not limited to, the following information **[6]**:

- Strategy to overcome the incident (in this case the realization of a terrorist threat);
- Minimum Requirements to Recover Continuous Action;
- List of team members, rights and responsibilities, and contact details;
- List of materials delivered outside the site;
- Activities organized by phases.

Technical part

In the technical part, three secondary models can be identified - a model of the site for the location of the site, a model of the risks and threats and a model of the equipment of the site. **[5]** They define parameters depending on the possible means of action by terrorists, characteristics of the technical means of monitoring and warning of the reaction forces - transport, communication-information systems, armament, and assessment of the territory and determination of the times for reaching critical.

The M**odel of the site** for the location of the site is done in order to present the security and protection of the CI with a digital analogue for the mathematical processing of the data. To solve this problem, the site model for site deployment is described by a peripheral area, lanes and segments.

Through the **Risk and Threat Model**, the following tasks can be solved:

- identification the most likely areas for committing terrorist attacks;
- determining the forces and means that will impact on the CI.

The **Model of the Equipment** is built to determine the types of tools and systems depending on the potential of terrorists to influence the CI (including security, containment and alarm security (sensors)).

Procedures for the implementation of policies, strategies and plans

In order to implement the established policies, strategies and plans to ensure the security and protection of CIs, management must create the necessary conditions for a detailed description of the activities to be performed, bound by time, place and responsibilities. The allegation that this is done within the sections / phases of the security and defense plan is incorrect and one of the most common cases of failure in the implementation of the plans is the lack of clear and streamlined procedures for their implementation.

4. Integrated security management system

„*The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures.*“ **[7]**

Following this approach, the CI security levels that may be at the core of building an Integrated Security Management System are as follows **[2]**:

- 1-st level – Risk Assessment (1) and Internal Security (2);
- 2-nd level - Risk Assessment (1); Internal Security (2) and External Security (3);
- 3-rd level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5);
- 4-th level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5); Information Security (6); Human Resources (7) and Financial Security (8);
- 5-th level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5); Information Security (6); Human Resources (7); Financial Security (8); Environmental Security (9) and Corporate Social Responsibility (10);
- 6-th level – All listed above and Business Continuity Management (11).

Of course, this is only a conceptual proposal. The structure and content of these levels is discussed and scientific and professional communities will determine their ultimate configuration. It is essential that, after defining the final levels of security for organizations, a practical and applied mechanism for their creation and assessment of their readiness to use has to be established, i.e. to assess the degree of security of the organization.

This mechanism may be covered by an international standard describing requirement for individual security levels. As for the assessment of their readiness for use and overall assessment of the security of the organization it is also necessary to create a unified methodology applied by individual standardization or other document to unify efforts in this direction. Only in this way will we have an objective assessment and a tool for comparing the security systems in place in different organizations.

Here it may be noted that the creation of CI security levels is not an end in itself. The ultimate result of their construction and operation should be the formation of an integrated security management system for organizations (Fig. 1).

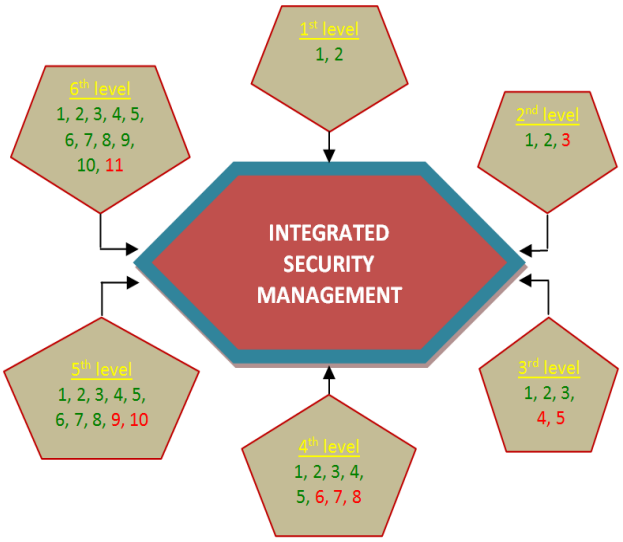

Figure 1: *Integrated security management system – security levels.*

It is true that there is a document that includes regulations for creation of such system, namely the ISO / DISSES 34001 Security Management System. However, the methodology described in this standard covers the processes of risk assessment and risk management. These two tools are the first and indispensable condition for creating and safeguarding the organization's security, but they are by no means the only.

The proposed approach to building an Integrated Security Management System takes into account the underlying nature of risk assessment and risk management, while covering all security-related elements / subsystems of the organization's management system, and focuses on detailing the individual requirements as well

in relation to these elements, and on the levels of security built on them.

Conclusion

The proposed model for integrated security and protection of CI covers the following basic directions: presentation of the structural framework of the integrated model, covering the organizational part, the technical part and the realization procedures; understanding business continuity management as an integrating link both between the individual subsystems of the business organization management system and between the elements of security and protection levels; definition of the security and protection levels of CIs, determining the creation of integrated systems in the area under consideration and last but not least, opportunity offering for choosing an alternative method for their construction, framing the methodology for the creation of integrated security and protection of CI.

Describing the integrity of security and protection, through the proposed levels of security, forms the framework of the integrated system. The security level elements correspond to the subsystems of business management system of the organization. This is precisely the uniqueness of the proposed approach - the mutual penetration of security within the overall CI management to ensure the fulfillment of its mission.

Literature:

[1] Dimitar Dimitrov, Valentina Nikolova, Martin Asenov, Petia Vasileva "TECHNICAL AND ORGANIZATIONAL ASPECTS OF THE APPROACHES, USED FOR ASSURING EFFECTIVE SECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE-G00D PRACTICES AND RECOMMENDATIONS", Proceedings of the Sixth National Conference with international participation "Materials science, hydro- and aerodynamics and National Security '2017, ISSN 1313-8308, 210 ÷ 216;

[2] Kiril Stoichev, Dmitar Dimitrov, Valeri Panevski "Integrated Security and Critical Infrastructure Protection" Monograph, Chapter Two, ISSN 978-619-90310-6-3, 2016.;

[3] Yachev R. and Project team by NDA, Stoichev K. and Project team by IMSETHC-BAS, "Development of a security and protection model of the airport external perimeter", Collection of materials with the results of the project: "Development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. Increasing of the protection capacity of key CIP objects in BULGARIA – BULCIP", ISBN 978-954-92552-6-3, 2013;

[4] Vitanov L. and Project team by NDA, Stoichev K. and Project team by IMSETHC-BAS, "Modeling of advanced system for security and water channels protection of the NPP", Collection of materials with the results of the project: "Development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. Increasing of the protection capacity of key CIP objects in BULGARIA – BULCIP", ISBN 978-954-92552-6-3, 2013;

[5] Stoichev K., Business Continuity Model of the NPP' System for removing the heat, International Workshop: "Business Continuity Management of the Nuclear Power Plant System. Modeling and Procedures Development of Advanced System for Security and Water Channel Protection of the NPP", Kozloduy NPP, 05 of June, 2012;

[6] Stoichev K., (2014), The Role of Business Continuity Management in the Business Management System, Science Journal of Business and Management, 2(3), 97-102, DOI: 10.11648/j.sjbm.20140203.12, ISSN: 2331-0626 (Print); ISSN: 2331-0634 (Online);

[7] ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls", "0 Introduction", "0.1 Background and context".