BUSINESS CONTINUITY MANAGEMENT OF CRITICAL INFRASTRUCTURE, MODERN APPROACH TO THE INCREASE OF THE SECURITY AND PROTECTION

Valeri S. Panevski, Dimitar L. Dimitrov

Institute of Metal Science, Equipment and Technologies "Akad. Angel Balevski" with hydro and aerodynamics center - Bulgarian Academy of Sciences
1574 Sofia,"Shipchenski prohod" blvd. № 67

BUSINESS CONTINUITY MANAGEMENT OF CRITICAL INFRASTRUCTURE, CONTEMORARY APPROACH TO INCREASE SECURITY AND PROTECTION

Valeri S. Panevski, Dimitar L. Dimitrov

ABSTRACT: Introduction of Business Continuity Management is closely associated with increasing the security and ensuring the protection of Critical Infrastructure. This process entails the need to take into account all the threats which are in the result of man-made activity (terrorism), technological accidents and / or natural disasters. That why this paper is an attempt to present the current status of Business Continuity Management in our country, as well as it relation to the security and protection.

KEY WORDS: business continuity management; security and protection.

1. Introduction

There are two main directions in policy related to strengthening and development of anti-terrorist activity: fighting the source of threat and protection of individuals and infrastructures **[2]**. Fighting the source is a function of intelligence bodies as the basis of their work is the fight against "insecurity" - where?, when? and how? there will be carried out terrorist attack. Protection of individuals and infrastructures is a public product and as such is a function of the state authorities at all levels.

The degree of uncertainty and the need to protect significantly affect the economic and psychological costs and lead to painful changes in the established norms of behavior and lifestyle.

To make it possible to achieve sustainable and effective results in combating the threats of terrorist attacks, efforts need to be streamlined and focused on solving problems in key locations.

Given these proven by the time truths in 2009, the Institute of Metal Science, Equipment and Technologies "Akad. A. Balevski" with hydro and aerodynamics center - BAS (IMSETHC-BAS), has developed a concept to enhance the ability to protect key sites of critical infrastructure (CIO) in Bulgaria. The concept is not only the first and only in Bulgaria but also in the European Union (EU) as a whole, which marks the beginning of a systematic approach to the security and protection of European CI (ECI).

The developing and implementing of the concept has the following main objectives:

- Increasing the ability to counter terrorist threats to the key for the economy and the country's development, energy and transport infrastructures;

- Improving the management of the process of decision making against multivariate terrorist threats.

Usefulness and effectiveness of the implementation of the concept can be clearly identified in the intended results **[2]**. For the purposes of the systematic research approach and maximizing of practical and applied results of research and development activities, the approbation of the concept is divided into four interrelated and complementary modules, namely:

First module – Analysis of the conditions for continuous operation of the System in NPP "Kozloduy" to remove heat and its transformation into kinetic energy of the steam generator (in the following text written as "the System"), and improving protection against terrorist threats - with results:

- Model for Continuous Action of the System;
- Model for increasing the capacity of the System to protect against terrorist threats.

Second module – Increasing the anti-terrorist protection of underground gas storage facility "Chiren" (UGS ":Chiren") - with results:

- Unified methodology for protection of gas storage facilities against terrorist threats in the EU member states;
- Risk assessment of the system for protection of UGS "Chiren" in terms of adequate response against terrorist threats;
- Model for protection of gas storage facilities against terrorist threats;
- Operating procedures in case of a terrorist threats and in case of emergencies in gas storages.

Third module – Increasing the capacity to protect the "Sofia" airport against terrorist threats through improved security of adjacent areas - with results:

- Methodology for developing a security system for the outer perimeter of airports in order to increase the internal security;
- Model for security and protection of the outside perimeter of airports for the purposes of the internal security.

Fourth module – Operational management procedures in high-risk environments against multivariate terrorist threats - with results:

- Operational procedures for decision making in case of multivariate terrorist threats;
- Technical and technological solution of a unified management system in case of multivariate terrorist threats;
- Model of an integrated management system in case of multivariate terrorist threats, implementable at national, regional and European level, with established parameters and characteristics;
- Trained operators and personnel to respond in a situation of multivariate terrorist threat.

On this basis is developed a methodology for planning, and model for management of continuous operation of the sites of national and ECI, initiating the process of creating conditions for increasing the security and protection of the population.

2. Nature of the problem

Field continuity processes/business incorporates management activities and integrated plans that create conditions for maintaining the continuity of critical processes for an organization **[3]**. This area covers all aspects of an organizational unit,

involved in the maintenance of critical processes, namely: personnel; buildings; suppliers; technology and data. Its decisive role is especially serious when it comes to ensuring the continued functioning of organizations, especially those identified as such in the energy sector.

Ensuring the continuous operation of nuclear power plants is a key part of their business, related both to the risk of significant economic losses and the presence of danger to life and health of people working there, staying in their territory or the area in which are situated.

From this perspective, the methodology for planning and the model of the management system for the continuous functioning of the OCI are designed for the System of NPP "Kozloduy".

There are numerous approaches, ways and means to create conditions for continuous operation of the OCI, which in varying degrees affect their specifics. From there on, are several different degrees and levels of security to ensure the continuity of their operation.

Rounding out the theory and practice for planning of continuous operationing, and the exchange of experience and good practices, contribute to increase the security of the economic or organizational entities, but the lack of a models for the identical objects gives rise to uncertainty about the degrees of their viability.

Considering the fact that such objects are the basis of the CI of all EU member states it is essential to create conditions for a reliable assessment and achieving of the required extent and level of security to ensure the continuity of their development.

All this necessitates the creation of unified methodology and model of management system for continuous operation of the OCI like nuclear power plants, which will be used for other OCI in the energetics sphere such as gas storages. Creating and testing methodologies and models on real objects in Bulgaria (NPP "Kozloduy" and UGS "Chiren") contributes to achieving the following benefits for OCI in energetics:

- Creating conditions for a reliable assessment of critical activities and processes, and increase of their resilience, ensuring acceptable performance of facilities in terms of impact on their work performance and parameters;
- Increasing the effectiveness of the training of officials responsible for the continued functioning of the objects;
- Creating conditions for the improvement of the best practices for continuous operation;
- Reducing the cost for development of management system for continuous operation for the OCI;
- Repeating the above results on CI of the energetics of the member states of the EU.

Thus, by developing and testing a complete toolkit for development of management system for continuous operation of CI in energetics and transport spheres, are formulated the parameters for a uniform methodology for planning and a model of management system for continuous operation of one of the main systems of the nuclear power plant, with the prospect of applying it to gas storage facilities and international airports as OCI for energetics and transport.

3. Methodology for planning of the continuous functioning of organizations

Based on the research of critical processes and activities in both infrastructure objects of energetics, the description of interdependencies and assessment of the likely effects of the impact of various factors has been proposed a methodology for planning the continuous operation of nuclear power plants **[4]** and gas storages.

The methods include, but are not limited to, the following elements **[1]**:

- Standardization of terminology;
- Identification of the main, minimal mandatory stages of the planning;
- Determination of approaches in creating a policy for continuous operation and strategy for its implementation;
- Description of the mandatory preliminary analyzes (such as Impact Analysis on the Activities (IAA)), which to be held at the stage of preparation of the plans in order to identify critical processes and the impact on them of different kinds and types of threats;
- Determination of alternatives and priorities to ensure the continuous operation, and also approaches to their implementation;
- Determining the types of plans (Plan for Response in case of an incident; Plan for Activity Management, Plan for Reconstruction and continuation of the business, Plan for communication and media relations, etc.), the relationships between them and their relations with other elements of the management system. Development of modular plans, depending on the type of the threat;
- Identification and selection of different methods and ways to bring the plans into action in order to obtain best results;
- Determining the appropriate means, forms and approaches to staff training;
- Selection of the approaches to create a database, and process automation;
- Creating a mechanism to monitor and control the planning and implementation of the activities in support of the continuous operation.

4. Model of management system for the continuous functioning of organizations

Management of continuous operation is not only the preparation of plans. It is neccessary after the planning phase to be developed activities in support of the development of efforts towards the continuous improvement of planning and the conversion of accompanying processes in part of the overall culture of the organization **[5]**.

For this purpose is developed the System for continuos functioning of the System of reactor type BBEP of NPP "Kozloduy".

Pre-developed methodology for planning of the continuous operation is used to create a documentary base of the planning phase of the Management System for continued functioning. Within this layer is defined and its scope, which is necessarily included, but not limited to:

- Policy for continuous technological/business development;
- Sources and methods for providing the necessary resources;
- The procedure for selection of suppliers of critical materials and services;
- Procedures for training of personnel and establishing traceability of the level of competence, and maintenance of the competence of the specialists;

- Procedures for conducting IAA, risk assessment and strategy for continuous operation of the System;
- Structure for the implementation of the management activities for the continuous operation of the System;
- Various plans to counteract to the effects of different kinds and types of threats;
- Procedures for implementation of the plans;
- Procedures for maintenance, review and audit of the activities;
- Procedures for preventive and corrective actions;
- Procedures for management review and provision of evidence for the continuous improvement;
- Creation of Handbook for Management of Business Continuity System, respectively for NPP.

5. Testing of the methodology and the model

The Methodology and the Model of the System for business continuity are tested for suitability in terms of OCI of energetics, such as NPP "Kozloduy" and UGS "Chiren". For this purpose is developed software based on the tests which have been conducted and which became the basis of the future Integrated Control and Information Centre (ICIC) **[1]**. It is expected ICIC to be based on testing the methodology to ensure the security and protection of OCI of the energetics, across the country (incl. methodology for the planning of continuous operation) and the model of the system to increase the opportunities for protection of such sites (incl. the model of the system for business continuity). The software covers all aspects of the protection of OCI **[1]**, as a separate module in it is developed the ability to manage the processes for continuous operation. ICIC has all the features of the management of security and protection of OCI:

- Preparation and deterrence:
  - Planning of the mission;
  - Reduction of the risk;
  - Training and simulations;
  - Resource Management;
  - Prevention through monitoring and fast response of specialized sensors (developed specifically for this purpose in IMSETHC-BAS);
  - Detection and Warning.
- Response:
  - Creation of a common operational picture;
  - Real-time management and distribution of guidance and information;
  - Coordination, leadership and communication.
- Recovery:
  - Planning and management of the reconstruction;
  - Analysis of actions and creation of conditions for education and training, based on past experience.

The advantages that contribute to the development of the software for business management ICIC are the following, but not only:

- Presenting real-time common operational picture;
- Creating of conditions for fast and accurate orientation in the given situation;

- Ensuring minimum response time;
- Effective location and use of the available and required resources;
- Creating conditions for close and effective cooperation between the different authorities involved in the organization;
- Accurate and effective debriefing after dealing with crisis;
- Providing opportunities for reliable connections for integration with external databases and communications within the multifunctional systems.

Developed is a plan to conduct tests and simulate various scenarios of threats, and depending on the specifics of the latter, are implemented various plans or just separate modules from them. Major emphasis is placed on the means for putting plans into action, as widely are used computer technologies for collecting, processing and disseminating of data. At the maximum extent are developed and practically implemented, advanced interfaces between decision-makers, performers and actuators for the automation of processes, quick responses and increase of the reliability of the results obtained.

During the testing of the Methodology and the Model were conducted internal audits over a period of time, as well as a management review. On their basis are classified the results that outline the directions for improvement of the best practices for continuous operation of the test subjects.

In conclusion, it should be noted that within the dynamic environment, Republic of Bulgaria becomes a key factor in the building and maintaining in national, regional and international plan, of the strategic energetics facilities, which significantly increase the risk of terrorist actions. Increasing the quantity, diversifying their type and extension of territorial areas in which they are, combined with increasing risks of terrorist acts, is calling for a synchronized measures for their protection, not only in the use of adequate systems but also in the development of appropriate methodologies and models to enhance the capabilities of their security. By the described methods, models and systems will not only be created a systematic approach to enhance security and protection of OCI in Bulgaria, but it will also provide a significant contribution to strengthening of the European security in this area **[6]**.

That was one of the objectives of the project "Developing the tools necessary to coordinate the internal sectoral activities to protect the critical infrastructure in case of multivariate terrorist threat. Increasing the capacity to protect key sites of the critical infrastructure in Bulgaria - BULCIP ", HOME/2010/CIPS/AG/019, under Programme of the European Commission "Management of prevention, preparedness and consequences of terrorist threats and other related risks", in the frame of which for the first time in our country was tested the methodology to ensure the continuity of OCI.

6. Conclusion

In conclusion, it should be noted that one of the main objectives of the management of business continuity is to prevent interruptions, that can be avoided in the activity of OCI. From here on, particularly important is to understand the threats to the continuity of individual operations and the activity as a whole, as well as the vulnerability of the OCI to these threats. The prioritization of the threats contributes to setting the priorities for risk reduction. On its part, the hierarchy of business functions, in terms of the likelihood of their interruption, contributes to determining which functions require

specified strategies to ensure the continuity. This is related to the IAA, which realized in the development of the model of the system for managing of the business continuity leads to increase of the capabilities of OCI to counter multivariate threats, thereby laying the foundations of a systematic approach to provide advanced security and protection.

References:

[1.] Stoichev K., System for effective Business Continuity Management, June 2013, ISBN: 978-954-644-470-7.

[2.] Stoichev K., Foundations of development of defense research and technology in Bulgaria, ISBN 978-954-92552-2-5. София, 2011.

[3.] Good Practice Guidelines, A Management Guide to Implementing Global Good Practice in Business Continuity Management, Business Continuity Institute, 2008.

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

[5.] Vodenicharov S., Stoichev K., Conceptual characteristics of a national strategy for research and technology to combat terrorism and piracy, international scientific conference "Marine power and fight piracy and terrorism at sea", May 18-19, 2011, Naval Academy, Varna.

[6.] 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.