*Open Access Library Journal*

# Integrated Model for Security and Protection of Critical Infrastructure

**Kiril Stoichev**

Institute of Metal Science, Equipment and Technology, Hydroaerodynamics Centre, Bulgarian Academy of Sciences, Sofia, Bulgaria
Email: kstoichev@ims.bas.bg

Received 24 October 2014; revised 28 November 2014; accepted 17 December 2014



## Abstract

**The creation of a matrix of minimum mandatory requirements for building a reliable system to counter potential terrorist threats is essential to increase the security and protection of critical infrastructure. In order to obtain an objective assessment of the success achieved in terms of necessary level of security and the extent to which is reached the reliability of critical infrastructure we should use a standardized approach and criteria. This is the purpose of this article, namely, to present the characteristics of a methodology for creation and the characteristics of an integrated, standardized model in this area, which can become the foundation of a comprehensive approach to the successful implementation of the so called L-strategy, *i.e.* protection of the individual and infrastructures against the threat of terrorism.**

## Keywords

**Integrated Model for Security and Protection, Critical Infrastructure, Terrorist Threat**

**Subject Areas:** **Engineering Management, Management Organization, Risk Management**

## 1. Introduction

In response to the need to strengthen the capacity of the European Union (EU) for the prevention of terrorist attacks involving critical infrastructures as well as to optimize the Union's readiness to respond to them on December 8, 2008 was accepted Directive 2008/114/EC of the Council of the EU on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

With the adoption of the Directive were laid the foundations for the systematic efforts of the Member States in their desire to raise the necessary amount of levels of security and protection of sites of critical infrastructure in the areas of "energy" and "transport". Of course, this was not the first attempt in this direction (for example, on 17 November 2005 the European Commission adopted a Green Paper on a European Programme for

**How to cite this paper:** Stoichev, K. (2014) Integrated Model for Security and Protection of Critical Infrastructure. *Open Access Library Journal*, **1**: e1124. http://dx.doi.org/10.4236/oalib.1101124

Critical Infrastructure Protection), but this document defined the legal requirements in terms of improving the security and defense of these objects.

Given these realities, in 2011, under the leadership of the Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre—BAS, was pioneered one of the largest European projects in the field of combating terrorism—HOME/2010/CIPS/AG/01. For the first time in the theory and practice of research and development in this field in our country (and in the EU as a whole I think) was made a successful attempt to create an integrated model for security and protection of sites of critical infrastructure. Efforts of the project team in this direction focused on the modeling of advanced systems for security of NPP, underground gas storage and the outer airport perimeter for internal security purposes.

Within the above tasks separate teams used similar in structure but different in content methodologies. And this was done in order to allow forming the outline and describing the characteristics of an integrated model for security and protection. On the other hand, it was necessary experts in this field to have a starting point for discussion and improvement of the system properties of the model.

This is the purpose of this report, to provide a matrix of minimum mandatory requirements for building a reliable system to counter potential terrorist threats, leading to the increasement of security and protection of sites of critical infrastructure.

In the following lines, the idea of systematizing these requirements in an integrated model for security and protection will be described.

## 2. Description of the Model

Regardless of the different methodologies adopted in the development of security models as a starting point for all of them, it is adopted a common terminology. For example, to describe the concept of "Security and Protection" was adopted the following definition: "The system for security and protection is a set of components operating in a single security concept, purposefully managed in a common informational environment to ensure processes, aimed early detection of threats and preventive response to prevent adverse effects" [1]. As for the term "critical infrastructure", it has determined on European level as: "System or parts of it, which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of the population and the disruption or destruction of which would have a significant impact in the given Member State as a result of the failure to protect those functions" [2].

On the base of above mentioned the following functions of the model are proposed:

- Detection of terrorist attacks, awareness and response;
- Keeping of constant preparedness for response;
- Ensuring continuous and normal operation of the object of critical infrastructure.

The purpose of the Model for security and protection is through organizational and technical activities to identify threats, to propose response and reaction to prevent unauthorized access to the secure area of the critical infrastructure [3], by offering the following features:

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

Accepted theoretical approaches to the realization of the parameters of model characteristics are described in the next section of this article.

### 2.1. Organizational Part

Organizational part can be composed of several components (depending on the approach used by the researchers), but in this case the structure is appropriate to include the development of:

- An analysis and risk assessment;
- Security and protection Policy;
- Strategy for security and protection;
- Plan for security and protection (including Business Continuity Plan);
- Corrective and preventive actions; and
- Training programs.

Of course, analysis and risk assessment can be carried out using different methodologies. This is not the sig-

nificant, but linking the results of this process with subsequent steps by the authorities involved, aimed at increasing of the security and protection of the object of the infrastructure. So, without claiming to be exhaustive, the process may include the following elements [3]:

- Evaluation of risk factors, such as the following groups threats:
  - Natural threats (natural disasters);
  - Threats to machines, facilities and buildings (fires, explosions, etc.);
  - Threats against staff (strikes, epidemics, etc.);
  - Threats to technology (loss of data, failure of software or hardware, etc.);
  - Threats to operations (financial crises, losses of key suppliers, etc.);
  - Social threats (riots, protests, sabotage, vandalism, etc.).
- Vulnerability assessment of the elements of the object;
- Sustainability appraisal of the staff and the public.

In turn, the vulnerability assessment of the structural elements of the object can be made as to the effect of external influences, as the result is card of the vulnerable junctions and interconnections [4]. It includes the evaluation of each item with the following parameters:

- Overall reliability—a measure of the extent and ability of the elements of the site to protect the equipment, machines and working with them of the actions of terrorists;
- Availability of external influence—measured in terms of relative ease, relaxation or particular difficulty in movement of terrorists to the protected object or inside it;
- Recognition of an outside watcher—characterizes the difficulty of defining the functions and importance of the object or machinery and technology lines located in it.

On the basis of this review we have to determine the extent for most effective implementation of activities for assurance of security and protection of the site.

Sustainability appraisal of staff and the public from the effects of risk factors can be done with the use of multiple methodologies for human resources management.

Based on the analysis and risk assessment is necessary to develop a conceptual framework to guide our efforts in the right direction *i.e.*, to formulate a Policy for security and protection of the site.

A security policy is nothing more than a well-written strategy on protecting and maintaining availability to your network and it's resources [5].

The policy sets out the principles and responsibilities for responding to interruption of technical processes as a result of the terrorist threat in a manner ensuring timely maintenance or restoration of critical functions (processes), as in the same time providing minimized impacts on critical functions (processes) and equipment [3]. It should be aimed towards:

- Ensuring the continuity of the critical functions (processes) of the object;
- Sharing between management and the reaction forces of the roles and responsibilities of management in the event of a terrorist threat;
- Ensuring a consistent approach to ensure the security and protection in accordance with international and national standards;
- Integration of the system for ensuring the security and protection within frameworks and processes of risk management of the site.

At the same time, the Strategy for security and protection defines the basic framework of rules and instructions for operation of the System for security and protection. It regulates the determination of the means and procedures as well as the responsibilities of all staff involved in the process. The result of the implementation of the Strategy is to achieve support from the senior management for the overall system for security and protection.

Development of the Plan for security and protection describes the processes and resources required to achieve the objective—ensuring business continuity of the object of critical infrastructure. It should contain, but without limitation, the following information [6]:

- Strategy for overcoming of the incident (in this case the realization of terrorist threat);
- Minimum requirements for the recovery of continuous operations;
- List of team members, rights and responsibilities, and contact information;
- List of materials delivered off-site;
- Activities organized by phases.

The description of each activity must respond to the following questions: What should be done?; How it

should be done?; Who should do it?; What is needed to do this?; Where is possible to do the action?; When to start?; How long can it last?; When should it finish?

On the other hand, operations need to be grouped into the following phases (phase-grouping of actions to provide the logic structure of the plan) [7]:

**Phase 1—**Initial assessment and response;

**Phase 2—**Temporary measures for unforeseen events (to limit the impact of the event);

**Phase 3—**Provision of resources;

**Phase 4—**Recovery of operations;

**Phase 5—**Return to normal condition.

The steps in organizing preventive actions should be related to [8]:

- Taking preliminary steps to make sure, that will not appear any already found discrepancy;
- Analyzing system processes to determine how to build safeguards or their change/update to prevent the occurrence of inconsistencies.

As interconnected, integral part with the preventive actions, corrective, in turn, should be directed to:

- Identifying and documenting the reason for the discrepancy;
- Review of the overall system to make sure that would not occur any other similar discrepancies;
- Analysis of the effect that non-compliance can cause and take appropriate action for a detailed review of the situation;
- Conducting follow-up inspection to make sure that the corrective action is effective and re-occurrence of non-compliance is prevented.

Throughout the training is minimized the difference between the competence required for the job and the personnel, that is designated to meet the requirements for this position. Throughout the training the organization has to ensure that officials who are assigned on a specific job are competent on the basis of education, training and experience [9]. Application of a uniform policy for the training and qualification of personnel, aimed at achieving the objectives of security and protection, it is necessary to:

- Maintain strict and accurate control of the quality of teaching of the study material;
- Ensure and guarantee the high qualifications of the personnel conducting the training of various professionals;
- Provide and maintain modern educational facilities for quality education.

## 2.2. Technical Part

In the technical part of the Model of system for security and protection can be divided to three secondary models [3]:

- Model on the territory for deploying the critical infrastructure;
- Model of risks and threats; and
- Model of the equipment on site.

They set the parameters, determined by possible means for influence by terrorists. In the same time are presented and characteristics of technical means for monitoring and warning of reaction forces—transport, IT, weaponry, evaluation of the area and determine the times to reach critical points, etc.

Modeling the territory for deploying the critical infrastructure is performed in order to provide security and protection of this infrastructure by digital analogue for mathematical processing of the data. To solve this problem, the Model on the territory for deploying the critical infrastructure is described by a peripheral zone, lanes and segments.

Depending on the risks and threats to the peripheral zone is divided into:

- Green lane—this is the lane that is not guarded and is actually off-site;
- Lane for detection, bounded by two lines:
  - Line to indicate entry into the peripheral zone of the object;
  - Line for light and sound warning for entry in the peripheral zone.
- Detection lane bounded by:
  - Line for recognition of techniques and personnel;
  - Line for controled access.
- Reaction lane.

The purpose of the segments is to identify sectors with similar characteristics and identical facilities to provide effective security and protection of the site.

Throughout the Model of risks and threats can be solved the following tasks:

- Determine the most likely areas to carry out terrorist attacks;
- Determination of forces and means that will have influence on the object;

In conclusion, the Model of the equipment is built to determine the types of devices and systems, depending on the ability of terrorists to influence the object of critical infrastructure (including security, retention and intruder alarm (sensor environment)).

### 2.3. Procedures for Realization of Policies, Strategies and Plans

To be able to realize the established policies, strategies and plans to ensure the security and protection of critical infrastructure, the relevant managements should create the conditions for a detailed description of the implementation activities that are bound by time, place and responsibilities. The claim that this is done within the sectors/phases of the plan for security and protection is wrong and one of the most common cases of failure in the implementation of the plans is the lack of clear and orderly procedures for their implementation.

The procedure is a way of carrying out a process or activity (may or may not be documented) [10] and its main goal is to support of the implementation of the policy and describes who, what, where, when and why needs to be done to achieve the set objectives on desired levels of security and protection. The final results from the creation of the procedures are converted into operating instructions, a set of actions or operations to be performed in the same way to achieve the desired effect under the same conditions. In many cases, the structure and content of procedures includes the question "how?", which in practice are specific instructions that detail the elements of the activities described in 2.1.

## 3. Results

An integrated Model for security and protection of critical infrastructure is not an end in itself and does not intend solely the effectiveness for the created for this purpose system. In this report is presented just of the alternatives that can be discussed between the experts and this version of the model has the following characteristics:

- Organizational part—development of:
  1) An analysis and risk assessment;
  2) Security and protection Policy;
  3) Strategy for security and protection;
  4) Plan for security and protection (including Business Continuity Plan);
  5) Corrective and preventive actions; and
  6) Training programs.
- Technical part:
  1) Model of complex for the deployment of the object;
  2) Model of risks and threats; and
  3) Model of the equipment on site.
- Procedures for the implementation of policies, strategies and plans.

On the basis of the above mentioned was developed and a Model for decision making in multivariate terrorist threat, which together with considered integrated Model creates the necessary conditions to significantly increase the systems efficacy. The Model for decision making in multivariate terrorist threat is the main result of the considered approach—through the development of models of the elements of an integrated security system to create conditions for increasing the security of critical infrastructure. This model allows the initial response forces to be adequate to the surrounding environment which will help to avoid such tragedies that occurred on 11 September 2001 in the US.

The developed models have set the basis for standardization of a large part of the activities related to the construction of the Systems for security and protection. And the last is crucial, given that for an adequate response to the same emergency authorities involved and organizations in a country (not to mention the various countries) react in very different ways, leading to disparate results in many cases with insufficient effect. To significantly reduce insecurity and increased relevance of these reactions can be successfully used the above system models

that have been developed by the project team with reference number HOME/2010/CIPS/AG/01.

Another direct result of the development of the considered integrated Model is the opportunity of creating security levels for critical infrastructure which can form the basis for objective assessment of the security of the critical infrastructure. What this means? We are not sure how many reliable is an infrastructure. To make sure that our actions to ensure security have been adequate to our environment by implementing security levels we will have objective criteria for this evaluation. The latter will allow these evaluation criteria to be standardized, which will enable them to be used by all specialists in this area.

And last but not least, the integrated system for security and protection of sites of critical infrastructure provides an unsurroundable, key benefit—provides significant time resource for the forces for initial response, which allows to maximum extent to reduce the response time and creates conditions for preservation of life and health of personnel and protection of the integrity of the material resources.

## 4. Conclusions

On the basis of the above, the following conclusions can be made:

- Ensuring adequate reaction of the forces for initial response to the terrorist threat can not be achieved with only organizational or technical means. Timely and targeted symbiosis between them embodied in integrated system for security and protection, can ensure a high level of adequacy against the threat, which in most cases can be a combination of multiple hazards;
- Many possibilities for combating terrorism need to be systematized, various configurations of abilities to be tested and on this basis to select the most appropriate option for countermeasures. And this was done in the framework of this project, in the result of which was identified the model of the integrated system, subject of this document;
- Response time of the forces for initial response is crucial for the number of fatalities, injuries and material losses in any terrorist attack. The integrated system allows the time to be significantly reduced;
- The integrated model for security and protection is an open system that can and will be upgraded with the help of all specialists in the field of defense and security not only in our country but also by the member states of the EU;
- The process of standardization for building integrated security systems of critical infrastructure will contribute the increasing the security of the latter and will give an opportunity for objective assessment of the level of security;
- The use of uniform and standardized approaches to building security systems will allow to enhance success of learners and increase their skills and experience;
- And the last but not the least, the exchange of experience between specialists involved in the fight against terrorism in different parts of the world will be much more effective because they will "speak the same language" using a unified methodology.

## Acknowledgements

Presenting the results of the realization of the project: "Development of the tools needed to coordinate intersectoral activities to protect critical infrastructure in a situation of multiple terrorist threat. Enhance the ability to protect key sites of critical infrastructure in Bulgaria" we can not ignore the enormous contribution of Mr. Stefko Burdzhiev last director of Genera Directorate "Civil Protection", who actively participated in the formulation of the goals and objectives of the project and provided support to the state administration for its successful implementation. Special thanks to our colleagues from Russe University "Angel Kanchev" for the great development of the software assurance of the model, to the colleagues from National Defence Academy "GS Rakovsky" who actively participated in the development of different models for security and protection and Associate Professor Dr. Georgi Botev's unique risk analyzes, that he made for the different objects of the critical infrastructure in the country, which I am sure will become a desktop reading for all professionals in the EU Member States, operating in the "security" and "defense" sectors.

## References

[1] Yachev, R., Project Team by NDA, Stoichev, K., Project Team by IMSETHAC-BAS (2013) 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".

[2] Directive 2008/114/EC of the Council of the EU on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.

[3] Vitanov, L., Project Team by NDA, Stoichev, K., Project Team by IMSETHAC-BAS (2013) 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".

[4] de Léon, J.C.V. (2006) Vulnerability: A Conceptual and Methodological Review. Source 4.

[5] Security Policy: What It Is and Why—The Basics. SANS Institute InfoSec Reading Room.

[6] Stoichev, K., Business Continuity Model of the NPP' System for Removing the Heat, International Workshop (2012) 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.

[7] ECP-601: Effective Business Continuity Management. The Institute for Business Continuity Training, US.

[8] ISO 9001:2008 Quality Management Systems—Requirements; ISO 22301:2012 "Societal Security—Business Continuity Management Systems—Requirements".

[9] ISO 22301:2012 Societal Security—Business Continuity Management Systems. Requirements.

[10] ISO/IEC 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements.