Journal of Applied Security Research
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/wasr20

Security Levels of Critical Infrastructure

Kiril Stoichev[a]

[a] Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre-Bulgarian Academy of Sciences, Sofia, Bulgaria

Published online: 14 Jul 2014.

To cite this article: Kiril Stoichev (2014) Security Levels of Critical Infrastructure, Journal of Applied Security Research, 9:3, 328-337, DOI: 10.1080/19361610.2014.913233

To link to this article: http://dx.doi.org/10.1080/19361610.2014.913233

Journal of Applied Security Research, 9:328–337, 2014

ISSN: 1936-1610 print / 1936-1629 online
DOI: 10.1080/19361610.2014.913233

Routledge
Taylor & Francis Group

Security Levels of Critical Infrastructure

KIRIL STOICHEV
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre-Bulgarian Academy of Sciences, Sofia, Bulgaria

There are numerous international standards and national requirements for the creation of physical and information security and protection of sites of critical infrastructure, risk management, and ensuring business continuity, as well as providing financial security for the environment, health and occupational safety, management of human resources, corporate social responsibility, and many other sectors. All of them in one way or another are directly or indirectly related to the provision of security and protection of the given site. Many of them are united by common methodologies and understanding of their nature, but between requirements to relevant systems in most cases there is no correlation and awareness of their integrity. At the same time, what is the criterion by which we can evaluate to what extent is ensured the security and protection of an organization? The last is of great importance, not only for insurance companies, but in most cases it is vitally crucial for the life and health of employees in the organization and society as a whole. It is therefore necessary to determine the scale of the levels of security and protection of sites of critical infrastructure, as well as to identify and codify requirements for them.

KEYWORDS Security levels of critical infrastructure, security management system, business continuity management

INTRODUCTION

Various aspects of creating management systems[1] for security and protection is regulated by a number of institutions, national, regional, or international

Address correspondence to Kiril Stoichev, Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre-Bulgarian Academy of Sciences, 67 Shipchenski Prohod Blvd., Sofia 1574, Bulgaria. E-mail: kstoichev@ims.bas.bg

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/wasr.

regulations and/or standardization documents. Bases, which set the framework of the requirements, are the following:

- In the field of information security:
  - International Organization for Standardization (ISO) 15443: "Information technology–Security techniques–A framework for IT security assurance";
  - ISO/International Electrotechnical Commission (IEC) 27002: "Information technology–Security techniques–Code of practice for information security management";
  - ISO-20000: "Information technology–Service management;"
  - ISO/IEC27001: "Information technology–Security techniques–Information security management systems–Requirements" are of particular interest to information security professionals;
  - ISO/IEC 27005:2011: Information technology–Security techniques–Information security risk management, and so forth.
- In the field of Business Continuity Management:
  - ISO 22301:2012 Societal security–Business continuity management systems–Requirements;
  - ISO 22300:2012 Societal security–Terminology;
  - ISO 22320:2011 Societal security–Emergency management–Requirements for incident response;
  - ISO 22313:2012 Societal security–Business continuity management systems–Guidance, and so forth.
- In the field of Security Management:
  - ISO/DIS 34001 Security Management System.
- In the field of Risk Assessment:
  - ISO 31000:2009, Risk management–Principles and guidelines, provides principles, framework, and a process for managing risk;
  - ISO Guide 73:2009, Risk management–Vocabulary;
  - ISO/IEC 31010:2009, Risk management–Risk assessment techniques, and so forth.

On the one hand, they all define detailed requirements for different aspects of the process of ensuring the protection of the organization[2] and contribute significantly to increasing its security. On the other hand, there are two main objective facts that do not allow these and other related documents to provide a much needed efficiency of effort toward the creation of the required level of security for the object of critical infrastructure:

- They lack a unified structure, common terminology, and basic definitions. In 2011 the International Organization for Standardization (ISO) launched a new approach to determine the requirements for the management of organization—creating integrated standards of ISO management systems (ISO management system Standards). This approach is developed

in ISO Guide 83 of 2011 and amended in Annex SL (April 2012) of the International Register of Certificated Auditors. It is aimed at developing new standards for management systems through a unified structure, identical text, general terms and basic definitions to improve their compatibility (Panevski, 2013);
- Lack of conventional matrix, generally accepted methodology for linking them into a single system to provide a synergistic effect of their implementation.

At the same time, in ensuring safety, different methods are introduced to determine appropriate levels of safety (particularly and not only in nuclear energy). In support of this, the methodology for determination of Safety Integrity Level (SIL) can be indicated, which represents the relative level of reducing the risk of accidental damage of technological equipment (IEC, 2004). This means SIL is a measurement of performances for requirements of Safety Instrumented Function (SIF). In the current European safety standards there are defined four levels of safety. The highest reliability level is 4, and the lowest level is 1.

On the other hand, in the determination of Information Security the following three architectural levels are used :

- Strategical or conceptual,
- Logical, and
- Systematic or technological (often referred to as level of realization).

If we add three vertical divisions to the above—people, information, technology, as proposed by Gartner, Inc. (Newman, Gall, & Lapkin, 2008)—it forms a comprehensive Architectural Model for Information Security.

All this shows that it is necessary to try to formulate certain levels for overall security of critical infrastructure sites.

To overcome these problems (the lack of different methodologies for building systems that provide security to the organization) that prevent the maximum use of available standardization, normative, and institutional tools to create high levels of security is necessary not only to build on the already gained vast experience from the application of some of them (e.g., in the field of information security and ensuring the internal security) and to unite around a single methodology for integrated use for the purposes of increasing the security level of the organization.

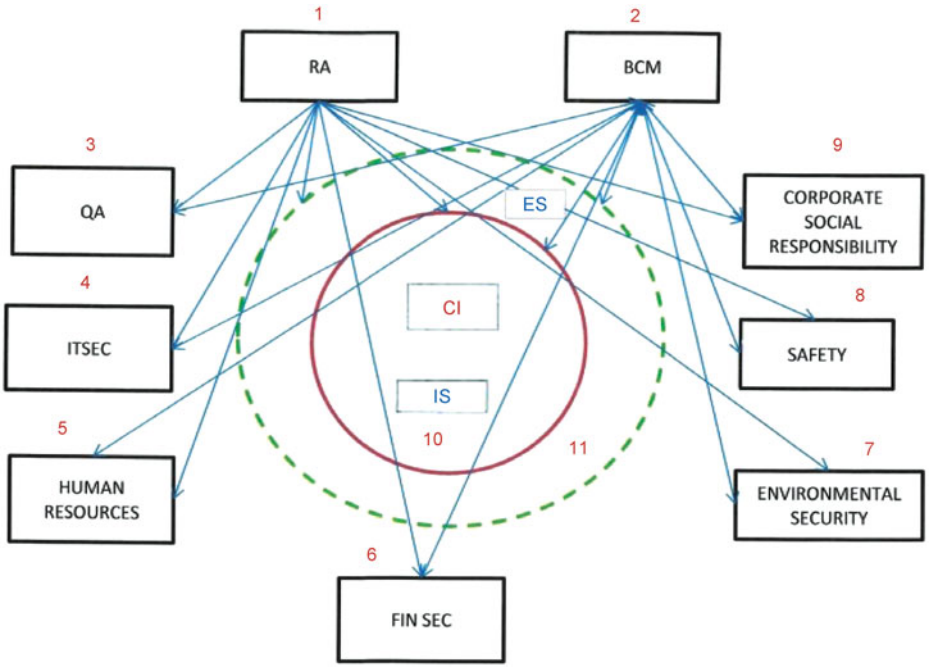

FIGURE 1 Management system through the prism of security.
Note. RA = Risk Assessment, BCM = Business Continuity Management, QA = Quality Assurance, ITSEC = Information Security, FIN SEC = Financial Security, CI = Critical Infrastructure, IS = Internal Security, ES = External Security.

CONCEPTION OF THE CRITICAL INFRASTRUCTURE SECURITY LEVELS

The management system of an organization consists of many subsystems that individually implement various organizational functions. If these subsystems are projected in the sphere of security and protection of the organization, we can confidently say that we have the picture presented in Figure 1.

The figure is an attempt to visualize the relationships between the different elements of the management system of the organization. Of course, these elements are not fixed and their number can be increased or reduced accordingly, as all of this depends on the analytical section of the goal we have set for researching (e.g., Financial Security, in terms of security can be assigned to Information Security, taking into account its direct dependence on Information Systems). However, this is not the focus of this article.

First of all, probably all would agree an input signal for the building of modern subsystems of the management system is the result of the conducted risk assessment. And this relationship is one-way—from risk assessment (RA) to each subsystem. And this is because RA is the source of information about

TABLE 1 Structure of Security Levels and Level Elements

Level	Level elements
1st level	1,10
2nd level	1,10,11
3rd level	1,3,8,10,11
4th level	1,3,4,5,6,8,10,11
5th level	1,3,4,5,6,7,8,9,10,11
6th level	1,2,3,4,5,6,7,8,9,10,11

how likely a certain event is to happen that allows the subsystem to take the necessary preventive and corrective measures to ensure the stability of its operation. As for the connection that is being unidirectional, it is clear that the source of information for RA is the surrounding environment of the organization which provides data on potential threats to one, several, or all of these management subsystems (here we assume that this is the beginning of the construction of these subsystems because if they are already established, the situation is different—RA receives information and from the process of its operation, not only from the environment).

At the same time, the relationships between Business Continuity Management (BCM) and other subsystems are bilateral (in the general case BCM is constructed after the other systems are developed). The input signal to the other subsystems is Business Impact Analysis (BIA), and the reciprocal relations of each subsystem to the BCM are being commodificated from the data for the state of the critical elements of the subsystem (it is well known that RA is committed to all potential threats, while the BIA assesses only the critical for the system elements).

The figure shows only the connections between RA and BCM without attempting to illustrate relations between other subsystems. The reason for this is the danger of shifting the focus of the objective—codification of the different sublevels for a comprehensive/integrated security of objects of the critical infrastructure.

This is why I will try to present a vision on the structure and content of security levels that should be formalized for the sites of critical infrastructure if we want to increase their security and protection. For a better view and to avoid repetitions I present to the attention of the colleagues in the scientific community in the security field the following structure and content of the security levels of the organization, presented in Table 1.

The topic is controversial and therefore this article will mark only the basic reasons which boosted my reasoning to suggest the structure of the levels and their content.

1st Level is suggested to include RA and IS. Why? This is the lowest Level of Security that a self-respecting organization (especially if it is an object of the critical infrastructure) must establish. There is no case in which an object

of the critical infrastructure has no system of internal security. Of course, in many occasions RA is either not a mandatory step in the construction of IS or is executed proforma. Here is the place to note that it is assumed RA is not a subsystem or system and is a process that underlies each of the subsystems presented here. Conversely, if perceived RA is a system, that means it will "obsess" the rest and then we will not talk about a number of other subsystems or systems, only a single system—RA. But in all cases, if one wants to build a (not stating if effective or efficient) system for Internal Security (Access Control System), this combination of RA and IS should be available.

The subsystems RA, IS, and ES are included in the 2nd Level. Why? In many buildings and objects (Critical Infrastructure), there are internal security systems (Access Control System). But their security bodies are not able to use an external security system that enables them to do their duties in the best way (it is proven that the cameras that watch outside the building or object are not enough). This fact is widely distributed in sites located in cities or for organizations that "coexist" with other organizations in the same building. Even then it is possible to build a system for external security; it depends largely on the designer of the system, which can build the External Security System using both its own sources of information and those that are owned by other organizations (in the shared building, for example).

The 3rd Level includes RA, QA, Safety, IS, and ES. Why?

The new subsystems are: QA and Safety. Not all organizations, especially the sites of critical infrastructure systems, have QA and even Safety subsystems. Of course, elements of these systems are developed at the sites of critical infrastructure, but in most cases, excessive "stumbled" on confidentiality does not allow the management to "swallow" the truth that international standards, which set requirements for these systems, can help both to improve the management of the sites and to enhance their security. Practice has proven on many occasions the logic and veracity of international standards and/or a combination of them increasing the level of security for an organization. Establishment of clear rules for effective management of organizations was first enshrined in the spirit of the standards ISO 9000 series (not accidentally, structure of the standard in 2012 was accepted as a standard in the creation of standardization documents, regulating requirements for management subsystems), which no one can argue is in the base of the good organization of the provision of security and protection.

As for Safety, this is not just about safety, which will ensure the health and lives of the employees in the organization, but emphasis is placed on safety and lives of citizens near the site of the critical infrastructure and society as a whole (so it is critical infrastructure because it can threaten one or another group [e.g., social, ethnic, or professional, etc.] in society). Therefore, these two additional subsystems (which should "go together")

are included in the third, higher level with the idea to become the subject of discussion and finally get into the "arsenal" of tools that organizations' management uses to enhance their security and protection.

The Fourth Level forms subsystems RA, QA, Information Security (ITSEC), Human Resources, Financial Security (FINSEC), Safety, IS, and ES. Why?

The new subsystems here are: ITSEC, Human Resources, and FINSEC. One of the most advanced subsystems of the Management System of the organization is for the providing of ITSEC. It is not available to previous levels because: (a) not all of the critical infrastructure sites have Information Systems (e.g., certain ammunition depots), (b) it requires significant investment to build them, and (c) ITSEC systems are applicable, especially for complex organizations where Information Systems are at the heart of their operation. However, if the organization wants to move to a new higher level of security for its own good it should build such a subsystem (even ammunition depots must have such security because they do not operate independently and are incorporated by a common system of warehouses and levels of government in which there is no way not to use Information Systems).

Human Resources are regarded primarily as an important element of the financial prosperity of the organization, providing qualified personnel and developing its skills over the years. This is exactly its crucial role in providing security. In many cases, however, this system is not used for security purposes because it is considered that it just needs to arrange the hiring of security guards and nothing more. In most organizations, these are not accepted as mandatory elements of the security system (i.e., special procedures are not created for the selection of these employees and there is lack of management of development of their capabilities). The staff providing security and protection are the foundation of success!

Systems for FINSEC on the one hand can be referred to as elements of ITSEC, and on the other hand at first sight they are not familiar with the objects of the critical infrastructure (they are connected mainly with the financial-credit institutions). In the first case, we have in mind the Information Systems which are used to provide the Financial Security of the organizations. However, it is not so much about them as about the ability and willingness of the organization to timely and adequately fund the activities necessary for ensuring their security and protection that is its financial stability and understanding on the side of the management. In the second case, it only seems at first sight that this subsystem is not valid for some of the objects of critical infrastructure. However, if applied to the above mentioned considerations it will be seen that this is not the case. Of course an organization's ability and the willingness of the management is not enough to say that there is a FINSEC subsystem. The subsystem itself must be

systematized in an orderly documentary framework, including (but not limited to) a clear policy, strategy, plans, and procedures to ensure financial security as an essential element of the security and protection of the organization.

The Fifth Level consists of the subsystems RA, QA, ITSEC, Human Resources, FINSEC, Environment Security, Safety, Corporate Social Responsibilities, IS, and ES. The new subsystems here are: Environment Security and Corporate Social Responsibilities. Both subsystems are somewhat "aside" to the objects of critical infrastructure, in terms of the main goal is to protect at all costs that for which the site provides security. However, this is only at first sight. For example, providing Environment Security is closely related to Safety in the organization and, aspreviously noted, that this is for the safety of citizens outside the site and the general public too.

Corporate Social Responsibilities are a relatively new field which yet goes at a fast pace in practice. In this case, it is extremely important for the motivation of the personnel and especially the staff responsible for the security and protection of the organization. If one clearly and accurately recorded the commitment of management and there is a build system that ensures its implementation in the event of a realized terrorist threat that there will be compensation for not only the employees but also their families, then the performance of the professional duties will be at an incomparably higher level from the daily activities when the slogan "it would only happen to me" is enshrined permanently in the minds of employees. Indicative is the case with Cantor Fitzgerald (The Institute for Business Continuity Training, 2011).[3]

Finally, the main element of the Sixth Level, which includes all the subsystems pointed to so far, is the BCM system. For me, it is the link between all the other subsystems presented in this article. In terms of security, it is essential not only to BIA, which is a detailed image of RA, but mostly by the plans for the operation of the system. Establishing such a subsystem completes the final step of an integrated security and protection system of the organization. In practice, there is no other subsystem except for the BCM system, which in one way or another includes mandatory requirements in relation to the other subsystems of the management system of the business organization (Stoichev, 2013).

RESULTS

The above mentioned detail of the elements/levels of security aims primarily, but not exclusively, to create conditions for increased security and protection of sites of the critical infrastructure. Of course, the last may be achieved in various ways, the base of which, according to some experts, is a refinement of the technique and technology which are used in this field. However, this is a special case of the integration approach proposed here. By themselves,

the technologies are not able to do anything if they are not managed. This is the biggest confirmation of the claim that security is ensured by the joint use of technologies and organizational procedures for their management both together and united by individual items or complete systems for security and protection.

Determining the different levels of security in these systems is a fundamental criterion for assessing the degree of confidence in the organization, which the systems can and should generate in the users of its services, as well as in society as a whole. This trust can be materialized aside from anything else through the insurance system, which is its objective measure. But before we get there, it is necessary to develop detailed requirements for each of the previous levels of security, which subsequently form the basis created for the purpose of international standardization documents. Development of technique and technologies separately for the subsystems is not sufficient to ensure our security. Therefore, the skillful combination between them, combined with the best practices of management can create a flexible, reliable environment for the use of different combinations of tools and receive a synergistic effect of their use to ensure the required level of security of our organization.

CONCLUSIONS

In the realization of the project HOME/2010/CIPS/AG/019 on the Program of the European Commission, "Prevention, Preparedness, and Consequence Management of Terrorism and Other Security Related Risks," the need for an Integrated Security System for critical infrastructure sites was clearly demonstrated.[4] However, that was only the first step toward proving the need to develop new methods and mechanisms to enhance the security and protection of critical infrastructure and for increasing the confidence in the society that adequate actions are taken against the realization of potential terrorist threats. This article represents the second step in this direction and through it aims to provoke active discussion on the questions given here. I do not claim therefore that the proposed structure and content of security levels are exactly those that will remain in the future and are exactly those that can form this trust in the management of both organizations and society, but I am convinced that such levels must exist! The procedure for their implementation can follow the already known approach adopted by the ISO—development of standards with requirements to these levels and standards for their audit and certification. Only in this way can we say that we have passed to the next stage of its development toward ensuring increasingly higher and higher reliability of our efforts to preserve the lifestyle that we have chosen, democracy.

NOTES

1. Two terms will be used here—"system" when it comes to self-examination of the various areas of requirements to individual aspects of the functioning of an organization and "subsystem," where they are regarded as elements of the management system of the organization.

2. To avoid repetition, the terms "objects of the critical infrastructure" and "organizations" will be used synonymously in this article.

3. Cantor Fitzgerald loses all of its 658 employees, on September 11, 2001, in the building of one of the World Trade Center Twin Towers. The company undertakes agreement to provide 25% of its profits over the next five years for compensation, and within the next ten years to pay health insurance to families of the victims of its 658 former employees. Currently it is engaging more workers than before the September 11 attacks.

4. The author was the coordinator of this project.

REFERENCES

The Institute for Business Continuity Training. (2011). *ECP - 601: Effective Business Continuity Management*. Retrieved from http://www.ibct.com/

International Electrotechnical Commission (IEC). (2004, May). *Functional safety and IEC 61508. A basic guide*. Retrieved from http://www.charter-tech.com/general/safe_iec_basic.pdf

Newman, D., Gall, N., & Lapkin, A. (2008). Gartner defines enterprise information architecture (ID Number: G00154071). *Gartner, Inc*. Retrieved from http://w3.ualg.pt/~mzacaria/gic/gartner_ia.pdf.

Panevski, V. (2013, March 15). *Actual approaches for Management Systems integration elaborated on the base of ISO standards - ISO 22301:2012 and ISO 9001:2008*. Workshop on "Development of a methods and criteria for examination, analysis and assessment of the adjoining to the airport areas. Development of a security and protection model of the airport external perimeter," Project: HOME/2010/CIPS/AG/019, Sofia Airport, Bulgaria. Retrieved from http://www.homeland-security-center.bg/bg/projects

Stoichev, K. (2013, April 16). *The role of business continuity management in the business management system*. Seminar: "Development of a model for decision making at a situation of multilateral/complex terrorist threat. Development of unified integrated system for effective management against multilateral/complex terrorist threat," Project: HOME/2010/CIPS/AG/019. Representation of EC in Sofia, Bulgaria. Retrieved from http://www.homeland-security-center.bg/bg/projects