International Journal of Economics, Commerce and Management
United Kingdom Vol. IV, Issue 6, June 2016
http://ijecm.co.uk/ ISSN 2348 0386

METHODOLOGY FOR ASSESSMENT OF THE LEVEL OF SECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE

Kiril Stoichev ✉
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre
Bulgarian Academy of Sciences, Sofia, Bulgaria
kstoichev@ims.bas.bg

Valeri Panevski
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre
Bulgarian Academy of Sciences, Sofia, Bulgaria
panevski@ims.bas.bg

Dimitar Dimitrov
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre
Bulgarian Academy of Sciences, Sofia, Bulgaria
ddimitrov@ims.bas.bg

Nikola Obreshkov
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre
Bulgarian Academy of Sciences, Sofia, Bulgaria
nikola.obreshkov@ims.bas.com

Abstract

The 'Security Levels and Model of Integrated Security Management System' forms the basis for increasing the security and protection capacity of a critical infrastructure. This paper proposes a methodology for assessing to what extent is provided the security and protection of the respective key asset. In the Methodology are included key requirements and evaluation criteria *which are not used so far for assessing of Integrated Security Management System adequate to the thematic specifics in this area, especially in the context of constantly changing security environment as a result of increased terrorist activity.*

Keywords: Critical Infrastructure, Security Levels, Integrated Security Management System, Methodology for Assessment

INTRODUCTION

Kiril Stoichev published in the Journal of Applied Security Research three articles ("Conditions for Increasing of the Viability of Critical Infrastructure Objects"; "Security Levels of Critical Infrastructure" and "Alternative Method for Establishing of Security Levels") that raised the issue of critical infrastructure security by building an Integrated Security Management Systems (InSMS) on the basis of the security and protection levels that were implemented. There were presented different levels of security (Alternative Method for Establishing of Security Levels) for the critical infrastructure that could be identified and that can underpin the construction of InSMS, namely (See Fig. 1):

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

Figure 1: Integrated Security Management System

INTEGRATED SECURITY
MANAGEMENT SYSTEM

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

In this article we continue the development of theory and practice through presenting at your attention a draft methodology for assessment the security and protection level of critical infrastructure.

On the basis of above mentioned articles were determined the structure and content of the integrated security management of the organization. It should be emphasized, that in the world practice there is no such complete set of tools (there are developments in advanced stage - in Germany, for example, using the approach, which we here apply, but elements implemented are very limited) that allow the management (operators) of critical infrastructure to create conditions for high availability of the necessary security and protection of the key assets (to avoid repetition, in this publication the terms "critical infrastructure" and "key assets" are synonymous). So that we need a tool to evaluate the effectiveness of InSMS, since its introduction in operation, we will have the opportunity to reach pre-planned security and protection.

Unfortunately, there is no objective and verified in practice reliable mechanism for this. Currently available documentary base does not imply an objective assessment of level of security and protection. Of course, standardization documents in this area follow the guidelines of ISO 9000 series, as this is a basic ISO requirement (International Organization for Standardization (ISO) published in the month of December 1987 the standard "ISO 9001 Quality systems - Model for quality assurance in design / development, production, installation and servicing", which launched a new approach to determine the requirements for the management of business organization - creating integrated ISO standards for management systems (ISO management system standards (MSS)). At the present moment, the framework of this approach to develop ISOMSS has been developed in ISO Guide 83 by 2011 and supplemented in Annex SL (April 2012) of the International Register of Certificated Auditors (IRCA)). But as you'll see below in this article, the subjective moment dominates significantly in practice, as during the creation of the requirements and evaluation criteria for the respective organizations (which is permitted by the standards), so in the auditing of InSMS. If this is acceptable, for example for the assessment of quality systems and other management systems in business organization, then those related to the establishment of high levels of security and protection is absolutely inadequate and inappropriate. Why? Because the health and lives of employees should not be assessed in a way, that makes for tangible assets, regardless of the available insurance system. Loss of health and life cannot be measured with any other values!

It is therefore necessary to develop a methodology for assessing the level of security and protection of critical infrastructure and to present an acceptable option for such methodology. We say acceptable, because it needs a serious debate to be provided on this issue, especially at international level, within the EU and NATO for example, because only in this way will be able to consider all variables in the creation of such a security instrument. And that this should happen as quickly as possible doubt should not have.

STANDARDISATION BASIS FOR MANAGEMENT SYSTEMS ASSESSMENT

There are different in nature and content, and numerous standards that address some or other aspects of the assessment of management systems. Here, however, we will examine only those who have the most in common with the issue subject to security and protection.

Above all, these are the standards of the series ISO/IEC 27000 (the standards for the information security are leaders, in terms of their universality with respect to their treatment of security aspects), especially ISO/IEC 27004 and ISO/IEC 27007.

ISO/IEC 27004 presents guidelines for the development and implementation of measures and measuring mechanism to assess the effectiveness of an Information Security Management System (ISMS) and controls or groups of controls as specified by ISO/IEC 27001.

These guidelines include policy development, risk management of information security control objectives, controls, processes and procedures and process of system revision with the aim of its improvement (Information security management - Measurement).

Applying this approach allows to create a program for the evaluation of information security. The latter can become a reliable tool in the hands of the managements of organizations to identify and evaluate inconsistent and inefficient processes of ISMS, organizing their control and prioritization of actions related to improving or changing these processes and / or controls.

It is highly appropriate to note that the requirement to assess the effectiveness of information security derives from the ISO/IEC 27001, which requires organizations to "conduct regular reviews of the effectiveness of the ISMS, taking into account the results from the measurement / evaluation of effectiveness" and "measure / assess the effectiveness of controls to ensure that the requirements in terms of security have been met."

Another standard of the above series, which refers to the material evaluation of management information systems, is ISO/IEC 27007. It gives guidance on accredited certification organizations, internal auditors, external auditors / auditors from a third party and other organizations that perform audits of the ISMS (audit management system for compliance with ISO / IEC standard 27001) (Guidelines for information security management systems auditing).

Used in the standard approach is consistent with the logic of the sequence with ISO 19011, the standard of the International Organization (ISO) for Standardization to audit the management systems of quality and environment.

ISO/IEC 27007 covers:

- specific aspects of the audit for ISMS compliance with the identified by the standard requirements: program management audit of the ISMS (determining what to audit, when and how; determining the auditors, management of audit risks; maintain records of inspections; continuous improvement process);
- conduct an audit of ISMS (audit process - planning, implementation, key audit activities, including field research, analysis, reporting and follow-up corrective actions);
- guidance for auditors of the ISMS (competences, skills assessment).

But all that has been said until now is not to retell standards (so they only marked their topics and scope) and see if we can use them for the purposes of the methodology for security assessment and protection. Unfortunately, none of them was suitable! The initial reading showed that ISO/IEC 27004 is able to meet our expectations in this direction, but in practice it turns out that this is impossible. For example, the initial perception when we meet with the standard leads to the feeling that there is underlying mechanism for objective quantitative assessment of management systems. But it turns out that it treats issues solely in terms of policy development; risk management of information security; control purposes; controls, processes and procedures, as well as the process of revision of system to its improvement (i.e., carries only a qualitative assessment based on the elements of the program for the evaluation of information security). All this is necessary but insufficient condition not only to assess information security, but to apply the same approach to the assessment of InSMS.

If we turn ISO 19011 we will see that it is the same situation (must emphasize, however, that this is the main international standard to audit the management systems of any kind).

This conclusion is confirmed by its object and field of application - the standard only contains guidelines for auditing management systems, including the principles of auditing, managing audit program and audits of management systems, and provides guidance on evaluation of auditors (Guidelines for auditing management systems (ISO 19011:2011)). That is, there are no quantitative criteria for assessment of these systems - the first and indispensable stage of the assessment and present only the second - the audit.

And the third document, which must take into account when considering the standardization basis for assessing the management systems is EGESIF_14-0010/18.12.2014. This is a document of the European Commission for assessment of management systems and governance in the European structural and investment funds (Guidance for the Commission and

Member States on a common methodology for assessment of management and control systems in the Member States, 18.12.2014).

Its main advantage is that for each key requirement to criteria for assessment of control and management systems are applicable the following categories:

First Category

Works well. No improvement necessary or required minor one. No deficiencies were identified or insignificant / minor deficiencies are identified. These drawbacks no impact or have such minor on the functioning of system, under assessment.

Second Category

Works, but some improvements are needed. There are found some drawbacks. These drawbacks have a moderate impact on the functioning of the system under assessment.

Third Category

Works, but partially. Considerable improvements needed. Serious flaws identified. The impact on the effective functioning of the system under assessment is significant.

Fourth Category

Substantially does not work. Serious and / or broad gaps are discovered. The impact on the effective functioning of the system under assessment is considerably - the system assessed functions poorly or not at all functions.

The above is extremely important in terms of quality of assessment and reliability of the results. These categories, as well as in the preparation of the evaluation program of ISMS will be included key requirements and criteria for its evaluation.

In conclusion, it is necessary to say again that there is no available regulatory or standardization model, as well as there is no developed a methodology for assessment the degree of security and protection of critical infrastructure. In the following lines we will try to present at your attention an adequate thematic and specific methodology in this area.

NATURE OF METHODOLOGY

The methodology we want to create may possess three main elements:

- Key requirements, or if it is more acceptable, we can determine them as a key evaluation criteria. These are the identified eleven subsystems (see Stoichev K., (2014) Security Levels of Critical Infrastructure, Journal of Applied Security Research, Volume 9:3, 328-337, DOI:

10.1080/19361610.2014.913233) of the management system of business organization, configuration of which in levels of security and protection provide the framework / structure of requirements to the InSMS.

- Evaluation criteria, or if we follow the above mentioned logic - sub criteria. They represent activities and the documentary basis of the elements of each subsystem / key requirement and form the content of the ISMS.
- Categories of assessment to be applied for each key requirement and each evaluation criterion.

On each key requirement and each criterion are determined their weights in the frame of overall assessment. Indicative coefficients are listed in an Appendix. Of course, their values are subject to discussion and expert assessment of the maximum possible number of specialists in this field. But this is a stage of subsequent development of the methodology.

Also, it is necessary to point out that in the process of development of the methodology we introduced the following limitations:

- Current methodology can be used for assessment of the security of critical infrastructure;
- The methodology can not be used in the field of security and fight against terrorism.

It is important to be emphasized what is the main difference between the proposed methodology and audit methodologies for assessing such systems in the field of quality assurance, environmental and generally of the management systems. This methodology is based on relatively objective approach, quantifying the status of InSMS. If we look out above in the text, we will see that this is an European Commission approach for assessment of control and management systems of the European structural and investment funds, i.e., systems that manage huge financial arrays. While all other standardization documents for evaluation of management systems provide guidance on conducting audits of systems and formulating a final assessment of their condition based on the subjective assessment of the auditor. Of course, here in the proposed methodology we cannot escape from subjectivity, but through quantitative scale that define, reduce significantly this potential risk - subjectivity in the evaluation of InSMS.

That is when you need to evaluate the management of financial assets or management of security and protection of life and health of people and material values necessary to apply a quantitative approach to get close as possible to the true state of things (in the case comes to life, we cannot rely on abstract conclusions of specialists with put it mildly "other qualifications").

But what are the key requirements and evaluation criteria of InSMS?

Key requirements cover the existence of these procedures and management subsystems:

- Systematic procedures for Risk Assessment and Risk Management;
- Internal Security System;

- External Security System
- Quality Assurance System;
- Safety System;
- Information Security System;
- Financial Security System;
- Human Resources Management System;
- Environmental Security System;
- Corporate Social Responsibility System;
- Business Continuity Management System.

For its part, the key requirements contain in themselves the following InSMS evaluation criteria:

Systematic procedures for Risk Assessment and Risk Management

1. Policy and Strategy for Risk Assessment and Risk Management;
2. Procedure for Risk Assessment and Risk Management;
3. Plan for risks treatment (selection and acceptance of one or more suitable options for changing the likelihood of risks, their effects, or both, and to implement these options);
4. Risk Management Plan (containing clear rights and responsibilities of employees);
5. Training system for employees in the field of Risk Assessment and Risk Management.

Here it should be noted that the procedure for risk assessment and risk management; the plan for risks treatment and Risk Management Plan must include all assessments and procedures for Risk Management associated with each subsystem identified as sympathetic to the InSMS. This does not mean that we should form uniform documents, but must be saved links/references from this procedure and plans to everyone else in these subsystems assessment procedures and Risk Management Plans for their treatment and management.

Internal Security System

1. Requirements and design of the system;
2. Policy and Strategy for Internal Security;
3. Procedure for determining the reliability of staff;
4. Clearly defined rights and responsibilities of personnel - directly and indirectly related to the security and protection;
5. Audit procedure of the Internal Security System;
6. Self-assessment procedure, including assessment of the reliability and efficiency of the system;

7. Plans for: contingency/emergency situations; respond to identified threats; communication between the security and protection team members and plans, or other suitable, in terms of the functions fulfillment by key staff (incl. and records of staff education and training plan);
8. Program for system maintaining and developing, including ensuring its sustainability;
9. Education and training.

It should be noted again, in the context of comments by key requirement № 1, for example that everything related to staff this subsystem (incl. training and qualification) must be included in or referred to: the Human Resources Management System; the self-assessment procedure to be related to the audit procedure on quality assurance management and plans for emergency situations should correspond to the Business Continuity Management Plan.

External Security System

1. Requirements and design of the system;
2. Policy and Strategy for External Security;
3. Procedure for determining the reliability of staff;
4. Clearly defined rights and responsibilities of personnel - directly and indirectly related to security and defense;
5. Command and Control Center;
6. Audit procedure for the External Security System;
7. Self- assessment procedure, including assessment of the reliability and efficiency of the system;
8. Plans for: contingency/emergency situations; respond to identified threats; communication between the security and protection team members and plans, or other suitable, in terms of the functions fulfillment by key staff (incl. and records of staff education and training plan);
9. Program for system maintaining and developing, including ensuring its sustainability;
10. Education and training.

In most cases, the documents describing various aspects of internal and external security are the same. But for the purposes of the effectiveness of systems, if it is not appropriate to be separate, it is necessary in each of joint documents both systems to be clearly defined as separate but interrelated modules.

The Command and Control Center is listed as one of the main evaluation criteria for the external security system, in terms of the key character of this system. As for the internal security system, this system element is not always determinative of its efficiency and reliability (depends on many factors, especially by the specificity and size of the object).

Quality Assurance System

1. Policy and Strategy for Security and Protection;
2. Quality Assurance Manual;
3. Quality assurance management plans, related to the security and protection;
4. Procedure for amending and monitoring of changes in the documents, related to the security and protection;
5. Audit procedure for InSMS.

Based on this key requirement is to be noted that the policy and strategy must concentrate itself all the requirements in terms of security policies and strategies of other subsystems management. Quality Assurance Manual should contain absolutely all procedures from other subsystems, related to security and protection, or refers to them. The procedure for submission and review of the changes apply to all subsystems, as well as the procedure for auditing the systems.

Safety System

1. Policy and Strategy for Risk Assessment and Risk Management associated with safety;
2. Risks treatment plan (selection and acceptance of one or more suitable options for changing the likelihood of risks, their effects, or both, and to implement these options);
3. Life cycle management plan of the risk, safety related (with clear rights and responsibilities of employees and workers);
4. Training system for employees for Risk Assessment and Risk Management, associated with safety.

The safety system is integrated into the InSMS in a manner, described above for the other subsystems.

Information Security System

1. Policy and Strategy for Information Security;
2. Procedure for organizing the Information Security;
3. Procedure for access control;
4. Procedure for management and control of IT operations;
5. Procedure for acquisition, maintenance and development of information systems;
6. Management Plan for incidents, related to the Information Security;
7. Education and training of specialists in Information Security and all others indirectly associated with this activity.

The Information Security System is integrated into the InSMS in a manner, described above for the other subsystems.

Financial Security System

1. Policy and Strategy for Financial Security;
2. Procedure for Financial Risk Assessment and Risk Management;
3. Procedure for reporting the requirements of ISO/IEC TR 27015: 2012 in the organization;
4. Education and training of personnel, directly and indirectly engaged with the financial security.

The Financial Security System is integrated into the InSMS in a manner, described above for the other subsystems.

Human Resources Management System

1. Policy and Strategy for Human Resources Management, related to the security and protection;
2. Procedure for analysis, design of the positions and human resources planning in the field of security and protection (including identification of clear rights and responsibilities of security and protection officers);
3. Procedure for the staff selection and appointment;
4. Procedure for staff assessment;
5. Procedure for staff career development;
6. Procedure for ensuring the security of information relating to staff safety and security, including after the release of position by these officers;
7. Training procedures and training of security and protection forces in terms of building, operation, maintenance and development of the InSMS.

The Human Resources Management System, on the one hand, is integrated into InSMS in the manner, described above for the other subsystems, on the other hand, procedures for training and workout accumulate all requirements for employees and workers, directly or indirectly related to the security and protection that are educated and trained in accordance with these subsystems.

Environmental Security System

1. Policy and Strategy for Environmental Security;

2. Procedure for Risk Assessment and Risk Management, related to the Environmental Security (based on indicators for environment condition assessment that could be affected by the activities of the organization);
3. Procedure for the management of the organization to ensure Environmental Security (based on the indicators to improve efficiency of management and environmental performance of activities of the organization in the direction of enhancing the environmental security);
4. Education and training of personnel to ensure the Environmental Security by increasing the efficiency of the activities performed.

The Environmental Security System is integrated into the InSMS in a manner, described above for the other subsystems.

Corporate Social Responsibility System

1. Policy and Strategy for Corporate Social Responsibility (CSR) in support of security and protection;
2. Procedure for Risk Assessment and Risk Management, related to the impact of CSR on security and protection of the organization;
3. Procedure for motivation of employees (not just those related to security and protection) the tools of corporate social responsibility, directly and / or indirectly related to security and protection of the organization;
4. Education and training to assess and manage the risks, associated with the impact of CSR on security and protection of the organization.

The Corporate Social Responsibility System is integrated into the InSMS in a manner, described above for the other subsystems.

Business Continuity Management System

1. Policy and Strategy for Business Continuity Management;
2. Risk analysis and Risk Assessment, related to threats against business continuity;
3. Business Impact Analysis (BIA);
4. Action plan for crisis situations:
    a. Ensuring business continuity;
    b. Response to implemented threats to business continuity
    c. Business Continuity Recovery.
5. Education and training to ensure the business continuity.

By this system the InSMS should be plugged directly BIA and Action plan for crisis situations is necessary to cover all planned activities of other subsystems that are related to security and protection.

In conclusion should be noted that the basic structure and content of the InSMS may include the following (but not limited) arranged in a sequential order and unifying subsystem:

- Policy and Strategy for security and protection - quality assurance system is integrating system;
- Procedure for Risk Assessment and Risk Management, Plan for risks treatment and Plan for Risk Management – Procedure for Risk Assessment and Risk Management is an integrative procedure;
- Business Impact Analysis of the organization - Business Continuity Management System is an integrative system;
- Plans for Quality Assurance Management, related to security and protection - Quality Assurance System is an integrative system
- Action plan for crisis situations - Business Continuity Management System is an integrative system;
- Procedure for amendment of the documents, a process control included, in the field of security and defense - Quality Assurance System is an integrative system;
- Procedure for InSMS audit - Quality Assurance System is an integrative system;
- Training procedures and training of security and protection forces in terms of building, operation, maintenance and development of the ISMS - Human Resources Management System is an integrative system;
- InSMS Manual - Quality Assurance System is an integrative system.

Practically, the above represents the documentary base of the integrated management systems for security and protection of the organization. It is obvious that the majority of the documents that describe the InSMS are elements of the procedure for risk assessment and risk management and quality assurance and business continuity management systems. That is why they have been awarded the highest weight factors in the assessment. Score sheet, by which can be determined its current status is presented in Appendix.

Once again it must be emphasized that the weighting factors, presented in this assessment sheet are based on the expert evaluation. They can be changed, based on the number of factors, but their objectivity can be checked by using mathematical apparatus.

That is why we will stick to the proposed assessment methodology whereby expressed subjective moment exists only in determining the weighting coefficients of the key requirements and criteria (or put another way, the key criteria and sub-criteria). Therefore we developed below presents a mathematical framework through which the result of the methodology gained a numerical expression that objectively can provide us with information about the level of security and protection of critical infrastructure / key asset / key resource.

In this case, let's define these numerical sequences:

$$A = (\alpha_n)_{n=1}^{11} = (0.14, 0.10, 0.08, 0.14, 0.08, 0.12, 0.04, 0.07, 0.05, 0.04, 0.14)$$

$$B_1 = (\beta_{1,n})_{n=1}^{5} = (0.20, 0.20, 0.20, 0.20, 0.20)$$

$$B_2 = (\beta_{2,n})_{n=1}^{9} = (0.14, 0.10, 0.12, 0.12, 0.08, 0.12, 0.12, 0.10, 0.10)$$

$$B_3 = (\beta_{3,n})_{n=1}^{10} = (0.12, 0.10, 0.12, 0.08, 0.08, 0.10, 0.10, 0.10, 0.10)$$

$$B_4 = (\beta_{4,n})_{n=1}^{5} = (0.20, 0.20, 0.20, 0.20, 0.20)$$

$$B_5 = (\beta_{5,n})_{n=1}^{4} = (0.25, 0.25, 0.25, 0.25)$$

$$B_6 = (\beta_{6,n})_{n=1}^{7} = (0.15, 0.15, 0.14, 0.14, 0.14, 0.14, 0.14)$$

$$B_7 = (\beta_{7,n})_{n=1}^{4} = (0.25, 0.25, 0.25, 0.25)$$

$$B_8 = (\beta_{8,n})_{n=1}^{7} = (0.15, 0.15, 0.14, 0.14, 0.14, 0.14, 0.14)$$

$$B_9 = (\beta_{9,n})_{n=1}^{4} = (0.25, 0.25, 0.25, 0.25)$$

$$B_{10} = (\beta_{10,n})_{n=1}^{4} = (0.25, 0.25, 0.25, 0.25)$$

$$B_{11} = (\beta_{11,n})_{n=1}^{5} = (0.20, 0.20, 0.20, 0.20, 0.20)$$

where with A we denote the weighting of the key requirements and with B1, B2, B3,…., B11 - weighted coefficients of the criteria. Let us to define numeric row L, for which $(l_n)_{n=1}^{11} = card(B_n)$, i.e. L row contains the lengths of the rows $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3, \dots, \mathrm{B}_{11}$:

$$L = (l_n)_{n=1}^{11} = (5, 9, 10, 5, 4, 7, 4, 7, 4, 4, 5)$$

As seen for the weighted coefficients of the key requirements and criteria are met:

$$\sum_{i=1}^{11} \alpha_i = 1 \wedge \sum_{j=1}^{l_i} \beta_{i,j} = 1; \text{за } \forall\, i = 1, \dots, 11$$

Then overall assessment $\mathrm{O} \in [0, 1]$, indicating the level of security and protection of sites of critical infrastructure is given by the formula:

$$\mathrm{O} = \sum_{i=1}^{11} \alpha_i K_i = \sum_{i=1}^{11} \alpha_i \sum_{j=1}^{l_i} \beta_{i,j}\, \kappa_{i,j}$$

where with $\mathrm{K}_{i\ i=1,\dots,11}$ are marked the assessments of key requirements and with $\kappa_{i,j\ i=1,..,11;\ j=1,..,l_i}$ are marked the assessments criteria, such as:

$$\mathrm{K}_{i\ i=1,\dots,11} = \sum_{j=1}^{l_i} \beta_{i,j}\ \kappa_{i,j}$$

Possible assessments of key requirements are in the range $\mathrm{K}_{i\ i=1,\dots,11} \in [0,1]$, and the possible assessment of the criteria are defined by the following multitude:

$\kappa_{i,j\ i=1,..,11;\ j=1,..,l_i} \in \Upsilon = \left\{0, \frac{1}{3}, \frac{2}{3}, 1\right\}$, i.e. in the assessment of each criterion we use the four identified above categories. The numerical value of the first category is a unit, and a fourth is zero. For the second category is 0, 66, and a third is 0, 33.

But as the development of a comprehensive, practical and applied mathematical apparatus, as well the creation on its base software for automated assessment of InSMS is a challenge of the next stages of this research development.

This is a "tailoring" approach by which the fastest and systematic way any organization can create the necessary conditions to increase their security and protection. On this basis, after a thorough professional discussion within the EU and NATO, for example, may be established a single document for the evaluation of InSMS, which significantly increase the security and protection of critical infrastructure objects (which is one of the main goals of our business).

CONCLUSION

Enhancing security and protection of critical infrastructure is an ongoing process and it is not possible to prove that at a certain point we have reached a level that will ensure 100 percent security for society in terms of activity of the objects or assets. Regardless of the numerous approaches, methodologies, regulatory and standardization documents, which are used to solve the problems in this area is not developed theoretical framework, based on which to create practical application tools for the development and assessment of more reliable and more effective security and protection systems.

Unfortunately, in support of the above statement are conducted terrorist acts in Brussels on March 22, 2016. Once again it was clearly shown that we need to use new, unknown for the terrorists' way of providing an adequate response to their willingness to injure or destroy our way of life. And such could become the proposed in this paper approach. Integrated security and protection is a fundamental way of thinking and action that is expressed the attitude and the ability to analyze and evaluate the relationships between many seemingly incompatible factors but taking into account that can guarantee us high levels of security and protection.

Indeed, in conclusion, we believe that by using the selected methodology (but not only) the major new developments in the theory and practice of the respective area are proven. It is presented an advanced and new tool for the development of theory and practice in the field of security and protection of critical infrastructure in Bulgaria, the EU and Member States. In the developed methodology for unified assessment of the levels of security and protection of critical infrastructure objects, based on objective evaluation criteria, are described interdependencies between various aspects / sub-systems by business management system of the organization. And last but not least it was proven that through their mutual commitment in a unified system significantly is increased the security and protection, which contributes to synergy of efforts and results in this area.

We sincerely hope that this work will create a new dynamic of the discussion on how to assess the level of security and protection, how to determine to what level have created conditions, expected by us and our associated security and protection of critical infrastructures, we manage.

Only in this way we will be adequate to the rapidly changing security environment at national, regional and international levels, especially in terms of threats from "the plague of the century" terrorism in all its manifestations, nature and content.

REFERENCES

Guidelines for information security management systems auditing, ISO/IEC 27007

Guidelines for auditing management systems (ISO 19011:2011), BDS EN ISO 19011:2011

Guidance for the Commission and Member States on a common methodology for assessment of management and control systems in the Member States, 18.12.2014, EGESIF_14-0010

Information security management – Measurement, ISO/IEC 27004

Stoichev K., Conditions for Increasing of the Viability of Critical Infrastructure Objects, Journal of Applied Security Research (ID: 710131 DOI:10.1080/19361610.2012.710131)

Stoichev K., (2014) Security Levels of Critical Infrastructure, Journal of Applied Security Research, Volume 9:3, 328-337, DOI: 10.1080/19361610.2014.913233

Stoichev K., (2015), Alternative Method for Establishing of Security Levels, Journal of Applied Security Research, Volume 10, Issue 1, January 2015

APPENDIX

ASSESSMENT SHEET

Level of Security and Protection of Critical Infrastructure

№	Key requirement / Criterion	Weighting factor *in* the group	Weighting factor *of* the group	Given points
1.	***Systematic procedures for Risk Assessment and Risk Management***		0,14	
1.1	Policy and Strategy for Risk Assessment and Risk Management;	0,20		
1.2	Procedure for Risk Assessment and Risk Management;	0,20		
1.3	Plan for risks treatment (selection and acceptance of one or more suitable options for changing the likelihood of risks, their effects, or both, and to implement these options);	0,20		
1.4	Risk Management Plan (containing clear rights and responsibilities of employees);	0,20		
1.5	Training system for employees in the field of Risk Assessment and Risk Management.	0,20		
2.	**Internal Security System**		0,10	
2.1	Requirements and design of the system;	0,14		
2.2	Policy and Strategy for Internal Security;	0,10		
2.3	Procedure for determining the reliability of staff;	0,12		
2.4	Clearly defined rights and responsibilities of personnel - directly and indirectly related to the security and protection;	0,12		
2.5	Audit procedure of the Internal Security System;	0,08		
2.6	Self- assessment procedure, including assessment of the reliability and efficiency of the system;	0,12		
2.7	Plans for: contingency / emergency situations; respond to identified threats; communication between the security and protection team members and plans, or other suitable, in terms of the functions fulfillment by key staff (incl. and records of staff education and training plan);	0,12		
2.8	Program for system maintaining and developing, including ensuring its sustainability;	0,10		
2.9	Education and training.	0,10		
3.	**External Security System**		0,08	
3.1	Requirements and design of the system;	0,12		
3.2	Policy and Strategy for External Security;	0,10		
3.3	Procedure for determining the reliability of staff;	0,12		
3.4	Clearly defined rights and responsibilities of personnel - directly and indirectly related to security and protection;	0,08		
3.5	Command and Control Center;	0,10		

3.6	Audit procedure for the External Security System;	0,08	
3.7	Self- assessment procedure, including assessment of the reliability and efficiency of the system;	0,10	
3.8	Plans for: contingency / emergency situations; respond to identified threats; communication between the security and protection team members and plans, or other suitable, in terms of the functions fulfillment by key staff (incl. and records of staff education and training plan);	0,10	
3.9	Program for system maintaining and developing, including ensuring its sustainability;	0,10	
3.10	Education and training.	0,10	
4.	**Quality Assurance System**		0,14
4.1	Policy and Strategy for Security and Protection;	0,20	
4.2	Quality Assurance Manual;	0,20	
4.3	Quality assurance management plans, related to the security and protection;	0,20	
4.4	Procedure for amending and monitoring of changes in the documents, related to the security and protection;	0,20	
4.5	Audit procedure for InSMS.	0,20	
5.	**Safety System**		0,08
5.1	Policy and Strategy for Risk Assessment and Risk Management associated with safety;	0,25	
5.2	Risks treatment plan (selection and acceptance of one or more suitable options for changing the likelihood of risks, their effects, or both, and to implement these options);	0,25	
5.3	Life cycle management plan of the risk, safety related (with clear rights and responsibilities of employees and workers);	0,25	
5.4	Training system for employees for Risk Assessment and Risk Management, associated with safety.	0,25	
6.	**Information Security System**		0,12
6.1	Policy and Strategy for Information Security;	0,15	
6.2	Procedure for organization of the Information Security;	0,15	
6.3	Procedure for access control;	0,14	
6.4	Procedure for management and control of IT operations;	0,14	
6.5	Procedure for acquisition, maintenance and development of information systems;	0,14	
6.6	Management Plan for incidents, related to the Information Security;	0,14	
6.7	Education and training of specialists in Information Security and all others indirectly associated with this activity.	0,14	

7.	**Financial Security System**		0,04
7.1	Policy and Strategy for Financial Security;	0,25	
7.2	Procedure for Financial Risks Assessment and Management;	0,25	
7.3	Procedure for reporting the requirements of ISO / IEC TR 27015: 2012 in the organization;	0,25	
7.4	Education and training of personnel, directly and indirectly engaged with the financial security.	0,25	
8.	**Human Resources Management System**		0,07
8.1	Policy and Strategy for Human Resources Management, related to the security and protection;	0,15	
8.2	Procedure for analysis, design of the positions and human resources planning in the field of security and protection (including identification of clear rights and responsibilities of security and protection officers);	0,15	
8.3	Procedure for the staff selection and appointment;	0,14	
8.4	Procedure for staff assessment;	0,14	
8.5	Procedure for staff career development;	0,14	
8.6	Procedure for ensuring the security of information relating to staff safety and security, including after the release of position by these officers;	0,14	
8.7	Training procedures and training of security and protection forces in terms of building, operation, maintenance and development of the InSMS.	0,14	
9.	**Environmental Security System**		0,05
9.1	Policy and Strategy for Environment Security;	0,25	
9.2	Procedure for Risk Assessment and Risk Management, related to the environmental security (based on indicators for environment condition assessment that could be affected by the activities of the organization)	0,25	
9.3	Procedure for the management of the organization to ensure Environmental Security (based on the indicators to improve efficiency of management and environmental performance of activities of the organization in the direction of enhancing the environmental security);	0,25	
9.4	Education and training of personnel to ensure the Environmental Security by increasing the efficiency of the activities performed;	0,25	
10.	**Corporate Social Responsibility System**		0,04
10.1	Policy and Strategy for Corporate Social Responsibility (CSR) in support of security and protection;	0,25	
10.2	Procedure for Risk Assessment and Risk Management, related to the impact of CSR on security and protection of the organization;	0,25	

10.3	Procedure for motivation of employees (not just those related to security and protection) the tools of corporate social responsibility, directly and / or indirectly related to security and protection of the organization;	0,25	
10.4	Education and training to assess and manage the risks, associated with the impact of CSR on security and defense of the organization.	0,25	
11.	**Business Continuity Management System**		0,14
11.1	Policy and Strategy for Business Continuity Management;	0,20	
11.2	Risk Analysis and Risk Assessment, related to threats against business continuity;	0,20	
11.3	Business Impact Analysis (BIA);	0,20	
11.4	Action plan for crisis situations: a. Ensuring business continuity; b. Response to implemented threats to business continuity; c. Business Continuity Recovery.	0,20	
11.5	Education and training to ensure the business continuity.	0,20	
	Sum of the weights		1,00