International Journal of Economics, Commerce and Management
United Kingdom Vol. VI, Issue 8, August 2018
http://ijecm.co.uk/ ISSN 2348 0386

STRUCTURAL-FUNCTIONAL APPROACH TO THE MANAGEMENT OF SECURITY AND PROTECTION OF ORGANIZATIONS

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

Abstract
The security and protection of organizations is immanently inherent in their financial and economic sustainability. How to achieve reliable security and protection is a matter of particular relevance to them, taking into account the complex and dynamic environment, including threats of terrorism. The present manuscript builds on the already proven necessity of building and implementing Integrated Security Management System of the organizations to present the characteristics of the individual elements of such a system and the interconnections with the others. To this end, a structural and functional approach to the integrated security management systems and organizations' protection is applied.

Keywords: Security; protection; integrated security management; management of security; protection levels; HR management system; environmental security system

INTRODUCTION

The struggle against the terrorism has always been and is in the center of our attention and not only because terrorism is one of the basic problems of human civilization and leads after it ruins and destruction of human lives but also because the mere fact that this phenomenon undermines the moral fundaments of the society. Those who live with the thought to cause damages by terrorist acts do not know good from evil, do not respect the established national and international legal norms, strive to achieve their purposes by all means and at any cost, neglecting various rules and disregarding universal values of all kinds.

During the past years we all are witnesses of what happens in the Near East, Africa and Europe where history does not know such dimensions of the terrorism wave, where people are placed in situations which have never been predicted and where the terrorist attacks are remarkable for extreme defiance, inventiveness and use of all kinds of devices and methods to cause material damages and bring about human casualties.

The international terrorism passed over to a qualitatively new stage of its development and acquired a global character. It is already used not only as instrument to achieve concrete political purposes in an individual country or regional conflict but is directed towards change in principle of the existing system of international relations. The aim is chaos and economical destabilization in the target countries and provocation of fear and psychosis among the population, pursuing in the long run a global crisis.

Considering what has been said so far, in a series of publications (Stoichev K., (2014), Integrated model for security and protection of critical infrastructure, Stoichev K., (2014) Security Levels of Critical Infrastructure, Stoichev K., (2015), Selection of an Alternative Method for Establishing Security Levels), we considered the need to create an Integrated Security Management System (ISMS) for Critical Infrastructures (CI) based on the establishment of security and protection levels to be the basis for assessing CI.

The starting point is an organization's Management System, which consists of multiple subsystems that individually implement the various organizational functions. If these subsystems are projected on the security and протецтио of the organization, we can assume with sufficient confidence that the picture shown in Figure 1.

The Figure attempts to visualize the interrelationships between the various elements of the organization's management system through the security prism. Of course these elements are not fixed and the number of them can be increased or reduced accordingly, all depending on the analytical section we have set ourselves to study.

On this basis, the purpose of this publication is to present the individual elements of this model of the Integrated Security Management System, their interconnection and the synergy of the interaction between them. The characteristics of subsystems that form the individual levels of security and protection management will be presented. We will attempt to present the framework of requirements to each subsystem of the management system of organizations that form the management of individual security and protection levels without seeking to describe each subsystem as a detailed development for practical application (this is the goal of separate research and development).The aim is to prove the involvement of each of these systems to create the appropriate levels as a basis for building ISMS in this area.

Considering the fact that the volume of the material for their performance is enormous, they will be presented in a series of publications.

Risk Assessment, Internal and External Security, Quality Assurance, and Information and Financial security are an integral part of security systems, and we will therefore allow not to burden the reader with additional information, which is largely well known to the general public .

Therefore, we will allow in this paper to justify the interconnection of the Human Resources Management System and Environmental Security System with the overall security and protection system.

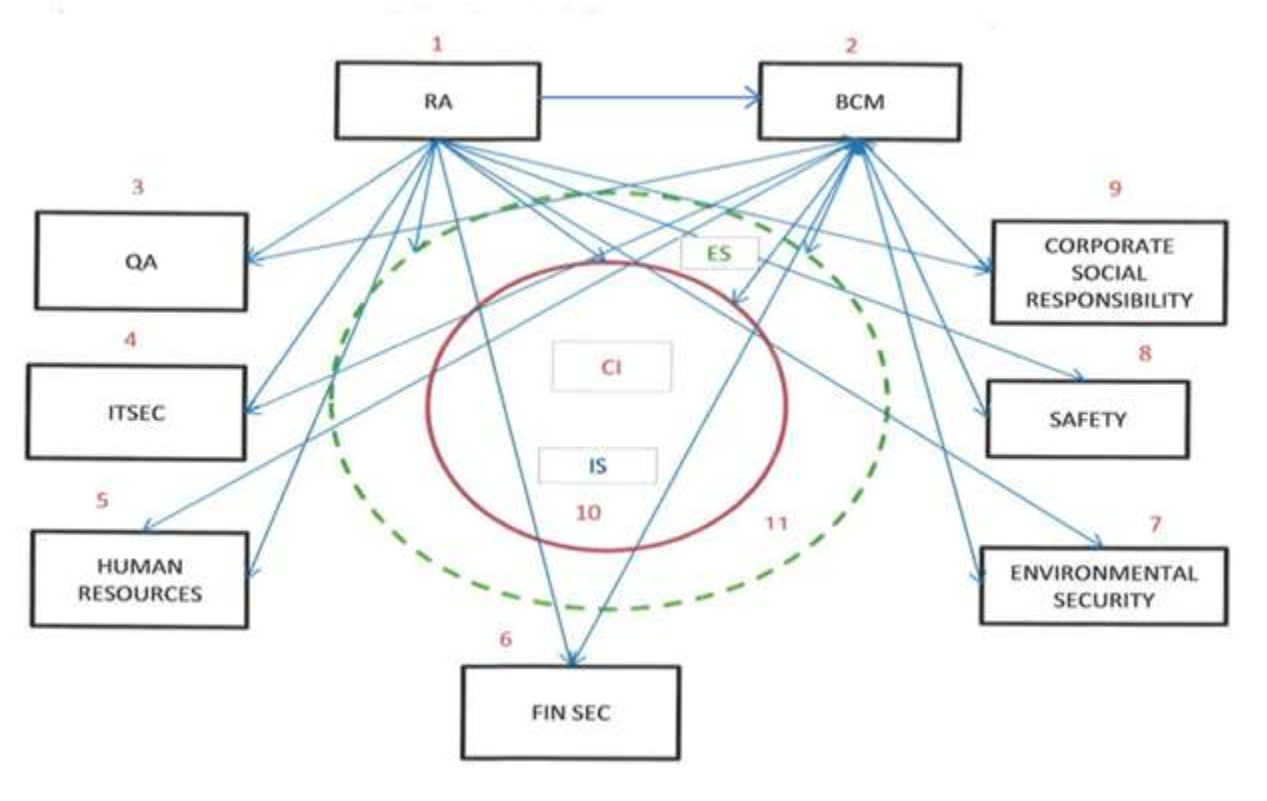

Figure 1. Management system through the prism of security

Legend: 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.

HUMAN RESOURCES MANAGEMENT SYSTEM

In order to carry out successfully the personnel policy in an organization it is necessary to build human resources management system. In the general case the definition of this system reads: “The human resources management system comprises all functions related to the management of these resources, the interrelations between them, relations with the environment, the ways of

labor organization for achievement of organization business purposes and the applicable tools of approaches, principles, methods and techniques" (Shopov D. and Atanasova M. (1998)).

However, here we speak of the personnel policy in relation to its engagement for increase of the critical infrastructure security and protection.

After the brief analysis about the contribution of this policy to the security made, we established that generally there are two main streams in the considered area: The first one is when the human resource management system does not put accent on any subsystem of the business organization management system but considers the items in their completeness (which is not bad but the absence of accent leads to responsibilities „washing out" and in the long run insufficient appreciation of the interrelations) (Harizanova M., Mironova N., Shtetinska T. (2009)). The second relates to ensuring the personnel information data base security and not to the contribution of the security personnel to the over-all object security and strengthening the connections of the personnel system with all other subsystems of the organization management related to security (ISO-27001/27002:2005 sects. 8.1 – 8.3,Centre for the protection of National Infrastructure (June 2013),Information Security Human Resource Development Program (July 8, 2011)).

If we take Margarita Harizanova's (Ph.D) and team model (Harizanova M., Mironova N., Shtetinska T. (2009)) we could note that the components of the human resources management system are the following: analysis and design of positions; human resources planning; recruitment and selection; human resources assessment; remuneration; training; career progress; motivation; ensuring healthy and safe labor conditions and improvement of labor relations.

But how can these components look through the prism of the critical infrastructure security and protection ensuring and improvement?

The positions analysis and design have to include systematic examination and determination of the content, the responsibilities and interrelations of the security specialists positions with respect to the remaining employees in all subsystems of the organization management system as well as specification of the requirements to these specialists.

The human resources planning is necessary to comprise the activities for determination of the needs of human resources in the field of security and protection and formulation of appropriate actions for their satisfying so that the purposes of the organization security policy to be achieved.

The process of personnel recruitment and selection is advisable to include attraction and assessment of candidates to work in various spheres and organization sections related to security and protection on the base of which the most suitable of them to be selected, that meet

the requirements formulated in the design stage requirements for the respective positions. It finishes with introduction of the appointed candidates in the organization, i.e., „orientation“ of the appointed person in the organization „labyrinth“. The purpose is to shorten the time of mastering the new job and the appointed people to be motivated to do it well. That is why the newly appointed personnel should be sufficiently informed about the main items of the organization activity related to security and protection, comprising, and most of all, the interrelations and responsibilities with and of other employees from other subsystems of the management system. The orientation also has long-term aims – to win the new people for the organization purposes, interests and future. This is achieved by means of development and mastering of the values, norms, traditions, manners, customs of the so called company culture by all the personnel.

At the stage „human resources assessment“ the work presentation of each one specialist engaged in ISMS is estimated. For that purpose a special assessment system is developed which is different for every organization and conforms to specific principles, rules, requirements and procedures.

In the human resources management particular attention is paid to the used material stimulation forms and systems. All over the world it rests on two basic principles: remuneration for the post occupied and remuneration for the results of the work. From the leader of security and protection high ability is required not only to conform to these principles but also to find various forms of their flexible application (additional remuneration for nonstandard workday, shift work – for guards, for responsibilities exceeding the direct duties, etc.).

The personnel training and career development comprises the activities of improvement of knowledge, skills and adjustments of the occupied with the purpose to increase the level of their work presentation and affording possibilities of career progress taking into account the individual needs of the occupied people and the future organization needs.

The training is a strategic function of the human resources management, it determines the professional development and personnel growth. Particularly in the security and protection field the training equals to investment in stable development of the organization. On its side, the career management is directed to the official progress and growth of human resources in the organization in compliance with its needs and requirements for effectiveness, results, development and approval.

The motivation of the personnel in the considered field, in our opinion, is engaged not so much with binding the tasks fulfilment and the achievement of certain aims with the personal interests and needs as to the recognition on the part of everybody in the organization (and most of all the leaders) the importance of the profession „security officer“. From our own observation we can say that in more than 90% of the cases in Bulgaria the critical infrastructure security

functionaries do not have the sensation of acknowledgement by the management for the performed by them activity . And here we do not speak about acknowledgement in words but about acknowledgement by providing the necessary resources in order to guarantee high security levels of the respective objects.

The ensurance of healthy and safe labor conditions reflects various interests that should be combined in the human resources management (this relates completely to those working in the security and protection sphere where the functionaries are in constant interrelations of supporting and/or controllers with respect to the remaining employees). The safety and labor conditions are factors which affect the complete organization activity and contribute in maximum degree to stable security and protection of the respective infrastructure.

The above said is adapted to the security and protection model of generally approved human resources management system.

As already noted, the other direction is ensurance of the personnel information data base security. The purpose of this activity formulated in ISO-27001/27002:2005 sects. 8.1 – 8.3, Personnel Security Risk Assessment, is as follows: „The policies and practices in relation to the human resources should reduce the risk of theft, deceit or misuse of the information data base used by employees, contractors and third persons."

On its side, the policy in relation to the human resources as a whole should comprise all persons in the frames of the organization and external to it that use (or may use) the information about the personnel resources or the equipment for its processing. This can include:

- Clear and traceable requirements are written down for each one employee having access to this information;
- Creation of condition which to guarantee that the employees fully understand their own and these of the others responsibilities concerning the information security related to the personnel resources;
- Creation of procedures by which all engaged in the human resources management to realize clearly the threats for the information security and the necessary steps for reducing the probability of these threats realization;
- Equipment for all persons that to support the organization security rules and policies in the course of their everyday activity, by appropriate training and explanatory programs which provide possibility to reduce human mistakes;
- Guaranty that all activities connected with leaving the organization or change of office responsibilities in the frames of the organization on the part of employees are done in strict correspondence with the established internal rules.

Still much more could be written on the human resources management. This is an area and subject of rich history and it is in the range of attention of the specialists that apply and develop it. But as we already said, this is not the question. For the present development it is important to say that in the frames of the human resources management system a subsystem has to be differentiated which to treat the problems related to security and protection, that is to say:

- Determination of clear rights and responsibilities of the security functionaries which is necessary, besides being understood and realized by them, to become generally known by all the remaining employees in the organization. Only this way, besides creating conditions of ISMS stable action and development, the conflicts with the representatives of the other organizational structural sections will be avoided;

- Clearly written down principles of interaction and control between the security functionaries and the remaining employees in the organization. These principles have to be written in the position records of both (with the designers, financiers, operators and computer systems service personnel, specialists of quality assurance, security, machines and equipment maintenance, responsible for the corporate social responsibility, etc.). Currently, almost in every organization these interrelations are described in the different plans and/or internal regulating documents. The last said is very superficial approach which up to now has not shown success in supporting the corresponding organization to achieve the maximum in the considered field;

- In the internal for the organization regulating documents, for each one of the management system subsystems, differentiation of special sections with requirements to every system with respect to the rights and responsibilities of the working in it employees related to security and protection;

- Training and systematic carrying out of drills both with the security personnel and with all the remaining employees who have written down in their position records rights and responsibilities in this area. This training and drills are radically different from those applied in the establishment of the applicability of various crises action plans.

And all said above, adding it to the presented here adapted to the security and protection model of the generally accepted human resources management system, proves in practice the involvement of the latter as component of the critical infrastructure security and protection levels.

ENVIRONMENTAL SECURITY SYSTEM

What is the environmental security?

The connection between the environment and the security of the people and nature is object of many investigations and publications in the last decades but only recently it becomes an important focus of the international policy in the field of the environment.

A broader view on the problems of the environmental security gives us reasons to say that:

- the environment is the most transnational of the transnational issues and its security is significant measure of peace, national security and human rights which recently finds more and more supporters all over the world (the international conference in Paris in the beginning of 2016, when the carbon emissions were discussed, is indicative);
- the environmental security is of basic importance for the national security, formed by the dynamics and the interrelations between the natural resources, state social structure and the economic motor of the local and regional stability.

Leading examples of the emerging changes in the environment are: exhaustion and contamination of the drinking water, drastic reduction of the activities connected with fishery, change for the worse and disappearance of the biological diversity, change for the worse and loss of agricultural lands, safety of foods and health, stratospheric ozone loss and global warming.

The first five of these fundamental changes in the environment which the humanity faces are already, or most probably will be, a growing threat for the environmental security in short-term plan and the last two will more and more affect people security in the next 50 years (Professor Norman Myers (May 2004)).

Another significant aspect in the relations between the environment and the security is the effect of the conflicts on the first. An acute regional conflict, war between states and/or coalition of states, refugee wave, terrorist act, etc. could result in decrease of the environmental security level and in spiral of vicious incidents (attempt is made with this term to generalize the regional and international conflicts and terrorist threats) caused by shortage of security and additional conflicts.

Just the said up to here once more confirms the importance and necessity of special attitude to the environment with respect to its effect on the critical infrastructure objects security and protection. If we go back to the critical infrastructure definition we shall see that its functioning directly affects not only the health and life of the working in it employees and/or functionaries and the completeness and availability of the material assets but also those at regional, national and even international level (the contamination of water, air and soil by the

respective infrastructure activity, as a consequence, besides all other, of terrorist actcould lead to such after-effects in similar scale).

Therefore, the national and international regulation and/or standardization organizations have developed a number of documents in the considered field which determine and regulate the necessary requirements to all engaged in the environmental protection agencies. From this point of view, the family of the standards ISO 14000 is worldwide recognized frame of requirements which presents practical tools for companies and organizations of all types that want to manage their responsibilities in the area of the environment. The standard are developed under the auspices of the Technical Committee of the International Standardization Organization ISO/TC 207.

ISO 14001:2015 and its supporting standards such as ISO 14006:2011, focus on the environmental protection systems. ISO 14001 is the basic standard of the family and we shall examine it in more details below in the text. The other standards accent on specific approaches such as for instance, audits, communications and life cycle analysis as well as ecologic challenges, such as for instance, the climate change.

As this subject matter is yet not quite realized and mastered by the management of many critical infrastructure objects it is advisable to present more information about the available standardization basis that could help not only for the environmental protection from the results of these objects activity but to be also practical-applied tools for benefit and in interest of their security. Why? Because being acquainted with the standards we shall know not only what sanctions will follow by the control agencies if they are violated but through them we shall be able to estimate the damages that our activity may cause to the vegetation and fauna as well as to the material valuables in case of its eventual interruption or disturbance as a consequence of terrorist activity.

So, the next standard that we should note is ISO 14004. It provides practical instructions for the successful fulfilment and maintenance of environmental management system, testing the action of such systems as well as conducting reviews by the management and it can be used independently or with BS EN ISO 14001. In practice, it complements ISO 14001 presenting additional directions and useful explanations.

The environmental audits are important tools for assessment whether the environmental management systems are correctly applied and maintained in compliance with the established norms. The standard for audit of such systems, ISO 19011, is equally useful both for environmental management systems and for audit of quality management systems. It provides directions in relation to the audit principles, audit programs management, carrying out the audits and auditors competence.

ISO 14031 presents instructions how an organization can assess its activity from the view point of the ecologic requirements (i.e., we need exactly this instrument in order to assess the probable consequences of potential terrorist attack against our activity). The standard considers also procedures of selecting suitable characteristics for assessment of the activity, so that this activity to be assessed on the base of criteria determined by the management. This information could be used as basis of internal and external consideration of the ecologic characteristics.

The series of standards ISO 14020 considers a number of approaches for marking the fulfilment of the ecologic norms and declarations in this direction, including the attachment of so called „ecologic labels“ (approval seals), issue of independent declarations of fulfilled requirements in relation to the environment as well as quantitative information about products and services in this field. The other standards of this series are ISO 14021, ISO 14024 and ISO/TR 14025.

Parts 1 and 3 of ISO 14064 consider the problems related to carbon emissions reading and verification and present a set of clear and provable requirements in support of the organizations and followers of projects for reduction of greenhouse gases emissions.

ISO Guide 64 provides directions for addressing the ecologic aspects in the product standards. Although mainly directed to the organizations that develop these standards, this Guide is also useful for the designers and manufacturers of the corresponding products.

But let us return to ISO 14001. Both it and the remaining standards of the family are designed and created in compliance with the cycle Plan-Do-Check-Act (PDCA) that is at the base of all ISO standards related to the management systems.

The standard defines the requirements to the environmental management system which could be integrated with other management requirements in order to help the organizations to achieve both their business purposes and the purposes connected with the environment. In this case we have to note completely confidently that this refers also to the achievement of the critical infrastructure security and protection purposes.

Main accent of the standard is the identification and assessment of the aspects in relation to the environment, in this way the organizations aiming at reduction of the negative effects of their activity.

ISO 14001 is applicable to any organization independently of its size, subject of activity, development degree or location, which wishes to improve the results of its activity considering the requirements with respect to the environment.

In the implementation of environmental management system each one management, including that of critical infrastructure, has to consider the following specific features:

- organization type and character and the risks related with it that could affect the achievement of the purposes both in relation to the environment and these related to the security and protection (but not only);
- the necessity of risks assessment and management related to threats and possibilities, not only directly affecting on the part of the organization activity or such potential which could be caused by natural calamities but also those that could be provoked by terrorist attacks;
- the necessity the high management to take leading role for improvement of the results of all activities in the organization connected with environmental protection;
- the need for development of product life cycle concept including the activities after delivery, the use and detoxification (the last said is extremely important from the view point of preventing the possibilities of potential terrorist act by non-permittance the enemy to use as weapon against us our products and services in wasted condition);
- the necessity of realizing stronger control on the outsourced processes – extremely important from the view point that by these processes the potential enemy could „introduce“ threat from outside;
- the necessity to engage all personnel levels in the organization, for instance in relation to wastes management (this is of exceptional importance for the nuclear power plants for example, but not only – the spent nuclear fuel is perhaps the clearest example in this relation).

What could be the advantages of implementation and certification of environmental management system in compliance with ISO 14001, but from the view point of the connection with ISMS?

- The confidence of partners and external interested parties grows in relation to the fact that all measures are taken both with respect to non-permittance of environmental contamination by the organization activity or natural calamity and for prevention of terrorist attack which could cause contamination of water, air and soil and there from cause serious or irreparable damages on people, animals or material valuables;
- The risk of ecologic incidents is minimized and the consequences of them reduced (in the context of the above said);
- The ecologic awareness of the employees grows, their habits and manner of thought change and they are presented the possibility to think integrally and act with a clear purpose to prevent security and protection problems by observing the ecologic norms and vice versa;

- Conditions of effective resources consumption control are created which leads to expenditures reduction;
- All applicable to the organization requirements are identified, obtaining of permits and observing their conditions is eased (including also from the national security departments).

In conclusion it should be noted that the interrelations between the environmental management systems and the remaining IMS subsystems should become object of discussion in the frames of the organization, using the method „tailoring" or at national and international level by their description in national or international standard for building and application of integrated organization security and protection management systems.

CONCLUSION

The rights and responsibilities of the security and protection functionaries have to become generally known by all workers and employees in the organization. To rely on that somebody has read the law of the private protection activity, the internal rules in the organization or position records of these functionaries is not serious. The knowledge of their rights and obligations on the part of the remaining employees will contribute to avoid misunderstandings, even incidents. So, the principles of interaction and control between the security functionaries and the remaining employees in the organization have to be clearly written. These principles have to be written in the position records of both (together with the designers, financiers, computer systems operators and service personnel, quality assurance specialists, safety personnel, machines and equipment maintenance, corporate social responsibilities, etc.).

The training and systematic conduction of exercises with the security personnel and all the rest of the employees, who have rights and responsibilities written down in their position records in this area, are completely different from those applied in the establishment of the applicability of the various crises action plans. The training and exercises should be directed mainly to improvement of the knowledge and experience of both parties in relation to realization and mastering of their rights and obligations and not to their action in crisis conditions (i.e. during fulfillment of the prepared plans in this sector).

In a word, a subsystem of security and protection human resources management has to be established which to comprise both the legislative requirements (such as for instance, the law for the private protection activity) and the integrated specific requirements of the security and protection system.

The environmental security systems are immediately, directly connected to the critical infrastructures security and protection ensurance. The disturbance of their activity by terrorist

actions is one of the basic prerequisites for the occurrence of significant, sometimes catastrophic consequences for the health and life of the people, completeness of the material valuables and normal functioning of the economies not only of individual regions at national level but at international scale. The establishment of functioning, reliable and maintained environmental security system that is adequately integrated in ISMS will guarantee higher levels of the respective critical infrastructure objects security and protection.

REFERENCES

BS EN ISO 14004:2016, Environmental management systems. General guidelines on implementation.

Centre for the protection of National Infrastructure (June 2013), UK, Human resources security, A Guide 4th Edition.

HarizanovaM.,Mironova N., Shtetinska T. (2009), Functional Analysis of the Human Resource Management System, Economic Alternatives, issue 5.

Information Security Human Resource Development Program (July 8, 2011), Information Security Policy Council, Japan.

ISO 14001:2015, Environmental management systems - Requirements with guidance for use.

ISO 14006:2011, Environmental management systems - Guidelines for incorporating ecodesign.

ISO 14020:2000, Environmental labels and declarations - General principles.

ISO 14031:2013, Environmental management - Environmental performance evaluation – Guidelines.

ISO 14064-1:2006, Greenhouse gases - Part 1: Specification with guidance at the organization level for quantification and reporting of greenhouse gas emissions and removals. Greenhouse gases - Part 3: Specification with guidance for the validation and verification of greenhouse gas assertions.

ISO Guide 64:2008, Guide for addressing environmental issues in product standards.

ISO-27001/27002:2005 sects. 8.1 – 8.3, Personnel Security Risk Assessment.

Norman Myers (May 2004), Environmental Security: What's New and Different?, The Hague Conference on Environment, Security and Sustainable Development.

Shopov D. and Atanasova M. (1998), Human Resource Management, S., Trakia-M.

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., (2014), Integrated model for security and protection of critical infrastructure, Open Access Library Journal, ISSN: 2333-9721, 1: Volume 1, e1124. http://dx.doi.org/10.4236/oalib.1101124.

Stoichev K., (2015), Selection of an Alternative Method for Establishing Security Levels, Journal of Applied Security Research, Volume 10:1, 48-59, 22 January 2015.

БДС EN ISO 190011:2011 – Указаниязаизвършваненаодитнасистемизауправление.