Risk Assessment of the Human Factor in the Field of Building and Infrastructure Defense

Tamás Berek[1], Judit Kovács[2]

[1] Institute of Military Leadership Training, Faculty of Military Sciences and Officer Training, National University of Public Service, Hungária krt. 9-11, H-1101 Budapest, Hungary, Berek.Tamas@uni-nke.hu

[2] Institute of Microelectronics and Technology, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, Tavaszmező u. 15-17, H-1084 Budapest, Hungary, kovacs.judit@kvk.uni-obuda.hu

Abstract: In order to establish the concept of building and infrastructure defense, a complex security system must be created by making, analyzing and interpreting an appropriate plan. This task is especially difficult and complex for defending buildings of unknown functions. Industrial projects usually differ from what was planned both in space and in time. The authors of the article introduce the general aspects of security personnel and the characteristics of risk assessment. The basic points of configuring the labor force components of building and infrastructure defense are also introduced.

Keywords: complex security; defense concepts; risk assessment; human factor

1 Introduction

The threat level for any building and its respective infrastructure is determined by several factors. Some of these factors are the security degree of operation, the demand and the value of the used materials, technical equipment and information, and the criminal infection of the area. The time of the day, the reliability of the applied security system, the speed of action and troubleshooting, and the features and territorial impact of undesirable acts are also of great importance [1].

Analyzing the question from a distant approach, the aim is to maintain a safe state of the building and its respective infrastructure. This state, providing the ideal status that the operation of the security system is fault-free, may seem steady in time, though this steady state is only an outward seeming. All acts that are performed inside the area of the building, the equipment, the quantity and the risk of the materials used are relatively easy to be determined. From certain points of view, the changes in the safe state may be prevised, knowing – among others – the

feature of the building, the acts performed inside, the applied technology and the materials used.

Security could be defined as the safe state of somebody or something. However, this safe state does not literally exist, because security is the complex outcome of some specific existence or actions and the endangering factors of them. It means that security may be interpreted only together with endangering factors. It is the very moment when an endangering factor appears that the expression of security gets its deeper meaning. The higher level the endangering factors of existence or normal operation are, the lower level of security is [2].

It follows that the status of security is fundamentally determined by the endangering factors and by the protection applied against them [3]. Creating the complex security system of a building and its respective infrastructure, one must be aware of and recognize the nature of outer and inner endangering factors that may affect security. After the evaluation of these factors, the acts in response and the whole structure of defense must be laid out.

Simplifying it, in the case of any building and its respective infrastructure, the subject of defense and the sources of dangers must be specified by recognizing and analyzing the endangering factors arising from the environment. The security system must be planned and carried out by knowing these factors.

2 The Role of Security Personnel in Property Protection Complexes

Complex property protection is made up of components based on one another. The aim is to reduce the probability of certain risks, as well as to moderate the adverse consequences of possible incidents [4].

To identify the rate of the components of the complex security system is an inevitable task during the design process, since this act will grant the effective and fault-free operation as well as the phenomenon of synergy: the interaction of subsystems will produce a combined effect greater than the sum of their separate effects.

Electronic and electrotechnic subsystems are among the most important elements of security systems and their reliable operation is essential. The development of low-voltage subsystems that are optimal from the aspect of reliability is greatly facilitated by the test method of the principle of determining disturbance states. As part of that process, the analysis of disturbances of both technological and human error origins must be worked out [5]. A disturbance state is a state of the system when it cannot perform its function, due to the effects of well-determined technological or human disturbances.

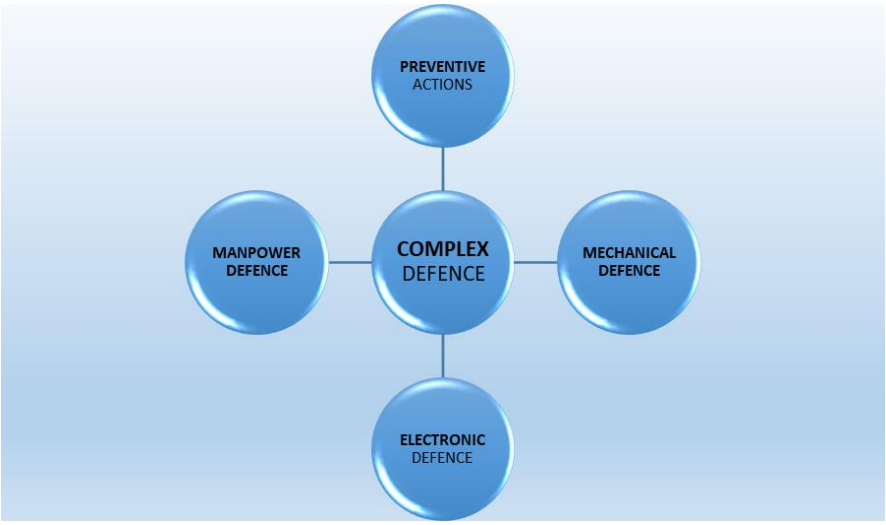

Figure 1
Components of complex property protection

Source: edited by Berek

Any type of errors cause a disturbance state when it is concerned with processes. Disturbances may also result in unacceptable consequences when critical failure is due to a disturbance state. Two main groups of the factors that lead to human errors causing disturbances may be distinguished as internal and external factors. The next basic categories of internal factors may be physical, emotional, cognitive and social effects that also include more categories like personality, intelligence, motivation and ability. External factors can be divided into organizational and environmental factors. In each of the categories, separate analysis is needed to determine to what extent certain factors cause a specific error. [6]

Nevertheless, in certain areas, special features apply. The mechanical, electronic and electrotechnic elements of security systems for construction-industrial projects, are generally inefficient and sometimes are even absent, especially at the early stages. In this case, due to the occurring variance, security personnel has the main role in defense.

Construction-industrial projects are especially the ones where rates of security components have to be changed at the different investment phases. These changes may only be handled properly with security systems that were designed to involve a possible option for flexibility.

This flexibility is provided mainly by security guard. It is also this flexibility that guarantees adherence to specific features of the security systems: at the loss of any elements – that often happens during constructions – active elements may cover all parts of security (though perhaps, at a lower level of efficiency) [7].

Another special issue is the physical security of facilities that store dangerous industrial materials. In order to prevent unauthorized access to and/or theft of radioactive and infectious materials and toxins, providing the defense of laboratories and other facilities is of extreme importance. At the same time, the special staff of these institutions, in certain positions, is exposed to physical, chemical, biological and radiological risks. However, these risks can significantly be reduced by the development of a well-designed defense program. In order to avoid direct threat by everyday working conditions to users of dangerous work areas, devices or materials, the careful construction of the physical protection of the affected areas and equipment is extremely important. The same protection is vital so that the potential hazards of costly devices and dangerous materials or devices containing dangerous materials do not leave the controlled working areas or property of the institution, by unlawful appropriation.

There may be serious risks of abuse by competent persons with access rights to hazardous substances, against which, not only certain components of security or protection should be reinforced, but also, protection elements against intentional personal abuse should be developed. Laboratory accidents and the release of dangerous biological materials may not be due solely to deliberate illegal activities or sabotage, but the accidental release of hazardous substances may also result from the improper use of infectious substances in laboratories or by their inappropriate packaging or transportation [8].

The protection of controlled work areas and working processes, in the lab complex, including the personnel involved and the protection of hazardous materials and waste storage facilities are also of great importance. The same degree of protection is required for the lab areas not considered to be working places and for the external environment of the laboratories.

In order to ensure a continuous and comprehensive protection, when designing the security system, there is a great need to coordinate the efficiency and harmonization of each independent autonomous subsystem and to ensure the conditions of supervision. The effectiveness of physical guarding is provided by the effective combination of mechanical and electric devices and security personnel and not overlooking the role of preventive measures.

When ensuring the protection of the hazardous areas of the lab facilities, there is little chance to use labor force, therefore, the rate of electronic protection devices should be increased. At the same time, the efforts to reinforce internal control are also in the forefront. It is the task of the lab staff to control the regulations and procedures, and to operate and maintain the security systems. It is well-known that the efficiency of the entire property defense system is determined by the efficiency of its weakest element. In improperly built systems, the living component is quite often the weakest link. So, it cannot be emphasized enough, how important it is that the human factor is taken into account, when structuring security systems.

There are situations where the presence of temporarily or operationally stored substances is a threat in itself. During the planning and development of protection in the controlled area, one of the main aspects, is that the safety engineering subsystems are designed to meet the intended function of the laboratory and to provide the highest level of technical, mechanical, electronic and personal security.

In an emergency event, the controlling system is able to perform several actions simultaneously; nevertheless, its basic task, is the prevention of emergency situations. So, in case of a possible occurrence, the personnel support of the operation of the system is needed. Monitoring the controlled areas, it has to alert the operator immediately so that they can intervene in time. Security guard has a very important role, in this case as well.

In contrast to technical systems with average parameters, security personnel is capable of managing compound or unforeseen situations [3]. However, the subjectivity of the human factor might as well be its own vulnerability, since personnel may base the sources of inside hazards that are difficult to detect and identify, and it is also hard to provide protection against them. The occurrence of events like damages due to any improper execution of tasks, sabotage, theft or participation in them, or releasing important information that would provide the strength of protection may threaten the whole defense system. The prevention of these events is extremely problematic.

Building and infrastructure defense is a very compound task. The lack or the weakness of any part of the property protection complex will affect the overall efficiency of the security system. The components of complex systems (access control systems, security monitoring systems, etc.) are also involute security subsystems. It is essential to meet the requirements of fault-free operation. In addition to the high-level integration of electronic, electrotechnic and mechanical security subsystems, the activities and preparedness of the operating crew are of great significance [9].

Since the human factor has a key role, the analysis of it may have a considerable influence on the establishment of risk assessment and risk management. Human performance has a fundamental impact on the reliability and security level of various systems. Generally, the role of the human factor, in connection with the occurrence of any events, may be divided into three main groups. People may cause, prevent or be the victims of particular events, thereby giving an improved approach to risk assessment and risk management.

From the aspect of security, the human factor appears in two, rather contradictory ways, of the previously mentioned, as follows. Within manufacturing security systems, design is a highly challenging activity. Since the environment is constantly changing, the proper designs do not perform as expected, with the frequent overestimation of how efficiently people will work [10]. On the other hand, people are able to cope with unforeseen situations, to analyze and to create

solutions. Without human actions many incidents could lead to accidents. Safe behavior does not mean the absence of errors, but the positive human contributions to safety, even in the form of prevention [11].

As the human factor is always present among the main reasons of accidents and disasters, human contribution has priority in any analysis of risk assessment. According to different surveys, 45-80% of errors are due to the human factor, varying with ways of approach. The special role of the human factor was recognized decades ago, and research on human factors has been present since then. Human errors have been categorized and the broad use and development of human reliability assessment has been urged. Initially, it was discovered that specific systems must be developed to analyze the events related to human factors. Later, it was shown, that human factor-associated common cause failures may appear in any kind of security systems.

3 Analyzing the Human Factor in Risk Assessment

Among the reasons that may turn incidents to accidents, as well as, among the main reasons of industrial accidents, the human factor is always present. Consistent explorations of consequences will recognize human errors even in the depths of technical reasons. Based on the research of Rankin and Krichbaum, the role of the human factor in the occurrence of accidents shows a dramatic rise, reaching up to a 70-80% level, regardless of the technological conditions [12].

This significant increase has two main reasons. One of them is the sophistication and the high-level reliability of the mechanical and electrical equipment, while the other one is the greater human involvement in the controlling processes that is due to the complexity of systems. Not only do the sophistication and the high-level reliability of the mechanical and electrical equipment greatly reduce the number of technical errors, but they also give opportunities to manage critical processes, even at the events of system failure and breakdown. The greater human involvement in the controlling processes, as a consequence of the complexity of systems, means that humans primarily become the supervisor of automated processes.

Human contribution has a place of utmost importance in any analysis of risk assessments. The first progressive development of risk-based approaches occurred in relation to the analysis of electronic and electrotechnic systems, in the fields of space technology, nuclear power and the chemical industry. However, due to the diversity of physical and chemical processes, as well as, control strategies and procedures, special techniques have been developed for the specific needs of each area. As an example, regard the method of hazard and operability study (HAZOP). It was first introduced in the chemical industry and has since been considered

necessary for the preliminary assessment of any complex system that consists of several processes of either serial or parallel structures that involve subsystems of dangerous chemical or thermodynamic reactions.

The estimation of the impact and consequences of the risk events on people, property and environment is realized in the risk assessment process. The calculation of the probability of these risk events actually happening, as well as, determining their potential impact are important parts of the risk assessment process.

By its nature, the process of quantitative risk assessment is based on probabilities. It recognizes that accidents are rare, and that the potential risks and events may not be completely avoided. As serious incidents occur or not, over the lifetime of a given process or building and its infrastructure, it is not appropriate to base the evaluation process on the consequences of isolated events alone. However, the probability of the cases that have actually happened should also be considered. These probabilities and the levels of risks derived from them must have an impact on both the design level and the operational and organizational controls and revisions.

In the process of integrated risk assessment, "risk identification" as the first step involves describing the system, determining the possible events and the responses to them, as well as the classification and the filtering of events. The second step, i.e. "modeling event scenarios", is based on event tree analysis, and its objective is to place the sequences of events among the states of losses. The main parts of the next step, "analysis of consequences", are the assessment of the consequences and the analysis of the moderating effects. The following "evaluation of the frequencies of events" is one of the most complex tasks. In addition to the actual evaluation of such frequencies and system analysis, the analysis of the human factor is usually performed at this step. Finally, in "risk assessment", determining the risks is brought off by means of the consequences and frequencies.

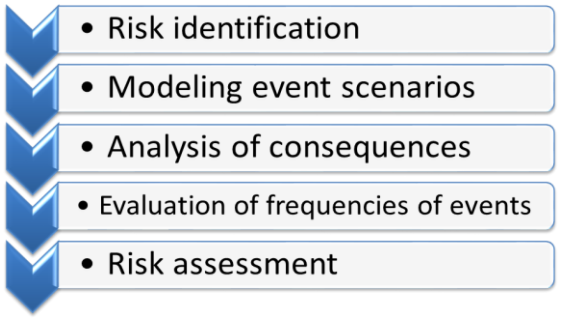

Figure 2
A detailed plan for the integrated risk assessment process

There is no doubt that integrated risk assessment is the best way for meeting the requirements of risk assessment today. In the comprehensive plan of the risk assessment process, human factor analysis is interpreted as a subtask of the evaluation of event frequencies. It means that analyzing the human factor does not get a role in the preceding or simultaneous steps of the process: neither in risk identification, nor in modeling event scenarios, nor in the analysis of consequences. However, it is very important to be aware of the impact of human factors even at the beginning of the processes, as in this case the corresponding details of plans may be modified easily and at a low cost. It is therefore recommended to take the human factor into account already from the first step in any integrated risk assessment.

The probability that certain events occur due to the human factors involved may be determined by an appropriate human error analysis method. Human error analysis covers the systematic specification of the factors affecting human performance and the exploration of situations that are likely to give rise to errors; this is the way leading to incidents. This analysis may involve the identification of interfaces that are influenced by the errors. Based on the frequency of occurrence or on the severity of the consequences, a relative ranking of the errors may be established. The results may be qualitative or quantitative as to their nature. They also involve the systematic listing of errors that are likely to occur during normal or emergency operation. The error rate depends on many factors, ranging from stress over experience to the complexity of the task or to the right skills, including situation-specific specialties.

Human error is a general concept, which includes every situation when the planned sequence of mental or physical actions fails to achieve its planned and desired aim. This failure is not due to any kind of stochastic circumstances [13]. Human error may also be considered a failure of a human action, due to internal human failure mechanisms, which is to loosely describe any sub-optimal human performance. Two main groups of human errors are errors of commission (wrong human actions) and errors of omission (missing human actions). A human error as the consequence of the difference between the planned and the realized action or performance, may be categorized as a slip, a lapse or a mistake. A separate group of errors is violation, when the action is not allowed, prohibited or not appropriate. Latent errors may also play an important role, although this type of errors is usually difficult to identify because of their distance from the occurring event both in time and in space [14]. Human failure is the failure of a defined human action in any Human Reliability Analysis (HRA) model. There may be more reasons leading to failures attributed to human errors. A human failure may affect components – that is called a fault, and it processes when disturbances occur. A failure that results in unacceptable consequences such as, unavailability or malfunction leading to personal or property damage is called a critical failure. Another possible classification of human errors, usually taking place in Probabilistic Safety Assessment (PSA) models, depends on the chronology of the

human error and the occurring event. Three types of errors may be distinguished by this chronology: an error of human performance type A is an error that is committed during a human action before the initial event, mainly in connection with the availability of the system (for example in connection with the actions of maintenance), an error of human performance type B is an error which causes a direct initial event, while an error of human performance type C is an error that is committed during the human actions made for averting breakdowns or accidents. In the case of errors of human performance type C, the following groups may be differentiated: the lack of a needed action, an action made by mistake and the error of an action made for compensating the lack of a needed action [15].

In any of the above categorizations, the role of violation is not handled as being as important as it is in reality. In Reason's categories, the violation of intentionally causing harm is not even regarded as being a human error. However, if human error is considered to be the consequence of the expected and the realized actions or behavior, violation is an error, as it differs from the expected human behavior. In reality, deliberate actions of this type may have serious conclusions, their number is significantly increasing and they cannot be regarded as "low probability", isolated events any more. The violation of intentionally causing harm being treated as a human error makes it possible to be a part of human factor research, which is the cornerstone of prevention.

In addition to the previous ideas on the violation of intentional causing harm, violation in the traditional sense is also a serious problem. Violation may be motivated by the search for simpler and faster solutions. For example when a worker crosses a conveyor belt because it is simpler than bypassing it, or by risk-seeking behavior as when the worker crosses the conveyor belt, because he wants to show his courage to peers. The offenders are often unaware of the risks; thereby violation may become a habit [6]. According to Skriver [16], after a specified period, the prescribed processes are no longer evident in these cases. They consider the main causes of violation in organizational factors: in the lack of adequate equipment, working environment and supervision and due to the fact that there is no consequence of the committed violation.

Prevention here, as in all other areas, has an important role. Moreover, the energy spent on prevention will be compensated. Based on the connection between violation and the number of rules to be kept, there is a number K given by the number of rules to be kept weighted by the difficulty of keeping them, which should be analyzed in the given situation. There exists a number K_0 such that if $K < K_0$, then no violation will happen (or only with negligible probability), and if $K_0 < K$, then violation will happen (with a considerable probability). The aim is to make a system of sufficient rules for the given task where $K < K_0$ [6].

In building and infrastructure defense, the implementation of the daily operational work is specified by the operational rules of the system and the service instructions of the security service. Among these rules, the daily tasks, protocols and procedures must be defined precisely for different situations. The daily work of a security guard's life is carried out according to an appropriately assembled policing scheme, with the tasks and procedures being unchanged. Though, there may be differences in its implementation. Each error resulting from time management may be declared a typical example that may cause a disturbance state based on human factors. One of the basic principles of an operational process, is the assumption, that workers are highly predictable and standardized in their behavior, regarding their schedule. They always start work on time, operate at a constant rate throughout the day, take breaks at planned times, rotate properly, etc. Nevertheless, such regular behavior of workers rarely occurs in practice. According to a test made in the UK [13], the analysis of the data suggested that up to one third of the potential time for production is lost due to stoppages, extended breaks and disruptions to the flow of the line. Not only does the loss of time cause a recession of production, but it may also cause disturbance states. [10]

Knowledge and awareness of the human factors are basically important in preventing the development of disturbance states, and therefore, they have a distinguished place in design processes. When the human factor is taken into account, the reliability of complex systems may indirectly be increased. There is no doubt that human performance has a fundamental impact on the reliability and safety level of complex technical systems, such as security systems. Among the major contributing factors of disturbance states, the human factor can be found in each case. As a consequence, the human factor must always be taken into account when analyzing disturbance states in building and infrastructure defense.

Conclusions

The maintenance of the labor force component of a complex property protection requires constant control, and security service managers must monitor the system. It is well-known that the effectiveness of a security system is characterized by that of its weakest component. That weakest link often happens to be the security personnel. Apparently, as far as crew becomes unreliable, the entire security complex is threatened. In the cases when it is recognized, the negative effects may often be outweighed by technical upgrades. Control systems that can be implemented are nowadays indispensable. Such systems may include the camera surveillance of workers, the establishment of patrol monitoring systems, etc. [17].

Generally, despite the fact that the vast majority of errors, including technical reasons, are due to the human factor, people are able to maintain safe and economical operations, and are also capable of providing a responsive action to disturbance states at the same time. In this way, human performance affects the probability of all unexpected situations and their consequences. Today, the well-established industrial security applications and the procedures of design and

operation make the basis of risk management. The wide-spread awareness of the possible dangers has implied the development and use of systematic approaches, methods and tools of risk assessment procedures. These are often referred to as hazard analysis or quantitative risk assessment [6].

A risk analysis is required in different areas of production: in business, industrial production and environmental protection in the field of work safety. Although laws and standards regulate its implementation, they do not include specific execution [18].

Risk assessment and risk management are two of the most important jobs done today to achieve maximum security levels. Analyzing human factor can have a major influence on the risk assessment and risk management process, because the role of the human factor is crucial. Human performance has a fundamental impact on the reliability and security level of various systems.

The maintenance and operation of the labor force component of a complex property protection requires an active presence, as the risk of this component is continuously assessed. It was concluded that human performance affects property protection – as a complex system, which is based on technological and human factors – on the whole. Also, it was shown that human performance has a basic impact on the safety levels and reliability of complex technical systems in building and infrastructure defense.

Beyond the exploration of errors, it is also vital that the mapping of the reasons of errors are done, which is proven to be suitable, by using methods based on cognitive theories.

Within manufacturing security systems in building and infrastructure defense, the design and redesign activities are both challenging. The competitive environment is constantly changing and there is a demand to make products cheaper, better and faster. In this kind of environment, people who carry out repetitive, manual tasks seem to remain critical to the success of the system. Designers of security systems often have little appreciation of the wide range of factors that influence human performance. This can lead to "proper" designs not performing as expected, with engineers frequently overestimating how efficiently and effectively people will work. [10]

The key to a successful solution is to improve the awareness of engineers, concerning the impact the human factor has on the design. It is especially important to improve this awareness at beginning of the design process; at this stage most negative factors can be more easily and inexpensively altered.

References

[1] Lukács György: Új vagyonvédelmi nagykönyv, CEDIT Kft., Budapest, 2002

[2] Berek Lajos: Biztonságtechnika ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel jegyzete NKE 2014

[3] Báthori B.- Bodrogi F. – Szili L.: Őrzés védelem, jegyzet, Pro Lex Oktató és Szolgáltató KKT, Budapest, 1995

[4] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009, ZMNE

[5] Zsigmond Gyula: Biztonságtechnikai rendszerek hibamentességéről Bolyai Szemle 2010:(4) pp. 207-213 (2010) http://uni-nke.hu/downloads/bsz/bszemle2010/4/15.pdf

[6] Kovács Judit: Az emberi tényező matematikai modellezésének lehetőségei a katasztrófavédelmi kockázatértékelés és kockázatkezelés területén Doktori (PhD) értekezés, 2011, ZMNE

[7] Teke András: Az őrzés mint rendészeti alaptevékenység VI., in: Rendvédelmi Füzetek 2000/45, a Rendőrtiszti Főiskola kiadványa, Budapest, 2000

[8] Berek Tamás - Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban 2011, Bolyai Szemle XX. évf. 2. szám, ISSN: 1416-1443

[9] Bodrácska Gyula – Berek Tamás: Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások során, 2010. Hadmérnök, www.hadmernok.hu/2010_1_bodracska_berekt.php

[10] T. S. Baines, R. Asch, L. Hadfield, J. P. Mason, S. Fletcher, J. M. Kay: Towards a theoretical framework for human performance modelling within manufacturing systems design (Simulation Modelling Practise and Theory 13, 2005, 486-504)

[11] NEA (2003): Nuclear Regulatory Challenges Related to Human Performance, ISBN: 92-64-02089-6, OECD, Paris, 21 pages

[12] W. Rankin, L. Krichbaum, Human Factors in Aircraft Maintenance, Integration of Recent HRA Developments with Applications to Maintenance in Aircraft and Nuclear Settings, June 8-10, 1998, Seattle, WA, USA

[13] James Reason & Alan Hobbs: Managing Maintenance Error- A Practical Guide, Ashgate Publishing Company, 2003

[14] James Reason: Managing the Risks of Organizational Accidents, Ashgate Publishing Company, 2004

[15] Gyula Zsigmond-Judit Kovács: Determination of Disturbance States with a Special Focus on the Human Factor Bolyai Szemle 2007 :(3) pp. 187-193 (2007) http://uni-nke.hu/downloads/bsz/bszemle2007/3/16_kovacsjudit_new.pdf

[16] Jan Skriver: The Human Factor Human and organisational aspects of RCA, part I and II, Resilience IAEA Workshop on Root Cause Analysis 9-13 November, 2009

[17] Berek Tamás - Bodrácska Gyula: Az élőerős őrzés az objektumvédelem építőipari ágazatában Hadmérnök, V. Évfolyam 4. szám - 2010. december http://www.hadmernok.hu/2010_4_berek_bodracska.php

[18] Berek Lajos- Tóth Georgina Nóra: Risk and chance of practices Hungarian Journal of Industry and Chemistry 38:(2) pp. 193-196 (2010), http://mk.uni-pannon.hu/hjic/index.php/hjic/article/view/300/279