KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 8, No. 2 (2018), p. 47 – 54

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Analysis as part of risk management to protect the system and its assets

Analýza ako súčasť manažmentu rizík pri ochrane systému a jeho aktív

Martin MAŠĽAN[1,2]

[1]Student of the 5th year of the external form of doctoral study, study program "Security and Protection of the State. In the field of study 8.4.4 National and international security of the Armed Forces Academy M.R. Štefánik in Liptovský Mikuláš,
[2]University of Security Management in Košice

The manuscript was received on 30. 10. 2018 and was accepted after revision for publication on 28. 11. 2018

Abstract:

Risk analysis and proper use of existing analytical methods are one of the basic assumptions of a proper risk assessment. The use of individual methods depends on the nature of the system under consideration, the amount of the necessary costs, the availability of the necessary data, and the possibility of using quantitative methods When estimating the likelihood of occurrence of risk phenomena, information may be drawn, for example, from historical and statistical data which will be used for estimate and quantify future developments. If such data is not available, it is possible to use prediction with qualitative data, which is then necessary to be subjected to further analysis. The assumption of an effective risk assessment is their identification, analysis and subsequent evaluation. The risk values obtained are the basis for setting the measures that are necessary to minimize them, ie adjusting them to an acceptable level.

Keywords: *Risk Management, Analysis, Extraordinary event, Value of the Risk, Risk Assessment, Preventive and Corrective Measures, Protected Asset.*

Abstrakt:

Analýza rizík a správne využívanie existujúcich analytických metód sú jedným zo základných predpokladov hodnotenia rizika. Použitie jednotlivých metód závisí od charakteru posudzovaného systému, od množstva nevyhnutných nákladov, od dostupnosti potrebných údajov s čím súvisí možnosť použitia kvantitatívnych metód. Pri odhadovaní pravdepodobnosti výskytu rizikových javov je možné použiť historické a štatistické údaje, pomocou ktorých je možné odhadnúť

a kvantifikovať budúci vývoj. Ak takéto údaje nie sú k dispozícii, je možné použiť predikciu s kvalitatívnymi údajmi, ktorú je potom potrebné podrobiť ďalšej analýze. Predpokladom efektívneho posúdenia rizík je ich samotná identifikácia, analýza a následné vyhodnotenie. Získané hodnoty rizika sú základom pre stanovenie opatrení, ktoré sú potrebné na ich minimalizáciu, teda ich úpravu na nami akceptovateľnú úroveň.

Kľúčové slová: *Riadenie rizík, Analýza, Mimoriadna udalosť, Hodnota rizika, Posúdenie rizika, Preventívne a nápravné opatrenia, Chránené aktívum.*

Introduction

The safety of systems is constantly increasing thanks to the technical improvement of their components. However, this is only one of the prerequisites for their safe operation. Another is to constantly explore the security risks associated with possible threats that the system is always exposed to. The development of individual threats can lead to the occurrence of extraordinary events (EE). Therefore, it is necessary to continuously monitor individual safety aspects by analyzing and assessing existing safety risks as a function of the probability of occurrence of undesirable phenomena and their consequences. Each extraordinary event requires a thorough analysis that examines the causes of its occurrence, its course, its consequences and the measures and recommendations adopted. The primary role of the measures is to restore functionality and to reduce risk to an acceptable level. An essential prerequisite for assessing the state of the system's security is therefore the knowledge of safe hazards expressed by the interaction of two parameters, which subsequently determine the focus of the measures and recommendations on two areas:

- reduction of the probability of occurrence of EE
- reduction of the severity of consequences after EE

The security of each system and its individual components depends to a large extent on readyness for possible risk situations, the adoption of preventive measures, the identification of existing risks, their investigation and knowledge, as well as the ability to respond to the situations that arise, ie the response. All of these activities are subject to risk Management, ie emergency management and crisis situations, with the basic premise of effective risk management being its analysis, a source of knowledge of the likelihood of its occurrence and possible consequences [1].

1. Risk management

Risk management is a logical and systematic method of determining relationships in activities and processes, identifying existing risks, analyzing, evaluating, reducing, and monitoring to minimize losses. Risk management is a culture, processes and structures geared to effective management of opportunities and possible unwanted consequences. It must be part of any management activity, regardless of the level of management and risk. Under the risk management structure, we understand the set of components that form the foundation and organizational layout for the design, implementation, monitoring, review and ongoing improvement of risk management across the organization.

In the application of risk management to the organization itself, it is essential to respect certain principles and sequence of steps:

1. Top management must promote and enforce the application of risk management principles in the organization's terms of reference. Instruments can be developed with a philosophy of risk, support for statutors, financial support, theoretical preparation and training of managers at lower levels.
2. The organization must develop a risk management policy that creates risk management prerequisites for the organization as a whole and for all its activities. The policy should include:
    - Policy objectives and its importance for the organization
    - The links between the strategy and the risk management policy
    - Definovaní úrovne akceptovateľného rizika v jednotlivých oblastiach činnosti organizácie a postupoch jeho stanovovania
    - Delegating of personal responsibility and powers in risk management
    - Support top management and its commitment to make available the necessary resources
    - Monitoring mechanisms to monitor and review the organization's activities in implementing policy
    - All managers and employees of the organization must be familiar with this policy.
3. Risk management at the organization level must be consistent with its strategy and implemented in all its activities.
4. A successful risk management is also a prerequisite for creating an effective system for monitoring and assessing risk management processes, because the risks themselves are not a static variable

The effectiveness of the risk management process itself (Fig. 3) is therefore conditioned by factors such as its incorporation into all existing structures of the organization, setting the rules for its implementation, responsibility and motivation of the employees, monitoring of efficiency, but also the necessary financial resources for its implementation and improving the functioning of the system from the point of view of risk management.

1.1. Risk assessment

Risk assessment is a complex activity in which we determine the areas to be assessed, identify their priorities, identify the security risks that operate in the system, analyze their potential impacts, determine the degree of acceptability of the individual risks, and then, on the basis of their assessment, we will decide if we accept a measure of certain risks or take measures to reduce them. When assessing the risks, environmental safety is directly linked to the value criteria, which raises the need for an economic analysis taking into account the possible consequences and impacts on protected assets, the probability of their occurrence and the cost of security measures that would be needed to reduce risk. Risk management is therefore very closely related to the availability of resources needed to implement the proposed security measures[2].

The risk assessment process itself consists of several phases:

Determining the context within the system under consideration: from the strategic point of view, the strategic objectives will be included and the means to achieve them. From the organizational point of view, we examine the connections between the various components of the organizational structure, ie internal links, processes, activities through which the goals are achieved. Consequently, it is necessary to identify the areas that will be subject to the risk management assessment, ie areas with a higher level of security risks and possible measures to reduce them. We always take into account the costs and their efficient spending on the one hand, in terms of the expected benefits and effects, as well as the resources and activities that need to be maintained[3].

Risk identification: a process in which all risks need to be detected, regardless of whether or not they can be affected by the organization. The basis for defining risk factors is the knowledge of workers who are familiar with the processes being evaluated. With higher uncertainty, it is necessary to look for analogies in similar processes. Gradually, all external and internal sources of risk that may affect the organization's performance are assessed. Output is a list of events that could disrupt existing processes and be subject to further analysis

Risk analysis: The basic prerequisite for effective risk management is its knowledge. The core of the safety risk assessment is their analysis. It is a process of assessing the causes and sources of risks, their positive and negative impacts, the severity of possible impacts, and the subsequent determination of the likelihood of such impacts occurring. The following characteristics of the risks are the result of the analysis:

- the likelihood of their occurrence at a specific time, space, and survey conditions
- economic characteristics quantifying the present value of objects and possible change of their value after disruption or destruction
- exposure to negative risks
- restoring the system to its original state
- Permanent change of system
- influencing the links between the objects of the examined system itself and the system with its surroundings.

Risk assessment: A complex process in which we determine the magnitude of the risk in terms of the extent of the damage and losses that a given crisis may cause and the likelihood of such a phenomenon occurring, we compare the degree of risk with existing standards, acceptable limits or other predetermined criteria. We determine the importance of individual risk factors, either by expert estimates or by sensitivity analysis. Expert assessment is the basic tool for determining overall risk from the point of view of the probability of occurrence of its factors and the intensity of its negative impact, ie the consequences. The instrument for determining the significance of risk factors is also the sensitivity analysis. This explicitly displays the impact of risk factors on the activity and safety of the subject. The primary objective of risk assessment is to determine a certain value (risk measure) for each specific risk of the compromised system. Based on the level of risk, we determine the order of the risks in terms of their importance, taking into account the influence of the likelihood of occurrence and possible consequences. We then compare the individual risks with the degree of acceptability and decide which risks we will continue to address[4].

Risk mitigation: is a heterogeneous process that depends on the nature of the risk itself, the degree of probability of occurrence of the crisis phenomenon that can cause

the risk and the predicted negative consequences. Risk reduction, for example, can be achieved through crisis policy, risk diversification (insurance), but also by creating reserves or optimizing processes. We also take into account the economic aspect of risk reduction measures. The amount of the costs incurred should be proportionate to the possible consequences and importance of the protected interest. With high prevention costs, it is possible to accept a risk with high negative impacts but with a low probability of occurrence. Risk mitigation measures may be aimed at preventing the occurrence of hazardous events - preventive, managing the course of the risk, mitigating the negative consequences and recovering, but also increasing the acceptability of existing unacceptable risks.

Familiarizing the persons concerned with residual risks: instructing competent staff on the risk factors that exist within the individual processes and activities

Continuous control of the level of risk and compliance and effectiveness of the measures in place. In this process, there is a need for feedback and continuous incorporation of control findings into the system[5].

2. Selected analytical methods of safety risks

The choice of method of risk analysis depends on the nature of the system under investigation, on the availability and complexity of the input information - these must be trusted, relevant and carry the required data, from the development stage. The choice of the analytical method is the primary prerequisite for an effective risk assessment. When estimating the likelihood of occurrence of risk phenomena, information may be drawn, for example, from historical and statistical data that can roughly extrapolate and quantify future developments. If such data is not available, it is possible to use a prediction with qualitative data, which should then be subjected to further analysis using methods such as Even Tree Analysis (ETA) or (Fault Tree Analysis). Choosing a suitable analytical method is a complex process that takes into account all of the facts above. The choice of the method itself also affects the fact whether a priori analysis will be carried out, based on the phenomenon that has occurred at least once in the past, or an apathetic analysis in which the analyst works with the phenomena they only think they might be able to do. The risk is estimated in this case on the basis of assumed behaviors[6]. The risk assessment is a process consisting of successive consecutive steps, in this respect it is possible to divide the existing analytical methods into groups, which are described in more detail in the following sections of chapter 2.

2.1. Identification of risk sources

The goal of identifying risk factors is to create a list of events that could cause undesirable disturbance of ongoing processes. At this stage we will define all the risks that will be subsequently analyzed and evaluated. When identifying risk factors, we will take into account both external and internal environmental impacts, which can be evaluated using SWOT analysis. Based on this, experts can process a framework overview of risks that could endanger the subject. One of the oldest methods for identifying risk sources is the safety review - this is the routine visual inspection aimed at assessing operational activities and personnel, introducing new technologies in the context of existing risks, maintenance levels and safety inspections. As a result, there are descriptions of possible problems and suggestions for remedying them. Other methods used to identify the risks are:

Checklist analysis-CA, which contains a list of items used to verify system status. Creating a checklist should involve authors with a various education and a look at how the system works. The purpose of the checklist is to compare the organization with the practice applied in comparable organizations. On the basis of a checklist, analysts define questions to identify possible system failures. After receiving and evaluating responses, the next step is set. To obtain a comprehensive list of risks, this method needs to be supplemented by a further analytical method[7].

Preliminary Hazard Analysis (PHA), which is used if we lack information. The purpose is to compile a list of risk sources in which hazardous situations will be arranged according to the degree of risk. When reducing the risk, it is necessary to focus on the situations listed at the beginning of the list. This analysis serves as the basis for further analysis such as WI, ETA, FTA or FMEA.

The What If (WI) method is based on a discussion of people well-informed about the process under review. The analyst asks what happens if? They try to detect events that could be a source of risk. The basic prerequisite for the success of the method is the compilation of questions, the answers of which should analyze the system to the maximum extent. The list of questions and answers shows the possibilities of protection against the consequences of undesirable events and contains proposals for risk reduction measures.

2.2. Determining the causes of occurrence of risk events and creating scenarios

When generating scenarios of the course of a risk event, the diagram of causes and consequences-Ishikawow diagram, which is an indicative analysis, is often used. In a simple form, the problem is analyzed based on its causes.

Other suitable risk modeling methods are ETA (Even Tree Failure), an event tree analysis that model the course of an event with a favorable and unfavorable possibility of its further development. The result is a branched chart that represents an accident scenario, ie a set of errors and deficiencies with varying degrees of impact on the system under review. This method allows you to quantitatively evaluate the event under consideration by using factors such as the probability of its occurrence and possible consequences[8].

Fault Tree Analysis (FTA) - Fault tree analysis, it is a graphical tool for deducting identification of causal disorders that can initiate undesired peak events. Based on the definition of peak events, there are analyzed and graphically illustrated the potential causes that may lead to its occurrence.

2.3. Basic analysis of assessed system

One of the most used methods is FMEA (Failure Mode and Effect Analysis) - An analysis of the causes of failures and their consequences, the role of which is to select the significant risks for the system under consideration. The initial step for this analysis is to identify the potential risks that are derived from previous risk analyzes (Ishikawa diagram, ETA ...), to the individual risks are assigned numerical values, which consist of the probability of occurrence, the possibility of detection and the severity of consequences [9]. Thus is counted the resulting risk rate (risk number), which is compared to the determined value of the risk acceptance rate. The result of the analysis is a clear tabular and graphical representation of both acceptable and unacceptable risks. When designing measures, it is always necessary to take into account how the individual components have been involved in the total risk number. If there is a possibility of high

severity of the consequences but a very low chance of occurrence, preventive measures will not be necessary[10].

2.4. Verification methods and techniques of risk assessment

In this group could be for example incuded, the Paret principle, the Lorentz curve, the CARVER method, or the risk matrix. If we have enough relevant information and we have chosen the appropriate method, the analysis of the security risks should provide us the information about the systemic or non-systemic nature of the risk, the degree of acceptability of individual risks as well as the recoverability of the funds spent on preventive measures[11].

Conclusion

Risk management has an increasingly important place in the functioning of any organization. It is a continuous process that enables effective risk knowledge and its assessment, design and implementation of the necessary measures. The most important activity in cognition and risk management is its analysis, which is a prerequisite for its overall assessment and the design of the necessary measures. The outcome of the overall risk assessment may, if necessary, also include preventive and corrective actions defined for risks whose value exceeds an acceptable level. When designing them, we always take into account the likelihood of event occurrence and its possible consequences as well as the value of the protected asset. The implementation of these measures is often linked to the spending of certain funds. In practice, we often meet the reluctance to spend the necessary funds, as they mean an increase the total cost of the system. We should also take into consideration the fact that the funds thus spent represent only a certain percentage of the total value of the asset that will be protected by the measures taken.

References

[1] BUZALKA,J. 2012.Teória bezpečnostných rizík.Bratislava: Akadémia PZ 2012. 168s. ISBN 978-80-8054-547-5.

[2] SMEJKAL,V.-RAIS,K. 2006.Řízení rizik ve firmách a jiných organizacích. Praha : Grada publishing,a.s. 2006. 300s. ISBN 80-247-1667-4.

[3] HOFREITER, L. 2004. Safety, security risks and threats Žilina : Edis – publishing house of University in Žilina. 2004. 146 s. ISBN 80-8070-181-4.

[4] Proceedings of the International Scientific Conference Methodology and Methodics of the Analysis of Internal Threats of the Slovak Republic, Academy of the Police Force in Bratislava 2011.

[5] REITŠPÍS,J.-BARTLOVÁ,I.-HOFREITER,L.2004.Securityrisk management. Žilina: Edis - publishing house of University in Žilina. 2004. 296s. ISBN 80-8070-328-0.

[6] PALEČEK,M. 2006. Risk prevention. Praha:University of Economics 2006. ISBN 80-245-1117-7.

[7] TICHÝ, M. 2006. Risk control: analysis and management. Praha:C.H. Beck. 2006. 396s. ISBN 80-7179-415-5.

[8] ŠALING, S. a kol..2008. Great Dictionary of Foreign Words. SAMO 2008. 1184s. ISBN 80-89123-07-0

[9] PŘIBIL, P.-JANOTA, A.-SPALEK, J. 2008. Analysis and management of transport risks. Praha: BEN-technical literature. 2008. 526s. ISBN 978-80-7300-2140-0.

[10] KURACINA, R.-FERJENČÍK, M. 2006. Tools for risk assessment and accident investigation. Reviewed Proceedings. ISBN 80-8073-649-9

[11] Proceedings of scientific conferences Resolving crisis situations in a specific environment, FŠI ŽU, Žilina 1996-2005

[12] Douglas J. Landoll. 2011. Security Risk Assessment Handbook. CRC Press, 2011,495s. ISBN 978-14-3982-148-0.

[13] Hopkin, P. 2013. Risk Management. Kogan Page 2013,288s. ISBN 978-07-4946-838-5.

[14] Vose, D. 2008.Risk Analysis. Wiley-Blackwell 2008, 752s. ISBN 978-04-7051-284-5

[15] Newsome, B. 2013. A Practical Introduction to Security and Risk Management. Sage Publications 2013, 408s. ISBN 978-14-5229-027-0.

[16] STN EN ISO 31000:2011: Risk management

[17] STN EN 60812:20006: Methods of system reliability analysis. Procedure to analyze the method and the consequence of the malfunctions (FMEA)

Author:

[1]**Martin Mašľan MSc. -** Student of the 5th year of the external form of doctoral study, study program "Security and Protection of the State. In the field of study 8.4.4 National and international security of the Armed Forces Academy M.R. Štefánik in Liptovský Mikuláš. University of Security Management in Košice. e-mail: martin.maslan@vsbm.sk