Vol. 7 No. 3, 2021
Baltic Journal of Economic Studies
DOI: https://doi.org/10.30525/2256-0742/2021-7-3-1-8

SELECTION AND APPLICATION OF APPROPRIATE ANALYTICAL METHODS NEEDED TO ASSESS THE RISKS REDUCING THE SECURITY OF THE PROTECTED SYSTEM

Josef Reitšpís[1], Martin Mašľan[2], Igor Britchenko[3]

Abstract. Risk assessment is one of the prerequisites for understanding its causes and possible consequences. We base our risk assessment on the principles described in the European standard EN 31000 - Risk Management Process. This standard comprehensively describes the continuous activities that are necessary in managing risks and minimizing their possible adverse effects on the operation of the system under investigation. In this activity, it is necessary to first identify the existing risks, then analyze and evaluate the identified risks. In the analysis of existing risks, it is possible to use both qualitative and quantitative analytical methods, or combine them. We use qualitative methods in cases where we do not have a sufficient amount of input information, these are more subjective. Quantitative methods are more accurate, but also more demanding on input information and time. The choice of a suitable analytical method is a basic prerequisite for knowledge of risks and their evaluation. The values of individual risks obtained in this way are the basis for determining the measures that are necessary to minimize them, i.e., to adjust them to an acceptable level. The draft measures are always based on the value of the individual components used to calculate the risk number, as well as on the value of the asset , which needs to be protected. Appropriately chosen analytical methods are one of the basic prerequisites for the consistent application of the principles of risk management, as a continuous process aimed at increasing the overall security of the system under study. In the article, the author describes the procedures used in risk assessment, as well as specific analytical methods that can be used in working with risks. The aim of identifying risk factors is to create a list of events that could cause undesirable disruption to ongoing processes. At this stage, we define all the risks that will be subsequently analyzed and evaluated. When identifying, we can use methods such as, e.g. SWOT, PHA (Preliminary Hazard Analysis) or CA (Checklist Analysis). Methods suitable for determining the causes and creating scenarios for the course of a risk event are ETA (Event Tree Analysis) or FTA (Fault Tree Analysis). The basic analysis of the system can be performed using the FMEA method (Failure Mode and Effect Analysis), which provides a numerical risk assessment. By comparison with the numerical value of the risk that we are willing to accept, we obtain 2 groups of risks. Acceptable, which will be given regular attention and unacceptable, which we will focus on in risk management and we will try to minimize its negative affect on the functioning of the system under study.

Key words: risk management, analysis, risk assessment, preventive and corrective measures, protected asset, value of risk.

JEL Classification: P40, F52

Corresponding author:
[1] University of Security Management in Košice, Slovakia.
E-mail: Josef.reitspis@vsbm.sk
ORCID: https://orcid.org/0000-0003-4248-5758
[2] University of Security Management in Košice, Slovakia.
E-mail: Martin.maslan@vsbm.sk
ORCID: https://orcid.org/0000-0003-1913-655X
[3] State Higher Vocational School
Memorial of Prof. Stanislaw Tarnowski in Tarnobrzeg, Poland.
E-mail: ibritchenko@gmai.com
ORCID: https://orcid.org/0000-0002-9196-8740

Introduction

The security of the systems is constantly increasing thanks to the technical improvement of their elements. However, this is only one of the prerequisites for their safe operation. Another is the constant knowledge and research of security risks associated with the possible realization of threats to which the system is constantly exposed. The degree of development of individual threats can lead to the occurrence of extraordinary events (hereinafter referred to as MU). Therefore, it is necessary to constantly monitor individual safety aspects by analyzing and evaluating existing safety risks as a function of the probability of the occurrence of adverse events and their consequences (Newsome, 2013). Every extraordinary event requires a thorough analysis, which examines the causes of its occurrence, course, consequences and measures and recommendations taken. The primary task of the measures is to restore the functionality of the system and try to reduce the risk to an acceptable level. A necessary prerequisite for assessing the security status of the system is therefore knowledge of the safe risks expressed by the interaction of two parameters, which then determine the focus of measures and recommendations in the area of necessary prevention or remediation.

The safety of each system and its individual components depends to a large extent on the preparedness 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 situations, i.e., responses. All these activities are subject to Risk Management, i.e., the management of emergencies and crisis situations, while the basic premise of effective risk management is its analysis, i.e., the source of knowledge of the probability of its occurrence and possible consequences (Buzalka, 2012).

1. Risk management affecting the organization's activities

Risk management is a logical and systematic method of determining the context of activities and processes, identifying the risks existing in them, their analysis, evaluation, reduction and ongoing monitoring in order to minimize losses. Risk management is a culture, processes and structures focused on the effective management of opportunities and possible undesirable consequences. It must be part of every managerial activity, regardless of the level of management and risk. By risk management structure we mean a set of components that form the basis and organizational structure for the design, implementation, monitoring, review and continuous improvement of risk management throughout the organization.

When applying risk management to the activities of the organization, it is necessary to respect certain principles and sequence of steps:

1. Top management shall support and promote the application of risk management principles in the context of the organization. Tools can be developed risk philosophy, statutory support, financial support, theoretical training and training of managers at lower levels.

2. The organization shall develop a risk management policy that creates the conditions for risk management in the organization as a whole and in all its activities. The policy should include information on:
– policy objectives and their relevance to the organization;
– the links between risk management strategy and policy;
– defining the level of acceptable risk in individual areas of activity of the organization and procedures for its determination;
– delegation of personal responsibility and authority in risk management;
– supporting top management and its commitment to make the necessary resources available;
-– control mechanisms to monitor and review the organisation's policy implementation activities;
– all managers and employees of the organization must be acquainted with the policy developed in this way.

3. Risk management at the level of the organization must be in line with its strategy, it must be implemented in all its activities.

4. The creation of an effective system of monitoring and assessment of risk management processes is also a prerequisite for successful risk management, as risks themselves are not a static quantity.

The effectiveness of the risk management process itself is therefore conditioned by factors such as its incorporation into all existing structures of the organization, setting rules for its application, responsibility and motivation of employees, monitoring effectiveness, but also the necessary financial resources in its implementation and implementation of measures necessary to improve the functioning of the system from a risk management perspective.

1.1 Procedures used to assess existing risks

Risk assessment is a complex activity in which we determine the areas that will be subject to assessment, determine their priorities, identify security risks that operate in the system, analyze their possible impacts, determine the level of acceptability of individual risks and then based on their evaluation we will find out accept a certain part of the risks or take measures to reduce them. When assessing risks, environmental security is directly linked to value criteria, which raises the need for an economic analysis that takes into account the possible consequences and impacts on protected assets, the likelihood of their occurrence and the costs associated with security measures, risk

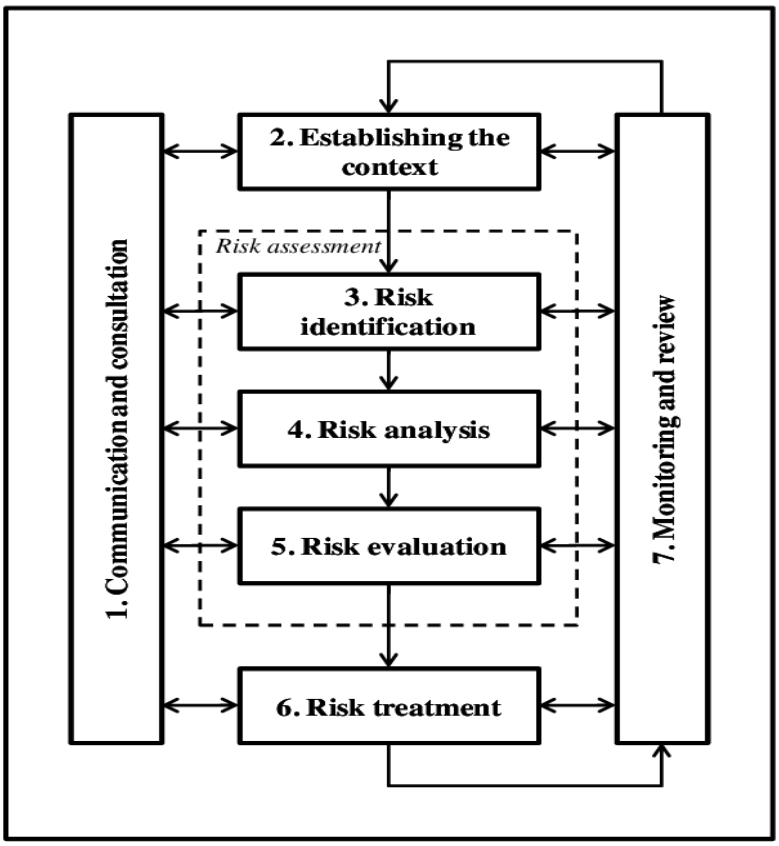

Figure 1. Risk management process following EN 31000

measures. Risk management is therefore very closely related to the availability of resources that are needed in the implementation of the proposed security measures.

The risk assessment process itself consists of several phases:

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

Risk identification: the process by which all risks need to be identified, whether they are controllable by the organization or not. The basis for defining risk factors is the knowledge of employees who are familiar with the evaluated processes. With a higher degree of uncertainty, it is necessary to look for analogies in similar processes. Gradually, all possible external and internal sources of risks that may affect the operation of the organization are assessed. The output is a list of events that could disrupt existing processes and will be subject to further analysis.

Risk analysis: The basic prerequisite for effective risk management is its knowledge. The core of research into security risks is their analysis. It is the process of assessing the causes and sources of risks, their positive and negative impacts, the severity of possible impacts and then determining the likelihood that these impacts may occur. The result of the analysis should be the following characteristics of the examined risks:

– the likelihood of their occurrence in a specific time, space and conditions of the investigation;
– economic characteristics quantifying the present value of the objects and the possible change in their value after disruption or destruction;
– exposure to negative risk manifestations;
– restore the system to its original state;
– possible permanent change of the system;
– influencing the connections between the objects of the examined system and the system with its surroundings (Hofreiter, 2004).

Risk evaluation: a complex process in which we determine the amount of risk in terms of the extent of damage and loss that a given crisis phenomenon can cause and the probability that such a phenomenon

will occur, we compare the degree of risk with existing standards, acceptable limits or other predetermined criteria. We determine the significance of individual risk factors, either through expert estimates or sensitivity analysis. Expert assessment is a basic tool for determining the overall risk in terms of the probability of occurrence of its factors and the intensity of its negative impact, i.e., consequences. Sensitivity analysis is also a tool for determining the significance of risk factors. This explicitly shows the degree of influence of risk factors on the activity and safety of the entity (Hopkin, 2013). The basic goal of risk assessment is to determine a certain value (risk level) for each specific risk of the endangered system. Based on the degree of risk, we determine the order of risks in terms of their significance, while also taking into account the influence of the probability of occurrence and possible consequences. We then compare the individual risks with the level of acceptability and decide which risks we will address further.

Risk treatment and reduction: is a diverse process, which depends on the nature of the risk itself, the degree of probability of a crisis phenomenon that may cause the risk and the expected negative consequences. Thus, risk reduction can be achieved, for example, through crisis policy, risk diversification (insurance), but also by creating reserves or optimizing processes. When taking measures to reduce risk, we always take into account their economic side. The amount of costs incurred should be proportionate to the possible consequences and importance of the interest protected. With high prevention costs, it is also possible to accept a risk with high negative impacts, but with a low probability of occurrence. Risk reduction measures can be aimed at preventing the occurrence of risky events-preventive nature, at managing the course of the risk phenomenon, at mitigating negative consequences and recovery, but also at increasing the level of acceptability of existing unacceptable risks.

Familiarization of the persons concerned with the residual risks: instruction of competent staff about the risk factors that exist in the individual processes and activities.

Ongoing monitoring of the level of risks and the implementation and effectiveness of the measures in place. In this process, the existence of feedback and the continuous incorporation of control findings into the system is essential (Reitšpís et al., 2004).

2. Analytical methods for the examination of security risks

The choice of risk analysis method depends on the nature of the system under investigation itself, on the availability and complexity of the input information – this must be reliable, relevant and must carry the required data, from the stage of development of the research. The choice of analytical method is a primary prerequisite for effective risk assessment. When estimating the probability of occurrence of risk phenomena, the information can be drawn e.g. from historical and statistical data, on the basis of which it is possible to approximately extrapolate and quantify future developments. If such data are not available, it is possible to use a prediction with qualitative data, which must then be subjected to further analysis using methods such as ETA (Event Tree Analysis) or (Fault Tree Analysis). The selection of an appropriate analytical method is a complex process in which all the above facts must be taken into account (Tichý, 2006).

The choice of method itself is also influenced by whether an a priori analysis is performed, which is based on a phenomenon that has occurred at least once in the past, or an a posteriori analysis in which the analyst works with phenomena that he only thinks could occur. In this case, the risk is estimated on the basis of the expected behavior of the phenomena. Risk assessment is a process consisting of successive steps, in this respect, existing analytical methods can be divided into groups, which are described in more detail in the following sections of Chapter 2.

2.1 Methods of identifying sources of risk

The aim of identifying risk factors is to create a list of events that could cause undesirable disruption to ongoing processes. At this stage, we define all the risks that will be subsequently analyzed and evaluated. When identifying risk factors, we will take into account both the effects of external and internal environments, which can be evaluated using SWOT analysis. Based on it, experts can prepare a general overview of risks that could pose a threat to the entity. One of the oldest methods for identifying sources of risk is safety review – these are routine visual inspections aimed at assessing operational activities and personnel, the introduction of new technologies in the context of existing risks, the level of maintenance work and safety inspections. The result is descriptions of possible problems and suggestions for their correction. Other methods used to identify risks are:

Checklist analysis (CA), which contains a list of items used to verify the status of the system. Authors with different backgrounds and perspectives on how the system works should be involved in creating the checklist. The purpose of the checklist is to compare the organization with the practice applied in comparable organizations. Based on the checklist, analysts define issues to identify possible system deficiencies. After receiving and evaluating the answers, the next procedure is set. To obtain a comprehensive list of risks, it is necessary to supplement this method with another analytical method.

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

The What-if – WI method is based on the discussion of people well acquainted with the research process. The analyst is using the question "What happens if"? It seeks to identify events that could be a source of risk. The basic precondition for the success of the method is the compilation of questions, the answers to which should analyze the system to the maximum extent. The list of questions and answers points to the possibilities of protection against the consequences of adverse events and contains proposals for measures to reduce the risk.

2.2 Methods for determining the causes and creating scenarios for the course of events

When creating scenarios of the course of a risk event, a cause-and-effect diagram is often used – the Ishikawa diagram, which represents an indicative analysis. Displays the analyzed problem in a simple form based on its causes.

Another suitable method of risk modeling is ETA (Event Tree Failure): an event tree analysis, which models the course of an event using a favorable and unfavorable possibility of its further development. The result is a branched graph that represents an accident scenario, i.e., a set of errors and deficiencies with varying degrees of impact on the system under study.

This method makes it possible to quantify the investigated event using the probability of its occurrence and possible consequence. FTA (Fault Tree Analysis) method: a fault tree analysis, it is a graphical tool for deductive identification of causal faults that can initiate the occurrence of an undesirable peak event. Based on the definition of peak events, potential causes that can lead to its occurrence are analyzed and graphically represented here (Přibil et al, 2008).

2.3 Methods for basic system analysis

One of the most commonly used methods is FMEA (Failure Mode and Effect Analysis): analysis of the causes of failures and their consequences, the task of which is to select significant risks affecting the system under investigation. The first step in creating this analysis is to determine the potential risks that are obtained from previous risk analyzes (the Ishikawa diagram, ETA ...), individual analyzed risks are assigned numerical values within this analysis, which are the product of the probability of occurrence, detectability and severity of consequences. In this way, the resulting risk measure (risk number) is calculated, which is compared with the determined value of the risk acceptability rate. The result of the analysis is a clear tabular and graphical representation of both acceptable and unacceptable risks. When designing measures for individual risks, it is always necessary to take into account how the individual components contributed to the total amount of the risk number. If there is a possibility of a high severity of consequences but a very low probability of an event, it may not be necessary to take precautionary measures (Smejkal, Rais, 2006).

2.3.1 Analysis of the causes of failures and consequences of FMEA

FMEA (Failure Mode and Effect Analysis): failure analysis is an inductive method that has been developed for the analysis of failures in various systems. It is one of the basic methods used in semi-quantitative risk analysis. Its origins date back to the 1940s, when it was formulated under US military regulations (MIL-P-1629). In the1960s, NASA applied this method as part of the APOLLO program, where it was to improve and verify the hardware of the space program. At present, it has a wide application, it is an integral part of ISO 9000, QS 9000 standards. In Slovakia, it was issued in 2006 as a standard STN EN 60812 under the name Methods of system reliability analysis (STN EN 60812:20006). The application of this method itself can be divided into two basic phases:

1. The identification phase, in which experts focus on:
– any potential errors that may occur under both normal and extreme operating conditions, regardless of their severity and probability of occurrence;
– all possible consequences of errors;
– all possible causes of the error, taking into account that one error can have several consequences and one consequence can have several causes.

2. Numerical phase in which the risk level in the form of a risk number (RPN-Risk Priority Number) is calculated. Risk number, i.e., the risk measure is calculated as the product of the probability of occurrence of the risk (PV), the significance of the error-severity of the consequences (VN) and the probability of detection (PO).

RPN = PVxVNxPO

In the following text, there will be analyzed security risks affecting the functionality of logistics systems. The values of individual parameters are chosen using numerical scales; we have chosen the numerical range 1-5. A value of 1 corresponds to the best evaluation. The individual parameters and their evaluation are clearly shown in the following table.

In the risk assessment itself, we also have to take into account the analysis of past security incidents and the analysis of the current situation.

Table 1
Value parameters for FMEA analysis

RLR	The resulting level of risk	VC	Significance of the error, severity of the consequences
0-5	Insignificant risk	1	Small injury, tort, pity
6-12	Acceptable risk	2	Injury – sick leave, more damage
13-50	Moderate risk	3	Transport to hospital, higher damage
51-100	Undesirable risk	4	Permanent consequences, high damage
101-125	Unacceptable risk	5	Death, very high property damage
PO	**Probability of occurrence**	**PD**	**Probability of detection**
1	Random, unlikely	1	Detectability of risk during the offense
2	Rather unlikely	2	Easily detectable
3	Probably-real	3	Detectable risk approx. a week
4	Very likely	4	Hard to detect for more than a week
5	Persistent threat	5	Undetectable

Source: Own interpretation

Table 2
Risk assessment using the FMEA-structural aspect

N	Event	Rating			RLR
		PO	VC	PD	
1	Unsuitability of the means of transport for the given material	3	3	2	**18**
2	Material storage	3	2	2	**12**
3	**Capacity of means of transport**	4	4	3	**48**
4	**Technical level of means of transport**	5	4	2	**40**
5	Security of transported cargo-THEFT	2	3	1	**6**
6	The possibility of a terrorist attack	2	3	4	**24**
7	**Insufficient level of used IT**	4	3	4	**48**
8	Outdated and poorly maintained infrastructure	2	3	3	**18**
9	**Open information flows in logistics systems**	4	5	5	**100**
10	**Using of IT systems with various security**	3	3	5	**45**
11	**Outsourcing of transport services**	5	3	3	**45**
12	**Service level of equipment used**	4	4	4	**64**
13	**Interruption of information flows**	4	4	4	**64**
14	Leakage of hazardous substances	3	3	2	**18**
15	**Traffic accidents**	4	3	5	**60**
Σ					**610**

Source: Own interpretation

Table 3
Risk assessment using the FMEA-process aspect

N	Event	Rating			RLR
		PO	VC	PD	
1	Breach of secrecy of transported messages	3	3	3	27
2	**Unauthorized use of personal data**	4	5	3	**60**
3	**Hazards under the influence of an addictive substance**	3	4	4	**48**
4	Organized crime	3	3	3	27
5	The growing volume of cost theft	2	2	2	8
6	Carelessness during transport	3	3	2	18
7	**Insufficient knowledge of the technologies used**	4	4	5	**80**
8	Intentional damage to the device	2	2	4	16
9	**Open information flows in logistics systems**	4	3	4	**48**
10	**Motivation of transport staff**	4	4	4	**64**
11	**Outsourcing of transport services**	3	4	4	**48**
12	**Participation of civilians**	4	3	5	**60**
13	**Infiltration by IT misinformation**	5	5	3	**75**
14	Fastening of material during transport	3	3	2	18
15	Traffic accidents	3	3	4	36
Σ					**633**

Source: Own interpretation

The result of the FMEA analysis is a representation of either structural or process risks, which will provide information on their severity and level of acceptability in a clear form.

Risks exceeding the level of acceptance are those with an RPN> 30, which are marked in red. The risks thus identified will be taken into account in the subsequent design of the measures necessary to increase the security of the system under investigation.

Conclusion

Using the FMEA method provides the calculated RPN values and possibility to compare risks in terms of their causes and consequences on the basis of a uniform scale. For individual types of risks (structural and procedural), it is necessary to determine the level of acceptability and compare it with the obtained RPN values. As the maximum value of 125 is set, the acceptability rate can be set at 1/4 of the whole, which represents risks with an RPN> 30. Based on the results, it is possible to set priorities for corrective and preventive measures, after their implementation to re-assess the values of parameters PV, VN and PO. When calculating the RPN, it is necessary to pay increased attention to the value of the severity of the consequences. The total calculated RPN can be low in this case, because the PV and PO values can be equal to 1, only the VN value is high. This applies to very serious events, the probability of which is low. In these cases, it will be necessary to assess the possible costs of preventive measures. In the event that these costs would be disproportionately high and the probability of an event low, the existing situation can be accepted (Kuracina-Ferjenčík, 2006).

Risk retention, risk sharing and risk prevention are recommended for treatment of risks (Milind, 2018). The ability to recognize and manage risks is playing an increasingly important role in the functioning of any organization. It is a continuous process that is a means to effectively identify and assess risks, design and implement the necessary measures (Paleček, 2006). The most important activity in recognizing and managing risk is its analysis, which is a basic prerequisite for its overall assessment and proposal of necessary measures. The output of the overall risk assessment may be, if necessary, preventive and corrective measures defined for risks whose value exceeds an acceptable level. When designing them, we always take into account the probability of the event and its possible consequences, as well as the value of the protected asset. The implementation of these measures is often associated with the need to spend certain funds. In practice, we often encounter a reluctance to spend the necessary resources, because they mean an increase in the total cost of running the system.

Therefore, in order to increase the resistance of the system, it is constantly necessary to innovate existing ones and add new security elements. The problem is the rapid development of information technology and cyber threats. When procuring these funds, we take into consideration their price and functionality from the point of view of system operation, less importance is placed on the integration of modern active and passive safety elements. When procuring devices with a low level of security features, it is then necessary to make changes to the security parameters, their configuration, or the software itself, which may conflict with the licenses and warranties provided by the original suppliers. These changes may also have their limits on the technical level of the innovated devices. When procuring new equipment, it is therefore necessary to take into account the supplied safety and the technical level of the safety elements that are part of the delivery. This will significantly reduce the additional costs incurred during their period of operation. However, account must also be taken of the fact that the funds thus spent represent only a certain percentage of the total value of the asset, which will be protected, if necessary, by the measures taken (Hubbard, 2009).

References:

Buzalka, J. (2012). Teória bezpečnostných rizík. Bratislava: Akadémia PZ Slovensko.

Hofreiter, L. (2004). Bezpečnosť, bezpečnostné riziká a ohrozenia. Žilina: Edis – vydavateľstvo Žilinskej univerzity. Slovensko. 146 s.

Hopkin, P. (2013). Risk Management. Kogan Page. 288 s.

Hubbard, D. (2009). Failure of Risk Management. Wiley-Blackwell. 304 s.

Kuracina, R., & Ferjenčík, M. (2006). Nástroje pre oceňovanie rizika a vyšetrovanie havárií. Recenzovaný zborník. ISBN 80-8073-649-9

Milind T. Phadtare; A. D. Gosavi; & T. K. Ganguli (2018). Risk management in small and micro construction firms undertaking repairs and modernisation of residential houses: a case of India. *International Journal of Risk Assessment and Management,* vol. 21 no. 3. DOI: 10.1504/IJRAM.2018.093742

Newsome, B. (2013). Practical introduction to Security and Risk Management. Sage Publications. 408 s.

Paleček, M. (2006). Prevence rizik. Praha: VŠE Česká republika.

Přibil, P., Janota, A., & Spalek, J. (2008). Analýza a řízení rizik v dopravě. Praha:BEN-technická literatura. Česká republika. 526 s.

Reitšpís, J., Bartlová, I., & Hofreiter, L. (2004). Manažérstvo bezpečnostných rizík. Žilina: Edis – vydavateľstvo Žilinskej univerzity. Slovensko. 296 s.

Smejkal, V., & Rais, K. (2006). Řízení rizik ve firmách a jiných organizacích. Praha : Grada publishing, a.s. 300 s.

STN EN ISO 31000:2011: Manažérstvo rizika.

STN EN 60812:20006: Metódy analýzy spoľahlivosti systému. Postup analýzy spôsobu a dôsledku porúch (FMEA).

Tichý, M. (2006). Ovládání rizika: analýza a management. Praha: C.H.Beck. Česká republika. 396 s.