

**TECHNICAL UNIVERSITY IN ZVOLEN**  
**Faculty of Wood Sciences and Technology**

Andrea MAJLINGOVÁ

**SAFETY AND SECURITY RISKS THEORY**



**2024**

This publication was created thanks to the grant support of the Cultural and Educational Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic as one of the outputs of the project KEGA 009TU Z-4/2023 "*Preparing of multilingual electronic study materials as a support of internationalization of education in study programs Fire Protection and Safety*".

Author:

prof. Dr. Andrea MAJLINGOVÁ

Department of Fire Protection  
Faculty of Wood Sciences and Technology  
Technical University in Zvolen  
T. G. Masaryka 24, 960 01 Zvolen

Reviewers:

assoc. prof. Dr. hab. Péter PÁNTYA      Ludovika - University of Public Services, Hungary  
assoc. prof. Dr. Lenka BRUMAROVÁ      VSB - Technical University of Ostrava, Czechia  
assoc. prof. Dr. Peter LOŠONCI          University of Security Management in Kosice, Slovakia

I.– 2024, 122 p. (7.96 AS, 8.10 ES)  
Document form: electronic (online pdf)  
Publishing house: Technical University in Zvolen  
Design: prof. Dr. Andrea MAJLINGOVÁ  
Translated to English by authors

Publishing of this publication was approved by the Editorial Board of the Technical University in Zvolen on 19. 2. 2024, No EP 30/2024, as a university textbook. The author and the reviewers are responsible for the professional and linguistic standards of this publication. The manuscript has not undergone linguistic proofreading.

© Technical University in Zvolen  
© prof. Dr. Andrea MAJLINGOVÁ

ISBN 978-80-228-3417-9

All rights reserved. No part of the text or illustrations may be used for redistribution in any form without the prior permission of the authors or the publisher.

**TECHNICAL UNIVERSITY IN ZVOLEN**  
**Faculty of Wood Sciences and Technology**

Andrea MAJLINGOVÁ

**SAFETY AND SECURITY RISKS THEORY**  
University textbook

**Zvolen 2024**



## FOREWORD

Safety / security and risk should be considered like linked vessels. High safety implies low risk and vice versa, whether it is in the safety of people, property, environment, facilities, that are underground, on the ground, or above the ground.

To build an acceptable level of safety / security, which can be viewed from a social or economic point of view, it is necessary to implement risk management activities into the management practice of the society / company. The risks to which the society / company and its activities / operations are exposed are of a different nature.

Safety / security risks represent a broad group of risks. The risks of fires, explosions or leakages of hazardous substances and the risks of occupational accidents and diseases are of the greatest importance for the company. These cause economic damage which ultimately limits the investment capacity of the company. Based on this, it is also possible to talk about continuous vessels. The two groups of risks interact with each other.

Therefore, if we want to talk about effective business management, we should consider causality and plan and implement measures simultaneously in both areas.

The university textbook deals mainly with the issue of safety / security risk management.

It is intended primarily for students of the Safety and Security Sciences at the Technical University in Zvolen and universities teaching related subjects. However, due to its exclusively electronic form, its further dissemination is expected not only among the professional but also among the public.

# CONTENTS

- 1. RISK..... 7
  - 1.1. INTRODUCTION ..... 7
  - 1.2. RISK PERCEPTION IN SAFETY / SECURITY PRACTICE ..... 9
  - 1.3. RISK PROGRESSION.....12
  - 1.4. DOMINO EFFECT .....14
  - 1.5. SYNERGISTIC EFFECT.....14
  - 1.6. RISK FUNCTION.....15
  - 1.7. RISK EXPRESSION .....15
- CONCLUSION.....17
- REFERENCES .....17
- 2.1. TYPES OF RISKS .....19
- 2.2. RISK CLASSIFICATION .....21
  - 2.2.1. GENERAL RISK CLASSIFICATION .....21
  - 2.2.2. CLASSIFICATION OF RISKS ACCORDING TO THE OBJECT OF ACTION .....24
- CONCLUSIONS .....26
- REFERENCES .....26
- 3. SAFETY AND SECURITY RISK MANAGEMENT .....27
  - 3.1. RISK MANAGEMENT.....27
  - 3.2. RISK MANAGEMENT PROCESS .....29
    - 3.2.1. RISK ANALYSIS .....32
    - 3.2.2. RISK ASSESSMENT .....32
  - 3.3 BASIC REQUIREMENTS FOR THE MANAGEMENT OF SAFETY / SECURITY RISKS OF THE ORGANISATION .....35
  - 3.4 THEORETICAL BACKGROUND OF DISASTER RISK MANAGEMENT .....37
- CONCLUSIONS .....40
- REFERENCES .....41
- 4. SAFETY AND SECURITY RISK ANALYSIS METHODS .....42
  - 4.1. CLASSIFICATION OF SAFETY RISK ANALYSIS METHODS.....42
  - 4.2. CHARACTERISTICS OF SELECTED RISK ANALYSIS METHODS .....44
    - 4.2.1. CHECK LIST ANALYSIS (CLA) .....45
    - 4.2.2. SAFETY AUDIT (SA) .....46
    - 4.2.3. WHAT HAPPENS IF ... (What If Analysis - WIA).....46
    - 4.2.4. PRELIMINARY HAZARD ANALYSIS (PHA) .....47
    - 4.2.5. FAILURE MODE AND EFFECT ANALYSIS (FMEA).....48
    - 4.2.6. FAULT TREE ANALYSIS (FTA) .....52
    - 4.2.7. EVENT TREE ANALYSIS (ETA) .....54

4.2.8.	HUMAN RELIABILITY ASSESSMENT (HRA) .....	55
4.2.9.	HAZARD AND OPERABILITY STUDY (HAZOP) .....	58
4.2.10.	RATING METHOD .....	61
4.3.	COMPARISON OF RISK ANALYSIS METHODS .....	64
4.4.	SELECTION OF AN APPROPRIATE RISK ANALYSIS METHOD .....	67
	CONCLUSIONS .....	69
	REFERENCES .....	70
5.	METHODS FOR REDUCING AND MONITORING SAFETY AND SECURITY RISKS ....	71
5.1.	RISK REDUCTION AND MONITORING .....	71
5.2.	REDUCING AND MONITORING SAFETY / SECURITY RISKS .....	73
	CONCLUSIONS .....	76
	REFERENCES .....	76
6.	FIRE RISK MANAGEMENT IN THE SLOVAK REPUBLIC .....	77
6.1.	BACKGROUND OF FIRE PROTECTION IN THE SLOVAK REPUBLIC .....	77
6.2.	RISK ASSESSMENT .....	78
6.2.1	RISK ASSESSMENT IN ACCORDANCE WITH DECREE NO. 611/2006 OF THE MINISTRY OF HEALTH OF THE SLOVAK REPUBLIC .....	79
6.2.2.	RISK ASSESSMENT IN ACCORDANCE WITH DECREE NO. 94/2004 .....	82
	CONCLUSIONS .....	83
	REFERENCES .....	83
7.	OCCUPATIONAL HEALTH AND SAFETY RISK MANAGEMENT IN THE SLOVAK REPUBLIC .....	84
7.1.	INTRODUCTION TO THE OCCUPATIONAL HEALTH AND SAFETY IN THE SLOVAK REPUBLIC .....	84
7.2.	RISK ASSESSMENT .....	88
	CONCLUSIONS .....	90
	REFERENCES .....	91
8.	RISK MANAGEMENT OF MAJOR INDUSTRIAL ACCIDENTS IN THE SLOVAK REPUBLIC .....	92
8.1.	BACKGROUND TO THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS IN THE SLOVAK REPUBLIC .....	92
8.2.	MAJOR INDUSTRIAL ACCIDENT RISK ASSESSMENT .....	94
8.3.	MEASURES TO PREVENT AND MINIMISE THE CONSEQUENCES OF MAJOR INDUSTRIAL ACCIDENTS .....	98
	CONCLUSIONS .....	99
	REFERENCES .....	99
9.	RISK MANAGEMENT IN THE FIELD OF CIVIL PROTECTION IN THE SLOVAK REPUBLIC .....	100
9.1.	BACKGROUND OF CIVIL PROTECTION OF THE POPULATION IN THE CONDITIONS OF THE SLOVAK REPUBLIC .....	100

9.2. RISK ANALYSIS OF EMERGENCIES.....	102
9.3 REDUCING AND MONITORING SECURITY RISKS.....	104
CONCLUSION.....	105
REFERENCES.....	105
10. APPLICATION OF MAPPING, GIS AND COMPUTER-AIDED MODELLING IN THE RISK MANAGEMENT.....	106
10.1 SUSCEPTIBILITY ASSESSMENT.....	106
10.2. VULNERABILITY ANALYSIS OF THE TERRITORY .....	109
10.3. WARNING SYSTEMS .....	112
CONCLUSION.....	118
REFERENCES.....	118
ABBREVIATIONS .....	120
GLOSSARY .....	121
REGISTER.....	123



# 1. RISK

Risk is a concept associated with any human activity. It can be perceived not only in a negative sense, where it represents a loss, but also in a positive sense, where it is perceived as an opportunity or a chance.



*The aim of the chapter is to be familiar with the concept of risk, to understand its nature and to know the ways of its expression.*

## 1.1. INTRODUCTION

It is possible to find different definitions of risk in the literature, as it is associated with different human activities. Only a negligible number of human activities take place under conditions of certainty, which are deterministic in nature. Certainty can only be expected in some physical and chemical processes, having the same internal as well as external conditions during the processes and actions taking place. Certainty is the observance of the planned parameters of the ongoing activities without any deviations and the unambiguity of all facts. In human activity, the dominant processes are characterised by uncertainty (indeterminacy), which is conditioned by the stochastic nature of the processes. Thus, most human activities and performed activities take place under conditions of uncertainty. The uncertainty is involved in the variation of the results of sub-activities, which then cause uncertainty in relation to the final goal to be achieved.

A common feature of all definitions is that risk contains an element of uncertainty that undesirable actions and adverse situations will occur.

**Risk** arises in situations where the outcome is uncertain, but the probability of different outcomes is known or, in the extreme case, can be estimated.

**Uncertain** is when an unknown outcome cannot be foreseen even as a certain probability, in other words, it refers to unforeseeable circumstances that cannot be protected against based on known insurance principles.

The notion of risk has been defined differently in the literature, sometimes without more precise definitions, and such divergent views have emerged:

- ✓ **Risk is the degree of uncertainty.** Risk is a certain value that describes uncertainty by leaving it out of the uncertainty frame and setting the probability of occurrence in some interval.
- ✓ **Risk is the relative deviation between actual and expected loss.** The main importance of risk analysis is mainly in comparison. It is useful to compare the risk

ratings of the phenomena being compared and to draw conclusions from them to cover the risks.

- ✓ **Risk is the degree of uncertainty given by the degree of variability of the observed phenomenon.** It can be expressed in terms of the standard deviation or, more accurately, in terms of the variation coefficient.
- ✓ **By risk we mean the possibility or danger of a future breach of system safety / security.**
- ✓ **Risk represent uncertainties that can be measured by statistical methods.** Uncertainties are random phenomena that cannot be measured exactly, only assumptions can be made about them.
- ✓ **Risk is considered to result from adverse events for which there is a statistical probability.** Risk becomes part of uncertainty (Figure 1.1).



*Figure 1.1 Relationship between risk and uncertainty*

*(Source: Author)*

From the above notions of understanding risk and uncertainty, we can draw the following conclusion:

Uncertain is the uncertainty, randomness of conditions or the outcome of certain phenomena or processes; uncertainty is understood as the impossibility of reliably determining future factors that affect the safety of systems. Risk is a type of uncertainty, where it is possible to quantify the probability of different states occurring; risk is the danger that the safety / security of systems will deviate from assumptions or expectations (i.e., it is a measurable deviation).

For the purposes of safety / security practice, the concept of risk can also be interpreted as the ***probability of occurrence of technogenic, or natural phenomena accompanied***

***by the emergency, formation and action of hazards, whereby social, economic, ecological and other damage or harm to human health (i.e., consequences) occurs.***

Risk can also be understood as the *expected abundance (number), or probability of occurrence of a hazard of a certain category, or the magnitude (degree) of potential damage (harm, loss) when an adverse event occurs, or a combination of these variables.*

Risk however, is most often defined as the *probability of an event/phenomenon occurring, which is most often calculated based on the frequency of occurrence (relative frequencies) of any type of emergency / negative phenomenon in the past.*

Even questions such as 'when' or 'how often' indicate that risk is being discussed. It can be recorded and observed by looking at the relationship between the damage caused by a negative (adverse) event (emergency) and the frequency of its occurrence, or by defining a return period for a particular scenario related to a specific emergency.

It is often stated in the literature that the assessment of risk depends on a set of factors that are part of what is called the causal nexus of the occurrence of an emergency.

The definition of risk according to STN ISO 31 000 - "*Risk Management*" describes risk as "*the impact of uncertainty on stated objectives*".

Each definition of the term risk has several specificities. It expresses views, capabilities and attitudes of the expert towards the problem. The translation from the expert's language may not be accurate because each language has its own specificities in the content of the terms, one term may be defined in different terms, and there is no single correct definition applicable to all areas of human activity. Most definitions are based on the likelihood of a crisis phenomenon occurring, some definitions emphasize the potential damage and loss, with an emphasis on the loss of human life. Definitions of business risks emphasise the differences between planned and achieved status as well as the possibility of loss of invested resources. Some definitions are based on the existence of uncertainty, which is a random phenomenon.

A correct definition of risk should consider the characteristics of risk as an event (conditions of occurrence, time course, intensity of action, resilience of the subject, etc.), specific characteristics of risk (specific features in terms of the risk action and the environmental response to the risk).

Most definitions of risk are based **on two basic facts**: the occurrence of a negative consequence and the probability with which these consequences may occur (i.e. the uncertainty that the intended outcome of ongoing events will be achieved).

## **1.2. RISK PERCEPTION IN SAFETY / SECURITY PRACTICE**

All events, processes, and concrete activities, which are purposeful human activities, do not, in most cases, take place in the way a person plans them. Only a negligible number of

human activities that are deterministic in nature take place under conditions of certainty. A certainty can be expected only in some physical and chemical processes, given the same internal as well as external conditions during the ongoing events and processes. Certainty is the observance of the planned parameters of the ongoing activities without any deviations and the unambiguity of all facts. In human activity, the dominant processes are characterised by uncertainty (indeterminacy), which is conditioned by the stochastic nature of the processes. Thus, many human activities and performed activities take place under conditions of uncertainty. Uncertainty is involved in the variation of the results of sub-activities, which then cause uncertainty in relation to the final goal to be achieved.

To introduce the discussion, it should be noted that in the available literature, and especially in common parlance, we often encounter the use of these terms in the field of crisis management, as well as in describing the level of security in various systems. When analysing the relationship between risk and threat, we must distinguish the environment in which these terms are used.

This relationship is perceived differently in the field of social systems and differently in the field of technical or technological systems.

In technical or technological systems, these categories have the following meanings:

- ✓ **Threat** is the activated property of an object to cause a negative phenomenon; it is the possibility to activate a hazard in a specific time and space, or the source of possible injury or damage to health. It can also be a designation of all factors that can cause a negative phenomenon.
- ✓ **Risk** is a quantitative and qualitative expression of the threat to a system, the degree or degree of its vulnerability. It can be seen as the probability of a negative phenomenon occurring and its consequence, or also a combination of the probability and magnitude of possible injury or harm to health in a hazardous situation.

In societal systems, the approach for defining the categories of risk and threat are somewhat different. In societal processes, risks are seen as primary. Risks are seen as part of the security environment, as potential hazards that may occur at certain times and under certain conditions. They are defined as follows:

- **Risk** is a category used to express that there is a potential possibility of a breach in the security of the system. This is also the perception of states of the security situation (internal and external), the manifestations of which, if left unaddressed, may develop into an imminent threat to the security subject (individual, social group, state, humanity). By their content and nature, they represent a potential threat security. Thus, it is "...a probable, more or less real threat that the integrity of a certain subject (individual, social unit) will be threatened by a criminal act or by the imminent consequences of other people's actions".
- **Threat** is an activated risk that acts against the interests of the security subject.

As such, it may represent, for example, specific negative attitudes and activities of a state (group of states) or relevant domestic or foreign entities or situations, which pose an imminent threat to the interests of the security subject.

According to other approaches, the threat perceived as an activated risk, as an actual hazard that is already immediately at work. The category 'threat' is also sometimes understood as synonymous with the category 'risk', but sometimes it is understood as a higher stage of risk. This implies that the existence of a risk should precede the emergence of a hazard.

Threats and risks have accompanied man throughout the evolution of human civilization. **Threats** exists objectively and independently of the actions and behaviour of both the referent and the threatener. It is defined as either a deliberate threat (based on the intention of a threat actor, e.g., state, group, individual) or an unintentional threat, where the threat actor may be natural phenomena - floods, droughts, earthquakes, etc. It is essential that the threat exists independently of the will of the threatened object, confronting it with the necessity of decision-making and a certain response, action, triggered by the threat, i.e., action with the knowledge of a certain risk.

**Hazard creates the source of the threat and risk expresses the degree (potential) of the threat.** In this context, it is interesting to understand risk in terms of the different phases of its existence. **In the latent stage, risk is understood as a threat to endangerment, in the acute stage as a crisis.** In this understanding, the relationship between risk and crisis is not precisely defined (more precisely, the fact that crises also have a latent stage is ignored).

The concept of threat or threat expresses the way the danger manifests itself. It expresses the dynamics of change in a specific time and space, a condition. It expresses the action when the hazard is activated (active property of the source of action).

The relationships between risk, hazard and threat in social practice are expressed in the Occupational Health and Safety Act (OHSA). It defines these terms as follows:

- **Dangers** is a condition or characteristic of a factor of the work process and the work environment that can harm the health of an employee.
- **Threats** is a situation in which it cannot be ruled out that the employee's health will be harmed.
- **Risk** is the likelihood of an employee's health being harmed at work and the degree of possible health consequences.

In risk management practice, but also in some theoretical approaches, we encounter a certain voluntarism (sometimes caused by inconsistencies in translation, especially from the Anglo-Saxon environment) in the use of such basic categories as: threat, threat and risk. Threats are sometimes understood as a summative category for threats and risks, with their interrelationship being expressed in such a way that, while risk is considered a potential hazard, threat is considered an actual hazard that is imminent. In the present period, there is

a tendency towards greater precision in the different conceptualisations of these categories.

The concept of threat expresses the disruption of standard functions, links, relationships in the relevant space and time. Threats arise from the disruption of defined laws by initiating the characteristics of the hazard in question. In some approaches, the term initiation is used to highlight the mode (source) of initiation in causal dependence. The term hazard itself can be defined to also describe initiation.

The degree, or potential, of threat is expressed by the concept of **risk**. In practice, the degree of threat (magnitude, extent, etc.) can in some cases be determined in an exact manner<sup>1</sup>, but in most cases it is only possible to determine to a limited extent how secure a system is. For this reason, when assessing the degree of threat, parameters such as measuring the consequences of a threat based on how often it occurs and what the threat may have consequences. The combination of these two parameters is defined as the **risk, i.e., the probability of a negative phenomenon occurring and its consequence**.

Unexpected negative phenomena are characterized by the following basic characteristics:

- occur sometimes with minimal probability of occurrence - thus causing significant damage due to the unpreparedness of the system at risk.
- occur with a certain (known) periodicity but can have unpredictably devastating consequences (their intensity can be several orders of magnitude higher than we expect).

To eliminate the consequences of these features, it is necessary to carry out a thorough analysis of the system, to find the weaknesses of previous practices and to adopt qualitatively better measures. This means retrospectively analysing all previous actions and activities and an analysis of the natural sources of the threat. At the same time, it is essential to anticipate the possible negative consequences of new sources of threat of a civilisational nature (new technologies, technical systems, information systems - especially those dealing with the considerable potential of matter, energy, and information), together with the elimination of violent manifestations of human behaviour (terrorism, wars).

The experience of countries where safety / security risk theory is developed to a relatively higher-level shows that one of the options for indicating, identifying, and analysing a threat or risk is the preparation of risk **scenarios**. The aim of using these scenarios is to analyse the possible consequences of an escalation of risk and to propose adequate measures, using the necessary crisis management forces and resources, to eliminate or reduce the anticipated negative consequences.

### 1.3. RISK PROGRESSION

Each risk can only exist in real time under specific conditions (internal and external). The

---

<sup>1</sup> Note (e.g., ionising radiation intensity, concentration of hazardous substances).

specific conditions in which a risk has been identified may cause also give rise to several other risks.

Individual risks may be operative circumstances:

- independently,
- negating each other,
- interacting with each other.

An important step in risk management is to take a systems view of causality and understand the different interfaces of causality. Figure 1.2 provides a depiction of the causal nexus and loss quantification without distinguishing between types of crises. Causal nexus is a sequence of states over time. By knowing the regularities of the different phases of a crisis (I to IV), it is possible to apply the different methods to minimize losses.

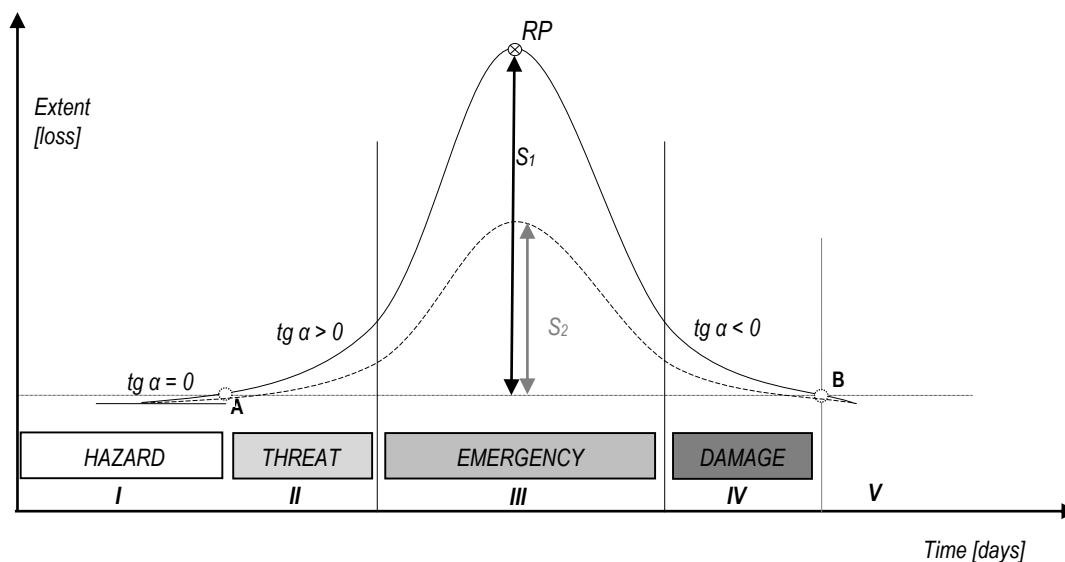


Figure 1.2 General description of causal dependence and crisis phases (Oravec et al., 2021)

The basic problem is to define the boundary conditions that lead to the significant deviation represented by point A, Figure 1.2. At point A, a change in parameters ( $\text{tg } \alpha > 0$ ) occurs, which creates instability and the emergence of a crisis. At the point of reversal (RP), the opposite process occurs, based on the measures, up to point B, where a steady state with new parameters occurs. The fifth phase of the crisis is the beginning of a new situation in the system under study. The criteria at points A, B can be quantified. The difference of losses between S1 and S2 values is achieved by appropriate barriers (organizational, technical, social measures according to the system).

The term crisis is associated with a turnaround and a situation of disruption in the functionality of a system, where it is defined as a moment or period that may be followed by a fundamental change in the development of a given event or system. At the same time, the term is used as a general term for all emergency / crisis phenomena.

## 1.4. DOMINO EFFECT

There is a causal link between the individual risks that causes the risks in the cascade to be activated. The individual risks are mutually dependent, with the existence of one triggering the next, which in turn triggers the next (Figure 1.3).



*Figure 1.3 Domino effect - Cascading failure of parts of the system  
(Source: Enviroportal, 2021)*

Domino effect (The domino effect can be defined as "*an ongoing event with increasing consequences*". It is seen as analogous to the successive falling of dominoes, which then fall.

There is a domino effect in the Slovak Act on the Prevention of Major Industrial Accidents defined as "*the possibility of increasing the probability of a major industrial accident occurring or of its consequences being aggravated as a result of the proximity of installations, undertakings or groups of undertakings to each other and to the location of hazardous substances*".

An example of a domino effect is the major industrial accident in Flixborough (UK). The accident occurred in 1974 at a nylon fibre factory because of an inappropriately construction and material design of the reactor bypass piping shut down due to leakage. This bypass pipe burst, releasing approximately 30 tonnes of cyclohexane. A strong explosion equivalent to the explosion of the same quantity of trinitrotoluene (TNT) and a large fire followed. The consequences: 28 fatalities, 36 injured, operations destroyed, 1,821 houses and 167 other properties damaged, material damage was estimated at \$140 million.

## 1.5. SYNERGISTIC EFFECT

Synergistic effect can be broadly defined as the *interaction of elements of a system or systems to produce a new quality*.

Synergistic effect The risk correlation shown in Figure 1.4 confirms the fact, that there are risks that can initiate several other risks that co-exist with the source risk and



without its existence the whole group of related risks cannot exist.

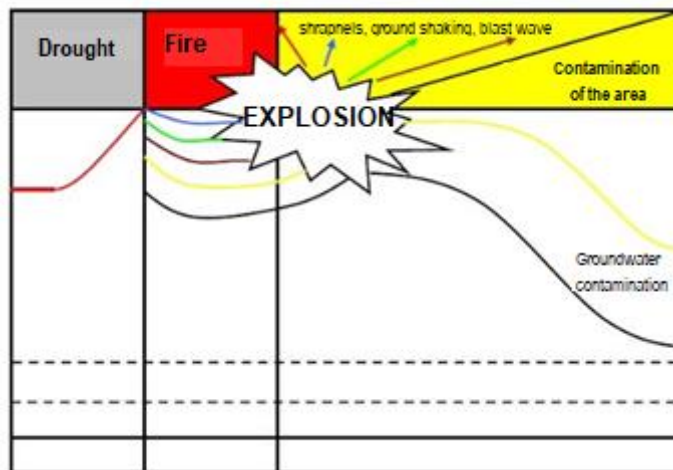


Figure 1.4 Synergistic effect of risk phenomena

(Source: Šimák, 2006)

The following causality is evident from the example. Drought can trigger a fire that causes an explosion with subsequent pressure wave generation, shrapnel dispersion, ground shaking, infestation of the area, soil and possibly groundwater.

## 1.6. RISK FUNCTION

Risk expresses the possibility of the subject/object being exposed to the consequences of various types of emergencies. It represents the expected damage and loss (loss of life, health, damage, damage to property, interruption of economic activities, etc.) caused by a change in external and internal conditions in a specific area and at a specific time. Its knowledge is the basis for establishing preventive measures aimed at avoiding emergencies that threaten human life and health, property, the environment, cultural and other values, as well as planning measures aimed at minimising the impact of these events.

## 1.7. RISK EXPRESSION

The following mathematical expression can then be used to determine the risk, which expresses risk by setting a risk measure which is the product of the possible probabilities of an emergency occurrence and the possible magnitude of the consequences:

$$R = \text{probability of occurrence} \times \text{loss} \quad (1)$$

On the other hand, risk (R) can also be expressed as a function of its individual components: threat (H), vulnerability (Z), exposure (E) and resilience/resilience (P) of the system:

$$R \in f(H_i, Z_i, E_i, P_i), \text{ for } i = 1, \dots, n \quad (2)$$

The following are brief descriptions of the individual components of risk that can be used for a comprehensive assessment.

- **Susceptibility** - It represents the 'weaknesses' of systems (predisposition of systems to damage) that can directly trigger or encourage the occurrence of a negative event/phenomenon under certain circumstances (conditions). In the process of susceptibility assessment, it is therefore necessary, as a first step, to determine the individual threats and to identify the areas with their potential occurrence. For example, in the case of flooding, the most susceptible areas in terms of flood occurrence include cultivated agricultural land, grassland, while the least susceptible are forest areas, due to their highest water retention capacity, i.e., the ability of the soil to retain water.
- **Vulnerability** - It is a dynamic, hidden characteristic of any community (a region, a forest stand, a threatened infrastructure, or other vulnerable elements), which is made up of several components. Vulnerability indicates the potential for harm and is a forward-looking variable. Vulnerability can be characterized as the potential impacts of exposure to a negative phenomenon. These can be modelled using mathematical or computer-aided modelling methods. For example, in the case of flooding, this is the area that will potentially be inundated under a particular flood scenario. Determining vulnerability means answering the question: "*What would happen if certain event(s) were to affect the elements at risk?*"
- **Exposure** - It can be understood as the number of people or other elements (objects) at risk that may be affected by a negative event. In uninhabited forested parts of the area, the exposure of people is zero, but the exposure of forest stands is high. For example, during floods, within an area temporarily inundated by water, it is possible to identify persons or population groups that will be at risk, structures and other objects or selected environmental features that will be inundated or damaged by the flood.
- **Resilience** - The ability of a system or its individual components to return to their original state after being affected by a negative phenomenon. This concept expresses a certain elasticity of risk. It is distinct from the concept of resistance, which describes the ability of a system to withstand the action of a negative phenomenon to such an extent that its functions may not be impaired or damaged at all. For a system to return to its functions after damage, it is necessary to ensure that it is not destroyed. This is possible through planning and subsequent implementation of measures aimed at minimising impacts or restoration and reconstruction. The planning and implementation of preventive measures are more linked to the prevention of damage and are therefore linked to the resistance (resilience) of these systems. The nature of the prevention but also mitigation and restoration measures can be personnel, material, technical, technological, legislative, financial, etc.

## CONCLUSION

From a risk perspective, it is important to know the suitable mathematical model for calculating the magnitude (level) of risk. Starting from this model, risk is inherently the probability with which the assumed scenario of the event under consideration will occur, irrespective of whether it is a positive or negative event. This model does not give us information not only about the probability or frequency of an event occurring, but also about its impacts, since we are already considering a specific scenario of the event in the calculation, to which specific impacts are attached.

In addition to determining the magnitude of the risk using a mathematical model, it is also possible to use an approach to determine the magnitude of its components, which are most often susceptibility and vulnerability, where vulnerability in combination with resilience gives an up-to-date view of the state of safety / security assurance of the system. This approach is mainly used in the field of crisis / emergency management, especially abroad.

## REFERENCES

- [1]. BURIANEK, J. 2001. *Bezpečnostní rizika a jejich percepce českou veřejností / Security risks and their perception by the Czech public. Sociologický časopis*, 1/2001, p. 48
- [2]. BUZALKA, J. 2001. *Vybrané otázky teorie krízového manažmentu a civilná ochrana / Selected issues of crisis management theory and civil protection*. Bratislava: APZ in Bratislava, p. 36.
- [3]. CANNON, T. et al. 2003. *Social Vulnerability, Sustainable Livelihoods and Disasters*. Report to DFID. Conflict and Humanitarian Assistance Department (CHAD) and Sustainable Livelihoods Office London.
- [4]. CROUHY, M., GALAI, D., MARK, R. 2014. *The Essentials of Risk Management*. McGraw/Hill Education, 672 p.
- [5]. DRÁBEK, J., PITTNEROVÁ, I. 2001. *Investičné projekty a náklady kapitálu / Investment projects and the cost of capital*. Zvolen: Matcentrum, 250 p.
- [6]. DRÁBEK, J., POLÁCH, J. 2008. *Reálne a finančné investovanie firiem / Real and financial investment of firms*. Zvolen: Technical University in Zvolen, 272 p.
- [7]. ENVIROPORTAL. 2021. *Domino efekt / Domino effect*. [Cited 25.09.2021]. Available online: <https://enviroportal.org/portfolio-items/domino-efekt/>
- [8]. HOFREITER, L. 2002. *Bezpečnostný manažment / Security Management*. Žilina: University of Zilina, p. 20.
- [9]. HOFREITER, L. 2004. *Bezpečnosť, bezpečnostné riziká a ohrozenia / Security, security risks and threats*. Žilina: University of Zilina, p. 67.
- [10]. MAJLINGOVÁ, A. 2010. *Základné pojmy z oblasti manažmentu rizík prírodných pohrôm a katastrof / Basic terminology in the field of risk management of natural disasters*. In *Delta: scientific and professional journal of the Department of Fire Protection*, No. 7/2010, pp. 18-22.
- [11]. MAJLINGOVÁ, A. 2016. *Teória rizík / Risk theory*. Zvolen: Technical University of Zvolen. 46 s.
- [12]. MAJLINGOVÁ, A., GALLA, Š., BUZALKA, J. 2016. *Využitie údajov a nástrojov GIS, SDSS a dynamického modelovania v manažmente rizík vybraných druhov mimoriadnych udalostí / Use of GIS, SDSS and dynamic modelling data and tools in risk management of selected types of emergencies*. Rev. Ján Tuček, Milan Oravec, Štefan Kočan. 1st ed. Bratislava: APZ in Bratislava, 2016. 132 p.

- [13]. ORAVEC, M. 2011. *Manažérstvo priemyselných havárií / Industrial accidents management*. Košice: ICV TU in Košice.
- [14]. ORAVEC, M., KOTIANOVÁ, Z., MAJLINGOVÁ, A., ADAMEC, V. 2021. *Úvod do krízového manažérstva / Introduction to crisis management*. Košice: Technical University of Košice.
- [15]. POLÁCH, J., POLÁCH, J., DRÁBEK, J., MERKOVÁ, M. 2012. *Reálné a finanční investice / Real and financial investments*. Prague: C. H. Beck, 2012. 263 p.
- [16]. STN EN 292-1: Safety of machinery. Basic terms, general design principles. Part 1: Basic terminology, methodology / Bezpečnosť strojových zariadení. Základné termíny, všeobecné zásady navrhovania.1. časť: Základné názvoslovie, metodika.
- [17]. ŠIMÁK, L. 2006. *Manažment rizík / Risk management*. Žilina: University of Zilina.
- [18]. SINAY, J. 1998. Nebezpečenstvá, ohrozenia a riziko, ako ich nepoznáme / Hazards, threats, and risk as we don't know them. Proceedings of the 3rd scientific conference. Žilina 1998, p.15.
- [19]. ŠKVRNDA, F. 2001. K vojensko-sociologickej charakteristike bezpečnostných hrozieb / Towards a military-sociological characterization of security threats. In. Vojenske obzory, No.2/2001, p. 3.
- [20]. Act of the National Council of the Slovak Republic No. 124/2006 Coll. on Occupational Safety and Health at Work, as amended.
- [21]. Act of the National Council of the Slovak Republic No. 128/2015 Coll. on the prevention of major industrial accidents, as amended.
- [22]. ZEMAN, P. 2002. *Česká bezpečnostní terminologie, Výklad základních pojmů, / Czech Security Terminology, Interpretation of Basic Terms*. ÚSS/2002-S-1-031, Brno.



## QUESTIONS

1. Define the difference in the terms risk, threat, and hazard.
2. List and briefly characterise the different components of risk.
3. What is the function of risk?
4. Define the difference between a domino effect and a synergistic effect?
5. What is the relationship between the risk components vulnerability and resilience?

## 2. RISK TYPES AND CLASSIFICATION SCHEMES

Risks occur in all areas of social life, in the natural environment as well as in technical and technological processes. Depending on the type of environment, the subject of action and other factors, their type and the classification scheme used may also vary.



*The aim of the chapter is to become familiar with the types of risks and to know and understand the classification of risks.*

### 2.1. TYPES OF RISKS

Risk is understood rather inconsistently in the literature. This then leads to different approaches to its classification. Authors approach its division based on different aspects (criteria), which gives rise to different categorisations of types of risk.

In terms of **substance**, risks at the entity/company level can be divided into:

- **Technical and technological risks** - arise directly from the condition and structure of fixed assets, their wear and tear, reliability. These risks are determined by the level of application of the knowledge of scientific and technical development and can be simplistically understood in such a way that the newest and most modern machines and technologies have these risks "zero".
- **Production risks** - these risks are often in the nature of a shortage (scarcity) of resources of various nature (raw materials, materials, semi-finished products, energy, etc.). They are determined by the type of production, organisation, and layout of the production process.
- **Economic (cost) risks** - represent risks associated with changes in cost items. For example, changes in the prices of individual inputs; these risks also include inflation, risks associated with monetary and budgetary policies, etc.
- **Socio-political risks** - are associated with changes in the macroeconomic, economic, and social policy of the state on the one hand, and changes in the international economic and political environment on the other.

According to the possibility of influenceability, the risk can be divided into:

- **Risk Influenceable** - can be reduced or eliminated in some way.
- **Risk Uncontrollable** - (cannot be influenced). These are risks emanating from a force majeure (lat. "*vis maior*"). They must be accepted (e.g., political situation in the country, tax system).

It is possible to reduce impactable risks by acting on their causes. For uncontrollable risks, the focus should be on reducing their adverse consequences.

According to the **frequency of occurrence**, the risks are divided into:

- **systematic risk** - related to business activity.
- **unsystematic risk** - refers to the use of specific special activities that occur exceptionally - energy crises, economic crises, natural disasters.

The boundary between these types of risks is determined through risk analysis.

From the point of view of **acceptability** (acceptability) **for humans**, we recognize two basic types of risks, which are:

- **Acceptable risk**: risk we are willing to accept.
- **Residual risk**: risk that remains after the measures have been implemented.

A special position in risk assessment is that of '**zero risk**', which is only a theoretical starting point for examining risk. Risk can only be eliminated together with the elimination of the system or process within which it was identified. In practice, we are more likely to encounter a **minimum level of risk** that we are trying to get to in the process of risk reduction. This risk sometimes has the character of a residual risk, which cannot be reduced any further without changes in the internal and external conditions, e.g., a fixed production price, or a fixed quality of raw materials, or a fixed level of plant safety.

According to the **area of the consequences**, we divide the risks into:

- **local**,
- **regional**,
- **sub-national** - in several regions of the country,
- **national** - state,
- **transnational** - transcending regions of neighbouring countries,
- **supranational** - extending beyond the territory of a single state (multi-state grouping),
- **continental**,
- **global**.

Most of the security risks that can endanger the life and property of a citizen are global security risks. Crime and organised crime are internationalising and crossing national borders.

According to the **extent of the consequences**, we divide risks, especially risks related to the security of systems, into:

- **Natural disasters** - the risk of an emergency caused by destructive natural forces, because of which accumulated energies and masses are released, or by the action of hazardous substances or other destructive factors having a negative impact on humans, animals, material values and the environment (Act No. 42/1994 Coll. on Civil Protection of the Population).

- **Catastrophes** - this is the risk of a large-scale emergency occurring because of the accumulation of the destructive factors of a natural disaster or accident, which

have serious direct consequences on the population, animals, material values and the environment.

- **Super catastrophes** - the risk of an extremely large disaster affecting hundreds of thousands of square kilometres of the Earth's surface (tsunamis, hurricanes, floods ...)

- **Global disasters** - this is the risk of a disaster whose effects extend over at least two continents (global warming causing changes in ocean currents, earthquakes, volcanic activity, river and sea flooding, tropical cyclones, tsunamis, El Niño causing a change in currents and winds, the fall of an extra-terrestrial body).

**According to the bearers**, security risks can be divided into those borne by **individual states, groups of states, organised groups** or **individuals**.

**Depending on the source** (cause, nature) of **the risks**, we distinguish between military, political, economic, social, ethnic, racial, religious, technological, and environmental security risks.

**According to the nature of the action**, the risks are mainly **hidden, latent** and **manifest**. According to this criterion, risks can also be classified as **direct** (immediate) and **indirect** (mediated).

**According to the time of exposure** to security risks, we distinguish between **short, medium, and long-term** risks.

**According to the development tendencies of** security risks, we know **old risks** (traditional, long-acting) and **new risks** (short-acting).

**According to the mechanism of occurrence and action of risks**, risks can be classified as **unilateral**, where one entity clearly threatens one or more other entities in the security environment, **bilateral**, when two entities threaten each other or **multilateral**, where more than two entities threaten each other.

## **2.2. RISK CLASSIFICATION**

### **2.2.1. GENERAL RISK CLASSIFICATION**

From a general perspective and depending on the origin, risks / hazards can be divided into two basic groups (Figure 2.1):

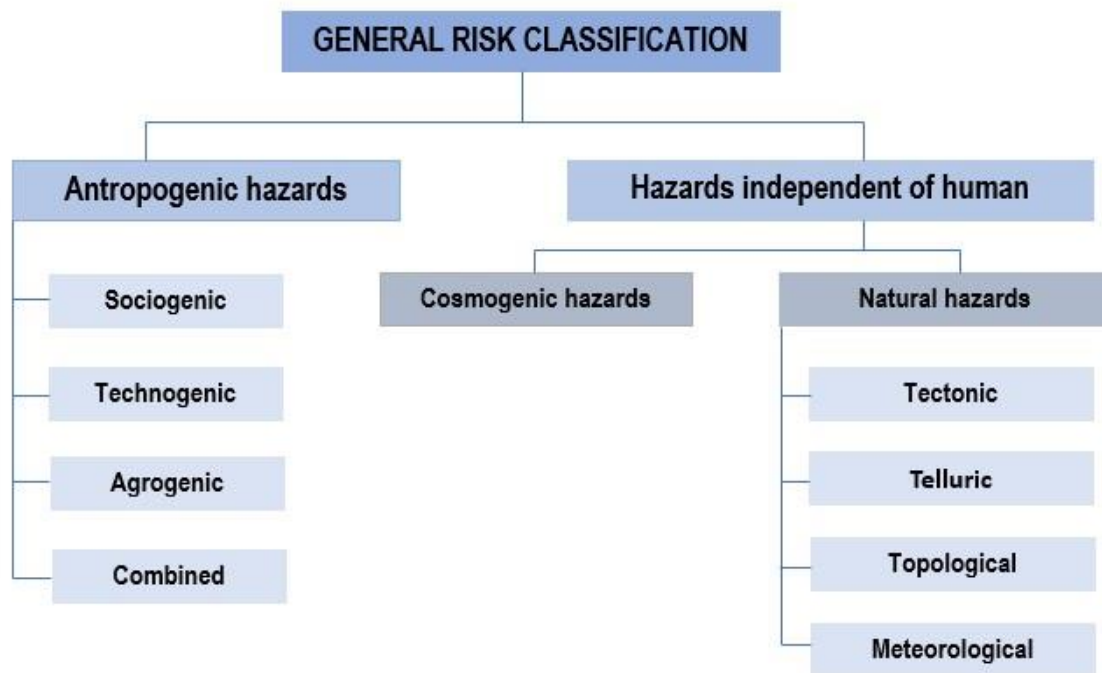


Figure 2.1 General risk classification  
(Source: Šimák, 2006)

**Anthropogenic hazards** are risks caused by intentional or unintentional human activities. Depending on the environment in which human activity takes place, they are divided into: **sociogenic** (the quality of individual work, the ability of people to communicate with each other, the effectiveness of the management of work teams, the working conditions created for employees, the level of quality of services provided to customers), **technogenic** (risks threatening technological processes in production and services, technical and technological equipment and means, the infrastructure and energy system of the state, management, information and communication processes), **agrogenic** (the use of genetically modified crops, the chemicals used in agriculture) and **combined**.

In this category of anthropogenic risks, we also include natural risks caused by deliberate, but also unintentional human activity, social and economic risks, but also risks with combined consequences.

The group of **natural hazards generated by human activity** includes risks of harmful emissions to air, water pollution, solid waste production, soil contamination, products of toxic and hazardous substances, use of energy resources, explosions, fires.

The social environment is one of the most important risk environments (**societal hazards**). It is created by individuals, social groups starting from the family through political parties, religious, ethnic, and cultural groups. We divide social risks into political, social, cultural, ethnic, religious, sports, etc. A person takes a risk to achieve a desired outcome, to avoid another



undesirable outcome, or to preserve a prize, a value. We call these social risks personal or individual risks.

**Economic hazards** are that the potential losses from the expected results of and the likelihood with which such losses may occur are unknown. The magnitude of the risk is determined by the difference between the expected and the achievable economic outcome. The measure of risk is the proportion of the loss or unattainable return to the projected return. There are two levels of risk:

- **strategic risks / hazards originating in** the application of national and supranational standards and measures to regulate the business space. These include national economic policy risks, financial risks from foreign investment, market risks, inflation risks.
- **operational risks / hazards** that originate in the internal design and functioning of the organisation and their links to the external environment. We call them internal or intrinsic risks. They also include social risks because man is a member of a social group.

**Hazards independent of human action** are independent of human will, and thus man has no way of preventing their occurrence. According to the space of their origin, they are divided into *natural* and *cosmic*.

Even though man today can exploit nature and energy, he can positively and negatively influence its quality, can predict the weather, he has not yet been able to control the natural elements that cause human suffering and widespread damage. Risk of occurrence exists independent of the will of man.

These include natural and cosmic hazards, which, once developed, can cause a variety of natural disasters, catastrophes, super catastrophes, and even global catastrophes. Natural hazards include *tectonic* (related to the movement of the Earth's crust), *telluric* (geological, related to the Earth), *topological* (spatial), *meteorological* (weather-related). *Cosmogenic hazards* are those related to space activity.

The fact that **natural hazards** are among the most frequent and cause enormous loss of life and property is evident from data from international agencies, which, for example, report that in 2004 alone, natural disasters claimed the lives of nearly a quarter of a million people and affected 146 million people. The biggest killer of people was the tsunami that hit thirteen states in the Indian Ocean on 26 December 2004. This super-disaster claimed the lives of 232,000 inhabitants. Volcanic eruptions and landslides following typhoons and earthquakes have also had tragic consequences.

**Cosmogenic hazards** are related to a deeper investigation of the risks of large-scale meteorite impacts and other cosmic bodies that could cause huge tsunamis with global effects on several continents when they fall into the oceans. Various effects of cosmic rays on our planet are being investigated, as well as cosmic explosions triggered by the extinction of stars as well as the effects of a cosmic black hole.

## 2.2.2. CLASSIFICATION OF RISKS ACCORDING TO THE OBJECT OF ACTION

Risks currently affect society, human activities, material values, the environment, as well as people's life and health. There are three groups of risks according to the object of action (Figure 2.2). These are directly related to the group of so-called **safety / security risks**.



Figure 2.2 Classification of risks according to the object of action  
(Source: Šimák, 2006)

**Safety / Security hazards** are states of the safety / security situation (internal and external), the manifestations of which, if not addressed, may develop into an imminent threat to the security subject (individual, social group, state, humanity). In their content and character, they represent a potential threat to security. From the social point of view, security risk can be understood as an effort of the subject of the secure environment (security relations) to harm the interests of another subject, as an activity of an actor of the secure environment that can have a negative impact on the interest of another subject.

Security risks are currently the main factor influencing the actions of states in security policy. A security risk can be understood as an effort by an actor in the security environment (security relations) to harm the interests of another actor, as an action by an actor in the security

environment that may have a negative impact on the interests of another actor. Classification of safety / security risks is one of the tools of risk analysis, which allows, with the applied criteria, to classify safety / security risks into groups according to common characteristics, causes or symptoms.

According to Škavrnda (2004), the criteria for classifying safety risks for the purposes of safety risk management can be:

- the territorial scope of the risks,
- risk bearers,
- the sources (causes or nature) of the risks,
- the nature of the risks involved,
- duration (action).

**Hazards of military conflict** are described below using the example of activities threatening the security of the Slovak Republic.

In general, military threats to the Slovak Republic are activities such as, which mainly involve the use of military forces and means against the State. By their size and scope, military threats represent a potential or direct threat to the security of the Slovak Republic by military forces and means and require the deployment of armed forces, the activation of the entire security system of the State, or possible military assistance from abroad to counter them. This group of risks and threats includes large-scale armed conflict and regional armed conflict.

**Large-scale armed conflict** – the likelihood of this type of conflict is currently low, and warning and preparation time can be expected to be sufficiently long. Nevertheless, the current environment may change, and conditions may develop for the emergence of a large-scale armed conflict, which would significantly threaten the security of the Slovak Republic.

**Regional armed conflict** – the Slovak Republic is in the vicinity of potential regional tensions, which increases the likelihood of being affected by a regional armed conflict.

**Risks of a non-military nature** – are associated with non-military threats to the territory of the Slovak Republic. They represent such activities threatening the security of the Slovak Republic, in which non-military means are predominantly deployed against the state. Non-military threats may not only be purposefully induced, controlled, and coordinated, but may also have a spontaneous, spontaneous trigger mechanism and course.

Non-military threats of a general nature include **crisis situations** of a type other than armed **conflict** and among the most serious are:

- terrorist activities,
- illicit arms trafficking, including nuclear, biological, and chemical weapons,
- internationally organised crime,

- uncontrolled migration or a mass influx of refugees,
- religious or ethnic extremism and divisions,
- Social unrest, criminalization of social relations.

## CONCLUSIONS

Recognising between types of risk (hazard) and understanding risk classification schemes is particularly useful in terms of identifying potential threats that may directly or indirectly affect the security of a particular system. Classification schemes are a kind of conceptualisation model for classifying and further exploring risk from several aspects and looking for potential threats to the system also from the point of view of synergies between different groups of risks.

## REFERENCES

- [1]. DRÁBEK, J., PITTNEROVÁ, I. 2001. *Investičné projekty a náklady kapitálu / Investment projects and the cost of capital*. Zvolen: Matcentrum, 250 p. .
- [2]. DRÁBEK, J., POLÁCH, J. 2008. *Reálne a finančné investovanie firiem / Real and financial investment of firms*. Zvolen: Technical University in Zvolen, 272 p.
- [3]. HOFREITER, L. 2004. *Bezpečnosť, bezpečnostné riziká a ohrozenia / Security, security risks and threats*. Žilina: University of Zilina, p. 67.
- [4]. POLÁCH, J., POLÁCH, J., DRÁBEK, J., MERKOVÁ, M. 2012. *Reálne a finanční investice / Real and financial investments*. Prague: C. H. Beck, 2012. 263 p.
- [5]. ŠIMÁK, L. 2006. *Manažment rizík / Risk management*. Žilina: University of Zilina. Available online: <[http://fsi.uniza.sk/kkm/files/publikacie/mn\\_rizik.pdf](http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf)>
- [6]. ŠKAVRNDA, F. 2004. In: Kolektív autorov. *Hodnotenie bezpečnostného prostredia / Evaluation of the security environment*. Bratislava: Inštitút obrany a bezpečnosti MO SR.



## QUESTIONS

1. List the main groups of risks in terms of the general classification of risks.
2. How do we classify risks according to the object of action?
3. Define the difference between military and non-military risks.
4. How do we classify risks in terms of consequence space?
5. What is the difference between residual and acceptable risk?

### 3. SAFETY AND SECURITY RISK MANAGEMENT

Every human activity carries some risks, and there is no such thing as "zero" risk. To ensure the safety of people, property, and the environment, it is essential to know the risks, their magnitude and to strive to reduce them to a socially acceptable level. The complex of activities and processes leading to this goal is called risk management. The importance of risk management has grown considerably, particularly in the last decade, and has been characterised by increasing importance, so that it has become part of routine management activity. Within the organisational structures of various entities, risk management segments and risk manager (crisis manager) positions have been created. The role of risk management has grown considerably, particularly in connection with the existence and integration of information technology into all levels and areas of management.



*The aim of the chapter is to become familiar with the types of risks and to know and understand the classification of risks in general as well as safety / security risks.*

#### 3.1. RISK MANAGEMENT

One of the important prerequisites for any human activity is to "manage" risk inherent in carrying out that activity. In this context, it is essential to anticipate future developments in which the risk may manifest itself and in which the threat may be realised by updating the hazard in the system.

"Coping" with risk can be understood:

- as its purposeful, deliberate, and systematic reduction to an acceptable level. In terms of knowledge of the developmental phases of risk. It is essentially the regulation of its development, i.e., its management (management, management).
- accepting the risk without reducing it (if acceptable).

**Risk Management** is a continuous activity, a recurring set of interrelated activities, the aim of which is to manage potential risks, i.e. to limit the likelihood of their occurrence or to reduce their impact.

**The purpose of risk management** is to prevent problems or negative phenomena, to avoid crisis management and to prevent problems from occurring.

**The foundations of risk management** is the guidance of processes, which result in the identification of risks, their purposeful reduction and minimisation of the probability of crisis situations.

The risk management process applied to a system with a human agent is intended to reduce the risk of to a socially acceptable limit through legislative, administrative, technical, and social

measures implemented at all stages of the risk development.

The basis of risk management is a thought process that is based on information about potential threats on the one hand, and the options and resources to minimise them on the other, with the aim of risk management being to use all available resources to prevent security risks escalating into crisis situations.

As regards the definition of the category "risk management", different approaches to its definition are used in the literature.

Risk management<sup>2</sup> is defined as "*the systematic application of management policies, procedures and practices to the communication tasks of determining the context, identifying, analysing, assessing, managing, monitoring and reviewing risk*".

Other authors identify risk management with risk management and define it as "*the complex process of detecting, controlling, eliminating, and minimizing uncertain events that may affect an entity*".

Risk management is also understood as "*an activity aimed at ensuring the safety or stability of the managed system, analysing risks and possible threats and seeking appropriate corrective and preventive measures to minimise the negative impacts of risk phenomena and their escalation into threats, into crises*".

Risk Management can also be expressed as a deliberate reduction or mitigation of all unacceptable risks whose probability of occurrence  $P$  in the selected time interval is higher than a specified value (most often  $P=0.05$ ).

In the technical or technological domain, it is about ensuring the inherent capability of systems to cope with design accidents.

The general normatively defined definition of risk management (STN 010 380) has the following form: '*a logical and systematic method of determining relationships identifying, analysing, evaluating, treating (managing), monitoring and communicating the risks associated with any activity, function or process in a way that enables the organisation to minimise losses and maximise opportunities*'. The above definition may be suggestive, but the definition of risk management **as a method** appears rather narrow.

A relatively comprehensive definition of risk management can be found in the current literature. Risk management is characterised by as an **interactive process** consisting of well-defined steps which, by their sequence, support better management decision-making by contributing to a better understanding of risks and their consequences.

It can also be said that risk management enables a realistic appreciation of the weaknesses

---

<sup>2</sup> Management - the term comes from Latin (*manus*). It characterizes the process of leading and directing all or part of an organization. Risk - the term comes from Latin (*risicum*). An activity in which an entity is at risk of some loss, the effect of uncertainty on goals. The probability of a negative phenomenon occurring and its consequence.

and strengths of management activities and creative processes, the improvement of management and work processes and the improvement of the functioning of the systems concerned. For these reasons, risk management should be an integral part of good management practice.

Since the mid-1970s, the concept of risk management has expanded from the purely business domain to the public and not-for-profit sectors. In addition to pure, insurable, and material risks, other risks were also included in risk management, which posed both external and internal threats to the entity. For example, natural risks, societal risks, technological, technical, environmental risks, and others.

**The aim of the risk management process is to design the optimal way to reduce risk to a socially acceptable level.** Risk reduction is implemented by a decision - the product of the risk management stage. The optimal method considers economic, social, technical, political, and other factors. The risk management process also includes the process of public participation (risk communication) and risk perception. In simplified terms, the **aim of risk management** is to reduce the **likelihood** of crisis events and minimise their **consequences** for the entity.

For **security risk management** similar rules to those extracted from the experience gained in dealing with risks in general apply. These rules are **as follows**:

- there is zero security risk,
- there is no absolute security,
- Security is the acceptance of a certain degree of risk,
- the threshold of risk acceptability is not fixed, it varies according to the level of technical and cultural sophistication and the capabilities of science and technology,
- residual risks must be communicated to those affected, the risk must be manageable by those who create it,
- Risk is defined as the combination of the probability of an adverse event occurring and the severity of its consequences.

### **3.2. RISK MANAGEMENT PROCESS**

Regarding the risk management process itself, different approaches are presented in the literature. Most often, the process consists of four interrelated phases, namely **risk identification, risk assessment, risk acceptance** and risk treatment, i.e., **risk monitoring and planning and taking measures to minimise risk** (Figure 3.1).

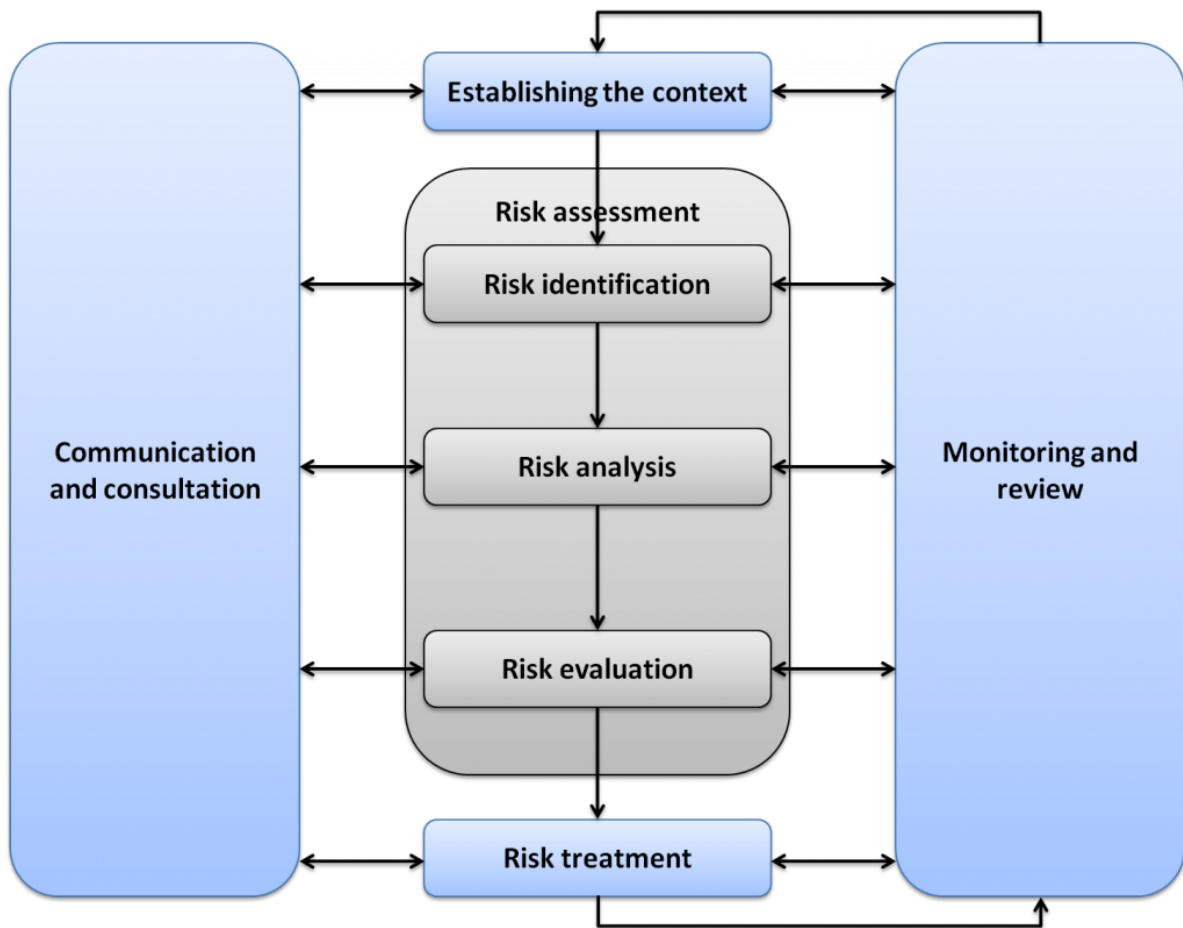


Figure 3.1 Safety / security risk management process  
(Source: STN 010 380)

Some experts define the risk management process as follows:

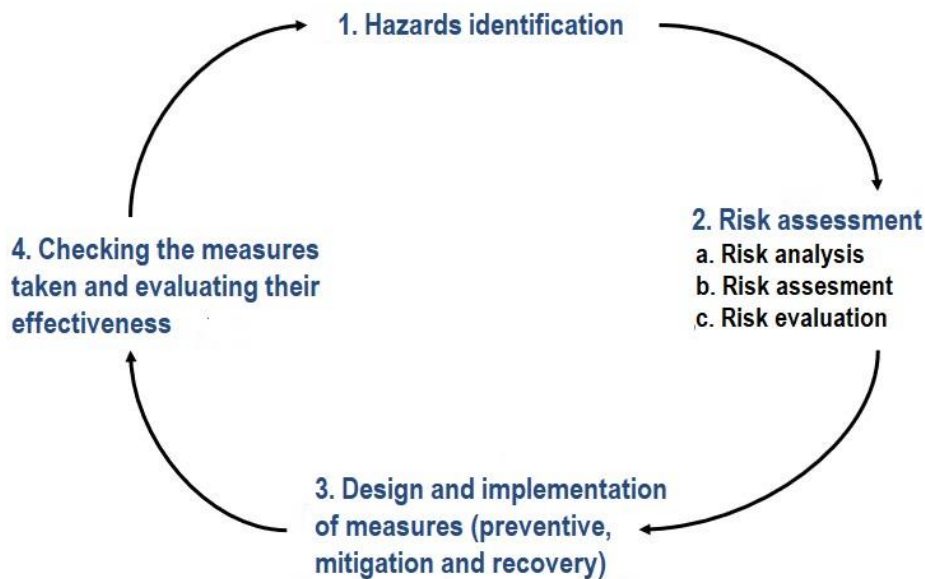
- Determining linkages (strategic, organisational, risk),
- risk identification,
- risk analysis - qualitative, quantitative, semi-quantitative,
- handling of risk,
- monitoring and reviewing,
- Communication.

The process of determining the context itself in these approaches is divided into:

- identifying the strategic context,
- identifying the organisational context,
- identifying the links with risk management,
- development of criteria,
- structure determination.

In a security environment, this process can also be described by the diagram in Figure 3.2.





*Figure 3.2 Principal steps of the risk management process  
(Source: Authors)*

According to Figure 3.2, the management process is broken down into four basic procedures. The first procedure is the identification of hazards, i.e., sites, technologies, technological nodes that can lead to hazardous or crisis situations. In this case, we identify specific scenarios of hazardous situations that may occur under certain circumstances in the systems under consideration in the future. In the next step, we subject the identified scenarios to an analysis where, first, we calculate the probability of occurrence of each of the scenarios, i.e., we determine the magnitude of the risk itself in terms of the basic mathematical model  $risk = probability \times impacts$ . In this case, the impacts are expressed directly in terms of the scenario considered in the analysis. An example is the 500-year flood scenario, where we calculate the probability with which the extent of the area flooded will occur, which are calculated for a 500-year flood. In industry, several risk analysis methods are used for risk analysis (e.g., FTA, ETA, HRA, ERA and others, see Chapter 5). Risk assessment consists of evaluating the magnitude of the risk for the scenarios considered, determining their order of importance, and finally classifying the risk into a risk grade, which we express verbally. In the risk assessment phase, we decide whether to accept a given level of risk based on the risk level, or its magnitude or frequency. If the conclusion of the risk assessment is that the risk is accepted, then the risk control and monitoring and communication phase follows. However, if the result of the risk assessment is non-acceptance, the third step is aimed at designing and implementing measures to prevent the occurrence of hazardous (emergency) events or to respond in a timely manner to the situation and to minimise the impact of such an event. This step is followed by a check of the implemented measures, their correct application, and their effectiveness. Their

effectiveness is assessed based on the elaboration of a risk analysis for the new conditions. If in this cycle, even after the implementation of the proposed measures, the risk magnitude has not been reduced to an acceptable level, we continue to propose measures and assess their effectiveness until we reach the required acceptable level of risk magnitude. Risk monitoring is carried out throughout the risk management process so that any change in the input parameters used in the risk management process can be responded to promptly.

### 3.2.1. RISK ANALYSIS

**Risk analysis** is a tool for comprehensive risk assessment. It is the process of determining whether it is systematic or unsystematic. It allows the risks to be divided into those that need to be monitored on an ongoing basis and those that can be neglected. It also makes it possible to assess the return on resources spent on preventive measures,

In terms of terminology and content, it is necessary to distinguish between risk analysis and risk assessment. However, some expert sources argue that risk analysis and risk assessment are separate phases of risk assessment. Others, on the other hand, consider risk assessment as part of the risk analysis process.

**The aim of risk analysis** is to *separate small acceptable risks from large risks and to provide data to assist in the assessment and treatment of risks*. Risk analysis includes an assessment of the sources of risks, the possible consequences, and an estimate of the confidence with which these consequences will occur. Taking 'likelihood' to mean is a property that is used to describe quantitatively the probability or frequency of occurrence of a phenomenon or event. Factors that influence the consequences and the likelihood of their occurrence can be identified.

Closely linked to risk analysis is a second process - risk assessment. Risk assessment is a mandatory part of the analysis. It includes risk frequency analysis, consequence analysis and their combination (consequences).

### 3.2.2. RISK ASSESSMENT

**Risk assessment** (*risk estimation, risk assessment, risk evaluation*) is a process designed to determine the magnitude (degree) of risk in relation to the analysed threat to human life and health, material values, environment.

Risk assessment based on the risk analysis, **assesses the** severity of the estimated magnitude (risk assessment) and assesses the need to reduce it (risk acceptability).

It involves comparing the level of risk obtained in the analysis process with predetermined risk criteria. Risk analysis and the criteria against which the risks are compared in the assessment shall be based on the same basis. That is, qualitative evaluation involves

comparing a qualitative level of risk with qualitative criteria, while quantitative evaluation involves comparing a numerical value of risk with a criterion that can be expressed by a specific number, such as mortality, frequency, or financial value.

The aim of risk assessment is to assign a value to each specific risk to the system at risk. Risk assessment is a process in which priorities are defined by evaluating and comparing the level of risk against accepted standards, acceptable threat thresholds or other criteria. The risk assessment of any system can be organised into several phases as listed in Table 3.1.

*Table 3.1 Risk assessment (Source: Buzalka, 2012)*

Phase	Content of the activity	Result of the activity
<b>Risk identification</b>	Survey, research, information storage.	Reports, tables, database.
<b>Risk analysis</b>	Quantitative and qualitative analysis, comparison.	Calculations, risk hierarchy.
<b>Determination of risk acceptability</b>	Selection of risk acceptability criteria.	Proposals, recommendations, decisions, risk management documents.

In general terms, there are three forms of risk assessment/evaluation:

- **Qualitative:** uses verbal expressions to describe varying degrees of probability and consequences. It is mainly used to give a general overview of risks when simple operations are involved or when numerical data for quantitative assessment are lacking.
- **Semi-quantitative:** a procedure where qualitatively described scales are assigned numerical values, the combination of which determines the degree of threat and consequently the value of the risk. It is a suitable method for screening workplace hazards, intended as a starting point for safety measures in the plant.
- **Quantitative:** uses numerical values for the probability and consequences of an undesirable phenomenon. It is used for accurate and rigorous risk assessment, especially in the design of machinery, the use of hazardous substances, etc.

When assessing risk, it is first necessary to obtain an overall estimate of the risk. This can be obtained by combining the probability of the risk and its severity according to the risk assessment matrix (Table 3.2).

Table 3.2 ICAO risk assessment matrix (Source: Šimák 2006)

Probability of risk	Severity of risk				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

Combining them gives the probability and severity of the risk, e.g., 4B (**random** risk with **hazard** severity). This implies that the risk can be expressed by an alphanumeric combination, even if it is in fact invisible and intangible.

The importance of a verbal assessment of the likelihood of risk occurrence:

- (5) **Frequent**: the likelihood of frequent occurrence (occurs regularly).
- (4) **Occasional**: the likelihood of occurring occasionally (it occurs irregularly).
- (3) **Remote**: unlikely but possible occurrence (rare).
- (2) **Improbable**: very unlikely (not known to occur).
- (1) **Extremely improbable**: almost unthinkable, unlikely to occur.

The resulting risk severity can be verbally assessed as follows (Table 3.2):

- **Catastrophic**
  - equipment destroyed,
  - the death of several people.
- **Hazardous**
  - Significant reduction in the level of safety, physical exhaustion, or workload to the extent that the operator(s) cannot be relied upon to perform their activities accurately and completely,
  - serious injury,
  - most of the equipment is destroyed.
- **Major**
  - Significant reduction in the level of risk, a reduction in the ability of operators to carry out activities to avert adverse conditions because of their increased workload or because of conditions impairing their performance,
  - serious incident,

- personal injury.
- **Minor**
  - harm (health, material),
  - restriction of the activity carried out,
  - carrying out emergency activities,
  - a minor incident.
- **Negligible**
  - small consequences.

The output of the risk assessment is therefore a prioritised list of risks for further processing. Decisions must consider the wider context of the risk and include tolerance of risks created by actors other than the organisation that benefits from it. If the resulting risks fall into the category of low risk or acceptable risk, they may be accepted with minimal additional consideration. Small risks and acceptable risks need to be monitored and periodically reviewed to ensure that they remain acceptable. If risks do not fall into the category of low risk or acceptable risk, they should be addressed.

**Safety / Security risk** assessment (especially as part of crisis management) is essentially concerning the expression of the risk consequences. The consequences of a safety / security risk express the extent, degree of probable (expected, potential) damage, loss or other negative consequences that may arise because of the activation of a safety / security risk into an imminent safety / security threat.

The consequences of a safety / security risk may be of the following nature:

- Pecuniary or non-pecuniary damage,
- Humanitarian damage and loss,
- Negative environmental impacts.

To conclude this section, it should be noted that for the purposes of risk assessment it is possible to apply up to 31 different models can be applied, these are contained in STN ISO 31010.

### **3.3 BASIC REQUIREMENTS FOR THE MANAGEMENT OF SAFETY / SECURITY RISKS OF THE ORGANISATION**

Among the basic requirements for the success of an organisation's risk management, the most common are:

- establishing a risk management policy,
- planning and resourcing,
- setting the deployment programme,
- management verification.

An organisation planning to implement a risk management system should have a **risk management policy** in place. The policy document should include the strategic and partial objectives that the organisation wants to achieve in this area and how it plans to use the results of risk management in the management of the organisation. The risk management policy should be based on the objectives, goals, and the nature of the organisation's activities.

For **planning and resourcing** it is essential to take the following into account:

- all obligations arising for the organisation from national legal standards, STN, agreements towards the organisation and the external environment (occupational health and safety, fire protection, flood protection, prevention of major industrial accidents, food safety, civil protection of the population, environmental protection, transport of dangerous goods, etc.).
- the performance of the organisation's risk management system.
- the responsibility, authority and interrelationships between the people who implement, control and influence risk management in the organisation.
- Identifying and providing adequate human, financial, technical, and technological resources, the necessary infrastructure, including management training.

To put in place a **risk management system** in an organisation is effective and meets all the requirements to meet its strategic objective, it requires several steps to be taken. The implementation plan should include tasks, time horizons for their completion, responsibilities of those responsible for their completion, and, where appropriate, financial, personnel and technical support. It should be ensured that the effectiveness of the organisation's risk management activities is **verified** at specified intervals. The results should serve as a basis for confirming its effectiveness in meeting the requirements of the organisation's risk management policy and its objectives, and records of such reviews must be maintained.

Responsibility for risk management is spread throughout organisations across management. The highest responsibility naturally lies with the owner, the statutory body, and the top management of the company. In small organisations, responsibility for risk management is concentrated at the level of the statutory body, as it is not efficient to employ a full-time dedicated risk manager. In medium and large organisations, responsibility is spread across individual managers. Large organisations or organisations operating in a risk environment (e.g., banks, insurance companies, petrochemical and energy industries, aerospace, transport) have a designated specialist (risk manager). Almost always, risk management is linked to the role of the financial director because the impact of risks (damages) and countermeasures can be quantified financially and have an impact on financial planning.

The standards in the field of risk management in business activities are only of a recommendatory nature. It is therefore not possible to force any organisation to follow them. More important is the motivation of the organisation. Increasingly, we are encountering with the term social responsibility. The ISO 31000:2018 standard '*Risk management* -

*Guidelines'* is currently in force. However, it is still applied in Slovakia as STN ISO 31000:2019 Risk management - Guidance. It formulates the principles, characterises the system and process and provides general guidance on the implementation of risk management. To implement the risk management process as efficiently as possible, ISO/TR 31004:2013 "*Risk management - Guidance for the implementation of ISO 31000*" has been developed. It provides guidance for organisations on how to effectively implement risk management and implement its principles according to ISO 31000. ISO 31000 was also the starting point for for the creation of the guide for SMEs and in 2015 ISO 31000 "*Risk management - a practical guide for SMEs*" was published. The purpose of ISO 31000 is to harmonise risk management processes in other types of standards and norms. It provides recommendations on how to develop, implement and continuously improve a risk management system, but cannot be used for certification purposes.

### **3.4 THEORETICAL BACKGROUND OF DISASTER RISK MANAGEMENT**

The increasing frequency and severity of natural disasters around the world highlights the vulnerability of communities and their lack of capacity to cope with such events. If these events are to be controllable in the future, it is essential to know and understand the multiple characteristics of the system that are interrelated - social, political, institutional, economic, technical, and environmental.

Researchers and practitioners working on disaster and risk management topics, as well as the preservation of sustainable development, have concluded that the mounting losses experienced by people and institutions in several developing countries have been steadily increasing in recent decades. The aftermath of such disasters is direct evidence that their development schemes are not geared towards ensuring long-term sustainability. They point to the need to recognize disasters as the result of unanswered questions of development schemes. The reasons for such conclusions include the following:

- There is a persistent view that the root causes of disasters are purely natural and therefore unavoidable. In this respect, disasters are seen as external or independent of the development framework used.
- the fact that risk and vulnerability remain invisible unless a natural event conditions their manifestation, unlike poverty, which is now becoming increasingly evident at local, national, and international levels.
- the incorrect view that nature can be managed through technical interventions and therefore disasters can be avoided through these means.

The integration of risk analysis into the risk management process is understood in different ways in professional sources. The most common concepts are:

- Risk analysis is understood outside of risk management itself as a relatively separate activity forming the prerequisites for dealing with risk. Alternatively, such a concept can be understood in different ways.

- Risk analysis as a process including risk assessment.

Risk analysis also aims to scientifically predict what the manifestations and consequences of risk will be so that it can be adequately managed. It is therefore essentially a matter of forecasting, by means of scientific methods based primarily on objective, relevant and significant facts about the system at risk, its behaviour as a whole in different crisis situations and defining the ways in which it will react, either spontaneously or in a controlled manner.

In this respect, from a risk theory perspective, a security risk analysis would should be preceded by:

- Development of variants of catastrophic scenarios with estimation of probability of their occurrence.
- Determining the worst-case risk and its impacts.
- Preliminary quantification of the impacts of the worst-case risk - potential losses and damage to protected interests.

Risk analysis, unlike other analyses carried out, is an activity which, with the help of systems analysis approaches and tools, takes place during the prevention period. Its results then form the content of the crisis (emergency) plans of the system at risk in the form of various purposeful syntheses.

Risk analysis is conditional on finding answers to questions **in the areas of**:

- locating objects that cause risk in the area.
- Identification and characterisation of threats and risks, their detection using modelling or expert judgement (estimates), or identification of areas requiring specific action.
- risk classification: classification into groups according to identifying features.
- assessment of threats and risks, quantitative and qualitative factors, prioritisation according to consequences, importance, etc.

Security risk assessment/assessment (from a crisis management perspective) is essentially about expressing the consequences of risk. The consequences of a security risk express the extent, degree of probable (expected, possible) damage, loss or other negative consequences that may arise because of the activation of a security risk into an imminent security threat.

The consequences of a security risk may be of the following nature:

- pecuniary or non-pecuniary damage,
- human damage and loss,
- negative environmental impacts.



A major challenge for the field of disaster reduction today is the change in people's sensitivity and their ability to recognize the early signs of disasters. This should be an outcome of the whole development process.

Disasters reveal the pre-existing situation within the social, economic, political, physical and environmental structures of communities and societies.

Infrastructure, services, processes, organisations, from the simplest to the most complex and disparate systems, are built in a way that makes them vulnerable to damage from a trigger event. Based on this, the conclusion has been drawn that **a disaster is preceded by at least two predispositions**: the possibility that a trigger event takes place, usually called a threat, in that very potential state; and the predisposition of people, processes, systems, infrastructure, services, organizations, or communities to be harmed, damaged, or destroyed by that trigger event is called vulnerability. The combination of these two predispositions is called risk by several practitioners.

Through systematizing the impacts of such disasters, it is possible to identify those conditions and processes that give rise to the risks involved, both in terms of the actors who are directly or indirectly responsible and the characteristics of the settings that allow these risks to arise and their increase in the urban and industrial environment. In this context, settings are defined as a mixture of social, economic, political, institutional, cultural, and environmental factors that influence actors' decisions according to certain patterns. The analysis following this procedure can help in identifying the source causes, that lead to disasters and consequently strategies and actions to counter these root causes and thereby promote more sustainable development.

While traditional risk scenario development focuses on threat analysis and vulnerability analysis, treating disasters as a completed event before they ever occur. In the context of sustainable development, risk scenario analysis progresses to other variables such as emerging opportunities associated with globalisation and public and private sector priorities incorporating lessons on risk and lessons from past disasters.

This type of analysis should lead to the planning of a strategy linking the manufacturing sector and geographical regions, identifying aspects of need in terms of communication networks and critical infrastructure elements. This change in approach to disaster and risk management should lead to a strategic analysis of the development of alternatives in geographical areas that are still uninhabited, comparing the benefits offered, that such areas may give way to the threats that exist in such territories. Similarly, this new approach should lead to the planning and implementation of infrastructure projects that prepare the environment for development, considering either identified vulnerabilities, to avoid new risks or to prevent disasters from occurring in the first place. At the policy level, supporting the transition from

response to prevention, risk management takes over the decision-making function. In this sense, legislation must also be amended, or new laws passed.

## **CONCLUSIONS**

The implementation of risk management processes, and in particular security risk management, is one of the basic prerequisites for ensuring an acceptable level of system security.

The first prerequisite is the identification of threats, or all scenarios of events that may threaten the system during its existence, or even lead to its demise. The starting point for the identification of potential threats and hazardous situations is the processing of an analysis resulting in a list of locations, activities, machines, and equipment, which, due to their characteristics, method, and technology of use, may lead to the occurrence of emergencies. The impact of these emergencies may, with varying degrees of severity, endanger the life and health of persons, damage property, cause widespread damage environmental damage and, ultimately, major economic damage to the company in which the event takes place.

From a risk management perspective, the key phase is prevention, i.e., preventing the occurrence of emergencies. In practice, appropriately selected and effective preventive measures implemented can protect the system from damage at the time of negative factors and ensure full functionality of the system. However, if the chosen measures are not sufficiently effective or have not been implemented correctly, there is a risk that the system functionality will be disrupted and the damage to the system may be reversible or irreversible when negative factors are present. The reversibility or irreversibility of the damage to the system and the restoration of its function will in this case be determined by the measures adopted and implemented to minimise the impact. Their planning is also part of crisis planning, i.e., they are planned and implemented at a time 'before the emergency'. These are the forces and resources that need to be deployed to deal with a crisis in a timely and effective manner. Their aim is to minimise the impact of a given emergency (fire suppression, hazardous substance spill response).

Lessons learned from the crisis are the basis for a new risk analysis, taking new measures to increase the system's preparedness and resilience to future damage. These measures also include measures for the recovery and reconstruction of systems after damage.

This approach to risk management can be applied at any level of management.

## REFERENCES

- [1]. CROUHY, M., GALAI, D., MARK, R. 2014. The Essentials of Risk Management. McGraw/Hill Education, 672 p.
- [2]. DRENNAN, L., MC. CONNELL, A. 2007. Risk and Crisis Management in the Public Sector. London (UK): Taylor & Francis Ltd, 264 p.
- [3]. FILIP, S., ŠIMÁK, L., KOVÁČ, M. 2011. Manažment rizika / Risk management. Bratislava: University of Economics and Public Administration Management in Bratislava, 61 p.
- [4]. HOPKIN, P. 2018. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page, 480 p.
- [5]. MAJLINGOVÁ, A. et al. 2013. Fire protection and rescue services selected chapters. Zvolen: Technical University in Zvolen, 2013. 273 p.
- [6]. MERKOVÁ, M., DRÁBEK, J. 2013. Possibilities of risk analysis in the investment decision-making of the company. In Intercathedra, No. 29/1 (2013), p. 41-49.
- [7]. ORAVEC, M. 2011. Vybrané kapitoly z manažerstva rizík 1: Základy teórie rizík / Selected chapters from risk management 1: Introduction to risk theory. Košice: Equilibria, 168 p.
- [8]. REITŠPÍS J. 2004. Security risk management. Žilina: University of Žilina, p. 113.
- [9]. STN 010 380: Manažerstvo rizika / Risk management.
- [10]. STN ISO 31 010:2009. *Manažerstvo rizík / Risk management.*
- [11]. ŠIMÁK, L. 2006. *Manažment rizík / Risk management.* Žilina: University of Zilina. Available online: <[http://fsi.uniza.sk/kkm/files/publikacie/mn\\_rizik.pdf](http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf)>



### QUESTIONS

1. Define the term risk management.
2. What is the objective of risk management?
3. Describe the procedures or steps of the risk management process.
4. What are the basic risk management requirements of an organisation?
5. Define the essence of disaster risk management.

## 4. SAFETY AND SECURITY RISK ANALYSIS METHODS

No risk assessment methodology has been created artificially, only in theory, but always as a product of a social order. Several methods used for risk analysis have gradually been developed in this way, ranging from traditional methods to the current complex methods using the tools of specialised software environments.



*The aim of the chapter is to know and understand the individual methods of risk analysis currently used in the security practice in the Slovak Republic and to be able to choose the appropriate method to achieve the set goal.*

### 4.1. CLASSIFICATION OF SAFETY RISK ANALYSIS METHODS

Risk is analysed by combining estimates of the consequences and the probability of their occurrence

and shall be related to existing control measures. It is recommended that a preliminary analysis is carried out to exclude similar or low impact risks from a detailed study. If possible, a list of excluded risks should be made to demonstrate the completeness of the risk analysis.

The choice of specific risk analysis methods is determined by factors such as the severity of the risk, the complexity of the problem being analysed, the availability of data, the difficulty of mastering the analysis and, finally, the expected cost of the analysis. In addition, existing management and technical systems and risk management practices are evaluated and their strengths and weaknesses are assessed in the selection of methods.

In terms of **information sources**, we distinguish between two basic methods:

- **Inductive risk analysis methods** ('ex ante'): they allow to anticipate the occurrence of a possible event and point to the circumstances that could cause the event to occur. They also help to estimate the number and consequences of events.
- **Deductive methods of risk analysis** ('ex post'): allow estimation of the frequency of and consequences of events based on events that have already occurred in practice and look for the context that caused the events.

In terms of **how the risk is assessed**, qualitative, semi-quantitative or quantitative risk analysis methods are used for the analysis.

**Qualitative analysis** uses verbal expression. They are used in cases where it is simple situations or where numerical values (data) for quantitative risk assessment are missing or difficult to express. Such analysis can be used to assess risk as e.g., acceptable, or unacceptable, small, low, medium, etc.

**Semi-quantitative (semi-quantitative) analysis** uses a qualitative description of scales (scales) that have some numerical values assigned to them that express a so-called risk score. The combination of these characteristics determines the risk value.

**Quantitative analysis** uses numerical characteristics to assess risks by expressing their probability, frequency, potential, etc. It can be used in those cases where there is sufficient relevant data that can be evaluated statistically. Such analysis mainly assesses quantitative risk factors.

The quantitative analysis method uses numerical values (rather than descriptive scales such as qualitative) to both quantify consequences and estimate the probability of risk occurrence and semi-quantitative analysis) obtained from data provided by various sources (corporate, departmental, national, and multinational event databases, statistical data, results of mathematical and simulation modelling).

The quality of the analysis depends on the accuracy and completeness of the numerical values used. The consequences of possible events can be assessed by modelling the outcome of the event or by determining even outside the set of events under study, so-called extrapolation from experimental studies or from previous data.

Consequences can be expressed in SI units, in terms of financial, technical, or human criteria, or using any risk assessment criterion. In some cases, more than one numerical value is required to specify consequences at different times, in different places, for different groups and in different situations.

The consequences of a financial loss or financial gain are quantified by multiplying the frequency of its occurrence per year to obtain the expected value in euros per year.

The fatal risk arising from an activity can be calculated as the number of deaths caused by an activity per year times the number of people involved.

In another very wide range of quantitative analysis methods, qualitative or semi-quantitative risk analysis approaches are also used in many cases. The description of these methods is based on the basic approaches of their characterisation and possible applications in the available literature. Many of these methods are already used in our context, including in the social sphere.

## 4.2. CHARACTERISTICS OF SELECTED RISK ANALYSIS METHODS

The introduction to the selected risk analysis methods is introduced in Table 4.1.

Table 4.1 Overview and characteristics of the group of methods used for quantitative risk analysis (Source: Author)

Method	Description of the method	Shortcut
Safety Audit	Systematic assessment of selected system parameters (walks, inspections, etc.) and their recording - the oldest method.	SA
Check list Analysis	Item-by-item control records that indicate the status of the system (they do not provide hazard information in other situations).	CLA
What - if Analysis	Use of brainstorming.	WIA
Preliminary Hazard Analysis	Quick background for detailed analysis. The basis is the determination of the subject of analysis, identification of problems, system diagram.	PHA
Hazard and Operability Study	The most common hazard identification procedure. Use especially in the evaluation of newly designed and reconstructed systems. (Use of the keyword system- NO, NOT, MORE, AS WELL AS; PART OF, REVERSE, OTHER THAN;	HAZOP
Failure Modes and Effects Analysis	Evaluation of equipment failures and their impact on the technological process at different levels of the system;	FMEA
Fault Tree Analysis	Sequential (top-down) assessment of combinations of failures that can cause a crash;	FTA
Event Tree Analysis	Using brainstorming and morphological search, a list of causes (from top to bottom) of the crash is compiled and the causes are linked;	ETA
Human Reliability Analysis	Identification of possible human errors, their causes, and their impact. This includes identification of important points in the system affected by human errors;	HRA
Point Method	Threat assessment. Probability values from 1 to 5 shall be assigned. consequence values from 1 to 4. The level of risk is determined in the form of a matrix - a combination of consequence and frequency values.	PM

#### 4.2.1. CHECK LIST ANALYSIS (CLA)

The method uses **item control records** against which the status of the operation is checked. The overall control record contains a rating of 'yes', 'no', 'not appropriate' and 'no further information required',

Control records are used to ensure compliance with regulations and standards (norms). The method is useful in detecting problems that have already occurred. It can be used for simple evaluations as well as for more costly, detailed analyses. It is particularly designed to identify traditional sources of risk.

An example of check list is introduced in Figure 4.1.


 <p><b>DALHOUSIE UNIVERSITY</b></p> <p>Department of Facilities Management Occupational Health and Safety</p>	<p><b>Workplace Inspection Checklist</b></p>		
<p><b>Building / Shop:</b> _____</p>			
<p><b>Supervisor in Charge:</b> _____</p>			
<p><b>Names of Inspection Team Members:</b> _____</p>			
<p><b>Date of Inspection:</b> _____</p>			
	<b>Yes</b>	<b>No</b>	<b>Comments/Actions</b>
<b>Health and Safety Bulletin Board</b>			
Is there a current copy of the Act?			
Is there a current phone number for the Occupational Health and Safety Division of the Department of Labour?			
Is there a current copy of the OHS Policy?			
Is the list of JOHS committee members posted?			
<b>Floors, Corridors, Walkways and Driveways</b>			
Are floor areas and corridors free of debris, materials or equipment?			
Are all doorways clear of debris, materials or equipment?			
Are the floors slippery, oily or wet?			
Is non-slip matting used where slippery conditions exist?			
Are floors kept clean?			
Are wet floor signs posted when floors are being washed?			
Are carpets and/or tiles clean and in good condition?			
Are areas designated as aisles well marked and visible?			
Has salt or sand been applied to icy walkways and parking lot?			
Are entries in the Salting / Sanding Log up to date?			
Are walkways and driveways being cared for as required?			
<b>Emergency Equipment</b>			
Is emergency lighting working? Has it been tested?			
Is the location of all fire extinguishers clearly marked?			
Are all fire extinguishers properly mounted on the wall?			
Have all fire extinguishers been professionally inspected within the past 12 months?			
Is employee fire extinguisher training up to date?			
Are emergency exits clearly marked?			
Are emergency phone numbers posted close to all phones?			
Are smoke detectors in good working condition?			

Figure 4.1 Check list example  
(Source: [Internet](#))

The analyst shall either use the control record from the previous activity or, if it is not available, the analyst or work team shall prepare and conduct a new assessment.

The time and cost of using relative classification methods depends on the technique chosen, the input data requirements and the number of processes and risk sources to be assessed.

**The study can be carried out by a single analyst, but in the case of a more complex system assessment, several analysts** with sufficient experience are needed and knowledge. In the case of cooperation, it is important that their judgement is consistent.

#### 4.2.2. SAFETY AUDIT (SA)

The oldest method used for existing operations.

Mostly **inspection visits** are used, which are visual inspections to a formal survey, which may take a longer period,

**The audit is carried out by a team drawn from different professions.** The application of the method requires cooperation and consultation between the analyst and the staff.

A safety audit identifies unsafe conditions and operating procedures, and the analyst suggests protective measures that can be verified by follow-up inspections.

The typical procedure is to prepare (usually control records), evaluate, recommend implementation of actions and record changes.

#### 4.2.3. WHAT HAPPENS IF ... (What If Analysis - WIA)

An inductive method that answers how failures and faults act to create threats. Checklists are used for greater complexity.

The aim of ensuring safety by the "What happens if..." method is to **identify unsafe conditions in the technological process.**

Using **characteristic questions** that begin "**What happens if...**" the **causes of failures** are identified, **and measures are suggested to increase safety.** It is also possible for a safety-related objection to be raised and does not have to be expressed as a question.

The preparation of characteristic questions that will help us to identify hazards is done by consulting selected experts intimately familiar with the process. '**Brainstorming**' - discussing the search for new solutions - is consistently applied. The method is effective when developed by an experienced team of experts.

The "What happens if..." method is a flexible method and can be used at any stage of the technological process.

The work team should be composed of **two or three workers**, or possibly more. This depends mainly on the complexity of the processes of the object under consideration and the



number of areas to be analysed. Preparation and documentation are mainly the task of the team leader and the recorder.

#### 4.2.4. PRELIMINARY HAZARD ANALYSIS (PHA)

In industry, it is primarily used in the design phase of a facility project, but can also be applied to existing facilities, usually as the first part of a comprehensive safety study with later use of a more detailed method.

The method allows to identify hazards in an inexpensive way before the actual construction of the facility, thus minimising the cost of any changes. It also helps in the choice of the location of the plant.

The advantage is the **early familiarisation of all workers with the potential hazards of the process and the mastery of safety from the beginning of the equipment's lifetime.**

The aim of the analysis is to quickly create an overview of the hazards in the plant, which will be the basis for a detailed analysis. This analysis can also be applied in the early stages of design, when only very general plans and technological schematics are available.

The main idea of the PHA is to select a subject of study and identify which hazards may arise. For this purpose, we can use the team method with any team composition with which we can solve a large area of problems. The analysis processor considers the hazards "loosely" at first, then uses e.g., a "checklist of possible hazard types".

For each hazard, both the relative frequency and consequences are considered, and potential accidents are identified. The selected accidents are estimated using the predicted frequency and degree of harm to individual and public health. This estimate is only approximate; therefore, the accident occurrence frequencies and consequences are only classified within certain ranges.

Once hazards have been identified, the possible causes and consequences of accidents are evaluated resulting in the classification of the incident into one of four hazard categories: **negligible, common, severe, and catastrophic.**

The results of the study can be recorded in a summary table that includes the identified hazards, the causes and consequences of accidents, the hazard category, and the recommended actions.

Potential hazards in most cases include fire, explosion, toxicity, corrosion, radiation, noise, vibration, electrocution, mechanical failure, and other special hazards.

The risk assessment is based on the determination of a **risk index:**

- The following classification scheme is used to **determine abundance (P):**
  - no accident, danger excluded => 0
  - less than 1 in 1,000 years => 1

- between 1 x per 100 and 1 x per 1,000 => 2
  - between 1 in 10 and 1 in 100 years=> 3
  - between 1 x per year and 1 x per 10 years => 4
  - More than 1 x per year => 5
- **The degree of impairment (I)** shall be determined as follows:
- without injury => 0
  - serious injuries => 2
  - fatal accident => 3
  - several fatal accidents => 5
- The risk index (I) can be determined as follows:  $R = P + I$

#### 4.2.5. FAILURE MODE AND EFFECT ANALYSIS (FMEA)

FMEA is currently the most used method for assessing and evaluating potential risks. By using this method, risks can be prevented or mitigated, that arise in the design of the management system, in product development and design, in technology in process development and in production itself.

The essence of the FMEA method is the systematic identification of all possible product or process defects and their consequences, the identification of actions to avoid, reduce or limit the causes of these defects, and the documentation of the entire process.

The method requires a great deal of team experience with the system being analysed. For more complex systems, FTA (fault tree analysis) may follow.

The role of the FMEA process:

- Identify the process functions or process requirements.
- identify all possible failures related to the process estimate the consequences of these failures for the customer.
- identify the possible causes of these failures in the manufacturing process or Council.
- Identify the process parameters to be targeted by process control to reduce the occurrence of defects or increase the probability of their detection, rank the defects according to their risk and, on that basis, propose actions to reduce it and, finally, document the results achieved in the manufacturing or Council processes.

The main working method is brainstorming. Simple problem-solving tools such as graphs, histograms, etc. are very useful.

The progress of the analysis is recorded in the FMEA form (Figure 4.2).

## FMEA

Process/Product Name: _____		Prepared By: _____													
Responsible: _____		FMEA Date (Orig.): _____ (Rev.): _____													
Process Step/Input	Potential Failure Mode	Potential Failure Effects	SEVERITY (1 - 10)	Potential Causes	OCCURRENCE (1 - 10)	Current Controls	DETECTION (1 - 10)	RPN	Action Recommended	Resp.	Actions Taken	SEVERITY (1 - 10)	OCCURRENCE (1 - 10)	DETECTION (1 - 10)	RPN
What is the process step, change or feature under investigation?	In what ways could the step, change or feature go wrong?	What is the impact on the customer if this failure is not prevented or corrected?	What causes the step, change or feature to go wrong? (how could it occur?)	What controls exist that either prevent or detect the failure?	What are the recommended actions for reducing the occurrence of the cause or improving detection?	Who is responsible for making sure the actions are completed?	What actions were completed (and when) with respect to the RPN?								
Fill carafe with water	Wrong amount of water	Coffee too strong or weak	Faded level marks on carafe	Visual Inspection	Replace old carafes	Mel	Carafe replaced 9/15	128				8	1	3	24
								0							0
								0							0
								0							0
								0							0
								0							0

Figure 4.2 Process FMEA form\*  
(Source: [Internet](#))

\*Note: By clicking on the Figure, you will be forwarded to the webpage with original template.

Completion of the FMEA form:

1. **Process / Product Name:** name (type) of the item to which the analysed manufacturing process / product relates.
2. **Responsible:** indicate the department/unit responsible for the process.
3. **Prepared by:** indicate the name and function of the person responsible for drafting and updating of the FMEA (usually also the FMEA team leader).
4. **FMEA date (orig.):** the date of completion of the original version of the FMEA shall be indicated.
5. **FMEA date (rev.):** the date of the FMEA revision.
6. **Process Step / Input:** a simple description of the process, operation description of the process or Council/technological step to be analysed (e.g., spinning, welding, etching, gluing, etc.) and a brief description of its purpose and its requirements.
7. **Possible failure:** expresses the way in which the requirements of a process (Council, part of an activity) may not be met and/or the design intent may not be met. Not specified as a symptom observable by the customer. It is to be considered that a failure could occur even though it may not be unavoidable.
8. **Possible consequence of a failure:** it always describes the consequence for the customer as it might be perceived by the customer. We do not consider the fact that there are checkpoints in our process, that will detect the failure and therefore the consequence to the customer is "none". To customers in this context could be the following operation, the finalising customer, the vendor and/or the owner of the product.
9. **Significance:** is expressed by an index of significance or materiality: it is an estimate of the severity of the consequence of the failure (listed in the previous column) for the customer, should this failure occur to him. The consequence significance index takes values ranging from '1' to '10'. The consequence of the failure is the only criterion for determining significance. Only major design or process changes, which also change the consequence of the failure, can reduce the value of the significance index.
10. **Classification:** used to indicate special - critical characteristics that may require extended requirements for their management or control. Classification is governed by principles established by the organisation.
11. **Possible cause/mechanism of the failure** defines (describes) the possible cause of the failure. Each possible cause and/or mechanism of the failure shall be recorded. Of human failures and equipment, only specific ones should be listed (e.g., operator misfits a gasket). Ambiguous and unclear phrases should be avoided (e.g., operator failure, machine malfunction).

**12. Occurrence:** expresses the probability that a failure due to a specific cause will occur (Table 4.2). The probability of occurrence is expressed by an occurrence index (ranging from "1" to "10"), which is a prediction of the number of failures, not their actual frequency of registration (detection). The occurrence index is more of an opinion than a specific probability value. When estimating the value of the incidence index, it is useful to use statistical data, e.g., from capability studies or process capability data.

Table 4.2 Criteria for assessing the probability of failure (Source: Author)

Probability of Failure	Time Period	Per Item Failure Rates	Ranking
<b>Very High:</b> Failure is almost inevitable	More than once per day	≥ 1 in 2	10
	Once every 3-4 days	1 in 3	9
<b>High:</b> Generally associated with processes like previous processes that have often failed	Once every week	1 in 8	8
	Once every month	1 in 20	7
<b>Moderate:</b> Generally associated with processes like previous processes which have experienced occasional failures, but not in major proportions	Once every 3 months	1 in 80	6
	Once every 6 months	1 in 400	5
	Once a year	1 in 800	4
<b>Low: Isolated failures associated with similar processes</b>	Once every 1 - 3 years	1 in 1,500	3
<b>Very Low:</b> Only isolated failures associated with almost identical processes	Once every 3 - 6 years	1 in 3,000	2
<b>Remote:</b> Failure is unlikely. No failures associated with almost identical processes	Once every 7+ years	1 in 6000	1

**13. Methods used to prevent the occurrence:** indicate the preventive measures and methods (e.g., preventive maintenance) currently used to prevent or detect the occurrence of defects.

**14. Methods used to detect:** the measures, methods of verification, evaluation and process control currently used to detect that a failure has occurred shall be indicated.

**15. Detection:** expresses the probability of detecting a defect before the product leaves the Council/workplace/operation. It is assumed that the defect (cause) has occurred and estimates the probability of its detection by the inspection methods listed in the previous column. The probability of detecting the defect (effectiveness of the control methods) is expressed by a detection index in the range '1' - '10'. It is not automatically assumed that if the occurrence rating is very low, the detection rating (index) will automatically be low.

**16. RPN - Risk Number:** is a measure of the risk resulting from the occurrence of individual failures and is given by the product of the indices →  $RPN = Severity \times Occurrence \times$

Detection. According to the RPN values, a ranking of importance can be made (e.g., in the form of a Pareto diagram and the application of the "80/20" principle).

17. **Recommended actions:** actions that should lead to a reduction in the Risk Priority Number (RPN) value, or actions that will provide us with information leading to this objective. Mostly measures oriented towards improving detection are generally costly and not very effective for improving quality. The greatest emphasis must be placed on failure prevention (i.e., reduction of occurrence).
18. **Person responsible/completion date:** indicate personal or organisational responsibility for implementing the recommended action and target completion date.
19. **Results of actions:** actions taken. The actions taken because of the recommended actions completed shall be recorded. After the implemented measures have taken effect, the team will estimate new values for significance, incidence, and detection. A new RPN value will also be calculated. All new values should be validated over time, as the measure in place does not necessarily guarantee the expected improvement.

For a group of potential failures with risk number values higher than the allowed limit, the team proposes measures that should reduce the risk of these potential failures (recommended measures). Priority should be given to measures that reduce the likelihood of failures occurring. For example, the introduction of statistical regulation and periodic evaluation of process capability is an appropriate measure in this area. A set of recommended actions shall be submitted by the team to the responsible manager for approval and assignment of responsibility and a deadline for implementation of the actions. Once the measures have been implemented, the FMEA team first analyses whether the executed measures correspond to the planned measures and reassesses the risk of the failures targeted by the measures. The new values identified allow the effectiveness of the individual measures to be assessed or new potential high-risk defects to be identified.

Each FMEA is a documented procedure, i.e., it is subject to record keeping and changes so, as normal documentation.

#### **4.2.6. FAULT TREE ANALYSIS (FTA)**

The method is based on an organised graphical representation of the conditions that cause or contribute to the occurrence of a defined undesirable disturbance identified as a peak event (disturbance).

The fault tree representation is in a form that can be understood, analysed and, if necessary, changed to simplify the identification of the fault being monitored. In this way, it is possible to investigate arbitrary contexts in the system as well as in its subsystems.

The aim of this procedure is:

- representation of the causal dependence model for investigating the reliability, safety of the monitored system to know the input and output interactions,
- defining the frequency of a fault in the system, or in any part of it,
- providing a clear analytical record of the logical operations existing in the monitored system,
- representation of the monitored system in the form of a graphical model in which quantitative and qualitative data are recorded.

The fault tree creation procedure is as follows:

1. Define the system being analysed, the purpose and scope of the analysis, and the basic assumptions that were made.
2. Defining fault. Specifying an undesired fault means defining the onset or existence of unsafe conditions, or the inability of the system to perform the required functions.
3. A graphical representation consisting of individual elements that are linked by logical operations describing the process being monitored (Figure 4.3). It is necessary to distinguish between conditional and unconditional states in the production process.

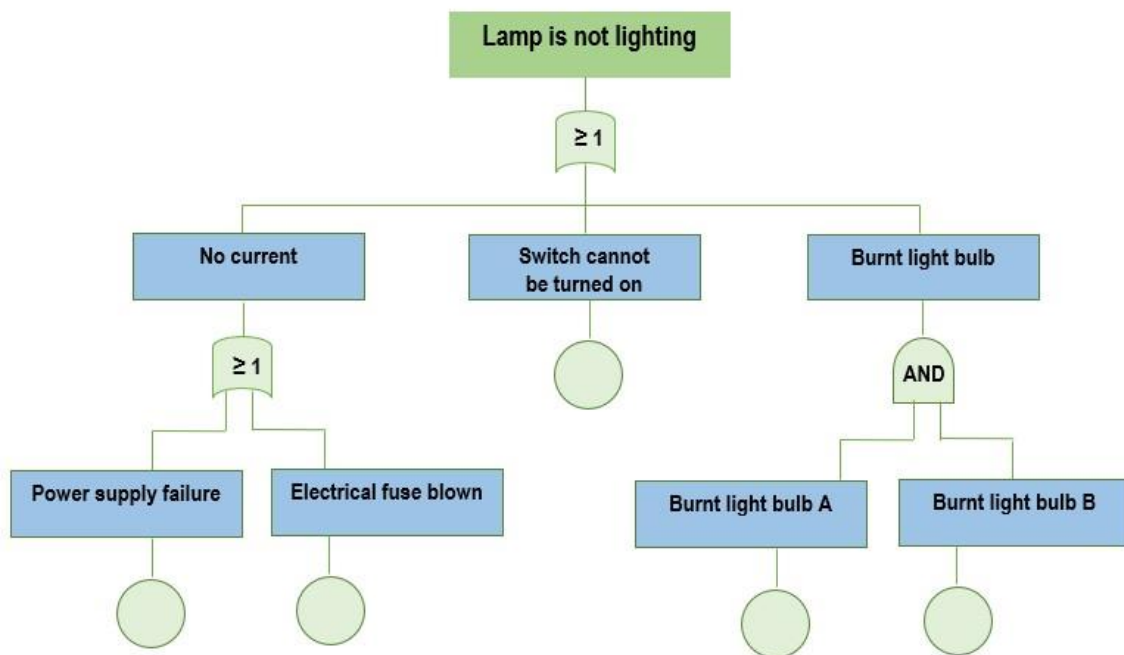


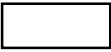




Figure 4.3 Example of a graphical representation of a fault tree (Source: Author)

4. Fault tree evaluation:
  - a. Logical (qualitative).
  - b. Numerical (quantitative) analysis of the system.
5. Assessing the credibility of information for critical elements of the system.
6. Identification of diagnostic approaches for the concept of improvement of the existing condition.

Steps 1, 2, 3, 4a are performed as part of the preliminary risk assessment, steps 4b, 5, 6 are specific to this method. The actual FTA is just displaying and calculating values for already identified faults.

**The critical path** in the FTA is made up of the most failed elements contributing most significantly to the overall fault rate. Table 4.3 lists the most used logical operators to indicate the relevant faults.

*Table 4.3 The most used logical operators in connection with the FTA method (Source: Author)*

Mark	Description	Meaning
	Fault description block	It describes the faults that occurred.
 OR	Logical sum	Fault A or B occurs.
 AND	Logical product	Event A and fault B occur simultaneously.
	Basic malfunction	The value needs to be determined.
	Underdeveloped disorder	Decomposition into basic faults is not contemplated.

The undesired failure must be defined with respect to the type of intended analysis (reliability, safety, etc.).

The analysis criteria must be proportionate to the purpose of the analysis. The analysis makes it possible to create a graphical representation of the observed links and subsequently to create a mathematical apparatus used to reveal the weaknesses of the system.

The standard output of this method is the **calculation of the peak event frequency**.

Where a risk assessment is required, this methodology should be supplemented by a consequence analysis.

After the fault tree is constructed and the functional links are mathematically expressed, the frequency of the peak event is calculated.

The fault tree also provides answers to the questions of replacing individual elements with less faulty elements.

#### **4.2.7. EVENT TREE ANALYSIS (ETA)**

The application of the ETA method is based on the representation of events that can occur in time and a specific space from the peak event. The individual branches of the event tree are quantitatively described in the form of probabilities.

Possible events in time are described. The sequence of events must be clearly defined in advance. This sequence is clear from the layout, the technological location of the object under investigation. Without knowledge of the interrelationships of the system under consideration,



it is not possible to construct a tree of events. The method of notation is in the form of a graphical representation. The quantification is performed by standard probability calculation, or it is determined tabularly for standard events.

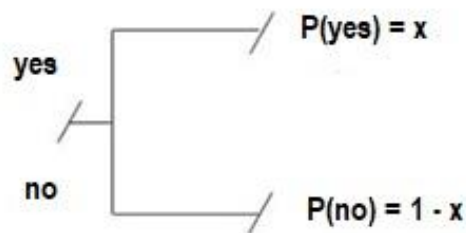
The aim of the analysis is:

- to allow easy understanding of the sequence of steps in the event being monitored,
- develop a model (causal dependence) for investigating safety,
- provide a clear graphical representation of the event being analysed,
- make input assumptions for the probability calculation.

Event tree creation procedure:

1. Defining each possible event.
2. Defining the individual factors that cause the event in question.
3. Defining the individual elements in the event and their action.
4. Graphical display of individual events in the form of a fault tree.
5. Calculation of probabilities of the observed events.
6. Evaluation of results.

Steps 1, 2, 3, are carried out as part of the preliminary risk assessment, steps 4, 5, 6 are characteristic of this method. ETA is used to display and calculate frequency values for already identified events. The frequency values at the end of the relevant branch are calculated as the product of the individual probabilities. The event tree (Figure 4.4) shows the sequence of events in a specific time and space. At each branch node, events are branched and take on logical yes or no values. In an event tree, only these two possibilities exist.



*Figure 4.4 Illustration of the logical event tree  
(Source: Author)*

At the end of each event tree are the resulting events relevant to the specific space and time.

#### **4.2.8. HUMAN RELIABILITY ASSESSMENT (HRA)**

The term Human Reliability Assessment (HRA) is a collective name for a group of methods and models that are used to identify and predict the occurrence of human errors in the work

environment. This philosophy is based on a detailed description of the functions, roles, and resources in the human-environment relationship.

For any combination of methods, sub-analyses shall be performed:

- Task Analysis (TA),
- Human Error Identification (HEI),
- Quantification of human reliability, or Human Error Probability (HEP).

When selecting analytical tools for HRA, the following need to be addressed:

- the issue of selection of activities with the potential for operator failure, i.e., determine for which activities to perform HRA, how to select?
- selecting simple activities where barriers are not applied. Human-machine interface.
- The human-machine-technological unit interface (e.g., machine start-up, start-up, shutdown, maintenance, etc. is usually treated by several barriers).

Figure 4.5 shows the sequence of steps in the human reliability assessment in the production process.

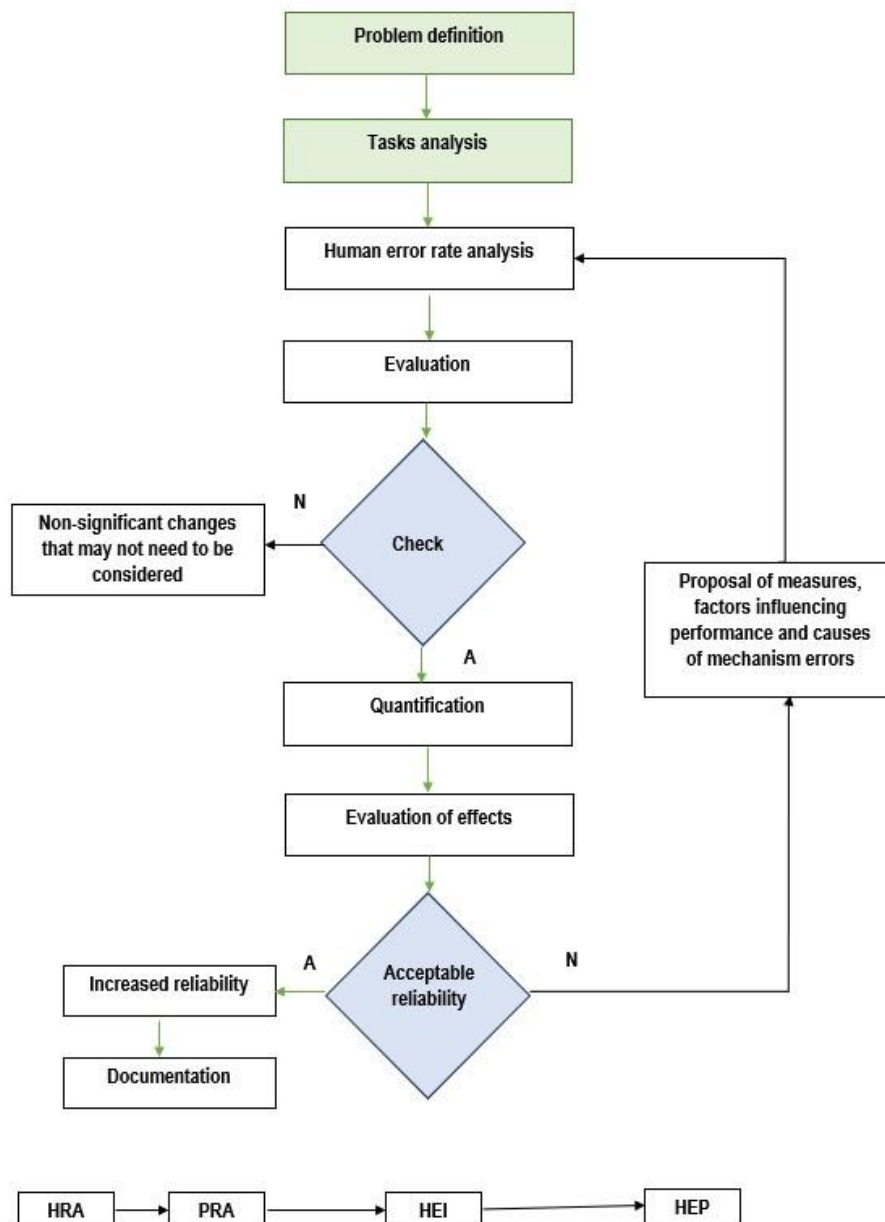


Figure 4.5 Sequence of steps in the human reliability assessment process  
(Source: Oravec, 2011)

An adverse event can be thought of as a process of several successive events following one another that stem from a particular cause. By overcoming successively all existing barriers, the causality ends with an undesired event. The basic prerequisite for the occurrence of an accident is the activation of a hazardous property of the object in question. Statistics confirm, that most chemical safety accidents are linked to human error. Human error can be prevented by preventive measures (technical or organisational barriers).

Task analysis is used to describe and understand human interactions with the system.

The results of the task analysis are used with the error taxonomy (classification scheme), which allows the identification of errors. The identified errors are analysed qualitatively or quantitatively. The process is repeated each time a design iteration occurs.

For the quantification of errors, i.e., modelling the reliability of the performance of dynamic systems, (solving repetitive tasks), it is more convenient to use the systems approach applied in classical reliability theory. For this case, Askren and Regulinski defined a reliability function of human performance:

$$R_h(t) = \exp\left(-\int_0^t er(t)dt\right) \quad [-] \quad (12)$$

The variable  $er(t)$  appearing in equation (12) represents the instantaneous value of the human error rate under the given conditions. In practice, a mean value related to an infinite time interval, the number of work operations performed, and the number of individuals is used. Such a quantity is referred to as HEP and can be simplistically expressed as the ratio of the number of  $N E_{0i}$  (Number of Erroneously performed tasks of type i) and the number of opportunities (occasions) for error  $N_0 T_i$  (Number of all Tasks of type i), equation (13).

$$HEP = \frac{N_0 \cdot E_i}{N_0 \cdot T_i} \quad [-] \quad (13)$$

To determine the HEP, it is necessary to precisely define the cases and states of human activity in the analysed system (i.e., to determine deviations from the prescribed scheme), which means that it is necessary to start from the knowledge of specific errors that a human can make while performing a given task. For operator actions where the actions are performed as independent, relation (14) holds. For activities performed as dependent, relation (15) applies.

$$P(A) = \sum_{i=1}^n P(A_i) \quad [-] \quad (14)$$

$$P(A) = \prod_{i=1}^n P(A_i) \quad [-] \quad (15)$$

The resulting probability of human failure is then determined as the logical product of these actions, which represents the work step being analysed.

#### 4.2.9. HAZARD AND OPERABILITY STUDY (HAZOP)

A risk analysis method developed by ICI **What is ICI?**- Petrochemicals Divisions in the UK. It is mainly used in the chemical industry to assess newly designed, refurbished, and existing plants. The method is suitable for both large and small companies. It uses guided brainstorming.

Each analysed element of the system section is considered systematically using a series of keywords and guiding words. A series of questions is used to develop an idea of the causality of the process being analysed and, accordingly, the likely deviations from the proposed operating parameters are identified.

Typical list of keywords:

- **"No, not"** = none, not
- **"More"** = more, higher frequency

- "**Less**" = less, lower abundance
- "**As well as**" = also, also
- "**Part of**" = part of something
- "**Reverse**" = reverse, reverse
- "**Other than**" = other than

The keywords are assigned guide words according to the process being analysed:

- Flow
- Temperature
- Pressure
- Density etc.

In addition to the basic concepts, HAZOP uses its own concepts in the process of risk identification and assessment:

- **Purpose**: defines the proper function of the facility as specified by the project. The function can be defined in different ways (graph, diagram, schematic). It is the basic function of the device under consideration.
- **Keyword**: a chosen word describing a change in an ordinary function, e.g., not, low.
- **Leading word**: a word designating a species.
- **Deviation**: a deviation from the proper function. It is generated systematically using keywords and guide words, e.g., low pressure.
- **Causes**: sources causing the deviations.
- **Implications**: definitive manifestations of possible deviations.
- **Measure**: intervention to minimize the damage caused by the deviation.

A combination of keywords and guide words are used to define deviations from the standard process.

The applicability of keywords and guide words is quite broad, especially when the purpose is defined broadly. When the purpose is described in more detail, the applicability of the purpose decreases as the types of possible deviations decreases.

If keywords are applied in conjunction with time data, then "more" and "less" can mean longer or shorter duration or also higher or lower frequency.

By systematically combining the keywords and the purpose of the device, all possible ways that can cause a deviation are analysed. Obviously, several theoretical deviations from the normal purpose are found by this procedure. Each of them needs to be assessed, its causes identified, possible consequences determined. Unless they are significant, there is no need to take these deviations into account. However, some deviations may have real causes and consequences, and may therefore be serious and dangerous. In this case, potentially dangerous conditions have been detected and need to be analysed in detail.

If one device is studied and potential hazards are noted, the next part of the system under consideration is moved on. This is done until the entire plant has been studied.

Procedure of steps in HAZOP application:

1. Description of the purpose (function) of the system (subsystem).
2. Description of the deviation from the desired state, defining keywords.
3. Finding the cause or combination of causes that lead to the deviation, finding answers to the questions What happens if; What could have caused, etc.
4. Determination of possible consequences and operational problems.
5. Draft measures.
6. Recording of actions.

The implementation of the procedure for the study of the selected facility can be formally divided into several basic phases:

1. Target setting about safety, operability, quality
2. Selection of the work team
3. Team preparation
4. Elaboration of the study
5. Recording of conclusions

To conduct the study, it is necessary to divide the system into simpler subsystems; such division is always deliberate. The aim is to create simpler subsystems that have a single purpose.

The objective should be expressed as clearly as possible, due to:

- Project controls.
- Deciding where to place the equipment.
- Decisions on the selection of a specific facility.
- Checks on operating regulations.
- Improving the safety of existing operations.

It is also necessary to consider and decide what impact and effect the identified hazard may have on operating personnel, equipment and process, production quality, the population, and the environment.

The main objectives are to be developed by a group of persons responsible for the project or operation, e.g., this may be the project manager, project engineer or operations manager.

The entire study shall be carried out by a designated team whose terms of reference shall be precisely defined.

If the relevant project (operations) manager is familiar with this method, defining the target is easier.

Particular attention should be paid to the constitution of the working group and the timetable for the individual sessions of the working group.

The process of identifying individual risks is conducted in the form of questions and answers, which are recorded in standard tables. Table 4.4 gives an example of the causal

relationship of an identified risk caused by a negative event - higher refrigerant flow.

Table 4.4 Example of the causal relationship of an identified risk caused by an adverse event (Source: Oravec, 2011)

Deviation function	Cause	Consequence	Measure
Higher refrigerant flow	Regulatory The valve remained open	Reactor undercooled, reactant freezes	Lessons learned operators on the procedure
	Failure Regulator, valve remained open		

A risk matrix is used to quantify the variance. The matrix consists of 5 categories of probability and 5 categories of consequence of the value of the risk described by the respective word variables (Table 5.5).

Table 4.5 Risk matrix for HAZOP (Source: Oravec, 2011)

Probability/Consequence	10 <sup>0</sup>	10 <sup>-1</sup>	10 <sup>-2</sup>	10 <sup>-3</sup>	10 <sup>-4</sup>
Low	medium	medium	low	low	very low
Acceptable	medium	medium	medium	low	low
Higher	high	medium	medium	medium	low
High	very high	high	medium	medium	medium
Disastrous	unacceptable	very high	high	medium	medium

The HAZOP analysis results in findings that identify sources of risk and recommended actions. They are also recommendations for subsequent analysis of at-risk facilities. The results of the analyses, which relate to causes, effects, and measures for each deviation and for each node or section, are recorded in the form of a table. HAZOP is mainly applied in chemical plants. It uses knowledge of the operation and the possible deviations from the operating conditions. It provides the operator, at all stages of the lifetime of the plant, with a picture of the hazards and risks with respect to the selected indicator (safety, reliability, etc.).

#### 4.2.10. RATING METHOD

The point method started to be used in the Slovak Republic in 1996 after the adoption of the MIL STD 882 C standard. Currently, a version of [MIL STD 882 E](#) is freely available, which already includes the environmental dimension.

In the case of the scoring method, it is a semi-quantitative risk assessment procedure. Numerical point values are assigned in the probability and consequence scales and evaluated by a matrix.

When estimating the **probability of an accident**, it is based on:

- from past accident data or similar operations,
- from reliability statistics,
- from qualified expert estimates.

Factors that affect the likelihood of an accident must be considered:

- **measurable factors:**
  - duration of exposure to the hazard, time of exposure,
  - system parameters (machine speed, etc.)
  - the rate of occurrence of the event.
- **immeasurable factors:**
  - human factor - qualification, attention, stress, etc,
  - the level of maintenance activities,
  - the quality of inspection, revision, and testing activities,
  - the reliability and maintainability of security measures,
  - recognisability of the existence of the hazard, etc.

Determining the impact of the severity of individual factors on the frequency of a particular negative phenomenon is the content of the expert discussions of the assessors. At the same time, the assessors shall consider whether other factors, which may be dependent on the type of activity or type of technology, need to be considered in this classification.

It uses five degrees of probability (frequency), see Table 4.6.

*Table 4.6 Classification scheme for assessing the likelihood of a phenomenon occurring - point method (Source: Oravec, 2011)*

Value	Characteristics		
1	<b>Very low</b>	The occurrence of the phenomenon almost excluded.	An almost impossible threat
2	<b>Low</b>	Occurrence of the phenomenon unlikely or possible.	A very rare threat
3	<b>Medium</b>	The phenomenon occurs sometimes during the lifetime of the equipment or activity.	A rare threat
4	<b>High</b>	The phenomenon occurs several times during the lifetime of the equipment or activity.	Temporary threat
5	<b>Very high</b>	The phenomenon will arise very often	Continuous threat

**The consequence of an accident** expresses the degree, severity of possible damage, harm. When estimating the consequence of an accident, it should be based on:

- the severity of the accident or injury - fatal, serious, other accident, occupational disease,
- the extent of the damage - one person, several persons, material damage.

Factors that affect the likelihood of an accident must be considered:

- **measurable factors:**
  - type of injury - other, severe, fatal,
  - the number of people at risk,
  - the financial loss including all costs of restoring the operating condition,



- system parameters (height of the workplace, weight of the load to be handled, speed of movement, etc.),
- **immeasurable factors:**
- the relationship between the hazard and its effect,
  - emergency measures, crisis plans,
  - the complexity of the technology or machinery.

The consequence of a negative phenomenon is classified according to the scoring method into one of four categories, see Table 4.7.

*Table 4.7 Classification scheme for assessing the consequence of a negative phenomenon - scoring method (Source: Oravec, 2011)*

Value	Characteristics	
1	<b>Negligible</b>	Less than minor injury, negligible system malfunction.
2	<b>Minor</b>	Minor injury, onset of occupational disease or minor system damage, financial loss.
3	<b>Critical</b>	Serious accident, occupational disease or extensive system damage, production losses, major financial losses.
4	<b>Catastrophic</b>	Death due to a work-related accident or complete destruction of the system, irrecoverable losses.

**The combination of the frequency parameter and the consequence of the negative phenomenon determines the value of the risk.**

According to the scoring method, a matrix can be constructed from the consequence categories and frequency classes.

**The resulting matrix** is the risk score as shown in Table 4.8.

*Table 4.8 Result matrix - point method (Source: Oravec, 2011)*

Consequence/Frequency	1	2	4	4
1	1	4	6	12
2	2	7	11	13
3	3	10	15	17
4	5	12	16	19
5	8	14	18	20

The highest risk value is achieved at very high abundance and catastrophic consequence and has been assigned a value of "20". The most favourable condition has a value of '1'. However, the matrix can also be constructed in another way and for the highest numerical value assigned to the highest risk.

In the following procedure, the numerical values of the risk should be classified, for example, into several groups (e.g., four) that characterise the **risk scale**. See Table 4.9.

Table 4.9 Risk scale - scoring method (Source: Oravec, 2011)

Value	Characteristics	
1 - 3	<b>Acceptable</b>	The system is safe, common procedures.
4 - 11	<b>Medium</b>	The system is safe subject to operator training, inspections, etc.
12 - 15	<b>Unwanted</b>	The system is unsafe - need for protective measures.
16 - 20	<b>Unacceptable</b>	The system is unacceptable - need for immediate protective measures, shutdown of the system.

### 4.3. COMPARISON OF RISK ANALYSIS METHODS

The comparison of security risk analysis methods is a complex process. When carrying it out, we must realize that each environment, system, object that we analyse has its own characteristics, properties and parameters. Respecting these differences, it is possible to state that there is no method that can be used in any environment or system without some modification and expect a correct result from it.

Each method has its advantages and disadvantages, its "pluses and minuses", see Table 4.10.

Table 4.10 Comparison of advantages and disadvantages of different risk analysis methods (Source: Author)

METHOD	ADVANTAGES	DISADVANTAGES
<b>SA</b>	<ul style="list-style-type: none"> <li>- time-tested, highly reliable method,</li> <li>- the systematicity of the method,</li> <li>- the choice between an informal approach (visual inspection) or a formal survey.</li> </ul>	<ul style="list-style-type: none"> <li>- increased requirements for the composition of the work team, which consists of experts from different professions,</li> <li>- the method is time-consuming for formal surveys,</li> <li>- administratively demanding method (lengthy procedure for applying the method).</li> </ul>
<b>CLA</b>	<ul style="list-style-type: none"> <li>- possible application in case of complex problems,</li> <li>- the possibility of using a large number of checklists,</li> <li>- the possibility to achieve completeness of information (collects all available information).</li> </ul>	<ul style="list-style-type: none"> <li>- the administrative complexity resulting from the method's property of achieving completeness of information.</li> </ul>
<b>WIA</b>	<ul style="list-style-type: none"> <li>- high reliability and efficiency of the method if it is developed by an experienced team of experts,</li> <li>- leverages the experience and knowledge of executive staff, not just management staff,</li> <li>- In addition to identifying the causes of the problem, it is also used to suggest measures to improve safety.</li> </ul>	<ul style="list-style-type: none"> <li>- the set-up of the pilot questions is not systematic,</li> <li>- high degree of subjectivity, dependence on the experience and expertise of the team of experts.</li> </ul>
<b>PHA</b>	<ul style="list-style-type: none"> <li>- The method can be applied even at an early stage of design,</li> </ul>	<ul style="list-style-type: none"> <li>- is focused only on hazard detection, it does not provide suggestions for action against hazards,</li> </ul>

METHOD	ADVANTAGES	DISADVANTAGES
	<ul style="list-style-type: none"> <li>- the basic material required is not content-intensive,</li> <li>- is applicable to a wide range of issues.</li> </ul>	<ul style="list-style-type: none"> <li>- the estimation of accidents is only approximate, for this reason the frequencies of occurrence of accidents and their consequences are classified only within certain ranges.</li> </ul>
<b>FMEA</b>	<ul style="list-style-type: none"> <li>- is applicable to different systems as well as their combinations (wide range of method application),</li> <li>- High efficiency ( if applied to key elements of the system that cause the whole system to malfunction).</li> </ul>	<ul style="list-style-type: none"> <li>- It does not consider human errors and actions, nor software bugs,</li> <li>- is limited to qualitative analysis only,</li> <li>- the complexity and time-consuming nature of the analysis process in the case of a large system,</li> <li>- all possible malfunctions are documented, even those that do not have serious consequences,</li> <li>- does not allow to analyse the functional links between the elements of the system.</li> </ul>
<b>FTA</b>	<ul style="list-style-type: none"> <li>- can be used for both qualitative and quantitative analysis,</li> <li>- its procedure allows to analyse arbitrary dependencies in the system as well as in its subsystems,</li> <li>- makes it relatively easy to find system vulnerabilities,</li> <li>- provides a concise, organized and clear description of possible faults inside the system, allowing easy recognition of the causal dependence of an undesirable condition.</li> </ul>	<ul style="list-style-type: none"> <li>- is mainly suitable for the analysis of complex, large systems,</li> <li>- if the fault trees are large, the process of verifying the constructed fault tree by conventional means is extensive (necessitating the use of computing).</li> </ul>
<b>ETA</b>	<ul style="list-style-type: none"> <li>- is suitable for application in all kinds of systems,</li> <li>- Although limited to quantitative analysis, its quantitative difficulty is small.</li> </ul>	<ul style="list-style-type: none"> <li>- Difficult to determine the limits to which depth it is appropriate to divide the system under analysis,</li> <li>- complex definition of the hierarchy of elements (determining which elements have a decisive contribution to the functionality of the whole system),</li> <li>- if the number of system elements describing a particular event is large, it is necessary to use computing.</li> </ul>
<b>HAZOP</b>	<ul style="list-style-type: none"> <li>- its structure and risk assessment method allows it to be widely used,</li> <li>- is applicable for the analysis of large industrial accidents as well as smaller complexes, down to the level of conventional plants.</li> </ul>	<ul style="list-style-type: none"> <li>- increased attention to the task force set-up and the timetable for each activity.</li> </ul>

The results of the comparison of selected risk analysis methods used in safety / security practice in terms of the predefined criteria are presented in Table 4.11.

The following scale was used to rate the degree of complexity:

- VM - degree of complexity VERY SMALL
- M - degree of complexity SMALL
- S - degree of complexity MEDIUM
- V - degree of complexity COMPLEX
- VV - degree of complexity VERY COMPLEX

Table 4.11 Comparison of methods according to defined criteria (Source: Author)

CRITERIA METHOD	Applicability (usability)	Time intensity	Professional complexity	Software complexity	Administrative complexity	Financial needs	Personnel needs	Information needs	Complexity of use
SA	M	C	VC	M	VC	S	C	C	M
CLA	M	C	C	S	VC	M	M	VC	S
WIA	C	S	C	S	S	C	C	M	S
PHA	VC	S	M	S	M	M	S	S	M
FMEA	VC	S	M	M	C	S	S	M	M
FTA	C	M	C	C*	M	M	M	C	C
ETA	VC	M	C	C*	S	M	M	C	C
HAZOP	VC	C	M	S	S	S	C	C	M

\* If the number of system elements describing a particular event is large, it is necessary to use computing.

\*\* Depending on whether an empirical-intuitive assessment of the risk as a whole or a careful consideration of individual risk parameters is used.

It considers that traditional methods of hazard and risk assessment (CLA, ...) are deficient in that they do not give a sufficient idea of the hazards that could occur in other possible situations.

The advantage of the PHA method, for example, is its simple and quick application in both existing and newly designed plants. It is flexible and can also be used by non-specialists. However, it does not give any information on how often individual cases may occur.

A basic assumption of the suitability of using the HAZOP method is that the design is developed for "normal" operating conditions, so that hazards or operational problems can only occur if these conditions change.

When using FMEA failure impact analysis and its consequences, deficiencies may be evident in terms of component lifetime, failure to handle multiple failures, and the effect of hidden defects. There are several operational operations that differ from each other. It may

therefore happen that the record of failures and consequences grows very large (record for start-up, shut-down, normal operation, etc.). Perhaps the biggest disadvantage of this method is that all possible component failures are studied and documented, even those that do not have serious consequences.

Fault tree analysis (FTA) is one of the most used methods for evaluating the reliability of systems, but it is also not comprehensive. This procedure provides a concise, organized, and clear description of the possible faults within a system that may lead to a predefined adverse event. It is these characteristics that guarantee the prospectivity of this method. Thus, by analysing the fault tree, we create a clear and systematic visual representation from which it is clear briefly how each of the basic elements contributes to the system's failure rate.

The FTA method can be used for both qualitative and quantitative analysis, makes it relatively easy to find "weak points" in the system and reveals aspects important from a reliability point of view. It is a well-established, well-developed procedure useful in the design and operation of technological processes and is also why it is found in all modern approaches to risk assessment.

It is clear from the above facts that neither in our country nor in the European Union there is a universal tool for a unified solution to the problem of major accident risk assessment.

#### **4.4. SELECTION OF AN APPROPRIATE RISK ANALYSIS METHOD**

The following criteria can be selected for comparing risk analysis methods:

- applicability (usability),
- time-consuming,
- professional complexity,
- software complexity,
- administrative complexity,
- financial intensity,
- staffing requirements,
- information intensity,
- complexity of use.

**Applicability (usability) of the method** expresses the possibility of applying the method in individual systems, subsystems, environmental conditions, indicates the scope of application of the method, considers the size and complexity of the system, the suitability of using the method at individual stages (design, operation, disposal of the system...) and the level of risk management (risk management).

**The time requirements of the method** represent the time requirements of the entire risk analysis process, i.e. the time requirements in the process of obtaining relevant information about the analysed system, environment, in the process of collecting, sorting, transferring and

using this information, the time requirements for the preparation of the basic documentation, for the identification and assessment of individual risks, threats, hazards, the time requirements for the implementation of a specific risk analysis method, for its evaluation and documentation.

**The technical difficulty of the method** considers the difficulty or otherwise of the specific method on the expertise, knowledge, skills, practical experience of security managers performing security risk analysis.

**The software complexity of the method** results from the necessity to use information technologies and specialised software in the process of security risk analysis. Most often, the use of software is necessary in the environment of information systems security, protection of classified information and in the environment of technical and technological security.

**The administrative complexity of the method** reflects the documentation detail requirements in the risk analysis process, considers the size and complexity of the system being analysed (system with a large number of elements logically increases the administrative complexity of the method as it requires a detailed analysis of each important element of the system under analysis).

**The financial complexity of the method** represents a requirement for the use of funds that must be available in the risk analysis process. Also, the larger and more complex the system, the more modern and sophisticated the software, the greater the financial requirements. The financial requirements are particularly high in information systems security and the protection of classified information.

**The staffing intensity of the method** results from the nature of the individual methods within the staffing framework. There are methods in which one security manager can provide the entire risk analysis process, but also methods in which it is necessary to assemble a quality team of experts (e.g., HAZOP).

**The information intensity of a method** considers the need for relevant information in terms of both quality and quantity (large and complex systems). Information intensity is influenced by the way information is acquired, stored, sorted, transferred, and used in practice. For example, the analysis using control records allows for completeness of information, i.e., the method has a high information intensity.

**The complexity of the method application** is a comprehensive summary of the difficulty of the method, which includes all the above criteria. The simplicity or complexity of the method thus results from the applicability (usability) of the method in individual environments and systems, the time demand, the demand on the expertise and knowledge of managers, the need to use specialised software, the administrative demand, the requirements for financial resources, the personnel demand and information needs.

In the process of applying risk assessment methods to a particular system, it is necessary to consider all the strengths and weaknesses of the chosen method. Often it is necessary to combine two or three methods to objectively assess the whole problem and achieve a correct result.

Based on the comparison of methods according to the selected criteria, the following recommendations are important for the selection and use of the optimal risk analysis method in the process of designing a security system:

- in the design process, the parameters to be monitored in the risk management system must be defined without delay, at all levels of risk management,
- it is also necessary to define the levels of structure at which risk assessment methods are to be applied,
- for operational risk management at the lowest levels of the monitored system, it is appropriate to use methods that do not require expertise (but must allow the assessor to consider the specificities of the monitored operation),
- in intermediate risk management, it is necessary to have methods in place to establish the basis for risk management,
- verification of the completeness of the information on the system under assessment is necessary and very important,
- the scale of the problem to be studied is largely determined by the amount of funding that must be made available,
- an important factor in this context is also the time complexity of the problem to be solved,
- it is necessary to consider the expertise, knowledge and practical experience requirements of the security managers carrying out the risk analysis,
- It is advisable to first use methods that can reveal the weaknesses of the system being analysed (e.g., FTA method) and then analyse these weaknesses using a more detailed (specific) method.

## **CONCLUSIONS**

The choice of the appropriate method for risk analysis depends on the level of detail and precision of the results we want to achieve as output from the analysis. Older risk analysis methods tended to be based on simple or preliminary risk assessment. The methods currently applied in the industry are more complex in nature, their real application is of a collective nature (group of experts), which leads to better identification of threats, their potential impacts, as well as effective preventive, repressive and remedial measures.

## REFERENCES

- [1]. FROHNHOEFER, R.W. 2019. *Risk Assessment Framework: Successfully Navigating Uncertainty*. PPC Group, LLC, 221 p.
- [2]. FUCHS, P., VALIŠ, D. 2004. *Metódy analýzy a řízení rizika / Methods of risk analysis and risk management*. Liberec: TU in Liberec.
- [3]. KANDRÁČ, J. 2000. *Metodický postup na hodnotenie rizík nebezpečných prevádzok a štúdia o podnikoch v Slovenskej Republike / Methodological procedure for risk assessment of hazardous plants and study of companies in the Slovak Republic*. Bratislava: RISK CONSULT, spol. s. r. o., 63 p.
- [4]. ORAVEC, M. 2011. *Vybrané kapitoly z manažérstva rizík 1: Základy teórie rizík / Selected chapters from risk management 1: Introduction to risk theory*. Košice: Equilibria, 168 p.
- [5]. ŠIMÁK, L. 2006. *Manažment rizík / Risk management*. Žilina. Available online: [http://fsi.uniza.sk/kkm/files/publikacie/mn\\_rizik.pdf](http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf)
- [6]. YOE, CH. 2019. *Principles of Risk Analysis: Decision Making Under Uncertainty*. CRC Press, 848 p.



### QUESTIONS

1. Define the difference between qualitative, semi-quantitative and quantitative risk analysis methods.
2. Which methods are based on the use of item control records?
3. Define the risk analysis processing procedure using the FTA method.
4. What is specific about the FMEA method?
5. Which methods are based on brainstorming?



## 5. METHODS FOR REDUCING AND MONITORING SAFETY AND SECURITY RISKS

The prerequisite for early and successful identification of possible sources of threat and then their quantitative, qualitative, and causal analysis is an effective monitoring system of selected security parameters of the system under consideration, as well as other environmental factors.



*The aim of the chapter is to understand the nature and methods used to reduce and monitor the safety / security risks.*

### 5.1. RISK REDUCTION AND MONITORING

**Risk mitigation** is closely linked to preparing to prevent or manage risk. This consists of:

- taking preventive measures to reduce the impact of risk factors or to eliminate them (actively or passively influencing them). In essence, it is about preventing or mitigating the occurrence of an unexpected negative phenomenon, either by acting on the potential source of the threat or by strengthening the resilience and reducing the vulnerability of the system in question.
- taking measures to actively influence the possible course of an undesirable phenomenon, preparing emergency and other crisis plans, including the preparation of measures to restore the function of the system.
- in taking mitigation and recovery measures if an unexpected negative phenomenon cannot be prevented, and we must prepare to deal with the consequences and to restore the system.
- identifying unacceptable risks and developing systemic measures to increase their acceptability.

In most cases in security practice, the risk falls predominantly on the company, only to a small extent on the state. Thus, if the decisive risk is on the company, it is obvious that it must protect itself against the action of possible risk factors, i.e., the company must have a risk (security) policy in place. This risk policy can be defined as an activity that includes:

- risk identification (causes, types),
- measuring the magnitude and determining the degree of risk,
- quantifying the impact of risk on business activity,
- risk protection.

Risk reduction protection (practices) is possible in two ways:

- **procedures to remove or eliminate the causes of risk:** these are activities aimed at acting on the actual causes of risk to reduce the likelihood of risk situations with adverse consequences occurring and to reduce the magnitude of adverse effects. This way of protecting against risk is often referred to as an offensive approach to risk (eliminating a competitor by economic, political force - use of force, risk transfer).
- **practices aimed at reducing the indirect consequences of risk:** these are activities aimed at reducing the adverse effects of risk to a certain, socially, and economically acceptable level. These activities and practices are certain remedial measures and are often referred to as defensive approaches (insurance, diversification, etc.).
- If we evaluate the above risk mitigation options, we see that in most cases the aim is not to minimise risk but to reduce it to a certain economic level. It is important to note that we still need to consider the implications of risk protection holistically as well, that greater security requires additional resources, i.e., it cannot be obtained for free.

**Risk monitoring** means continuous checking, surveillance, critical observation or status determination to detect a change in the desired or expected level. Reviewing is an activity undertaken to determine the suitability, adequacy, and effectiveness of risk management for achieving stated objectives.

Both monitoring and reviewing can be applied according to ISO Guide 73:2009 to:

- the risk management structure,
- the risk management process,
- risk itself,
- risk management.

The course of the risk assessment highlights contexts and other factors that can be expected to change over time and that could alter or invalidate the risk assessment.

The risk monitoring process should provide assurance that appropriate arrangements are in place for the organisation's activities and that the organisation's risk management procedures are understood and followed. Results of monitoring and review:

- can be integrated into the overall performance management of the organisation, and into external and internal measurement and reporting,
- are to be recorded, communicated internally and externally as appropriate, and used as inputs to the review of the risk management structure.

## 5.2. REDUCING AND MONITORING SAFETY / SECURITY RISKS

**The process of risk minimisation** from the perspective of crisis management is very diverse and clearly depends on the nature of the specific risk, the likelihood of the crisis phenomenon it may cause and its expected negative consequences.

The system consists of a set of measures aimed at preventing the occurrence of undesirable (preventive measures), from the perspective of crisis management, extraordinary events, as well as minimising the impact of such events, most often based on determining the potential impact of the most serious scenarios of their development. These include measures relating to the protection of life and health of persons at the site of such an event or in the vicinity, the protection of property or the reduction of material damage and, of course, the protection of the environment itself.

The whole process of risk minimisation is based on the knowledge of potential threats, the results of the analysis and the risk assessment. It is one of the key tasks of risk management.

Risk minimisation (reduction) is carried out:

- ***through the pursuit of an active anti-crisis policy:***
  - the appropriate structure of the security strategy to be adopted and its purposeful implementation,
  - highlighting positive development trends,
  - by creating the conditions to respond flexibly to current threats,
  - continuously assessing both external and internal security conditions and taking them into account in decision-making processes,
  - by creating an efficient and economic organisational structure,
  - effective staff work and continuous staff training,
  - by respecting international and domestic legal norms and practices, but also moral principles.
- ***using specific methods*** (Table 5.1):
  - **diversification of risk,**
  - **risk reduction/mitigation:**
    - addressing the causes of risk,
    - reducing the adverse consequences of risk,
  - **risk retention:**
    - conscious and unconscious,
    - voluntary and involuntary,
  - **transfer (relocation) of risk,**
  - **sharing risks,**

- **flexible/flexible system action**,
- **the creation of reserves** (e.g., state material reserves),
- **continuous refinement of information** (e.g., monitoring and warning systems),
- **Risk avoidance** (implementing countermeasures that either prevent unwanted events from occurring or prevent such events from having a negative impact),
- **process optimisation** (use of operational analysis methods).

Table 5.1 Risk reduction method (Source: Šimák, 2006)

Probability of occurrence	Anticipated consequence				
	Catastrophic	Critical	Significant	Minor	Negligible
Very large	Risk reduction <sup>3</sup>	Risk reduction	Avoiding risk	Insurance against risk	Transfer of risk
Great	Risk reduction	Avoiding risk	Insurance against risk	Transfer of risk	Diversification
Medium	Avoiding risk	Insurance against risk	Transfer of risk	Diversification	Flexible procedure
Small	Insurance against risk	Transfer of risk	Diversification	Flexible procedure	Risk retention
Very small	Transfer of risk	Diversification	Flexible procedure	Risk retention	Risk retention

Next, there is the decision-making flowchart (Figure 5.1) for the application of the method for minimising risks associated with natural disasters and accidents (Šimák, 2006).

<sup>3</sup> Risk reduction (measures to reduce vulnerability); Risk avoidance (cessation of risk-taking activity); Risk transfer (e.g. insurance); Risk retention (risk remains residual).

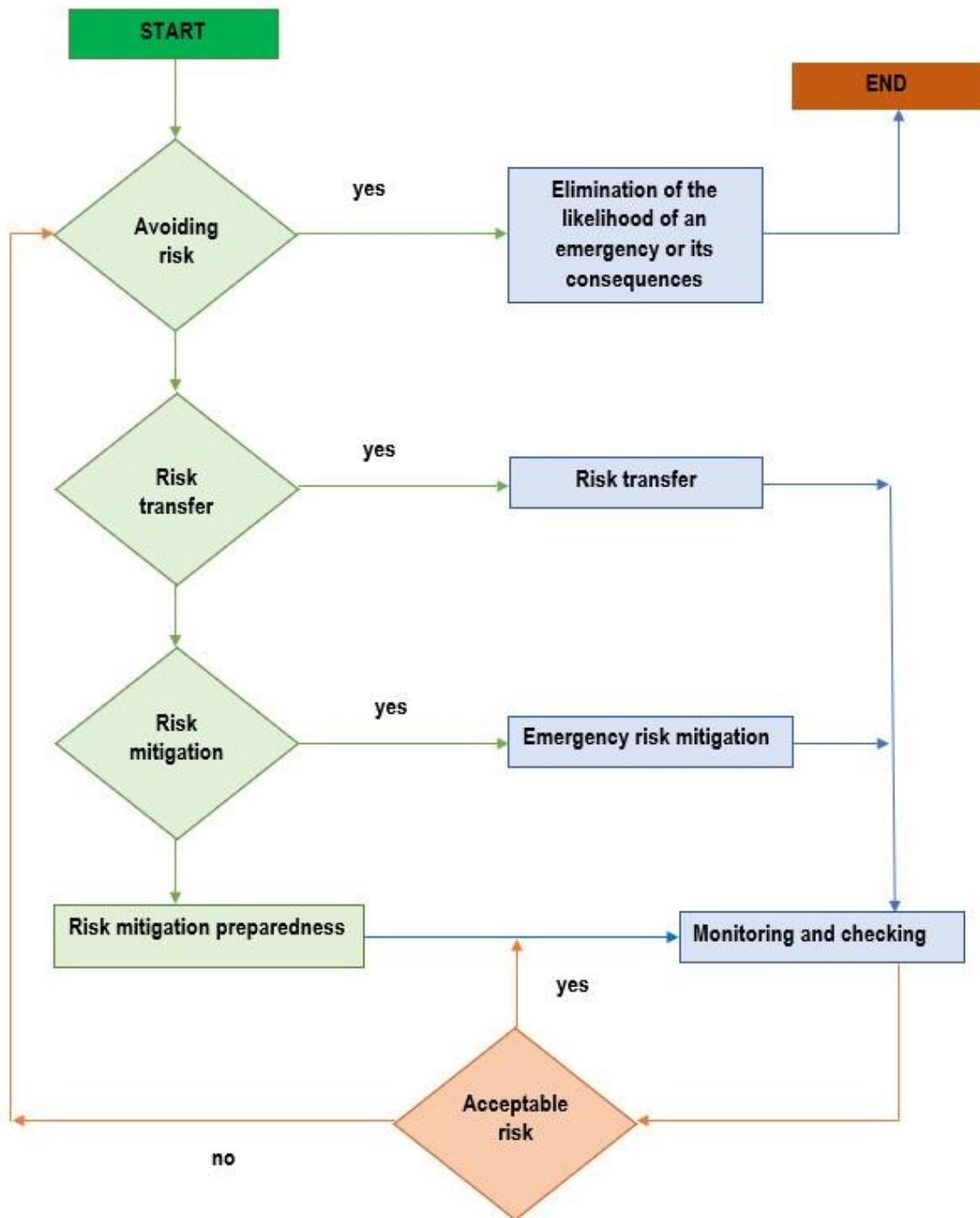


Figure 5.1 Methods of minimizing risks associated with natural disasters and accidents  
(Source: Šimák, 2006)

The diagram in the figure describes a comprehensive approach to reducing security risks with the aim of preventing crisis situations and ensuring a socially acceptable level of security for the population, property, and the environment.

**Risk monitoring** is based on regular operational monitoring of a specific risk by the risk owner and assessment of measures to manage it.

In this respect, the main objective from a risk monitoring perspective is to set up controls to ensure that the risk is prevented by implementing them on a regular basis.

In practice, several risk management and monitoring systems are used, linked to alert generation capabilities, often also linked to an automatic triggering system for warning and notification. These are based on information-based, less geo-information-based systems.

## CONCLUSIONS

Several methods are used to reduce and monitor risks. These are chosen depending on the type of risk and on the nature of the subject and object of the risk. Other methods are chosen for risk reduction in relation to investments and others in security of persons and property.

In terms of reducing and monitoring safety risks, we choose specific methods in relation to a specific area, i.e., fire protection, occupational health and safety, protection of the population or prevention of major industrial accidents.

From the perspective of company security, the optimal approach from the point of view of sustainability seems to be a combination of security risk assessment together with business risks (investment risks) and the subsequent synthesis and implementation of risk reduction measures simultaneously in both spheres of the company.

## REFERENCES

- [1]. BLOKDYK, G. 2021. Risk Monitoring Complete Self-Assessment Guide. 5STARCooks, 308 p.
- [2]. DRÁBEK, J., PITTNEROVÁ, I. 2001. Investment projects and the cost of capital. Zvolen: Matcentrum, 250 p.
- [3]. DRÁBEK, J., POLÁCH, J. 2008. Real and financial investing of firms. Zvolen: Technical University of Zvolen, 272 p.
- [4]. ISO Guide 73:2009, Risk management.
- [5]. JENSEN, R.C. 2019. Risk-Reduction Methods for Occupational Safety and Health. Wiley, 469 p.
- [6]. POLÁCH, J., POLÁCH, J., DRÁBEK, J., MERKOVÁ, M. 2012. Real and financial investments. Prague: C. H. Beck, 2012. 263 p.
- [7]. SADGROVE, K. 2016. The Risk Mitigation Handbook: Practical steps for reducing your business risks. Routledge, 261 p.
- [8]. ŠIMÁK, L. 2006. Risk management. Žilina. Available online: [http://fsi.uniza.sk/kkm/files/publikacie/mn\\_rizik.pdf](http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf)
- [9]. THOMPSON, E.E. 2018. The Insider Threat: Assessment and Mitigation of Risks. Auerbach Publication, 232 p.



### QUESTIONS

1. What is the main objective of the risk monitoring process?
2. Describe methods of minimising or reducing risks?
3. What are the risk minimisation measures?
4. What do you mean by risk transfer?
5. What do you mean by risk diversification?

## 6. FIRE RISK MANAGEMENT IN THE SLOVAK REPUBLIC

Fire risk management can also be seen as a separate management activity, especially for legal entities and natural persons - entrepreneurs who, due to the nature of their business activities and the technologies used, are not among the major threats. This activity can be carried out at the operational level by fire protection technicians in their premises and at the tactical and strategic level by fire protection specialists.



*The aim of the chapter is to understand the principles and objectives of risk management in the field of fire protection and to be familiar with fire risk assessment procedures based on the provisions of current legislation in this area.*

### 6.1. BACKGROUND OF FIRE PROTECTION IN THE SLOVAK REPUBLIC

Under Act No. 314/2001 Coll. on Fire Protection as amended, the Ministry of the Interior of the Slovak Republic (Mol SR), as the central state administration body, manages the performance of state administration in the field of fire protection, performs state fire supervision and main fire supervision, and issues generally binding legal regulations to ensure the protection of fire protection.

The implementation of state fire supervision is determined for individual state administration bodies in the field of fire protection in a differentiated manner, while the Ministry of the Interior of the Slovak Republic determines legal entities and natural persons - entrepreneurs in which the competent regional state authority performs fire inspections.

It is important to note that state fire supervision is a form of specialised control, which ascertains whether the actual state of fire protection in the inspected entity corresponds to the state required by the fire protection regulations. This inspection may also be based on an internal preventive inspection carried out by a fire protection technician, or a preventive inspection carried out by the founder or promoter of the legal entity, who must comply with their obligations under the abovementioned Act. The fulfilment of fire protection obligations is ensured by the holder of the licence for the operation of nuclear installations within the meaning of Article 4 and Article 5 of Act No 314/2001 Coll., as amended. From the point of view of the Act in question, the requirements for fire prevention of buildings are formulated not only in Decree of the Ministry of the Interior of the Slovak Republic No. 121/2002 Coll. on fire prevention, as amended, but also in other decrees with technical content: Decree of the Ministry of the Interior of the Slovak Republic No. 124/2000 Coll. laying down the principles of fire safety in activities with flammable gases and combustion-promoting gases,

Decree of the Ministry of the Interior of the Slovak Republic No. 719/2002 Coll, No 726/2002 Coll., laying down the characteristics, conditions of operation and regular inspection of portable fire extinguishers and mobile fire extinguishers, Decree No 726/2002 Coll. of the Ministry of the Interior of the Slovak Republic, laying down the characteristics of electric fire alarms, conditions of their operation, Decree No 726/2002 Coll., laying down the characteristics of electric fire alarms, conditions of their operation 94/2004 Coll., laying down technical requirements for fire safety in construction and use of buildings, as amended, Decree No 96/2004 Coll., laying down principles of fire safety in the handling and storage of flammable liquids, heavy fuel oils and vegetable and animal fats and oils, Decree No 611/2006 Coll., laying down technical requirements for fire safety in construction and use of buildings, as amended

No 699/2004 Coll. on the provision of water for extinguishing fires in buildings, as amended by Decree No 562/2005 Coll., Decree No 169/2006 Coll. of the Ministry of the Interior of the Slovak Republic

No. 478/2008 Coll. on the characteristics, specific conditions of operation and regular inspection of fire extinguishing systems, Decree of the Ministry of the Interior of the Slovak Republic No. 478/2008 Coll. on the characteristics, specific conditions of operation and regular inspection of fire dampers, as well as other decrees.

Legal entities and natural persons-entrepreneurs are also obliged to participate in the cooperation, creation of conditions and performance of tasks in the field of fire protection within the scope of their competence.

Procedures and methods of fire protection assessment are currently based primarily on the laws and implementing decrees of the Ministry of the Interior of the Slovak Republic in this area and technical standards for the design, planning and operation of production and non-production buildings. Based on analyses of fire and fire or explosion hazards, using knowledge of from developed European countries, the harmonisation of technical standards is also being implemented in the Slovak Republic and regulations and their approximation with the regulations of the European Union. In the field of fire protection, new generally binding legislation, in particular decrees with technical content, is thus being drawn up, which are followed by new technical standards. This legislative process also affects the management, control and evaluation procedures applied by the fire wardens of the State Fire Service of the Slovak Republic.

## **6.2. RISK ASSESSMENT**

Risk assessment procedures for fire protection are defined in two pieces of legislation. One of them is the Decree of the Ministry of the Interior of the Slovak Republic No. 611/2006 Coll.



on firefighting units as amended and the other is the Decree of the Ministry of the Interior of the Slovak Republic No. 94/2004, which establishes technical requirements for fire safety in the construction and use of buildings.

### **6.2.1 RISK ASSESSMENT IN ACCORDANCE WITH DECREE NO. 611/2006 OF THE MINISTRY OF HEALTH OF THE SLOVAK REPUBLIC**

Pursuant to the Decree of the Ministry of the Interior of the Slovak Republic No. 611/2006 Coll. on firefighting units as amended, a **Fire Hazard Analysis** is prepared for selected legal entities and natural persons - entrepreneurs.

The fire hazard analysis is processed by a legal entity or a natural person - entrepreneur based on a decision of the regional directorate of the Fire and Rescue Corps.

The result of the analysis is:

- Assessment:
  - the risk of fires in the premises or on the premises of the legal person and natural person - entrepreneur,
  - conditions for effective intervention and evacuation of persons and property,
  - equipping a fire section, building or space with fire protection equipment,
  - the capacity of water sources for firefighting and cooling.
- Determination:
  - the largest area of the predicted fire by calculation,
  - the verified arrival time of the first reinforcement firefighting units,
  - the quantity and type of extinguishing agent required to fight the fire and for cooling,
  - the minimum number of the firefighting unit needed to effectively fight the expected fire as well as the requirements for its material and technical equipment,
  - the shortest time to take effective action on a suspected fire.

If the changed conditions in the premises of the legal entity or natural person - entrepreneur also affect the changes in the fire hazard, the legal entity or natural person - entrepreneur shall adjust the analysis according to the actual situation within three months after the changes have occurred and submit it to the regional directorate for approval.

#### **✓ FIRE HAZARD ANALYSIS PROCEDURE AND ITS CONTENTS**

When processing the fire hazard analysis, a single fire compartment, building or premises in which a legal entity or a natural person - entrepreneur carries out activities related to the subject of business or a set of objects that are connected to each other by technological equipment and transport objects shall be assessed. The analysis shall be based on the assumption that, in the case of a legal person or natural person-entrepreneur, there cannot be

more than one fire at the same time, and that the staffing levels or the number of firefighters and firefighting equipment applicable to the designated premises are also sufficient to deal with a fire in each of the other premises of the legal person or natural person-entrepreneur.

The analysis shall consider the fire compartment, building or space in which:

- there is a **high fire risk and a difficult situation when carrying out intervention and evacuation of** persons and property, or **flammable liquids of class I and II hazard class or flammable gases** prevail in the technological equipment of the fire compartment, or for other reasons there is a difficult situation when carrying out intervention and evacuation of persons and property.
- there is a **high risk of fire** according to the type of activities carried out.

A high fire risk exists if the average fire load, including the concentrated fire load, is greater than  $180 \text{ kg}\cdot\text{m}^{-2}$  and the probability of fire occurrence and spread  $p_1 > 2$  or the flammable substance coefficient is greater than 0,9.

**A complex situation when carrying out intervention and evacuation of** persons and property in a fire section, building or area is especially when:

- are complex and cluttered in layout,
- cannot be ventilated of combustion products without the aid of mobile extraction equipment, the entry or operation of firefighters without notification of the special operating regime would put their lives at risk,
- the design of building structures or technological equipment is difficult to discern and allows the easy spread of fire.
- hazardous substances are present,
- the design of escape routes in terms of quality, number, length, and width does not comply with the generally binding legal regulations in force at the time of the construction or its modification,
- evacuation by alternative escape options or special firefighting equipment is foreseen,
- persons are in the premises in an unconscious state or persons with reduced mobility are in the premises.
- there is a risk of fire spreading to neighbouring properties due to the spacing distances.

The analysis consists of two parts, whereby:

- **Part one:** describes the factual situation in the premises or premises of the legal person or natural person - entrepreneur, as well as other entities located in its premises or premises, in terms of the overall provision of fire protection, including the assessment of the fire risk in individual fire compartments, premises or premises, their equipment with fire protection equipment and the provision of water for extinguishing fires; this section shall also identify the fire compartment, building or space with the most unfavourable rating,

- **second part:** contains a calculation of the number of staff or members required to the firefighting unit to carry out effective firefighting action in a designated building or set of buildings, as well as the need for firefighting equipment, extinguishing agents, and material resources.

When the analysis is carried out in individual fire compartments, buildings or premises, the following is considered:

- **a combustible substance**, considering its design quantity or actual quantity in stores, technical installations and technological installations, physical properties, chemical properties, fire characteristics.
- **technology**, considering:
  - documentation of the technology, e.g., opinion by a fire protection specialist, use of the analysis procedure according to the technical standard and the consequences of failures, use of the fault tree analysis according to the technical standard,
  - representative failure conditions of the technology according to the technical standard, for example, failure conditions caused by corrosion, misuse or lack of maintenance and resulting hazardous locations from which the substance being processed, used, or generated may migrate from the working area of the technology to another area of the technology where its presence is undesirable or to an area outside the technology,
  - application of planned maintenance and diagnostic maintenance of the technology according to the technical standard,
  - the method of starting and stopping the operation of the technology,
  - the use of inerting environments in which flammable substances are present in the technology; the use of phlegmatization processes.
- **the use of fire-fighting equipment**, water curtains or vapour curtains; the capacity of water sources for firefighting,
- **the level of control and monitoring systems of the technology** and their impact on the reliability of the technology,
- **the use of technology protection measures**, such as safety devices to protect components from destruction when pressure builds up,
- **initiating sources in technology**, e.g., hot surfaces, mechanical sparks, static electricity, atmospheric electricity, electrical equipment,
- **the development of the fire**, the paths of its spread, especially on the surface of solid combustible substances, combustible liquids in the technology or in the space outside the technology and the possibility of spreading the fire to adjacent fire sections, objects or spaces.

The calculation of the necessary number of firefighting unit personnel to carry out an effective firefighting intervention for a designated fire section, building or area, as well as the necessary firefighting equipment, extinguishing agents and material means shall be carried out in accordance with the applicable methodology.

The calculation establishes:

- the expected development of the fire due to the presence of combustible substances and the possibility of its spread to neighbouring fire compartments or objects.
- the largest area of the expected fire in the fire compartment,
- determination of the shortest expected time of free spread of the fire,
- the quantity and type of extinguishing agent required to fight the fire at the time of termination of the free spread of the fire,
- the quantity and type of extinguishing agent required to fight the fire for the normative fire-fighting time,
- the number of personnel or members, equipment with basic and special fire-fighting equipment and means of delivery of the required extinguishing agent to the destination,
- the yield of water sources usable for firefighting and cooling,
- the estimated number of evacuees and the conditions of evacuation,
- the necessary personal protective equipment to ensure the highest possible protection of employees,
- the possibility of helping by firefighting units with sufficient personnel or members and with sufficient firefighting equipment.

**Checklist (CLA)** and **Security Audit (SA)** methods are used to **identify risks**. **Fault Tree Analysis (FTA)** is used to **assess the level of risk in** the processing of the Fire Hazard Analysis.

## **6.2.2. RISK ASSESSMENT IN ACCORDANCE WITH DECREE NO. 94/2004**

Decree No. 94/2004 of the Ministry of the Interior of the Slovak Republic establishes technical requirements for fire safety in the construction and use of buildings.

The Decree defines the so-called fire risk as "*the probable intensity of a fire in a fire compartment or part thereof*".

The fire risk for a fire compartment or part of a fire compartment is specified in the technical standard.

The fire risk is expressed as:

- the equivalent duration of the fire,
- or the stored materials index and the economic risk index,
- or the design fire load.

## CONCLUSIONS

Fire hazard analysis, risk assessment documentation is documentation that requires the knowledge and experience of an expert in the field of fire protection. Its preparation is one of the competences of a **fire protection specialist** who has professional competence in this field.

## REFERENCES

- [1]. KANDRÁČ, J., HUSÁRČEK, J., CIGÁNEKOVÁ, M. 2020. *Požiadavky na zabezpečovanie ochrany pred požiarmi a protipožiarnej bezpečnosti jadrových zariadení z hľadiska jadrovej bezpečnosti / Requirements for ensuring fire protection and fire safety of nuclear installations from the point of view of nuclear safety*. Bratislava: ÚJD SR, 48 p.
- [2]. Decree of the Ministry of the Interior of the Slovak Republic No. 611/2006 Coll. on firefighting units as amended.
- [3]. Decree No. 94/2004 of the Ministry of the Interior of the Slovak Republic, laying down technical requirements for fire safety in construction and use of buildings.



### QUESTIONS

1. Define the fire risk management objective.
2. List the legislation governing the field of risk assessment in the field of protection from fires?
3. Who has the competence to prepare a Fire Hazard Analysis?
4. Which risk analysis methods are used by legal entities in the risk assessment process fire?
5. Define the term 'fire risk' and how to calculate it?

## 7. OCCUPATIONAL HEALTH AND SAFETY RISK MANAGEMENT IN THE SLOVAK REPUBLIC

Current occupational safety science recognizes that there is no absolute safety. Every activity, every piece of equipment, carries some risk, some degree of hazard. Safety at work is influenced primarily by the risks that arise from work processes, are caused by machinery, equipment or arise from the working environment or working conditions.



*The aim of the chapter is to understand the background and objectives in the field of risk management in relation to ensuring an acceptable level of safety at work and in the working environment, and to know the methods used to analyse safety risks, as well as the procedures for their reduction.*

### 7.1. INTRODUCTION TO THE OCCUPATIONAL HEALTH AND SAFETY IN THE SLOVAK REPUBLIC

Occupational safety and health can be characterized as a set of measures, principles, attitudes, behaviours, and activities that help eliminate adverse consequences of work. The term 'Occupational Health and Safety' is also known by the acronym OHS, but its content and application are much broader than the meaning of these words suggests.

In general, safety is inversely proportional to risks. This means that the greater the risks arising from a work activity, the less safe the activity is. Conversely, the smaller the risks, the safer the activity. The purpose of carrying out a risk assessment in the workplace is to provide a basis for the employer to establish measures to protect the safety and health of his employees which will prevent, eliminate, or minimise the exposure to potential risks.

According to the Constitution of the Slovak Republic, an employee has the right to protection and safety at work and the employer is obliged to fulfil this right. The most important European legislation concerning risk assessment is the Framework Directive 89/391/EEC. This Directive is transposed into national legislation. It requires that occupational safety be ensured regarding all work-related aspects. This means that the protection of employees includes conditions for satisfactory and dignified work, well-being at work, social protection for employees, favourable working relationships, but also the protection of material values, the working environment, and the environment. Therefore, factors such as stress, workload, monotony of work, working conditions, employment and labour relations, psychosocial factors, equal opportunities (non-discrimination), fair remuneration, appropriate workplace facilities, etc. must also be addressed in the context of employee protection.

Occupational health and safety is regulated by legislation based on EU legislation and ILO Conventions. It is also supported by technical standards, recommendations, principles, principles, and strategies of international institutions. However, the new approach requires more than just compliance with regulations to ensure OSH. It requires active assessment of occupational risks and the adoption of adequate measures to protect workers, with responsibility for OSH being placed primarily on the employer.

Occupational safety and health is also a key concern and responsibility of the state in its role to promote the protection of employees at work, social justice, strengthening the functioning of the labour market, eliminating losses from occupational accidents, occupational diseases and industrial accidents, promoting satisfactory working conditions and increasing the efficiency and productivity of work, competitiveness in the market with an impact on the prosperity of company and the overall development of the country.

The Slovak Republic systematically regulates this area through legislative measures and their enforcement through labour inspection and other control bodies.

Selected legislation to ensure health and safety at work:

- Act of the National Council of the Slovak Republic No. 311/2001 Coll., the Labour Code as amended.
- Act of the National Council of the Slovak Republic No. 124/2006 Coll. on Occupational Health and Safety and on Amendments and Additions to Certain Acts, as amended.
- Act of the National Council of the Slovak Republic No. 125/2006 Coll. on labour inspection and on amendment and supplementation of Act No. 82/2005 Coll. on illegal work and illegal employment and on amendment and supplementation of certain acts, as amended.
- Act of the National Council of the Slovak Republic No. 355/2007 Coll. on the protection, promotion, and development of public health and on the amendment and supplementation of certain acts, as amended.
- Act of the National Council of the Slovak Republic No. 377/2004 Coll. on the Protection of Non-Smokers and on Amendments and Additions to Certain Acts, as amended.
- Act of the National Council of the Slovak Republic No. 280/2006 Coll. on compulsory basic qualification and regular training of certain drivers, as amended.
- Act of the National Council of the Slovak Republic No. 8/2009 Coll. on Road Traffic and on Amendments and Additions to Certain Acts, as amended.
- Act of the National Council of the Slovak Republic No. 51/1988 Coll. on mining activities, explosives and state mining administration as amended.
- Act of the National Council of the Slovak Republic No. 67/2010 Coll. on the conditions for placing chemical substances and chemical mixtures on the market and on amending and supplementing certain acts (Chemical Act), as amended.

- Act of the National Council of the Slovak Republic No. 128/2015 Coll. on prevention of major industrial accidents and on amendment and supplementation of certain acts, as amended.
- Government Regulation No. 272/2004 Coll., establishing a list of jobs and workplaces prohibited for pregnant women and mothers up to the end of the ninth month after childbirth and for breastfeeding women, a list of jobs and workplaces associated with specific risks for pregnant women, mothers up to the end of the ninth month after childbirth and for breastfeeding women, and establishing certain obligations for employers in the employment of such women, as amended.
- Slovak Government Regulation No. 286/2004 Coll., establishing a list of jobs and workplaces prohibited to juvenile employees and establishing certain obligations for employers when employing juvenile employees, as amended.
- Slovak Government Regulation No. 276/2006 Coll. on minimum safety and health requirements for working with display units.
- Slovak Government Regulation No. 281/2006 Coll. on minimum safety and health requirements for manual handling of loads.
- Slovak Government Regulation No. 387/2006 Coll. on requirements for ensuring safety and health marking at work.
- Slovak Government Regulation No. 391/2006 Coll. on minimum health and safety requirements for the workplace.
- Slovak Government Regulation No. 392/2006 Coll. on minimum safety and health requirements for the use of work equipment.
- Slovak Government Regulation No. 393/2006 Coll. on minimum requirements for ensuring health and safety at work in explosive atmospheres.
- Slovak Government Regulation No. 395/2006 Coll. on minimum requirements for the provision and use of personal protective equipment.
- Slovak Government Regulation No. 396/2006 Coll. on minimum safety and health requirements for construction sites.
- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No.45/2010 Coll., which establishes details for ensuring health and safety at agricultural work.
- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No.46/2010 Coll., which establishes details for ensuring safety and health protection in forest work and details of professional competence for the performance of certain work activities and for the operation of certain technical equipment.



- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No. 356/2007 Coll., which establishes details on the requirements and scope of educational and training activities, on the project of education and training, on the maintenance of prescribed documentation and verification of the knowledge of participants in educational and training activities.
- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No. 500/2006 Coll., which establishes a model record of a registered work accident.
- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No. 508/2009 Coll., which establishes details for ensuring safety and health protection at work with pressure, lifting, electrical and gas technical equipment and which establishes technical equipment that is considered as reserved technical equipment , as amended.
- Decree of the Ministry of Labour, Social Affairs and Family of the Slovak Republic No. 147/2013 Coll., which establishes details for ensuring safety and health protection during construction and related works and details of professional competence for the performance of certain work activities, as amended.
- Decree of the Ministry of the Interior of the Slovak Republic No. 9/2009 Coll., implementing the Road Traffic Act and amending and supplementing certain acts, as amended.

Legislation to ensure health and safety at work in the field of occupational environmental factors:

- Slovak Government Regulation No. 355/2006 Coll. on the protection of employees against risks related to exposure to chemical agents at work, as amended.
- Slovak Government Regulation No. 356/2006 Coll. on the protection of the health of employees against risks related to exposure to carcinogenic and mutagenic factors at work , as amended.
- Slovak Government Regulation No. 253/2006 Coll. on the protection of employees against risks related to occupational exposure to asbestos.
- Slovak Government Regulation No. 416/2005 Coll. on minimum health and safety requirements for the protection of employees against risks related to exposure to vibration, as amended.
- Slovak Government Regulation No. 209/2016 Coll. on minimum health and safety requirements for the protection of employees against risks related to exposure to electromagnetic fields.
- Slovak Government Regulation No. 83/2013 Coll. on the protection of the health of employees against risks related to exposure to biological factors at work.

- Decree of the Ministry of Health of the Slovak Republic No. 541/2007 Coll. on details of requirements for lighting at work.
- Decree of the Ministry of Health of the Slovak Republic No. 99/2016 Coll. on details of health protection against heat and cold stress at work.
- Decree of the Ministry of Health of the Slovak Republic No. 542/2007 Coll. on the details of health protection against physical stress at work, psychological workload and sensory stress at work.
- Decree of the Ministry of Health of the Slovak Republic No. 448/2007 Coll. on the details of the factors of work and working environment in relation to the categorisation of work in terms of health risks and on the details of the proposal for the classification of work into categories, as amended.

## 7.2. RISK ASSESSMENT

One of the important steps in implementing a safety management system of occupational health and safety in any company is risk assessment. This obligation is underpinned by the law. § Section 6(1)(c) of Act No 124/2006 Coll. on Occupational Safety and Health imposes an obligation on employers to 'identify hazards and dangers, assess the risk and draw up a written document on risk assessment for all activities carried out by employees'.

Assessing risk means determining the likelihood of its occurrence and the severity of the consequence of a potential adverse event. Risk ( $R$ ) is a function of probability ( $p$ ) and consequence ( $C$ ). Thus:

$$R = p \times C \quad (16)$$

The  $\times$  sign expresses the functions according to the type of evaluation. It can be a matrix (application of the **Point Method**) or a product.

Forms of evaluation may vary:

- **Qualitative**: in a word. It is used when simple traffic or numerical data are missing.
- **Semi-quantitative**: when qualitatively described scales have assigned numerical values, for example, the point method.
- **Quantitative**: uses numerical probability values (1 time in 100 000 cycles, 1 accident per 100,000 workers...).

The negative consequences can be expressed in various forms, e.g., in numbers of injuries, damages (€), etc.

Risk assessment is not a one-off exercise. After a certain period, the risks of previously assessed systems need to be reassessed. Especially in cases where there have been changes

in the technological set-up, site conditions, materials used, changes in in the production process, etc.

Risk assessments should always be in writing. For the purposes of control activities to demonstrate the assessment procedures and results, to provide an overview of the assessments carried out and the measures proposed, for the purpose of repeated assessments of the system, etc.

The risk assessment of potential harm to the health of the employee does not assess the health of the employee, but the condition of the individual components of the work: the way the employee works, the condition of the work equipment and the working environment, including the workplace. At the same time, it assesses their impact on the employees. Finally, the employer is also obliged to assess the risk in relation to the physical and psychological strain on the employee.

When assessing risks, it is common to use terms that have a similar meaning in colloquial parlance: hazard, threat, risk. For the purposes of the risk assessment methodology, it is therefore necessary to define them:

- **Hazard:** a condition or characteristic of a work process factor and the work environment that can harm the health of an employee.
- **Threats:** a situation in which it cannot be excluded that the employee's health will be harmed.
- **Risk:** the likelihood of an employee's health being damaged at work and the degree of possible health consequences.

When assessing the risks, particular attention should be paid to:

- the layout and equipment of the workplace,
- the nature, degree, and duration of exposure to physical, chemical, and biological agents and their impact,
- the nature and extent of the work equipment (plant, machinery, apparatus, tools) used and the way in which they are used,
- the nature of the work process, work procedures and work organisation,
- the knowledge and level of training of the staff member, his physical and mental abilities and state of health.

### **7.3. REDUCTION OF OCCUPATIONAL HEALTH AND SAFETY RISKS**

**Once a risk assessment has been carried out, it is the employer's responsibility to plan and implement all necessary safety, protection, and health measures to reduce the risk of harm to the health of employees, considering all the direct and indirect contexts of the work process.**

If the risk assessment results in a '**high level of risk**' and the risk have been assessed as 'unacceptable', risk reduction **measures must be implemented immediately**.

If the risk assessment results in a 'medium level of risk' and is assessed as 'acceptable', it is **recommended that action is planned to reduce the level of risk**.

If the risk is small and judged acceptable, it is necessary to ensure that it remains at the same low level.

As regards risk reduction measures, the following basic rules should be considered:

**Eliminating or minimising risk must be the priority**, that is, **technical and organisational measures must be given priority over behavioural measures**.

Thus, the hierarchy of implementation of the measures is as follows:

1. **Elimination**: this is the best solution, but in some cases the risk cannot be (completely) eliminated.
2. **Substitution**: e.g., in the case of hazardous substances, the substitute must have a lower toxicity. The problem may be that the substitute substance may not have the same effect or outcome as the original (more hazardous) substance.
3. **Technical solutions** (safety equipment, ventilation, insulation, etc.). This is probably the most common practice. It involves physically altering the flow of the substance or isolating the worker from the hazard caused by the hazardous substance or environment.
4. **Personnel solutions** (i.e., training, training, personal protective equipment). These include Improving human behaviour and the consistent and correct use of personal protective equipment (PPE) such as respirators, gloves, work boots, goggles, face shields or hearing protection.

## **CONCLUSIONS**

In practice, however, a narrow understanding of the risk assessment obligation is often encountered. Many employers only comply with this obligation because they are required to do so by law or because they are ordered to do so by a labour inspector after an inspection. However, it is important to realise that risk assessment has a broader meaning.

Adverse factors of the work process negatively affect the health of employees. Often this is a subtle and insignificant effect, but with long-term exposure it manifests itself in numerous illnesses, possibly even in the form of occupational disease. In the worst case, an occupational accident may result. Whether it is a physical or psychological impairment of health, it will always have an impact on the employee's performance.

This translates directly into economic considerations - often draining more of the employer's funds than effective prevention would require. It has been shown that the search for hazards, threats and risk assessment followed by the implementation of safety measures is less burdensome (in terms of time and finances) for the employer than dealing with the consequences of dangerous events. After an accident or illness at work In the event of an occupational accident or injury, the employer has to bear not only the costs of implementing safety measures, but often also the sanction from the labour inspectorate and the costs of compensating the affected employee. And this, of course, adversely affects the operation as a manufacturing, both manufacturing and non-manufacturing businesses.

## REFERENCES

- [1]. MIKULA, J. 2018. *Opatrenia pri znižovaní rizík / Risk reduction measures. OHSPonline*. Available online: <<https://www.bozponline.sk/33/opatrenia-pri-znizovani-rizik-uniqueiduchxzASYZNbHI7G8uaRB3kl0wI4IIRvxeE61ttPd92s/>>
- [2]. JENSEN, R.C. 2019. *Risk-Reduction Methods for Occupational Safety and Health*. Wiley, 469 p.
- [3]. NIP. 2021. *Bezpečnosť a ochrana zdravia pri práci / Occupational health and safety*. Košice. Available online: <https://www.ip.gov.sk/bozp/>
- [4]. NIP. 2021. *BOZP/ Legislatíva / OSH/Legislation*. Košice. Available online: <https://www.ip.gov.sk/bozp/legislativa/>
- [5]. ŠIMÁK, L. 2006. *Manažment rizík / Risk management*. Žilina. Available online: [http://fsi.uniza.sk/kkm/files/publikacie/mn\\_rizik.pdf](http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf)



## QUESTIONS

1. What is the main objective of the OHS risk management process?
2. What methods of risk analysis/assessment can be applied to OSH?
3. Define at least 3 ways to reduce OHS risks?
4. Define the hierarchy of implementation of the measures.
5. Define the concept of risk from an OHS perspective.

## 8. RISK MANAGEMENT OF MAJOR INDUSTRIAL ACCIDENTS IN THE SLOVAK REPUBLIC

The introduction of new technologies, the use of more and more substances and the use of new substances bring with them significant risks with the potential for industrial accidents. In recent decades, several industrial accidents have occurred with consequences for life, health and the environment and human property. The causes of accidents have mainly been inappropriate handling of hazardous substances, neglect of technological procedures or human error.



*The aim of the chapter is to know and understand the objective of risk management in the prevention of major industrial accidents, to know the procedures and methods of assessing these risks as well as their reduction.*

### 8.1. BACKGROUND TO THE PREVENTION OF MAJOR INDUSTRIAL ACCIDENTS IN THE SLOVAK REPUBLIC

A major industrial accident is "an event such as a serious release of a hazardous substance, fire or explosion resulting from an uncontrolled development during the operation of an establishment, leading to a serious imminent or consequent endangerment of human health, the environment or property with the presence of one or more hazardous substances". (Act No. 128/2015 Coll.)

Prevention of major industrial accidents (PMIA) is "a set of organisational, managerial, personnel, educational, technical, technological and material measures to prevent the occurrence of major industrial accidents". (Act No. 128/2015 Coll.)

Within the European Union countries, the prevention of major industrial accidents has been regulated since 1996 by Council Directive 96/82/EC on the control of major-accident hazards with the presence of dangerous substances, also known as SEVESO II, which is aimed not only at preventing major accidents but also at limiting their consequences for man and the environment. Directive 2003/105/EC of the European Parliament and of the Council - SEVESO II - was adopted in 2003. Although the system established by the SEVESO II Directive has helped in reducing the likelihood and consequences of major accidents, several areas where changes would be appropriate have been identified. These are addressed in the new Directive 2012/18/EU of the European Parliament and of the Council on the control of major-accident hazards involving dangerous substances (SEVESO III).

Another of the basic international documents in this field concluded under the auspices of the United Nations Economic Commission for Europe is the Convention on the Transboundary

Effects of Industrial Accidents, which was opened for signature in Helsinki on 17 and 18 March 1992. The Convention entered into force for Slovakia on 8 December 2003. Its objective is, in the interests of sustainable development and based on the principles of international law and custom, to ensure conceptual and systematic action by the Contracting Parties in the field of prevention of industrial accidents which may have transboundary effects, preparedness for such accidents and the management of industrial accidents, including the limitation of their effects on people, the environment and property.

The area of serious industrial accidents in the Slovak Republic is regulated by Act No. 128/2015 Coll. on the prevention of serious industrial accidents and on the amendment of the Slovak National Council Act No. 128/2015 Coll. on the prevention of serious industrial accidents and on the amendment of the Slovak National Council Act No. and amendments to certain acts and the Decree of the Ministry of the Environment (MoE) of the Slovak Republic No. 198/2015 Coll., implementing certain provisions of Act No. 128/2015 Coll. on the prevention of major industrial accidents and on the amendment and supplementation of certain acts.

The Act on the Prevention of POPs lays down obligations for operators of establishments where certain quantities of hazardous substances are present to ensure the prevention of and minimise the consequences of a major industrial accident should it occur. In accordance with the Directive, the tasks of the public authorities in the field of prevention of HNS are defined. The standards for carrying out inspections at establishments are tightened; in the decision-making process for permitting the construction of industrial establishments, the national authorities should consider sufficient and appropriate distances between establishments, between establishments and between establishments and public spaces and buildings with many people.

The purpose of the Decree is to lay down the details of the notification of the classification of the undertaking and its model, the risk assessment, the content and processing of the HNS prevention programme, the safety management system, the content of the safety report, the content of the internal emergency plan, its development, maintenance, review and exercise, data collection on major industrial accidents, the content of training.

Act of the National Council of the Slovak Republic No. 128/2015 Coll. on the prevention of major industrial accidents and on the amendment of and amendments to certain acts defines the concept of hazard and risk.

It defines **a hazard** as "*a physical or physical situation giving rise to the possibility of a major industrial accident*".

**Risk** again defines risk as "*the likelihood of a specific effect occurring at a particular time or under particular circumstances*".

Decree No. 198/2015 of the Ministry of the Environment of the Slovak Republic implementing certain provisions of the Act No. 128/2015 Coll. on the prevention of major industrial accidents and on the amendment and supplementation of certain acts, contains the procedures used for risk assessment.

## **8.2. MAJOR INDUSTRIAL ACCIDENT RISK ASSESSMENT**

**The risk assessment shall be carried out for the purposes of:**

- the development of a prevention programme and the implementation of a safety management system,
- the development and use of the safety report,
- preparation of an internal emergency plan and documents for the preparation of a public protection plan,
- public information,
- the exercise of state supervision and coordination of control activities.

**The risk assessment process includes:**

- identifying and locating the initiators and sources of risk of a major industrial accident,
- identification of possible initiating events and transients and processes that may lead to the occurrence and development of a major industrial accident,
- Determination of possible human influences on events and processes,
- identification and evaluation of technical, administrative, personnel and organisational measures and barriers designed to prevent, limit, or suppress the occurrence and development of initiating events, phenomena, and processes,
- an estimate of the probability or frequency of a major industrial accident based on:
  - estimation of the probability of initiating events, phenomena, and processes considering possible impacts,
  - considering the effectiveness and reliability of measures and barriers,
- an estimate of the magnitude and severity of the potential consequences of a major industrial accident caused by the different sources of risk, including possible interactions between them, on human life and health, the environment and property within and surrounding the establishment,
- analysis of the risk of major industrial accidents to human life and health, the environment and property,
- a risk assessment resulting in scenarios of representative types of major industrial accidents and sets of scenarios for each representative type of major industrial accident, with the plotting of the zones of exposure to the thermal, pressure and toxic effects of major



industrial accidents and an assessment of the acceptability of the risk of major industrial accidents.

The risk analysis of major industrial accidents is based on well-known and proven risk assessment methods (PHA, FTA, ETA, FMEA and others) systematically applied to individual risk equipment, systems, and elements, as well as to other relevant internal and external factors.

The first procedural step of the risk analysis is the identification and description of the equipment at risk and systems of the company.

Based on the description of the risk equipment and systems of the company, a system analysis shall be carried out to identify potential system failures leading to a major industrial accident, including common cause failures, using a unified **fault tree analysis (FTA)** and dependent fault analysis **method**.

Based on the identified trees, potential sources of risk of a major industrial accident arising from normal operation, from extraordinary operational situations, from transients and processes, from natural events, from human failure, in the objects and facilities of the company are identified and evaluated by means of an accident chain analysis, which consists of sub-analyses:

- initiating events that may lead to a major industrial accident,
- success criteria, considering technical, material, personnel, organisational and administrative countermeasures, and barriers designed to prevent, limit or suppress the development of initiating events into a major industrial accident,
- event trees and which, based on the construction of event trees considering the potential development of initiating events into a major industrial accident, allow quantification of the probability or frequency of occurrence of unwanted accident chains considering human factors analysis and data analysis,
- equipment damage conditions to determine potential damage within and around the plant,
- to quantify the probability or frequency of a major industrial accident,
- determination of the uncertainty of the results if specific data from the operator's databases are used.

In preparing the data inputs for the individual analyses and for the quantification calculations, the following will be used:

- general data on the failure or reliability of components, systems and equipment taken from validated foreign or other off-site databases.
- specific data available in the operator's corporate databases to the extent required.

Input can also be prepared based on data analysis, where the selection of the necessary information is made by applying statistical methods or by using a combination of data from general and specific databases.

The **most relevant data for risk analysis purposes** include data on:

- inspection, testing and maintenance of equipment,
- the potential for simple faults, accidents, and dependent faults,
- frequency of initiation events,
- collecting and maintaining documentation of system and equipment failures and accidents,
- events when a major industrial accident almost occurred.

**Risk analysis shall also include an analysis of the reliability of the human agent**, where this enters directly or indirectly into the control and management of systems and equipment the failure of which may develop into a major industrial accident. This analysis need not be carried out in an undertaking or part of an undertaking where such passive safety systems, measures and barriers which preclude the potential for a major industrial accident due to human failure.

The human factor's reliability analysis includes sub-analyses:

- the state of control and management of the operation, including an analysis of the activities of the operating crew prior to the occurrence of a potential initiating event,
- the state of control and management of the operation, including an analysis of the activities of the operating staff, if an initiating event occurs which may lead to a major industrial accident,
- potential options for eliminating or limiting the occurrence and development of a major industrial accident and restoring normal operations by human resources.

**Risk analysis includes an analysis of external events that** may cause a major industrial accident or adversely affect its course and consequences in and around the establishment.

The analysis of external events shall include:

- analysis of the impact of fires and explosions,
- analysis of the impact of inundation by internal and external waters,
- seismic analysis,
- an analysis of the impact of adverse meteorological and geological conditions, in particular extreme temperatures and extreme precipitation, storms, gales, lightning, slope deformation or subsidence,
- analysis of the impact of road, rail, and air transport,
- other specific analyses, particularly the impact of neighbouring industrial activities.

The **estimation of the magnitude of the possible consequences** is based on the scenarios and their effects on human life and health, the environment and property.

**Other internationally recognised methods appropriate to the circumstances of a particular case may be used at different stages of the risk analysis and in estimating the extent of the possible consequences of major industrial accidents.**

**The societal acceptability of the risk of an identified major industrial accident in terms of the assessment of the possibility of a potential threat to the life of one or more persons is determined by the acceptable probability or frequency of occurrence of the major industrial accident.**

The criterion for assessing the acceptability of the risk of a major industrial accident, if it does not endanger the life of persons, is also a **determination of the acceptability of the extent and severity of the hazard or damage to the environment and property.**

At the end of the risk assessment, an assessment of the acceptability of the risk is made by comparing the value of the acceptable (tolerable) risk with the value of the calculated **individual risk** and **societal risk** for representative major industrial accident scenarios.

Individual risk is the threat to the life of one person. Societal risk is a threat to the life of several persons.

In practice, a set of methods known as Environmental Risk Assessment (**ERA**) is used to assess the environmental impacts of industrial activities.

This follows classical risk assessment procedures, i.e., the initial assessment selects the significant threats and hazards to the environment. In a subsequent step, they are analysed in detail to minimise the consequences.

The obligation to assess environmental risks (ER) arises for companies in the Slovak Republic also from Act 359/2007 Coll. This procedure is also applicable for the purpose of ERA for ZPH and consists of steps:

1. **Initial environmental risk assessment:** the objective of the initial assessment is to determine whether there are sources, facilities, and technologies for which a detailed ER assessment needs to be carried out. The proposed initial assessment procedure is based on engineering approaches that seek to quantify the causality of the scenario in question. In terms of describing causality, it is necessary to recognise that the transport of the contaminant is facilitated by water and air and the recipient is soil, habitats, etc. Therefore, at the end of the initial assessment, a decision mechanism is set up to select scenarios for detailed assessment, considering the causality of environmental damage.
2. **Detailed environmental risk assessment:** the detailed ER assessment is based on detailed analyses of the affected environment and the damage to the natural resources contained therein. To determine the damage, it is necessary to apply vulnerability analyses (calculation, quantification of the relevant damage) in combination with the probability of occurrence of the analysed event. A so-called probabilistic approach is

used, using standard risk assessment methods such as Fault Tree Analysis (FTA) and Event Tree Analysis (ETA).

3. **Defining the level of risk:** simple mechanisms need to be implemented in this part for determining the risk acceptability threshold, which is used for defining priorities for the implementation of preventive measures.
4. **Defining consequences:** knowledge of causal dependence is key to determining possible scenarios of damage to natural resources in the impact zone.
5. **Quantification of environmental damage:** the quantification of environmental damage provides the answer to the question of the appropriate amount of financial coverage. Based on the outputs of the initial assessment and, if necessary, a detailed environmental risk assessment, procedures are proposed to determine the expected total costs to be borne by the operator in the event of environmental damage.

A detailed description of the methodology of environmental risk assessment is contained in the [Methodological Manual](#).

### **8.3. MEASURES TO PREVENT AND MINIMISE THE CONSEQUENCES OF MAJOR INDUSTRIAL ACCIDENTS**

These measures stem from both the SEVESO III Directive and national legislation. In particular:

1. A comprehensive obligation for operators to take all necessary measures to prevent major accidents and to demonstrate to the competent authorities that they are complying with the obligations under this Directive.
2. Obligation for the operator to carry out a systematic assessment of major-accident risks and to use the results of that assessment:
  - so, in the activities of the operator,
  - as well as in the activities of the competent authorities.
3. Obligation for all operators to develop a major-accident prevention policy and to establish a safety management system to implement the policy for operators of category B establishments.
4. Obligation for operators of category B undertakings to prepare and submit to the competent authority a comprehensive documentation called a 'safety report', containing not only an analysis but also a management of the risks involved.
5. Obligation to pay special attention to the location of establishments with hazardous substances and to the spatial development around them.
6. Obligation to develop, test (practice) and update internal and external emergency plans.

7. Obligations of both operators and competent authorities in informing the public and allowing them to participate in decision-making processes, including the public of another State whose territory may be affected by the transboundary effects of a major accident.

## CONCLUSIONS

Risk Management in the prevention and management of major industrial accidents is based on a comprehensive assessment of the risks associated not only with the release of a hazardous substance and the associated impacts on the life and health of persons, property and the environment, but also the risks of fires and explosions, occupational injuries and illnesses, as well as accidents arising from the transport of hazardous substances and waste management. The assessment of the risks of major industrial accidents and the drawing up of the relevant safety documentation is the responsibility of a person with the appropriate professional competence, i.e., a specialist in the prevention of HAZMAT, whose certificate of competence is issued by the Ministry of the Environment of the Slovak Republic.

## REFERENCES

- [1]. KANDRÁČ, J. 2000. *Metodický postup na hodnotenie rizík nebezpečných prevádzok a štúdia o podnikoch v Slovenskej Republike / Methodological procedure for risk assessment of hazardous plants and study of companies in the Slovak Republic*. Bratislava: RISK CONSULT, spol. s. r. o., 63 p.
- [2]. ORAVEC, M. 2011. *Manažérstvo priemyselných havárií / Industrial accident management*. Nová Lesná, 68 p.
- [3]. ORAVEC, M., FIC, M. 2014. *Systém hodnotenia rizík pre posúdenie environmentálnej škody podľa zákona NR SR č. 359/2007 Z. z. / Risk assessment system for environmental damage assessment according to the Act of the National Council of the Slovak Republic No. 359/2007 Coll*. Handbook for operators and state administration. Banská Bystrica: Slovak Environmental Agency. 55 p.
- [4]. Decree No. 198/2015 of the Ministry of Environment of the Slovak Republic implementing certain provisions of Act No. 128/2015 Coll. on the prevention of major industrial accidents and on amendments and supplements to certain acts.
- [5]. Act of the National Council of the Slovak Republic No. 128/2015 Coll. on prevention of major industrial accidents and on amendments and supplements to certain acts.



## QUESTIONS

1. What is the main objective of the risk management process for the prevention of MIA?
2. Which piece of legislation sets out the procedure for assessing the risks of MIA?
3. What is the content of prevention of MIA?
4. List the sub analyses contained in the risk analysis of MIA.
5. What measures are emerging for entrepreneurs from the perspective of the PMIA?

## 9. RISK MANAGEMENT IN THE FIELD OF CIVIL PROTECTION IN THE SLOVAK REPUBLIC

Nowadays, in the Slovak Republic, in the European Union, but also in the whole world, extraordinary events of a natural nature, such as floods, windstorms, fires, landslides, hurricanes, etc., are occurring more and more frequently. As a result of the increasing frequency of natural and man-made disasters, countries around the world have begun to engage in risk management, which identifies potential threats to their populations, analyses them and takes measures to protect life, health, property, and the environment.

The most frequently occurring risks on the territory of the Slovak Republic include floods (recently especially flash floods), landslides, snow calamities, windstorms, fires, hazardous substances (leaks, explosions, landfill finds).



*The aim of the chapter is to understand the process of emergency risk management, which is implemented with the intention of protecting the life and health of the population, their property, cultural values, and the environment. This is carried out from the level of the legal entity, the municipality, up to the national level.*

### 9.1. BACKGROUND OF CIVIL PROTECTION OF THE POPULATION IN THE CONDITIONS OF THE SLOVAK REPUBLIC

According to the relevant legislation, individual types of threats are under the competence and responsibility of the relevant central government authority.

The following are involved in assessing the risks of emergencies in the Slovak Republic:

– **Central government bodies:**

- Ministry of Economy of the Slovak Republic,
- Ministry of Finance of the Slovak Republic,
- Ministry of Transport, Construction and Regional Development of the Slovak Republic,
- Ministry of Agriculture and Rural Development of the Slovak Republic,
- Ministry of the Interior of the Slovak Republic,
- Ministry of Defence of the Slovak Republic,
- Ministry of Justice of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Labour, Social Affairs and Family of the Slovak Republic,
- Ministry of the Environment of the Slovak Republic,

- Ministry of Education, Science, Research and Sport of the Slovak Republic,
  - Ministry of Culture of the Slovak Republic,
  - Ministry of Health of the Slovak Republic.
- **Other government bodies:**
- Office of the Government of the Slovak Republic,
  - Antimonopoly Office of the Slovak Republic,
  - Statistical Office of the Slovak Republic,
  - Office of Geodesy, Cartography and Cadastre of the Slovak Republic,
  - The Office of Nuclear Supervision of the Slovak Republic,
  - Office for Standardization, Metrology and Testing of the Slovak Republic,
  - Public Procurement Office,
  - Industrial Property Office of the Slovak Republic,
  - Administration of the State Material Reserves of the Slovak Republic,
  - National Security Agency.
- **Local government and local authorities, non-profit organisations, private sector.**

The legislative framework of the Slovak Republic on risk assessment is represented by the following legislation:

- Constitutional Act No. 227/2002 Coll. on State Security in Times of War, State of War, State of Emergency and State of Emergency, as amended,
- Act of the National Council of the Slovak Republic No. 387/2002 Coll. on State Management in Crisis Situations Outside Wartime and Martial Law, as amended,
- Act of the National Council of the Slovak Republic No. 42/1994 Coll. on Civil Protection of the Population as amended,
- Act of the National Council of the Slovak Republic No. 129/2002 Coll. on the Integrated Rescue System, as amended,
- Act of the National Council of the Slovak Republic No. 179/2011 Coll. on Economic Mobilisation and on Amendment and Supplementation of Act No. 387/2002 Coll. on State Management in Crisis Situations Outside Wartime and Martial Law, as amended,
- Act of the National Council of the Slovak Republic No. 314/2001 Coll. on Fire Protection as amended,
- Act of the National Council of the Slovak Republic No. 315/2001 Coll. on the Fire and Rescue Corps, as amended,
- Act of the National Council of the Slovak Republic No. 37/2014 Coll. on Voluntary Fire Protection of the Slovak Republic and on amendments to certain acts,
- Act of the National Council of the Slovak Republic No. 544/2002 Coll. on the Mountain Rescue Service as amended,

- Act of the National Council of the Slovak Republic No. 7/2010 Coll. on flood protection as amended,
- Act of the National Council of the Slovak Republic No. 128/2015 Coll. on prevention of major industrial accidents and on amendment and supplementation of certain acts
- Act of the National Council of the Slovak Republic No. 45/2011 Coll. on Critical Infrastructure,
- Act of the National Council of the Slovak Republic No. 579/2004 Coll. on Emergency Medical Services and on Amendments and Additions to Certain Acts, as amended,
- Act of the National Council of the Slovak Republic No. 171/1993 Coll. on the Police Force, as amended,
- Act of the Slovak National Council No. 51/1988 Coll. on Mining Activities, Explosives and State Mining Administration, as amended,
- Slovak Government Regulation No. 130/1994 Coll. on one-off extraordinary compensation for injury to health or death in connection with assistance provided in the performance of civil protection tasks, as amended,
- Act of the National Council of the Slovak Republic No. 575/2001 Coll. on the organisation of government activities and the organisation of the central state administration, as amended.

We also include other concept papers:

- Security Strategy of the Slovak Republic approved by the National Council of the Slovak Republic
- Landslide Risk Prevention and Management Programme (2014-2020),
- Adaptation strategy of the Slovak Republic to the adverse effects of climate change approved by a government resolution,
- Operational Programme Environmental Quality for the period 2014-2020.

## **9.2. RISK ANALYSIS OF EMERGENCIES**

The basic document for the identification of potential hazards in the territory of the Slovak Republic is the "**Analysis of the territory in terms of possible emergencies in the Slovak Republic**".

The document is prepared at all levels of government based on **the Act of the National Council of the Slovak Republic No. 42/1994 Coll. on civil protection of the population** as amended.

The development of the area analysis relies on good local and specialist knowledge of crisis management.

The analysis shall be prepared by:



- district offices at local level,
- district offices in the county seat at the level of the region.
- Ministry of the Interior of the Slovak Republic at the national level.

The district offices in the county seat prepare the individual points of analysis with the designation of the district, for which the threats are specified.

The district's analysis is not classified. The analysis of the territory of the Slovak Republic is classified "Restricted".

The analysis shall be updated as soon as changes or alterations in the conditions in the analysed area are reported which may affect the level of threat to the population from the possible occurrence of emergencies or have an impact on the performance of the tasks of civil protection of the population. The analysis shall be updated regularly once a year with the situation as of 31 December of the previous year and shall be submitted in writing and in electronic form.

The analysis shall be developed in structure and content as follows:

- **Section A** contains geographical, demographic, and economic characteristics of the territory.
- **Section B** contains possible risks of emergencies:
  - B.1. Threats extreme weather and climatic events
  - B.2. Areas of potential threat from slope deformation and seismic activity
  - B.3. Areas of potential flood risk, areas of potential flood risk in case of breach of a water structure (including tailings ponds)
  - B.4. Areas of potential fire and explosion hazards (forest fires, fires and explosions of an industrial nature)
  - B.5. Areas of potential threat from all modes of transport
  - B.6. Areas of potential hazard from a release of a hazardous substance from the characteristics of the hazardous substances
  - B.7. Areas of potential risk of disease and epidemics (human, animal diseases) and plant diseases)
  - B.8. Areas at risk from other types of emergencies (risks of a technogenic, sociogenic, environmental nature and areas with possible accumulation of different types of emergencies).
- **Section C** - contains an overview of the risks in the analysed area and an overview of the forces and assets for dealing with emergencies, including civil protection units.

The analysis of the territory includes a **Table of risks of possible emergencies in the analysed** territory (the type of threat is assigned to the selected objects). In it, district authorities identify possible crisis phenomena on the territory of the municipalities under their

jurisdiction. The table brings together data from all the individual chapters of the area analysis. In this way, by selecting a specific municipality, it is possible to identify all possible crisis phenomena that may occur in that municipality or, by selecting a crisis phenomenon, to get an overview of the municipalities and the territory where the phenomenon may occur. Each crisis event is linked to the source and location of the risk, the likelihood of occurrence, the number of inhabitants at risk, the size of the area at risk and the expected secondary crisis events.

- **Section D** - contains conclusions and recommendations for the development of plans for the protection of the population and recommendations for taking measures to reduce the risks of danger and measures necessary to prevent the spread and effects of the consequences of the emergency.
- **Section E** - contains tabular annexes:
  - list of municipalities (urban districts) in the assessed area, population numbers,
  - stationary sources of hazardous substances,
  - incinerators and hazardous waste landfills,
  - water structures,
  - a list of important manufacturing companies and their production focus,
  - a list of health facilities (hospitals, polyclinics, health centres),
  - a list of veterinary establishments (hospitals, polyclinics, outpatient clinics),
  - a list of social service facilities,
  - a list of facilities identified for emergency accommodation,
  - a list of school and pre-school facilities,
  - objects and places with many people at risk of a possible terrorist attack,
  - list of farms.

Graphical part of the document "*Analysis of the territory ...*" is processed in the civil protection geographical information system **CIPREGIS**.

### **9.3 REDUCING AND MONITORING SECURITY RISKS**

The adoption and implementation of measures aimed at monitoring and reducing security risks is the responsibility of the relevant public administration bodies as well as the relevant legal entities and natural persons - entrepreneurs.

For example, dealing with slope deformations is the responsibility of the Ministry of the Environment of the Slovak Republic (MŽP SR). In the event of the occurrence of slope deformations, the Geology and Natural Resources Section of the Ministry of the Environment of the Slovak Republic is governed by Act No 569/2007 Coll. on geological works (Geological Act), as amended. The management of accidental landslides also includes systematic

monitoring activities in the field of slope deformation. This activity is entrusted to the Dionýz Štúr State Geological Institute.

Measures of collective protection of the population, as well as the plan of material and technical provision of rescue work are defined in the "**Plan of protection of the population**", the lowest level for processing of which is the municipality. Legal entities most often draw up a '**Plan for the protection of employees and persons taken into care**'.

## CONCLUSION

Crisis management authorities and specific competent persons in this field are responsible for analysing the risks of emergencies at different spatial scales. In addition to the preparation of the 'Spatial analysis' document, the expertise at their disposal relates to the preparation and updating of the civil protection plan, the preparation and updating of the protection plan for staff and persons in their care. However, this competence is also required to carry out educational activities in the field of civil protection (e.g., training).

## REFERENCES

- [1]. SKR MV SR. 2015. *Posúdenie rizík Slovenskej republiky v súlade s článkom 6 rozhodnutia EP a R č. 1313/2013/EÚ / Risk Assessment of the Slovak Republic in accordance with Article 6 of Decision No 1313/2013/EU*. Bratislava, 71 p. Available online: <[https://www.minv.sk/?Bezpecnostne\\_rizika](https://www.minv.sk/?Bezpecnostne_rizika)>
- [2]. Act of the National Council of the Slovak Republic No. 42/1994 Coll. on Civil Protection of the Population, as amended.



### QUESTIONS

1. What is the main objective of the civil protection risk management process?
2. Who carries out the emergency risk analysis?
3. Define the content of the Territory Analysis in terms of potential emergencies.
4. In which program is the graphic part of the Territory Analysis processed?
5. Who is responsible for taking and implementing risk reduction measures?

## 10. APPLICATION OF MAPPING, GIS, AND COMPUTER-AIDED MODELLING IN THE RISK MANAGEMENT

Identification and updating of threats in terms of natural disasters, accidents, catastrophes, and terrorist attacks in Slovakia is already carried out at the level of district offices in the crisis management departments, within the framework of the elaboration and annual updating of the document "Analysis of the territory of the district in terms of the occurrence of possible emergencies" (hereinafter referred to as the "Analysis of the territory of the district..."). This is prepared based on the categorisation of the territory according to the Slovak Government Regulation of 16.12.1996 No. 25/1997 Coll. on the categorisation of the territory of the Slovak Republic.



*The aim of the chapter is to learn and understand the techniques, methods of mapping and risk assessment of natural and technical emergencies based on the application of geographical information systems and modelling tools.*

### 10.1 SUSCEPTIBILITY ASSESSMENT

**Susceptibility** (Susceptibility is part of one of the components of risk, namely exposure. Exposure can be understood as the number of communities or area of the environment or other elements of systems existing in the area under consideration that could potentially be damaged or destroyed by a particular agent of natural or technical nature. Susceptibility then represents the 'weaknesses' of these systems which, under certain circumstances (conditions), may directly trigger the occurrence of an emergency or encourage its progression. In the process of analysing the vulnerability of a territory, it is therefore necessary to determine the threats that arise from the nature of the territory or the type of industry that operates in the territory.

As already mentioned, the threats that occur in the territory of the district should be registered in the document "Analysis of the territory of the district...".

The most common natural disasters in Slovakia include floods (caused by torrential rainfall or ice floods), forest fires, windstorms, landslides (mainly because of long-term or torrential rainfall).

In terms of the susceptibility of an area to flooding, we need to consider not only the type of flooding (caused by torrential rainfall, glaciers...), but also the environment for which we are carrying out the analysis (forest environment, inhabited environment). Regarding the type and nature of the environment, it differs the assessment methodology used also varies.

Abroad, the issue of assessing the susceptibility of a territory to floods has been and is being dealt with by several experts. Some of them have also worked within the working groups of the COST Action "Flood risks and prevention in the medium and small catchments".

The aim of this action was to name, determine, describe, and quantify the different factors that, due to their characteristics, have a direct influence on the susceptibility of an area to flooding. It was their direct relationship to the retention capacity, the accumulation and infiltration of rainfall and the ability to slow the flow of water and help its equilibrium. In this case, the assessment of susceptibility is based on a multi-criteria assessment of multiple factors, processing, and subsequent synthesis of data in a Geographical Information Systems environment. However, this is a process leading more to an assessment of flood vulnerability in the natural environment. The groups of factors considered included: meteorological conditions (24-hour rainfall totals), soil conditions (soil infiltration parameters), terrain morphology (slope of the terrain), type of land use.

The problem of determining the susceptibility of the Poprad district (natural and inhabited area) is also addressed in their work by Lubinszká, Majlingová (2011), Majlingová, Galla (2015) and the problem of assessing the susceptibility of the small mountain catchment area of the Hučava watercourse in the massif of the Poľana Mountains by Majlingová, Závacká, Kliment (2012). Both approaches are based on data processing in a **Geographic Information Systems** (GIS) environment.

In the work of Lubinszká, Majlingová (2011) an approach to the assessment of the susceptibility of the territory in terms of flood risk in a GIS environment is presented, rather focused on the assessment of the natural environment of the Poprad district based on a modification of the methodology published by David (2008).

Four groups of factors were evaluated: meteorological, soil, morphological and land use type. Based on the mutual evaluation of the individual layers of factors, an overall category (degree) of susceptibility was determined. Susceptibility was categorised into 5 classes as defined by international classifications (Figure 10.1).

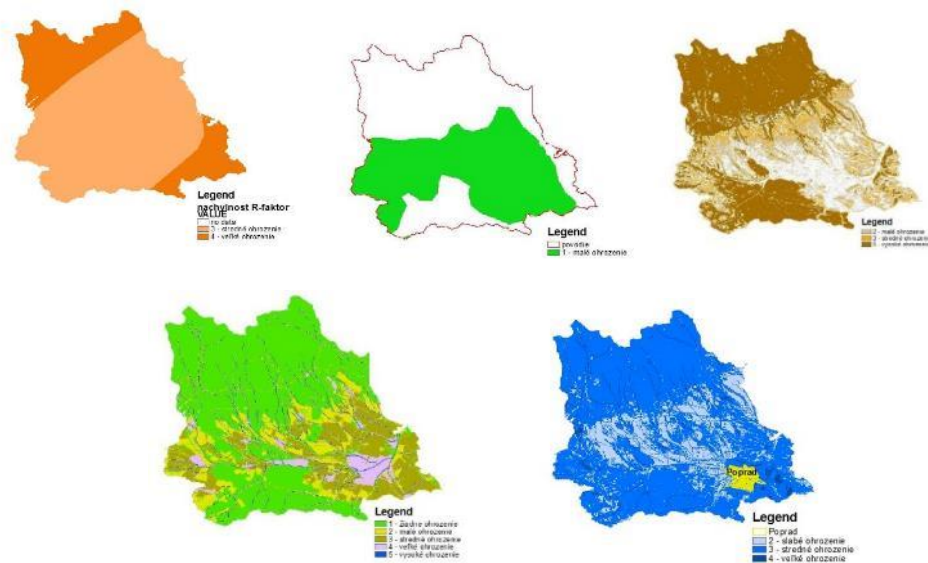


Figure 10.1 Result of the vulnerability analysis of the Poprad river basin area in the GIS environment  
(Source: Lubinszká, Majlingová 2011)

For the assessment of the susceptibility of the area to the occurrence of fire it is possible to apply the results of the analysis of the probability of the occurrence of fire in terms of the influence of factors in the area under consideration. This approach to fire risk assessment is based on statistical processing of analyses based on historical fire occurrence data. However, in some cases this approach cannot be applied due to the size of the base set, which consists of only a small number of forest fires that have occurred in the area in the past.

In such a case, a multi-criteria approach can be applied to assess the risk of fire occurrence, or to determine the susceptibility of the area, the so-called pooled susceptibility to fire (Figure 12.2), based on a multi-criteria assessment of the individual factors that are assumed to influence the occurrence and spread of fire in the natural environment.

**Susceptibility** The susceptibility of an area to fire in this case is assessed based on 2 groups of factors: natural and social.

The group of natural factors was represented by the relief shape factor, the terrain slope factor, the terrain exposure factor, and the tree species composition and stand age factor, the stand health or stand damage factor (wind or insect damage) and the fuel factor (fuel model representing the type of fuel and the amount of fuel occurring in the analysed area).

The group of social factors consisted of the following factors: distance from the nearest settlement, distance from the nearest road (state, forest, hiking trail and bicycle trail), the factor of berry picking, the factor of logging and forestry activities, and the factor of hiking and recreational areas.

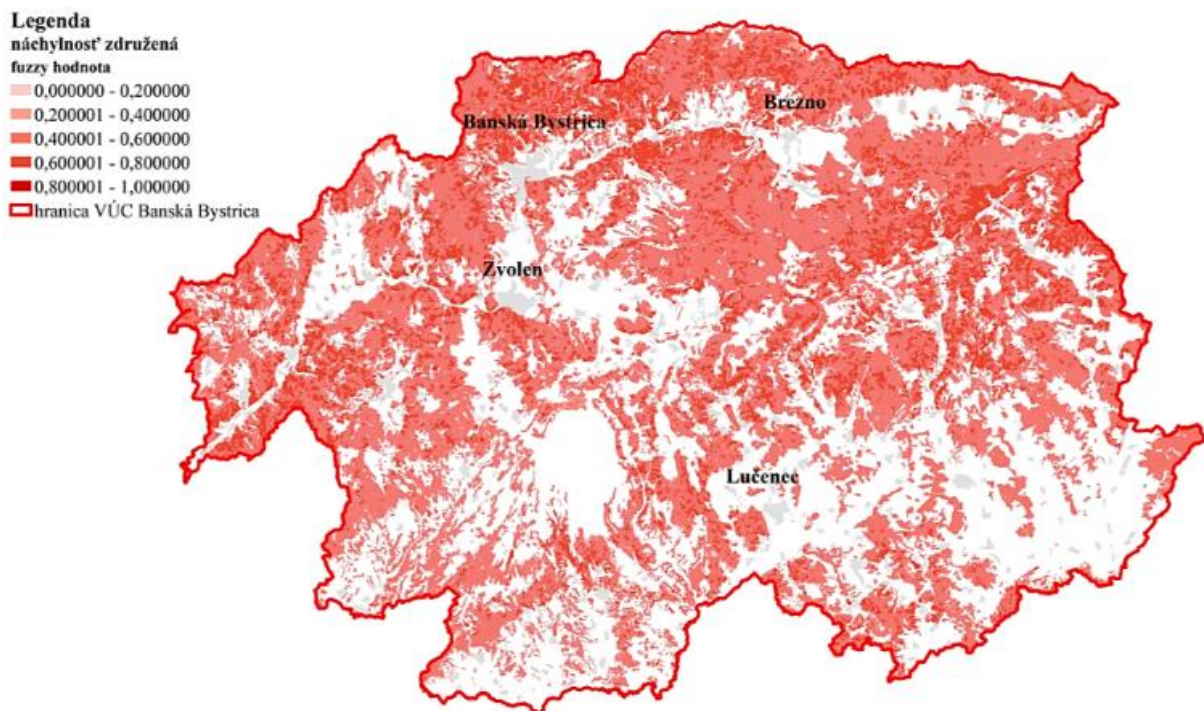


Figure 10.2 Results of the pooled susceptibility analysis on the territory of the Banská Bystrica self-governing region  
(Source: Majlingová, 2014)

## 10.2. VULNERABILITY ANALYSIS OF THE TERRITORY

**Vulnerability** The vulnerability of a **system**, infrastructure or any object at risk is made up of several components. The scope it presents is determined by the severity of the impacts of a given event. It indicates the potential for damage and is a variable that can be used to make forecasts. It has predictive qualities: it hypothetically represents a way of conceptualizing what can lead to the identification of a population in terms of the existence of risk and individual hazards. Determining vulnerability means seeking an answer to the question of what happens when any of the factors has affected any of the elements at risk (e.g., a community).

Vulnerability can often only be measured indirectly and in retrospect, and the dimension normally used for this indirect measurement is damage or harm in general.

What is commonly seen because of a disaster is not the vulnerability itself, but the damage caused. Vulnerability of the objects and features at risk is reflected in the relationship between the force of the hazard and the amount of damage it causes.

For vulnerability determination, it is advisable to use **means for modelling and simulation of phenomena**. These are often available as OpenSource software solutions that do not require a licence to work with.

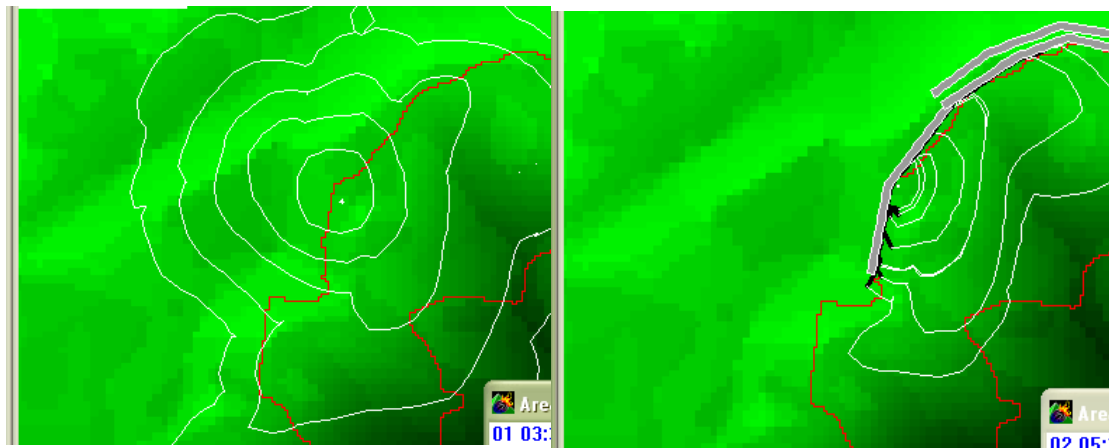
Among such systems, the hydrodynamic model HEC-RAS can be mentioned for modelling the extent of the flood zone (Figure 10.3). An alternative is the MIKE programme, but a licence must be purchased to work with it.

Both software applications are used in Slovakia. The **HEC-RAS** model is mainly used in research and the **MIKE** programme is also used by DHI Slovakia for modelling flood scenarios and determining the extent of the flooded area.



*Figure 10.3 Result of flood zone calculation in the HEC-RAS model  
(Source: Majlingová, Galla, 2015)*

To model the extent of the area affected by a forest/natural fire, it is appropriate to apply the forest fire behaviour modelling and simulation software **FARSITE** (Figure 10.4). In addition to the extent parameters (area, perimeter) of the fire area, it also provides information on fire intensity, flame height, fire spread rate, etc. It also allows to incorporate into the modelling information about an ongoing intervention (ground or air).



*Figure 10.4 Result of the calculation of the fire affected area in FARSITE  
(Source: Majlingová, Vida, 2008)*

For the purposes of estimating the source member, calculating impacts, and designing protective measures for the population and agriculture in the event of a nuclear or radiological accident anywhere in Europe, the **ESTE** programme is used (Figure 10.5).

In the event of a nuclear or radiological accident, ESTE: estimates the release of radioactive substances into the surrounding atmosphere (source term); models the propagation of radioactive clouds in the surrounding atmosphere (15 min step); calculates the radiological impact in the vicinity of the accident; doses to the population (from cloud, deposition,



inhalation); doses to emergency responders; doses during transfer of persons; doses to mobile groups (firefighters, rescue workers); proposes protective measures for the population, possibly for agriculture. This programme is currently used by ENEL Slovenské elektrárne a.s. and is specifically used by the Mochovce NPP crisis staff and the Bohunice NPP crisis staff.

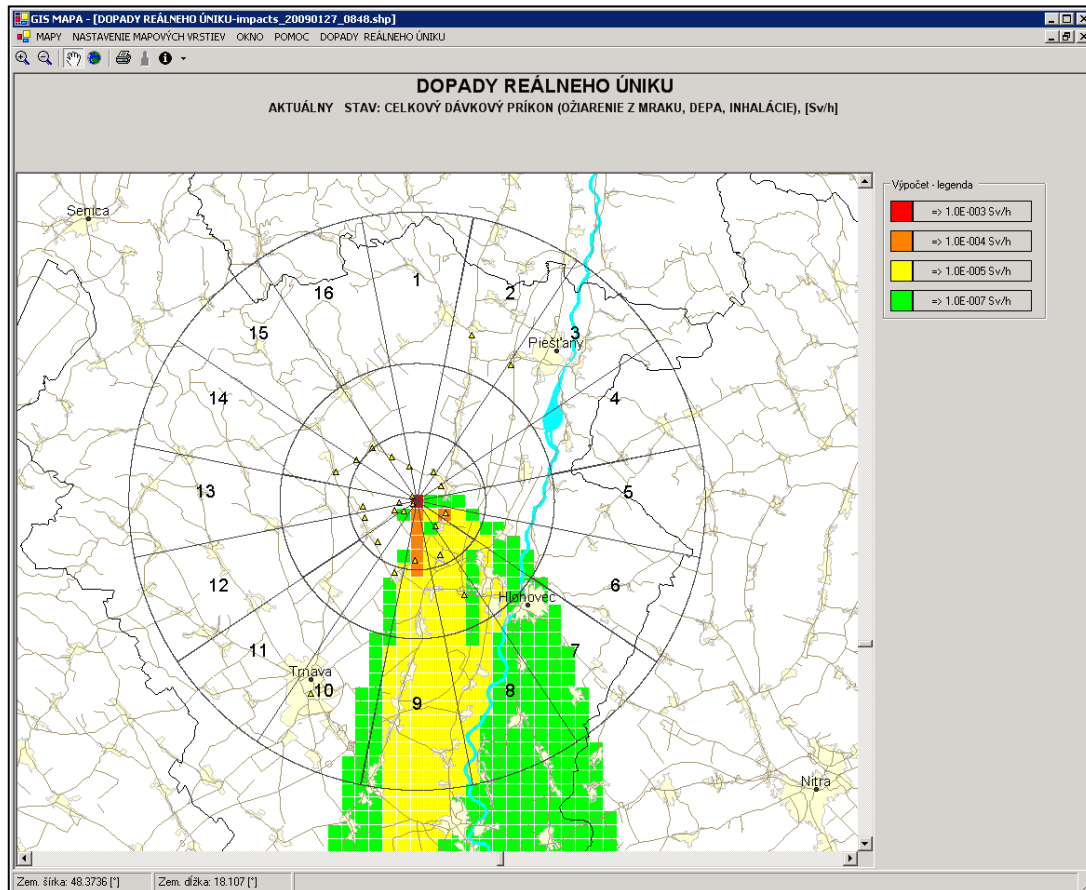


Figure 10.5 Calculated dose rates after a simulated accident in ESTE

From the point of view of prevention of major industrial accidents, specialists for prevention of major industrial accidents are increasingly turning to the available software tool ALOHA when drawing up emergency plans.

**ALOHA** is a tool for the chemical assessment of the area likely to be at risk following an accident with a release of a hazardous substance (NL) and for the detection of the consequences of a release of hazardous substances. The program assumes constant wind speed and direction in all horizontal directions, for dispersion of heavy gases and for evaporation from puddles, when performing numerical calculations. Reflection from the ground surface and from the low atmospheric inversion layer is also accounted for in the model. From a thermodynamic point of view, heat transfer from the evaporating pool is also accounted for and the ground surface.

Includes a database of the most used and transported hazardous substances and their physical properties. The result is a simple projection of the predicted threshold of injurious or lethal concentration in the field.

The program works with two mathematical models of dispersion of substances in the air, it allows to model the dispersion of liquids and gases in the air after their release. A Gaussian dispersion model is used to model the release of a gas lighter or of the same mass as air. This model can be used if some of the necessary information about the properties of the substance is missing or if a small amount has escaped. For heavier-than-air substances, the heavy gas dispersion model is used. This model is also used for two-phase leakage or if the substance is stored in a supercooled state.

The strength of ALOHA is the relatively accurate assessment of hazard zones and their subsequent plotting. It can evaluate the results in both text and graphical form (Figure 10.6).

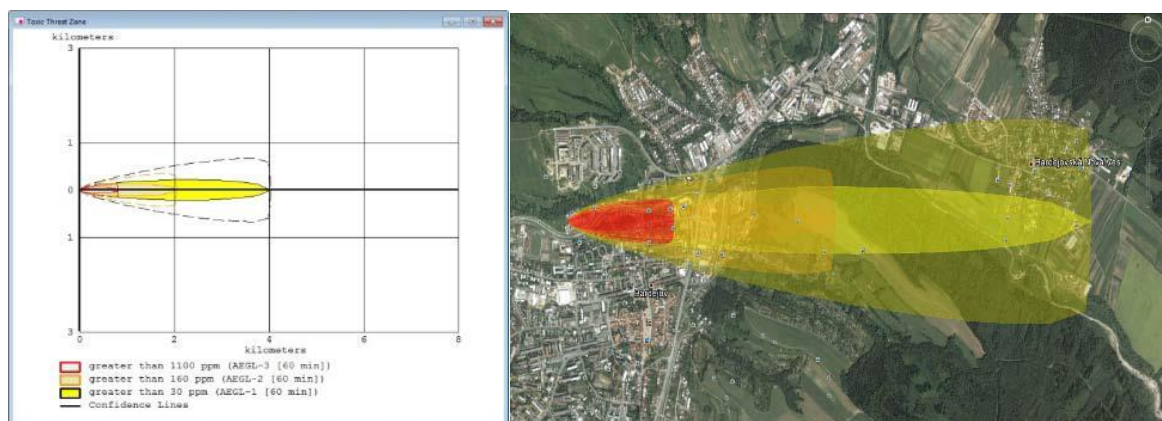


Figure 10.6 Result of the calculation of the area affected by the hazardous substance spill in ALOHA (Source: Majlingová, Boguská, Monoši, 2012)

### 11.3. WARNING SYSTEMS

One of the effective tools for minimizing the consequences of an emergency is **early warning**. Several warning systems have been developed and implemented abroad after previous negative experiences with large-scale emergencies.

For example, data on floods in individual EU Member States are collected, synthesised, and published through the European Flood Alert System (**EFAS**).

The European Flood Alert System (EFAS) is the first flood warning system to provide information free of charge to national and regional systems.

It was launched by the European Commission in 2003 with the aim of extending the time interval between the warning and the occurrence of the natural emergency itself, thus increasing the possibility for the population and emergency services to prepare, and clearly linking 2 main tasks: to complement the flood preparedness activities of EU Member States and to provide the European Commission with information leading to improved assistance and crisis management in the event of large-scale international floods requiring intervention at international level.

Since 2005, EFAS has provided national water and hydrological institutions and the European Commission with an early warning of an impending flood (for a time scale of 3-10

days), based on several inputs related to the current and forecast meteorological situation. The prototype is set up for the whole of Europe. It operates with a grid with a spatial resolution of 5 km and provides twice daily information to the national hydrological centres regarding the flood forecast for a given territory (Member State).

Only archived flood warnings are publicly available, real-time warnings are only available to national partner institutions.

In risk analysis based mainly on meteorological factors, sophisticated methods, datasets, and **data sets** ????? are applied in flood risk mapping activities and GIS tools. Hazard analyses consider the emergencies caused by the current climatic situation as well as the situation expected after its change.

**Flood risk assessment and monitoring and flood impacts** are implemented in accordance with continental approaches. In this respect, this activity provides support to several European Commission initiatives, including the European Flood Action Programme, the Directive on the Assessment and Management of Flood Risks, the Solidarity Fund and EU regional policy.

In terms of flood risk, areas are defined based on flood risk factors that contribute to the occurrence of floods as natural disasters. These are, for example, exposure and gambling.

Georeferenced data related to land use type are used to determine exposure. The hazard factor is implemented through hydrological methods at different scales and for multiple flood return periods. Random flood factors that can be triggered by a natural event include extreme rainfall and consequently extreme high flow in watercourses. The impending natural event (torrential rainfall - extreme rainfall) represents the hazard itself in the risk assessment. In addition, exposure is among the anthropogenic factors that contribute to increasing the risk of flooding in each location.

Advanced techniques based on GIS and datasets are essential elements of this approach to **flood risk analysis**. The issue of flood risk mapping has been studied at continental level. The objective of the warning system is to identify and map regions susceptible to flood occurrence and damage, as well as to quantify potential losses with the support of graded damage functions.

The results are usually presented in the form of **continental maps** (Figure 10.7).

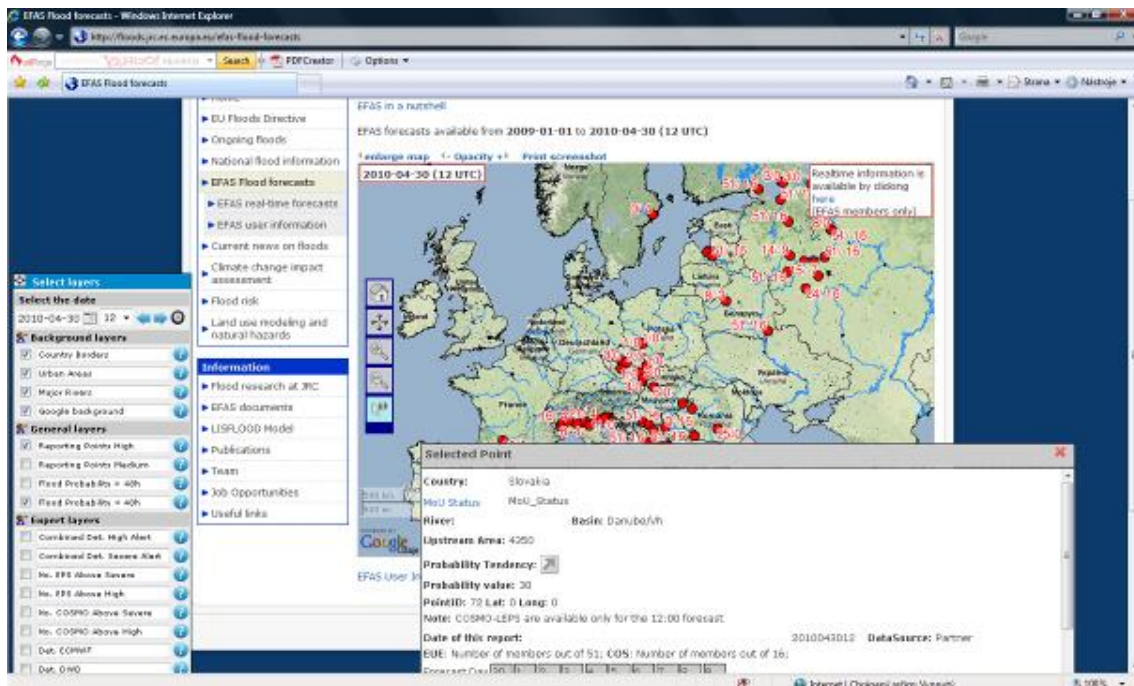


Figure 10.7 EFAS forecast map  
(Source: [EFAS](#))

The Global Flood Awareness System (**GloFAS**) is one component of the Copernicus Emergency Management Service CEMS. It is designed to support preparatory measures for flood events worldwide, particularly in large trans-national river basins. To provide information on both ongoing and upcoming flood events, GloFAS combines information from satellites, models, and in-situ measurements to produce: GloFAS forecasts, GloFAS Seasonal forecasts, GloFAS Impact Forecasts.

In terms of flood warnings, a flood warning system called **POVAPSYS** has been under construction in Slovakia for several years under the competence of the Slovak Hydrometeorological Institute (SHMI).

The Flood Warning and Forecasting System of the Slovak Republic (POVAPSYS) is aimed at innovation of flood warning and forecasting methods, operational operation and the necessary infrastructure. The Slovak Hydrometeorological Institute (SHMI) has been entrusted with its implementation.

The weather monitoring network of the SHMI was greatly modernized by the POVAPSYS program. Automatic Weather Stations (78) and Automatic Hydrological Stations (138) with various sensors sets were delivered within the scope of the project. The stations transmit data every minute to an acquisition centre where the information is checked for quality and processed further.

POVAPSYS integrates operational information from domestic and foreign sources for hydrological forecasting and flood hazard warnings. This information is publicly available to citizens and serves as data for flood protection and crisis management authorities.

The public is currently being informed about **hydrological warnings** via the SHMÚ web portal (Figure 10.8).

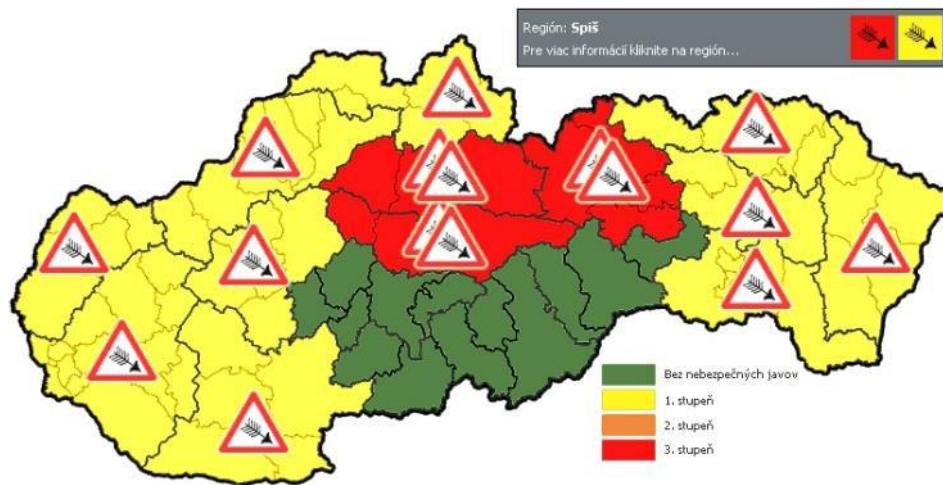


Figure 10.8 Map of hydrological warnings by SHMÚ  
(Source: [SHMÚ](#))

**EFFIS** – the European Forest Fire Information System is an EU tool to support decision-making within Member States by organisations responsible for forest fire protection. The system was set up in collaboration between the EU's Joint Research Centre (JRC) in Ispra, Italy, and the European Commission (EC). Since 2003, EFFIS has been regulated by Regulation (EC) No 2152/2003 of the European Council and of the Parliament (Forest Focus) on forest monitoring and the interactive effects of environmental factors. The services provided by EFFIS are operated through the web platform <http://effis.jrc.ec.europa.eu>. On this site, the available modules can be used to graphically visualise, and query information related to the current fire danger forecast, detection and location of existing forest fires, post-fire damage assessment. It also includes a database and mapping of historical fires within the EU Member States. The National Forestry Centre in Zvolen also contributes to this database annually with statistics on fires in the forests of Slovakia.

Figure 10.9 shows a view of the Fire Danger **Map**. Fire danger is determined based on the Canadian Fire Weather Index (FWI). In addition to the Fire Weather Index, the degree of fire danger can also be determined in terms of other characteristics such as Initial Spread Index (ISI), Fine Fuel Moisture Code (FFMC), Duff Moisture Code (DMC), Drought Code (DC).

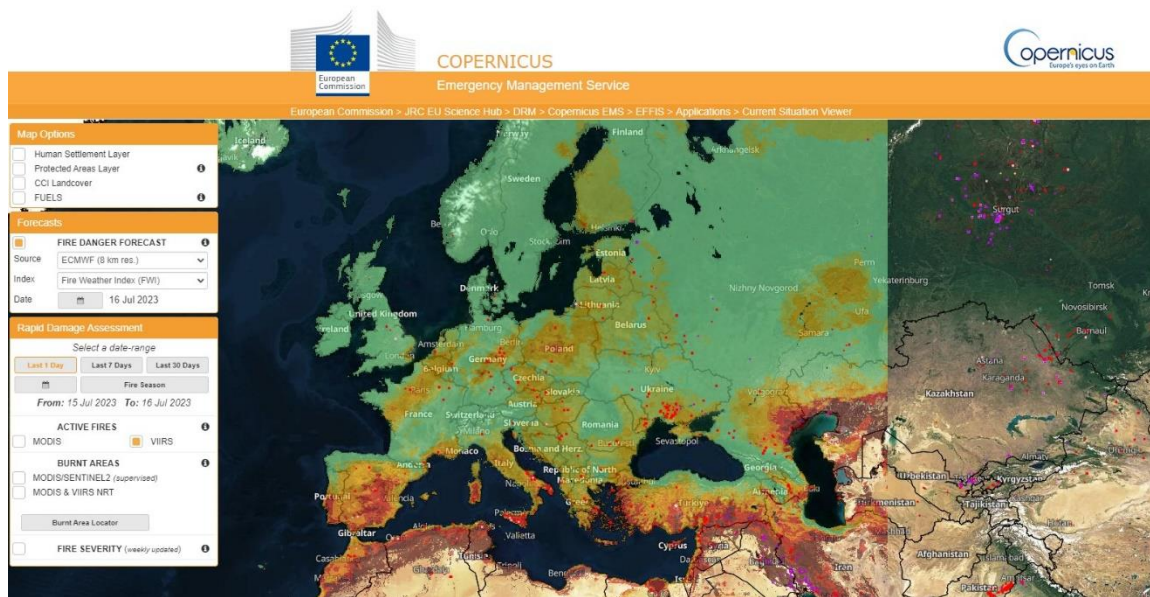


Figure 10.9 EFFIS fire danger map  
(Source: [EFFIS](#))

In Slovakia, a web portal operated by the Slovak Hydrometeorological Institute performs the tasks of a **fire warning system** and provides information on the so-called meteorological fire index (Figure 10.10), daily from April to the end of October each year.

**Predpoveď indexu požiarneho nebezpečenstva v lesoch dňa 21.05.2013**  
**Forecast of forest fire risk index in 21.05.2013**

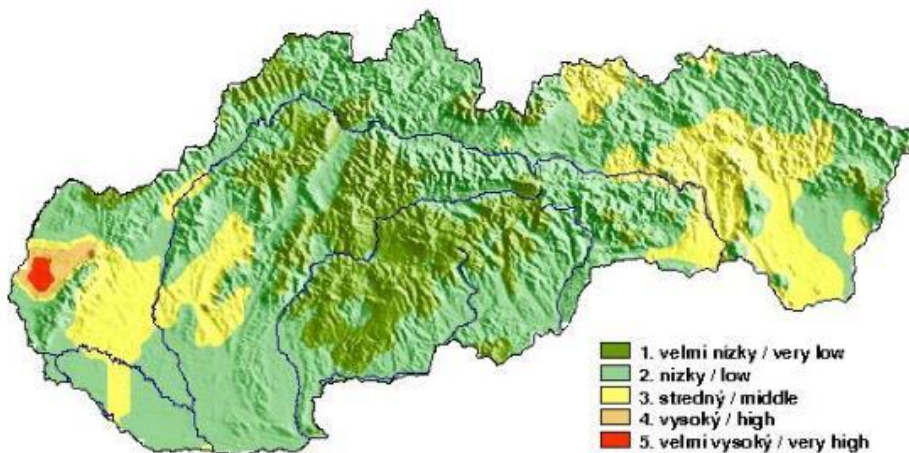


Figure 10.10 SHMI fire alert map  
(Source: [SHMÚ](#))

The SHMI updates the fire danger level in forests daily. Outside this period, only the map of Slovakia is shown on the screen with the colour of stage 1 and the inscription PATTERN across the map.

The calculation of forest fire danger indices is based on a model for determining the soil-climatic drought index. The classification establishes 5 forest fire DANGER grades: very low; low; medium; high; very high.

The map shows the current fire danger status for the day in a regionalised form. The distribution of the forest fire danger situation is calculated for the whole territory of the Slovak Republic based on data from 65 climatological stations and another 30 precipitation gauge stations, using special interpolation methods. Other maps reflect the fire danger situation in the previous 5 days. To illustrate the meteorological conditions, maps of daily precipitation totals and average daily air temperature for the days when we present the fire danger status are also shown.

The model for the determination of fire danger degrees in forests is based on a verified calculation of the soil-climatic drought coefficient for the territory of the Slovak Republic. The input data to the model are meteorological and phenological data and soil characteristics. Meteorological data are the average daily air temperature and daily atmospheric precipitation, phenological data include the onset of pollination of selected forest trees. The soil characteristic is the usable water capacity, determined as a function of the depth of the soil profile and the altitude. Based on the results of multi-year calculations, fire danger index boundaries have been established for 5 degrees, which determine the degree of fire danger in forests.

Available map outputs: map of fire danger indices in forests; map of daily rainfall (from 7 a.m. to 7 a.m. of the following day); map of average daily air temperature. Each of these maps can still be viewed in a larger format.

The fire danger of forests could be:

- **Very low** – Cumulative atmospheric precipitation greatly exceeds evaporation, moisture conditions in the topsoil profile are moist to wet.
- **Low** – Cumulative precipitation in the forest slightly exceeds evaporation, topsoil in the forest is moist.
- **Medium** – Cumulative precipitation in the forest is slightly lower than evaporation. The topsoil of the forest is slightly moist.
- **High** – Cumulative rainfall in the forest is below evaporation. The top layer of the forest soil is dry.
- **Very high** – Cumulative rainfall in the forest is well below evaporation. The top layer of the forest soil is overdried, traces of drought are also visible on the vegetation.

## CONCLUSIONS

Risk mapping and modelling using Geographic Information Systems tools and computer aided modelling tools are successfully used especially abroad. In the Slovak Republic these applications are unique. Although several risk analysis methodologies based on the application of these tools have already been developed in the academic sphere, security practice is not yet ready for their full use. There is a lack of specialists in practice who would be able to use these tools, and there is a lack of training of such specialists in the various security spheres.

Nevertheless, these are progressive procedures and techniques that have their use not only at the operational and tactical level, but also at the strategic level of crisis and emergency planning.

## REFERENCES

- [1]. DAVID, V. 2008. *Metodika stanovení povodňového rizika v malých povodích / Methodology for flood risk determination in small catchments*. In: GIS Symposium Ostrava 2008: proceedings of the international symposium held 27-30 January 2008 in Ostrava. Ostrava, VŠB Technical University, 9 p. ISBN 978-80-254-1340-1
- [2]. LUBINSZKÁ, Z., MAJLINGOVÁ, A. 2011. *An assessment of urban area flood susceptibility*. In Proceedings of the GIS Symposium Ostrava 2011, eds. Jan Růžička, Kateřina Pešková. VŠB - Technical University Ostrava, Ostrava, Czech Republic. 15 p. ISBN 978-80-248-2366-9.
- [3]. MAJLINGOVÁ A. 2010. *Základné pojmy z oblasti manažmentu rizík prírodných pohrôm a katastrof / Basic terminology in the field of risk management of natural disasters*. In Delta: scientific and professional journal of the Department of Fire Protection. Zvolen: TU Zvolen, 2010. ISSN 1337-0863. Vol. 4, no. 7 (2010), pp. 18-22.
- [4]. MAJLINGOVÁ, A. 2014. *Informačné systémy efektívneho nasadenia hasičských jednotiek pri lesných požiaroch na vybranom území SR / Information systems for effective deployment of firefighting units at forest fires in a selected territory of the Slovak Republic*. Dissertation thesis. Žilina: University of Žilina.
- [5]. MAJLINGOVÁ, A. 2015. *Multicriterial forest fire risk assessment applicable in Central Europe - Case Study*. In International Journal of Engineering & Applied Sciences (IJEAS). ISSN 2394-3661. Vol. 2, Issue 2 (2015), p. 45 - 50.
- [6]. MAJLINGOVÁ, A., BOGUSKÁ, D., MONOŠI, M. 2012. *Uplatnenie geoinformatiky v oblasti manažmentu mimoriadnych udalostí v podmienkach Slovenska / Application of geoinformatics in the field of emergency management in Slovakia*. In Advances in fire & safety engineering 2012 = Advances in fire and safety engineering 2012: proceedings of the I. international scientific conference: Zvolen, Technical University of Zvolen, 15-16 November 2012 / eds. Martin Zachar, Katarína Dúbravská. Zvolen: Technical University of Zvolen, 2012. ISBN 978-80-228-2375-3. s. 119-137.
- [7]. MAJLINGOVÁ, A., GALLA, Š. 2015. *Podpora priestorového rozhodovania krízových manažérov na lokálnej úrovni / Spatial decision support for crisis managers at the local level*. In Košice Security Review. Košice: University of Security Management, Vol. 1/2015. ISSN 1338-4880, pp. 57-69.
- [8]. MAJLINGOVÁ, A., VIDA, T. 2008. *Possibilities of forest fire modeling in Slovak conditions*. In Symposium GIS Ostrava 2008: proceedings of the international symposium held 27-30 January 2008 in Ostrava. Ostrava: VŠB - Technical University, 2008. ISBN 978-80-254-1340-1, 10 p.
- [9]. MAJLINGOVÁ, A., ZÁVACKÁ, M. KLIMENT, D. 2012. *An assessment of Hucava mountain stream catchment susceptibility to flooding*. In: Journal of Forest Science. Vol.



58/2012 (12). International lectured scientific journal of the Czech Academy of Agricultural Sciences, Prague, Czech Republic, p. 553 - 559.

[10]. Slovak Government Regulation No. 25/1997 Coll. on the categorisation of the territory of the Slovak Republic

[11]. ŠOVČÍKOVÁ, L. 2009. *Ako pracovať s programom Aloha 5.4.1 / How to work with Aloha 5.4.1*. Civilná ochrana, revue pre civilnú ochranu obyvateľstva, vol. 11(5),

[12]. TUČEK, J., MAJLINGOVÁ, A. 2007. *Lesné požiare v Národnom parku Slovenský Raj: Aplikácie geoinformatiky / Forest fires in the Slovak Paradise National Park: Applications of geoinformatics*. Zvolen: Technical University of Zvolen, 2007, p. 173. ISBN 978-80-228-1802-5.

[13]. TUČEK, J., MAJLINGOVÁ, A. 2009. *Forest fire vulnerability analysis*. In Bioclimatology and natural hazards. Dordrecht: Springer Science+Business Media B.V., 2009. ISBN 978-1-4020-8875-9, p. 219-230.13/XXVI/12 Instruction of the Director General of the Crisis Management Section of the Ministry of Interior of the Slovak Republic



## QUESTIONS

1. What software tools can be used to identify risks/threats?
2. What groups of factors are considered in a flood susceptibility analysis?
3. What software tools can be applied to analyse the vulnerability of an area to fire and flood?
4. What are the ALOHA and ESTE programmes used for?
5. List the warning/alert systems operated at EU level.

## ABBREVIATIONS

<b>OHS</b>	Occupational Health and Safety
<b>PR</b>	Point of Reveal
<b>CLA</b>	Check List Analysis
<b>DC</b>	Drought Code
<b>DMC</b>	Duff Moisture Code
<b>EFAS</b>	European Flood Alert System
<b>EFFIS</b>	European Forest Fire Information System
<b>EC</b>	European Commission
<b>ERA</b>	Environmental Risk Assessment
<b>ETA</b>	Event Tree Analysis
<b>EU</b>	European Union
<b>FFMC</b>	Fine Fuel Moisture Code
<b>FMEA</b>	Failure Mode and Effect Analysis
<b>FTA</b>	Fault Tree Analysis
<b>FWI</b>	Fire Weather Index
<b>GIS</b>	Geographical information systems
<b>HAZOP</b>	Hazard and Operability Study
<b>HRA</b>	Human Reliability Analysis
<b>ISI</b>	Initial Spread Index
<b>JRC</b>	Joint Research Centre
<b>MI SR</b>	Ministry of the Interior of the Slovak Republic
<b>ME SR</b>	Ministry of the Environment of the Slovak Republic
<b>NL</b>	Dangerous substance
<b>NC SR</b>	National Council of the Slovak Republic
<b>UN</b>	United Nations
<b>PHA</b>	Preliminary Hazard Analysis
<b>RM</b>	Rating Method
<b>POVAPSYS</b>	Flood warning and forecasting system of the Slovak Republic
<b>PZPH</b>	Prevention of major industrial accidents
<b>SA</b>	Safety Audit
<b>SHMU</b>	Slovak Hydrometeorological Institute
<b>SKR MI SR</b>	Crisis Management Section of the Ministry of Interior of the Slovak Republic.
<b>SR</b>	Slovak Republic
<b>STN</b>	Slovak Technical Standard
<b>TNT</b>	Trinitrotoluene
<b>WIA</b>	What If Analysis

## GLOSSARY

<b>Term</b>	<b>Description</b>
<b>Risk Analysis</b>	The process of assessing the sources of risks, the possible consequences and estimating the confidence with which these consequences will occur.
<b>Safety / Security Risks</b>	An aggregate concept in risk management and security management to refer to risks associated with the security of people, property, and information.
<b>Domino Effect</b>	A continuing event with increasing consequences.
<b>Risk Assessment</b>	The process of determining the magnitude (level) of risk in relation to the threat being analysed.
<b>Hazard</b>	The source of the potential occurrence of a negative event.
<b>Risk Management</b>	A systematic process in which risk is identified, analysed and the optimal way to manage it is defined at minimum cost and respecting the system objectives of the entity.
<b>Risk Monitoring</b>	Continuous checking, supervision, critical observation, or determination of status to detect a change in the desired or expected level.
<b>Susceptibility</b>	Predisposition of systems to damage.
<b>Dangers</b>	Anything that has the potential to cause harm, damage, harm, death.
<b>Resistance</b>	The ability of a system to adapt to the effects of a negative factor to the extent that the functionality of the system is not lost, and the system is not damaged.
<b>Threat</b>	A potentially dangerous situation that can arise.
<b>Risk Assessment</b>	Assessment of the acceptability of the risk in relation to its magnitude (level).
<b>Resilience</b>	The ability of a system or its individual components to return to their original state after being affected by a negative phenomenon

<b>Term</b>	<b>Description</b>
<b>Risk</b>	The probability of occurrence of an event/phenomenon, which is calculated most often based on the frequency of occurrence (relative frequencies) of a given type of negative event/phenomenon in the past.
<b>Synergistic effect</b>	Interaction of system elements of systems with the emergence of a new quality.
<b>Risk Mitigation</b>	Taking action to prevent or manage risk.
<b>Vulnerability</b>	Potential impacts of the negative phenomenon.

## REGISTER

- Acceptable risk, 22
- Anthropogenic risks, 24
- Causal dependence, 4, 47, 50
- Cosmogenic Risks, 25
- Credibility (likelihood), 35
- Danger, 11, 12
- Deductive methods of risk analysis, 58
- Determination of contexts, 30, 34
- Domino effect, 16, 20, 53, 54, 57, 148
- Economic risks, 24
- Exposure, 17
- Hazards of a non-military nature, 28
- Hazards of Military Conflict, 28
- Inductive methods of risk analysis, 56
- Managing risk, 29
- Managing the risk of an organisation, 40
- Qualitative analysis, 59
- Quantitative analysis, 59
- Residual risk, 21
- Resistance/Flexibility, 17
- Resource planning, 40
- Risk analysis, 33, 35, 36, 42, 43, 113, 131
- Risk assessment, 35, 36
- Risk assessment, 36
- Risk identification, 33, 87
- Risk Management, 29, 31, 32, 93, 116, 148
- Risk management, 36
- Risk, 7, 8, 9, 10, 11, 12, 16, 20, 21, 24, 30, 58, 104, 105, 110, 124, 129, 131, 132, 149
- Security audit, 61
- Security risk analysis, 42
- Security Risk Management, 32
- Security risks, 27, 148
- Security, 32
- Semi-quantitative analysis, 59
- Susceptibility, 17, 134, 135, 136, 148
- Synergetics, 54, 55, 57
- Synergistic effect, 15, 16, 54, 57, 149
- Terrorism, 13
- Threat, 10, 11, 12, 13, 105, 121, 148
- Threats, 12
- Uncertain, 7, 8, 10
- Vulnerability, 17, 137, 149

ISBN 978-80-228-3294-6