POLITICKÉ VEDY / POLITICAL SCIENCES

Časopis pre politológiu, najnovšie dejiny, medzinárodné vzťahy, bezpečnostné štúdiá / Journal for Political Sciences, Modern History, International Relations, security studies

URL of the journal / URL časopisu: http://www.politickevedy.fpvmv.umb.sk

Author(s) / Autor(i):	**Karel Kubečka – Magdaléna Náplavová – Petr Rožňák**
Article / Článok:	**The Possibilities of Employing Risk Analysis Methods and their Application to the Functioning of the Czech Republic's Integrated Rescue System**
Publisher / Vydavateľ:	**Fakulta politických vied a medzinárodných vzťahov – UMB Banská Bystrica / Faculty of Political Sciences and International Relations – UMB Banská Bystrica**
DOI:	**https://doi.org/10.24040/politickevedy.2022.25.2.208-229**

Recommended form for quotation of the article / Odporúčaná forma citácie článku:

KUBEČKA, K. – NÁPLAVOVÁ, M. – ROŽŇÁK, P. 2022. The Possibilities of Employing Risk Analysis Methods and their Application to the Functioning of the Czech Republic's Integrated Rescue System. In *Politické Vedy*. Vol. 25, no. 2, pp. 208-229. ISSN 1335 – 2741. Available at: https://doi.org/10.24040/politickevedy.2022.25.2.208-229

THE POSSIBILITIES OF EMPLOYING RISK ANALYSIS METHODS AND THEIR APPLICATION TO THE FUNCTIONING OF THE CZECH REPUBLIC'S INTEGRATED RESCUE SYSTEM[1]

Karel Kubečka – Magdaléna Náplavová – Petr Rožňák*

ABSTRACT
Based on risk analysis, the scientific study defines the possibilities of applying risk analysis methods and their application in the field of functioning of the integrated rescue system of the Czech Republic (hereinafter IRS). The study clarifies how the study understands the terms and categories: risk, security threats, risk management, risk analysis methods, integrated rescue system and IRS crisis management activities. It demonstrates the current dynamic and turbulent development of human society it brings with it many positive but also negative facts. The study presents a basic overview of risk analysis methods that can be applied in the field of IRS and defines the basic differences between the scientific method of SWOT analysis and UMRA. The scientific study submits proposals for the use of risk analysis methods and their application in the area of the functioning of the IRS of the Czech Republic.

Key words: risk analysis, security threats, risk management, risk analysis methods, Integrated Rescue Systém, risk

Introduction

Risk affects each and every aspect of human society, and is implicit in all decisions we make. Simultaneously, it permeates any environment in which

* doc. Ing. Karel Kubečka, Ph.D. is an Associate Professor at the Department of Economics and Management, AMBIS University, Lindnerova 575/1, 180 00 Praha 8 – Liben, Czech Republic, e-mail: kubecka.karel@ambis.cz.

* Ing. Magdalena Naplavova, Ph.D. is a Researcher at the Department of Security and Law, AMBIS University, Lindnerova 575/1, 180 00 Praha 8 – Liben, Czech Republic, e-mail: magdalena.naplavova@ambis.cz.

* Dr. Petr Rožňák, CSc., MBA, MCs. is a Lecturer at the Department of Security and Law, AMBIS University, Lindnerova 575/1, 180 00 Praha 8 – Liben, Czech Republic, e-mail: petr.roznak@ambis.cz.

DOI: https://doi.org/10.24040/politickevedy.2022.25.2.208-229

[1] Scientific study, created with the support of the project IGA-KEM-2022-01.

humans perform their activities – political, economic, social, life, security-related (obviously), and others. In other words, risk is people's everyday companion (Ivančík, 2022, s.133). Any human activity is burdened by a certain degree of risk, arising for instance from incorrect typological categorisation of a given region and its ground-level characteristics, conditions prevalent in that region, demographic composition of the region's population, urbanisation, migration processes, and so on. For example, a defective (in some way) survey of the population's opinion and attitudes towards the security and functioning of the respective components of the Integrated Rescue System (hereinafter also "IRS") may prevent the establishing of networks of police headquarters, fire stations for professional firefighters, or the health emergency rescue system – just because citizens' support seems to be lacking. In such cases, security goals as well as public investment may be frustrated.

The analysis of risks which is often described as a rather complicated task can employ a range of method, depending primarily on the availability of funding for the entire risk management enterprise. The cost of the risk analysis is determined, in the first place, by the type of analysis required. Also dubbed "screening", qualitative methods are notable for their quickness, simple application, lower demands regarding personnel and funding, and the relative ease of estimation of the result. On the other hand, while quantitative methods ("scooping") are much more demanding as regards time and funding requirements, they produce more precise, that is, more objective results.

The paper builds on the knowledge gathered by the study of risk management and the tools it offers for the preparatory, implementation, and project stages; during the implementation itself as well as for estimating the lifespan risks, including potential accidents and breakdowns. Besides that, the tools we discuss are applicable to expert decision-making under crisis management on all levels of responsibility. The main source of data for this paper are the expert activities the authors have performed between 1990 and 2021. In his role as an expert, the main author has provided over 500 expert opinions for various institutions. These include a substantial amount of opinions on matters related the topic of the paper, as requested by courts as well as the Police of the Czech Republic. The paper "*The Possibilities of Employing Risk Analysis Methods and Their Application to the Functioning of the Czech Republic's Integrated Rescue System*" thus builds on long-term experience with establishing and guaranteeing the proper operation of the Integrated Rescue System of the Czech Republic.

In our definition and understanding of risk management, we follow **M. Tichý's (2006)** book *Ovládání rizika: analýza a management,* as well as **Božek a Urban (2008)**, according to whom *approached qualitatively, risk is defined as the possibility that with some probability, an adverse event will occur that deviates from the expected state of affairs or trend, and that will cause greater or lesser losses of either movable or immovable property, damage to human health, or environmental stress*. The process of risk management, especially its respective stages and available methods, is also discussed in a monograph by **D. Řehák (2019)**.

1. Research Questions and Goals

Building on the risk analysis approach, the article has several aims. First, to to define the possibilities of application of risk analysis methods and their implementation in the functioning of the Czech Integrated Rescue System. For this purpose, it clarifies how several fundamental concepts are to be understood, including risk, risk analysis, risk management, methods of risk analysis, or integrated rescue system. Second, the study argues that the dynamic and turbulent development of human societies brings about many positive but also negative consequences. Third, the article provides a survey of risk analysis methods which can be applied to IRS-related issues. Fourth, it identifies key differences between the SWOT analysis and UMRA methods. Finally, the study proposes ways of applying risk analysis methods to the Czech IRS.

The article consists of four parts which address the main possibilities of employing risk analysis methods and their application to the Czech IRS::

1) Research questions and goals
2) Current security threats and risks, expressed by a mathematic formula
3) Risk management in the Czech Republic's IRS
4) Methods of security risk assessment applicable to the IRS

The study explores which developments and to what degree threaten the IRS's proper functioning, namely:

1) Insufficient application of risk analysis methods,
2) Current security threats and their underestimation
3) Lack of personnel and technical equipment, as well as political and financial support

There are several aspects in which the insights presented in the paper contribute to current knowledge:

1) Strategic importance: at stake are strategic plans and long-term visions for further development of the Czech IRS.
2) Importance of information: what are the main security risks and threats to the functioning of the Czech IRS system in the coming decade of the 21st century.
3) Importance of cognitivity: how to characterise the impact of threats, anticipated security risks, and possibilities of their prevention and overcoming.
4) Scientific significance: prediction of the probability of occurrence of threats in the respective components of the Czech IRS.

2. Current Security Threats and Risks

As pointed out by **Ivančík and Nečas (2019, p. 3)**, the dynamic and turbulent development of contemporary human societies brings about many positive but also negative realities which are manifested in various spheres of life of both individuals and the human civilisation as such. This is evidenced by the numerous threats and risks, both traditional and newly arising, that justifiably push security-related questions to the forefront. This is because security constitutes a fundamental, necessary condition of the development of any human society; moreover, in the current era of deepening globalisation, there is no sphere of social life left which would be isolated from threats and risks (Ivančík, Nečas, 2019, p. 3). The complexity and multidimensionality of the study of threats and risks is underscored by the manifold related concepts and adjectives. These are both general, such as security threats, or political, economic, environmental etc. risks, and specific, for example as embodied in the set of adjectives linked to the threat of terrorism – cybernetic, environmental, religious, subversive, repressive, ethnic, criminal, political, pathological and so on (Ivančík, Ušiak, 2014, p. 92). This is one reason why in this section we deal with current security hazards and risks as identified by the state authorities, thus representing potential threats to the security of the Czech Republic.

2.1 Current Security Threats

The "Security Strategy of the Czech Republic" adopted in 2015 defines a set of current security threats (or challenges), as listed in Table 1.

Table 1: Current security threats

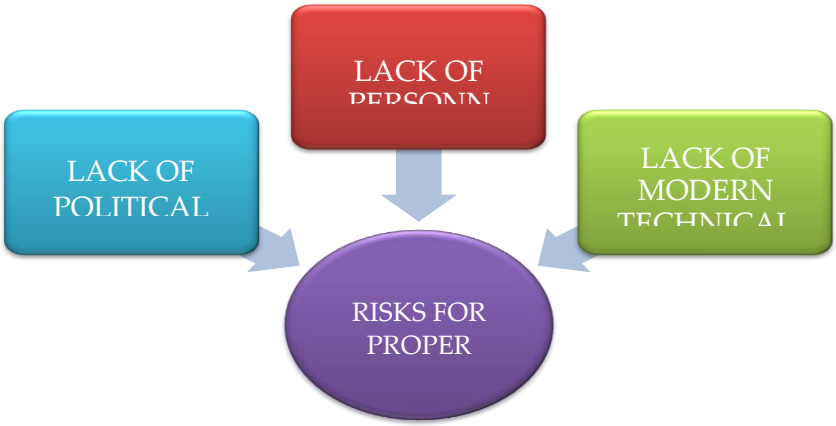
Extremism
Crime and socio-pathological phenomena in socially excluded neighbourhoods
Cyber attacks
International migration
Instability and regional conflicts in and around the Euro-Atlantic area
Instability in Northern Africa, the Sahel and the Middle East
Threats to the operation of critical infrastructure
Organised crime and corruption
Weakening of the cooperative security mechanism and of political and international legal commitments in the area of security
Disasters of natural and anthropogenic origin
Proliferation of weapons of mass destruction and their means of delivery
Interruptions of supplies of strategic raw materials or energy
All forms of terrorism

Source: (MZV, 2015), modified by authors

2.2 General Classification of Risk

The risk to the proper functioning of the IRS consists mostly in the potential lack of personnel and modern technical equipment, as well as of financial support for research and development. The lack of security professionals, also underpinned by political indecision and inadequate flow of funds to the IRS, proves, in terms of the smooth functioning of the security system, to be sand in the gears, as captured in Figure 1.

Figure 1: Risks for the proper functioning of the IRS



Source: authors

The degree of risk within IRS, that is, the probability of breakdowns in creating the respective units of the IRS, is countered by the the Act on the Integrated Rescue System (No. 239/2000 Coll.), the Ministry of Interior Decree No. 328/2001 Coll., on certain details of the security of the Integrated Rescue System, the Government Resolution No. 369 of 27. April 2016, on the Analysis of Threats to the Czech Republic, and other relevant normative regulations. This means that the degree of risk is largely covered by legal provisions, the compliance with which secures the limitation of likely risks to a socially and economically acceptable level; alternatively, these provisions cover the risks completely if complied with. Despite all these legal measures, the instituting of the IRS faces failures and defects. These are not negligible, especially from the economic point of view, which is why methods are being sought to identify the causes of these failures.

Risk is the probable damage resulting from a known hazard which happens to materialise. It is a combination of the probability of occurrence and the intensity of the negative phenomenon. The risk can be calculated for "n" independent sub-processes, as the product of probabilities of the occurrence of damage and the amount of damage (expressing the percentage of probability that the event under scenario 'i' will occur; usually up to 0.95, since a probability greater than 95 % is considered almost certain).

$$R = \sum_{i=0}^{n} (C_i \, . P_i)$$

Adopting the labelling and nomenclature, we can define the relationship as a portfolio of risks given by the product of the damage incurred and the probability of its occurrence:

$$R_S = \sum_{i=0}^{n} (Dm_i \, . \overline{P_i})$$

where

- ***i*** represents the respective situations (scenarios) studied as standalone risks;

- R_s is the risk the amount of which is expressed monetarily (in a given currency);
- P is a dimensionless quantity, expressing the probability with which the event according to the given scenario, and thus also the damage "D" will occur, ranging from zero (i.e. zero risk) to one (when the probability is one hundred percent, that is, it is certain to occur – then it ceases to be a "risk");
- D is the monetary damage (in a given currency) that will occur if the relevant hazard scenario is realised.

$$Rs \equiv (Rs_1;\ Rs_1;\ \ldots\ Rs_n)$$

In this way, provided we are able to quantify the expected amount of damage (in monetary or other units), we can determine the absolute degree of risk. Otherwise we deal with relative risk analysis, which results in ordering of a selected group of risks according to their severity. In such cases, we speak of risk prioritisation. One example of a qualitative method which aims at risk prioritisation is the risk matrix or risk map. This is constructed on the basis of appropriately selected parameters which allow comparison of risks within a given group. However, risk matrices/maps should not be seen as expressions of absolute values of risk, and thus cannot ground comparisons of the risks associated with different projects and their implementation.

Relative methods are sometimes referred to as "expert" methods, as they are based on the assessment by a group of experts. An important tool in the relative risk analysis is the RPN [Risk Priority Number] Index. In risk management as well as in the very establishing of the IRS, the concept of risk is to be construed as a defined and financially articulated uncertainty, or as a defined danger (threat) of a severe harm (again expressed financially), or even a loss of life which, with some probability bordering on certainty, can become severe harm. In the context of risk management, the concept of risk should not be confused with the concepts of danger/threat or harm.

In instituting the IRS of the Czech Republic, the benefits of the procedure should not be underestimated according to which the responsible person (e.g. the incident commander) becomes more acutely aware of the extent of the danger (hazard scenario) and estimates the degree of risk, in order to have the acceptable risks assessed by experts and include them in relevant economic

considerations. The goal is to either eliminate or limit to an acceptable degree (if the risk cannot be eliminated) the risk of failures and defects in the IRS's operations. Table 2 provides a register of potential risks which should be definitely avoided on the strategic, operational, and tactical levels of command and management. The respective risks in the register are ordered alphabetically, with the severity of risk categorised as "normal", "serious" or "critical"

Table 2: Risk register for modern equipment and R&D (in alphabetical order)

Risk register for IRS's modern equipment and R&D	
Reduction of funds for IRS units	Serious risk
Changing criteria for implementation audits	Normal risk
Non-acceptance of outputs within the resort	Normal risk
Non-acceptance of outputs vy involved parties	Normal risk
Failure to meet the schedule	Normal risk
Insufficient quality of the implementation team	Normal risk
Insufficient knowledge of strategic objectives by members of the implementation team	Normal risk
Insufficient staffing, time constraints of the implementation team	Normal risk
Inadequate management	Normal risk
Failure to meet objectives	Normal risk
Unmanageable process of public procurement	Critical risk
Inappropriate implementation plan	Normal risk
Unwillingness to execute implementation plans through ESIF-funded projects	Serious risk
Failure to secure funding for R&D	Critical risk
Staff turnover	Serious risk
Political risk	Normal risk
Advancing individual actors' self-interests in disregard of stated objectives (resortism)	Normal risk
Budget overrun	Normal risk
Employing different indicators, regardless of the established indicator system of operational programmes	Normal risk
Production of low-quality outputs	Serious risk
Protracted administration of applications for support from structural funds	Normal risk
Delays due to the need of legislative changes	Normal risk

Source: the authors

3. Risk management in the Czech Republic's IRS

Risk management is a part of the job description of managers at all levels of the IRS. The main task of the command staff in risk management is to identify and specify the hazard, determine the possible scenarios, define risks, and incorporate these risks into all phases of preparation and execution of the resulting order.

The extent to which the knowledge required to manage risks will be applied depends not only on the knowledge and skills of the incident commander, but also on the magnitude and complexity of the task (objective) – that is, its nature. In general, the authorised incident commander may act solely on the basis of his/her own experience or that of his subordinates, or he/she may invite risk experts.

The incident commander acts within a space defined by phenomena which may (or may not) occur; that is, he/she operates under conditions of uncertainty which are difficult to assess in economic or financial (monetary) terms. The scope of responsibility is defined by the following basic steps:

- identification of threats,
- analysis of threat scenarios,
- assessment of threats.

Employing this basic procedure, risk engineering seeks to answer the following specific questions:

- which adverse events may occur,
- if an adverse event occurs, what damage it causes,
- what is the probability of such an event occurring.

In establishing the Czech IRS, the benefits of the procedure should not be underestimated according to which the responsible person becomes more acutely aware of the extent of the danger (hazard scenario) and estimates the degree of risk, in order to have the acceptable risks assessed by experts and include them in relevant economic considerations. The point is to secure reliability; to prevent risk, damage, or technical and factual defects/mistakes in management; to ensure the longest possible service life of the equipment; and to avoid loss of life as far as possible.

Reliability – is the capacity of the IRS or its components to perform the function specified by the Integrated Rescue System Act and the Ministry of the Interior Decree on certain details of IRS security.

Damage – is the material or social effect of the occurrence of hazard; it is a

random variable. Its magnitude depends on the hazard scenario which changes over time. Within the IRS, damage is conceptualised as harm caused to property which can be objectively expressed in terms of financial losses (regarding technological equipment or material), but also of the loss of life of citizens. We can distinguish actual damage and loss of economic benefits. The standing principle is that damage is to be prevented, while the preferred compensation is restoration to the original state of affairs. Other means of compensation (e.g. money) become available only if restoration is not possible or expedient. In determining the amount of the damage, the value of the item at the time of the damage shall be taken into account. In criminal law, the amount of damage caused by a crime or offence co-determines its degree of danger to society. The concept of "damage" is frequently used especially in legal matters. Thus, we are not concerned about uncertainty, hazard, risk of harm or loss; rather, what matters is the harm or loss that has either already obtained or will obtain with certainty.

Technical lifespan (also *physical lifespan*) – is the timespan between the start of the use of the allocated combat equipment and human beings, and the moment when either the equipment or the IRS member ceases to perform the assigned function.

Factual defect – a factual defect occurs in case the relevant thing or action (management, command, decision-making) lacks the qualities it is normally expected to have, or that have been agreed upon, or that have been optionally or obligatorily stipulated by a superior's order. The usual legal consequence of a defect in a thing is the liability for defects as specified in civil or commercial law, military ordinance or regulation. Defects in things then may be either removable or irremovable, and either obvious or latent (i.e. those which do not surface immediately).

Lifespan – is the ability of armies to perform a required function under given technical conditions within a specified period of time.

3.1 The Probability of Occurrence of Risks Hazards in the units of the Czech IRS

To determine the likelihood of a risk occurring:

1) various exact procedures are employed. The most widely used is statistical analysis of the frequency of comparable situations. However, very often the only method available is expert estimate.

2) because hazard scenarios evolve over time, the probability of their occurrence must also be determined with respect to time.
3) The *P* variable is in fact a coefficient that reduces the amount of expected (future) damage which needs to be incorporated into calculations and budgets of the technical, material, and personnel equipment of the IRS. A situation in which the probability of the scenario becoming reality exceeds circa 90 to 95 % (P = 0.90 to P = 0.95) is usually no longer considered a risk, but rather a situation that will occur; the expected damage D is then included in the considerations without any reduction.

Shortcomings and errors in the management and command of the IRS

Management and command of the IRS or its components requires avoidance of defects and errors in the activities of incident commanders as well as managers responsible for the smooth operation of the apparatus which consists of the respective units of the Integrated Rescue System. In terms of time, errors in the management and command of the IRS emerge as either sudden or gradual errors.

As regards their magnitude, shortcomings of management and command (qua causes of failures) can be categorised as minor, major, and critical. Minor, less serious errors are those which do not substantively reduce the capacity of the army with respect to the given purpose. Major errors may result in a failure of any of the IRS component units, or limit or reduce their usability. Finally, critical errors may, as suggested by theoretical assumptions or previous experience, lead to hazardous consequences.

3.2 Using the Lessons from Shortcomings and Errors to Reduce the Command and Management Risks of the IRS

Experience makes it obvious that the extent and severity of failures in the IRS management and command impacts decision-making as well as the level on which information is communicated. Presently, there is information exchange at the expert level via R&D, exchange of experience during exercises, deployment of IRS units' members to international missions, and joint exercises.

3.3 Risks Accompanying the Establishment and Securing of Operations of the IRS

Risks can be categorised according to varying perspectives on the army and its activities. Technological and logistical risks are those which arise during the

preparation, construction, and supply phases.

The basic categorisation of these risks follows the chronology of establishment and lifespan of the necessary technological equipment, other material, and personnel required for securing the functioning of the IRS. As such, these risk may arise:

- during the construction of the IRS (via material, personnel aspects);
- during preparations for intervention;
- during the intervention itself, that is, the deployment of technological equipment and human resources
- during the period of use and the lifespan (of technological equipment and personnel)

Preparatory stage

This stage includes the creation of an effective integrated system for the protection of persons and property, the preparation and deployment of appropriate forces and assets, and the participation in the collective system. The conception is based on the security interests and principles of ensuring the protection and defence of the citizens and the state, as formulated in the relevant legislation and subordinate law. It responds to changes in the security environment and predicts its development in the relevant medium-term time horizon. It is based on the intention and plan for the deployment of the Czech IRS, as well as the expected budgetary framework.

Implementation stage

The implementation stage is the period between the commencement and the completion of all operations, sufficiently long so that all functions of the intervening IRS units can be tested. It also covers all relevant emergency meetings and management. The success of the this stage in mitigating the risk of construction and securing the smooth functioning of the mechanism depends on the IRS remaining a full-time job, replenished on a voluntary basis in time of peace, with a balanced structure which ensures that all capacities are maintained and further strengthened (with none of them being diminished).

Project stage

This stage responds comprehensively to threats, risks, trends and their future development, in order to minimise the possible strategic shock. It articulates how the IRS can be used in order to contribute to ensuring a stable security environment, strengthen the deterrence potential of collective defence arrangements, and deal with emergency situations across the entire spectrum of its operations.

Implementation

The implementation itself stands for management of development and modernisation projects that will achieve the highest degree of efficiency, effectiveness, and cost-effectiveness. In order to prevent the occurrence of various kinds of risk (emergencies, failures and errors in the command and management of IRS units), sufficient number of educated and well-trained personnel is necessary, matching the needs and requirements of modern technology and capable of performing demanding tasks in the conduct of a whole range of missions.

Lifespan risk

The lifespan of the construction, development and use of the IRS is affected by the rapidly changing external security factors, the predictability of which is constantly decreasing as a result of globalisation. This is a risk that requires permanent analysis of the security environment and security threats, while permanently updating the likely scenario of the deployment of the IRS in dealing with crisis situations.

4. Methods of security risk assessment applicable to the IRS

Risk assessment methods (predominantly of the relative kind) are tools and instruments readily available for IRS risk analysis and management. None of the methods on its own is to be understood as providing complete guidelines for risk analysis or management. Often, these methods at least partially overlap, and the modes of their application are highly varied. The very process of risk analysis and management, selection of the respective methods, their combination, securing

the input data as well as interpretation of both partial and final results is always the responsibility of the commander, or a group of military specialists authorised to conduct the analysis in question.

4.1 Brainstorming

This is a verbal expert method the goal of which is rapid and immediate gathering of as many of straightforward expert opinions as possible, with the number of experts in the group ranging from three to ten (or more). No attempt is made to unify their opinions. Experts thus act as mutual catalysts of their ideas.

4.2 Delphi Technique

This technique allows to obtain expert information and opinions without them having to meet in person, as required e.g. by the brainstorming method. The person in charge (e.g. commander of the territory or his/her risk analyst) picks a group of experts, compiles a set of questions (which should be "inspirational", rather than direct and thus possibly misleading), solicits responses from the experts, evaluates the opinions obtained, and summarises them. The questions, including the evaluation of the first round, are once again circulated among the group of experts so that they can review and update their judgements in the light of the views of the other participants. This procedure gets repeated several times (with the number of rounds subject to the incident commander's discretion).

4.3 Probabilistic Risk and Safety Assessment

This method determines the contributions of individual vulnerable parts to the overall vulnerability of the system. It has been developed specifically for the military, nuclear, aerospace and chemical industries, and is now making inroads into the areas of construction, finance and transport. Among others, FTA techniques are also used within this method (see below).

4.4 Event Tree Analysis – ETA

Event Tree Analysis visually illustrates the ways a given process may (or might) evolve. Each event causes another event, which can be either favourable or unfavourable, and occurs with a certain probability. Pictorial representation of the systemic tree of events amounts to a branching diagram described by agreed-on symbols and notation. The aim is to represent all events that may take place in the assessed system. The original application of this method was in the field of risk assessment of nuclear reactors, spacecraft, satellite and the like.

4.5 Failure Mode and Effect Analysis – FMEA

This is a mixed method combining verbal and numerical techniques of relative risk analysis. In the initial phase, a triplet is identified (project element; possible mode of occurrence of defect/fault/error; possible consequences of defect/fault/error) which may emerge in the project during the period of reference. In the next phase of FMEA, the risk priority index RPN [Risk Priority Number] is estimated for each of the triplets identified (Element; Mode; Consequence). Upon calculating the RPNs, the triplets are ranked from the highest RPN value to the lowest, thus obtaining a sequence revealing the relative level of risk for each triplet.

4.6 Failure Decomposition Analysis – FDA

The FDA is a method that enables risk assessment by constructing a two-dimensional matrix whose rows or columns contain the probability of occurrence of a defect, or the consequences of a defect for the project. It aims to categorise the expected situations into groups of acceptable risks and extreme risks. It is evaluated mathematically.

4.7 Failure Tree Analysis – FTA

Analysis of the tree of failures, defects, errors etc. involves systematic backward analysis of events (via a chain of causes) which may lead the analyst to the sought-for peak event. The FTA method is a graphic-analytic, or a graphic-statistic one. Visual representation of the systemic tree of failures, defects, or errors amounts to a branching diagram described by agreed-on symbols and notation. Employing analytical or statistical methods, the main objective of failure tree analysis is to assess the probability of a peak failure.

4.8 Hazard Analysis – HAZAN

HAZAN [HAZardANalysis] risk analysis allows to find the causes of project/plan failure by identifying the causes of failure, the probability of their occurrence, as well as the measures to reduce their occurrence.

4.9 Hazard and Operability Study – HAZOP

HAZOP is an umbrella term for the systematic assessment of complex processes or projects/plans in terms of risky and potentially dangerous sub-activities. The assessment is carried out by a team of experts. The HAZOP approach is based on a probabilistic assessment of hazard and the resultant

risks. Analysts use a spreadsheet in which they fill evaluation terms (guidewords). The unplanned or unacceptable consequences identified by the analysis are then reiterated in a final recommendation, with the goal of improving the process. This method was first utilised in the petrochemical and energy industries.

4.10 Monte Carlo Simulations

In technical-economic issues, the Monte Carlo method has a wide range of application. It consists in solving complex mathematical problems (involving random variables) by means of multiple computer-based simulations of these variables. The simulations proceed via pseudo-random numbers generated by the computer. The Monte Carlo method is used, among others, in nuclear physics or in operational research. With respect to the Czech IRS, this method facilitates solution of relatively complex mathematical problems of a random kind, provided the problem at hand can be modelled as a formally equivalent probabilistic problem. As regards our field of interest, the method can be used e.g. for estimates of the total costs and total time needed for building of an integrated rescue system and its respective components, as well as other facilities. Various types of simulation software can be put to use here. The random input variables in this case are costs and time required for the sub-activities. First, either the authorised military analyst or a team of experts create a model sensitive to mutual relationship between the input variables, define their distribution, and determine the criteria for evaluating the results of the simulation. Subsequently, using suitable software, they run a certain number of simulations (about 103 to 106) and record the frequency of the resulting values. Given a sufficient number of simulations, we obtain the values' probability distribution. Such results then make it easier to determine, for example, how likely it is that the implementation deadline proposed in the works contract will be exceeded, or that the specified costs of the purchase of equipment, the construction of facilities, their reconstruction and renovation, etc., will be exceeded. The computer programs used in these simulations can also perform a sensitivity analysis – that is, determine which activities have the greatest impact on the projects' total costs and which activities have the greatest impact on the lead time.

4.11 SWOT Analysis

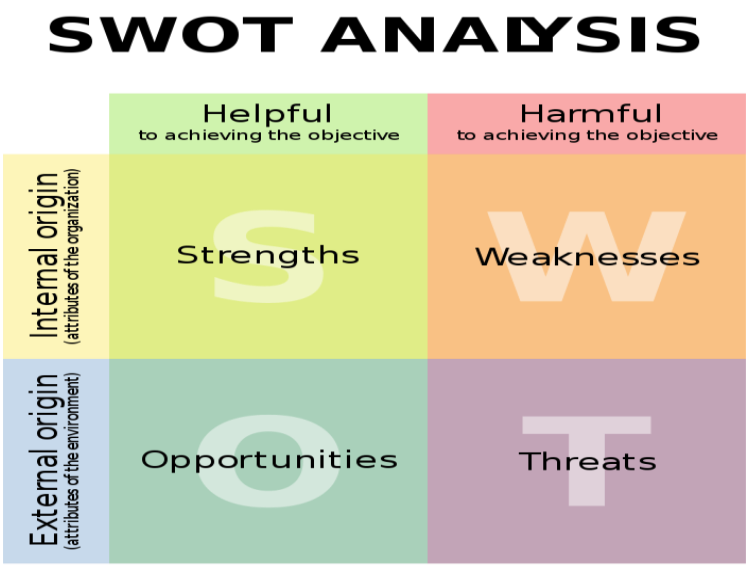
The SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is a widely used expert analysis applicable to projects, processes, and organisations. It takes into consideration both internal and external influences. The experts seek

to identify:

a) Strengths of the organisation/project/process;
b) Weaknesses of the organisation/project/process;
c) Opportunities presented to the organisation/project/process;
d) Threats that may harm organisation/project/process

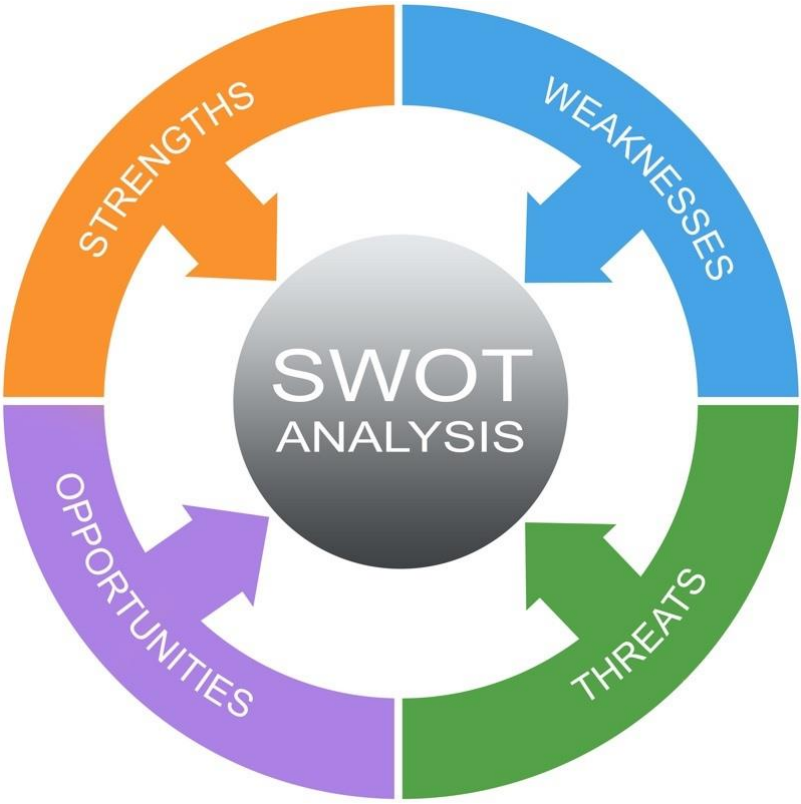
For clarity purposes, experts' responses (usually from among the organisation's employees) are arranged in a SWOT matrix.

Illustration 1: Schematic representation of a SWOT analysis matrix (Kubečka, 2017, p. 49)



The basis of the method consists in classification and evaluation of individual factors which are divided into four basic groups, as shown in Illustration 1. Evaluated mathematically, the respective groups represent sub-matrices, with the SWOT analysis data forming the matrix itself. By interacting the factors of Strengths and Weaknesses, i.e. the two internal sub-matrices of the process ("internal factors") against the Opportunities and Threats, i.e. the two external sub-matrices ("external factors"), new qualitative information can be obtained which captures and rates the level of their mutual conflict.

Illustration 2: Schematic representation of a SWOT analysis. Source: SWOT Analysis.projectsmart.co.uk, 2021



The SWOT analysis is among the foundational tools of strategic (crisis) management; in fact, it was originally developed for this very purpose. As stressed by **(Kubečka, 2017, p. 50)**, the method can be used to assess virtually anything which the evaluator is able to describe, provide the value of the evaluated factor, and estimate its significance or weight. In this way, a relationship is derived which captures the contribution of the evaluated factor to the resulting features of the whole. The place of SWOT risk analysis and its ability to provide information on the (in)appropriateness of the actions by incident commanders or individual officers of IRS units is difficult to replace. Moreover, compared to the UMRA, it can incorporate variable weights of individual factors and risks.

4.12 Universal Matrix of Risk Analysis – UMRA

The **Universal Matrix of Risk Analysis** method builds on the principle of comparative logical-numerical analysis, by a team of IRS experts, of the evaluation of the degree (severity) of hazard for the problem at hand (that is, either the intervention as a whole or any of its constitutive parts). The IRS expert team focuses on an identified part of an intervention which responds to a particular risk. There can be any number of analysed parts of the intervention which are evaluated by the expert team, with different (or identical) parts open to independent assessment by various expert teams consisting of variable numbers of experts **(Kubečka 2017, p. 78)**. UMRA is a mixed verbal and logical numerical expert method in which, first, the segments of the project at risk, the sources of hazard, and the conjunctions of the two are identified. Subsequently, these conjunctions are ranked according to their significance. This method can process responses by experts possessing varying levels of knowledge about the project as well as different sensitivity to hazard. The objective of this expert method of risk assessment is to provide, with the greatest accuracy possible, information on the source of hazard, as related to the consequences and the expected frequency of its occurrence. This has direct ramifications for economic indicators such as investment or financial costs. Assessment according to “specialisations” is considered preferable by the present authors.

Categorisation of Risk

The set of reasons why an adverse event has occurred may be vast. The categories are:

a) “common” imperfections of command and management of troops; i.e. randomness as a “natural” property of basic variables
b) difference in the way military equipment is utilised (as regards firepower, availability, load capability), as compared to baseline or typical values;
c) grave human errors and gross insubordination;
d) sabotage, terrorist actions, hitherto unknown effects.

In general, risks can be categorised according to different parameters. It has proved useful to distinguish at least four basic types, the scenarios of which significantly differ. However, we always need to consider their interdependence through interactions and combinations. From this point of view, we can further distinguish financial, force majeure, technological, and human failure risks

Conclusion

Building on the risk analysis approach, the present study has:

1. defined the possibilities of its application to the functioning of the Integrated Rescue System of the Czech Republic;
2. clarified and defined the following terms and concepts: risk, risk analysis, security threats, risk management, risk analysis methods, integrated rescue system;
3. argued that threats to proper functioning of the IRS consist in a potential lack of personnel, modern technical equipment, support for research and development, and financial backing;
4. presented a mathematical expression of risk;
5. demonstrated that the degree of risk is covered by norm provisions, the compliance with which ensures reduction of potential risks to a socially and economically acceptable level or, provided the provisions of the standards are fully complied with, covers them completely;
6. highlighted that the dynamic and turbulent development of human societies brings about many positive but also negative consequences;
7. provided a survey of methods used for initial assessment of risks.

In the context of the given subject matter, the article identifies key differences between the SWOT analysis and UMRA methods. Its added value consists in exploring the possibilities of application of risk analysis methods and their implementation in the functioning of the Czech Integrated Rescue System. The study highlights that despite all applicable legislative measures (such as the Act No. 239/2000 Coll.), failures and defects still arise in the construction of the IRS. The management of risks and prediction of threats is among the tasks of executives and incident commanders at all levels of the integrated rescue system. Technological and logistical risks are those which arise during preparation, construction, and supply of IRS component units. The article stresses that risk assessment methods represent tools and instruments available for risk analysis and management.

References:

ADAMEC, V., ŘEHÁK, D., ČERNÁ, L. 2012. *Základy organizace a řízení bezpečnosti v České republice*. V Ostravě: Sdružení požárního a

bezpečnostního inženýrství, 2012. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-123-1.

BILANIČ, M., VLČEK, P., KUBEČKA, K. 2016. Risk Analysis of Foundation Structures According to the Method of Founding. In Trans Tech Publications. Applied Mechanics and Materials. Switzerland: Trans Tech Publications, Switzerland, 2016. s. 132-139. ISSN 1662-7482. https://doi.org/10.4028/www.scientific.net/AMM.824.132

BOŽEK, F., URBAN, R. 2008. *Management rizika - Obecná část*. 1. vyd. Brno: Univerzita obrany, 2008. ISBN 978-80-7231-259-7.

CAMUS, R. 2020. *Velká výměna*. Přeložil Alan BEGUIVIN. V Praze: Dauphin, 2020. ISBN 978-80-7272-681-3.

HUZLIK, J., BOZEK, F., PAWELCZYK, A., LICBINSKY, R., NAPLAVOVA, M., PONDELICEK, M. 2017. *Identifying risk sources of air contamination by polycyclic aromatic hydrocarbons. Chemosphere*, 2017, vol. 183, s. 139-146. ISSN 0045-6535, https://doi.org/10.1016/j.chemosphere.2017.04.131.

IVANČÍK, R. 2022. Bezpečnosť. Teoreticko-metodologické východiská. Plzeň : Aleš Čeněk, 2022. 240 s. ISBN 978-80-7380-873-0.

IVANČÍK, R., NEČAS, P. 2019. Terorizmus: Globálna bezpečnostná hrozba. Ostrava : Key Publishing, 2019. 163 s. ISBN 978-978-80-7418-319-5.

IVANČÍK, R., UŠIAK, J. 2014. Teoretické a terminologické východiská skúmania problematiky vymedzenia a definovania terorizmu. In Politické vedy, 2014, roč. 17, č. 3, ISSN 1335-2741, s. 91-111.

JANÁČKOVÁ, S. 2020. *Obchodní války a pozice České republiky*. Praha: Institut Václava Klause, 2020. Publikace (Institut Václava Klause). 114 s., ISBN 978-80-7542-057-2.

JURČÁK, V. et al. 2020. *Teoretické prístupy k skúmaniu bezpečnosti*. Ostrava: KEY Publishing, 2020, 134 s. 464. ISBN 978-80-7418-358-4.

KRAUS, M., BEDNÁŘOVÁ, P., KUBEČKA, K. 2016. Risk Assessment of Airtightness of Building Envelope. In Applied Mechanics and Materials. Vol. 824 (2016). Curych (Švýcarsko): Trans Tech Publications, 2016. s. 657-664. ISSN 1662-7482. https://doi.org/10.4028/www.scientific.net/AMM.824.657

KUBEČKA, K. 2017. *Využití metod analýzy rizika ve forenzních vědách: aplikace metod analýzy rizik v oceňování nemovitostí a hodnocení škod a vad*. Ostrava: Key Publishing, 2017. Monografie (Key Publishing). ISBN 978-80-7418-281-5.

MAREŠ, M. 2019. *Ústavní zákon o bezpečnosti České republiky: komentář*. Praha: Wolters Kluwer, 2019. Komentáře (Wolters Kluwer ČR). 189 s., ISBN 978-80-7598-202-5.

BOŽEK, F., PAWEŁCZYK, A., NÁPLAVOVÁ, M., KRÁSNÝ, J. 2017. Application of CPR 18E method for efficient decision making process of risk analysis case study. *Krízový manažment*, 2017, vol. 1, p. 38-45. ISSN 1336-0019, https://doi.org/10.26552/krm.C.2017.1.38-45.

NEČAS, P., UŠIAK, J. 2010. *Nový prístup k bezpečnosti štátu na začiatku 21. storočia*. Akadémia ozbrojených síl generála Milana Rastislava Štefánika v Liptovskom Mikuláši, Slovensko,: Akadémia ozbrojených síl generála Milana Rastislava Štefánika v Liptovskom Mikuláši, 2010, 167 s. ISBN 978-80-8040-401-7.

PORTUGALSKO. Lisabonská smlouva: pozměňující smlouvu o Evropské unii a Smlouvu o založení Evropského společenství. Sdělení ministerstva zahraničních věcí č.111/2009 Sb. m.s. s přihlédnutím k opravám uveřejněných ve sděleních č.40/2010 Sb. m.s. a č. 68/Sb. ms. In: *ÚZ Úplné znění*. Ostrava: Sagit, 2010, číslo 764.

ROBEJŠEK, P. 2017. *Odstíny změny: evropská krize a české národní zájmy*. Praha: Novela bohemica, 2017. ISBN 978-80-87683-80-4.

ROŽŇÁK, P., KUBEČKA, K. et al. 2018. *Země Visegrádu a migrace;: Fenomén procesu migrace, integrace a reintegrace v kontextu bezpečnosti zemí V4*. Ostrava: KEY Publishing, 2018, 468 s. monografie. ISBN 978-80-7418-292-1.

ROŽŇÁK, P., HRALA, M., DROTÁROVÁ, J. 2020. Nobile Einhheit der Fremdenpolizei gegen illegale Migration in der Tschchischen Republik. Kriminalistisk10/2020, C.F. Muller, GmbH 2020, s. 610-615, ISSN 0023-4699. *Kriminalistik*. Heidelberg: Zimmermann Druck + Verlag, 2020, 74. Jahrgang(10), 610-615. ISSN 0023-4699. https://doi.org/10.9785/mdtr-2020-741029.

ŘEHÁK, D., MARTÍNEK, B. LEGIERSKÁ, P. 2019. *Ochrana obyvatelstva v kontextu aktuálních bezpečnostních hrozeb. 2. rozšířené vydání*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2019. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-220-7.

TICHÝ, M. 2006. *Ovládání rizika: analýza a management*. 1. vyd. Praha: C.H. Beck, 2006. ISBN 80-7179-415-5.