Generic Model for Safety Management of Critical Infrastructure Elements

DANA PROCHAZKOVA
Department of Energy
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6
CZECH REPUBLIC

Abstract: - The article summarizes the results of a detailed study of selected elements of critical infrastructure. Based on the interconnection of risk management and safety for technical installations and their selected critical elements and, above all, the lessons learned from the study of their accidents and failures, a generic model for managing their safety during the operation is compiled. Its main parts are and described, e.g. a process of risk management towards safety; structure of safety management over time, the division of responsibilities for risk management and the way of safety management process documentation.

Key-Words: - Critical infrastructure; critical element; risk; safety; security; the basic parts of the generic model.

Received: June 19, 2021. Revised: October 27, 2021. Accepted: December 27, 2021. Published: January 31, 2022.

1 Introduction

Critical infrastructure is the result of the human intellect, which allows humans to develop and survive the pitfalls of nature. It was, is and will be a public asset because it provides for the daily needs of citizens, i.e. energy, water, food, information, etc. It consists of hierarchically interconnected systems of systems, and at the territorial level it is managed by different sectors. Each sectoral infrastructure consists of elements and their interconnections, which are either in the nature of links of different kinds or flows of different kinds. Some of these elements are highly important to the functions of infrastructures, and therefore, are referred to as critical. From the point of view of the needs of human society, the goal is the safe critical elements operation. Safety in this sense means the highest quality, i.e. the critical element reliably performs the functions for which it was created, while not endangering itself or its surroundings even under critical conditions [1]. In a dynamically variable world, this ambitious goal is possible only realized by targeted safety management, i.e. high-quality risk management considering the risk sources of all kinds [1,2].

Critical elements are complex systems of the system of systems (SoS) type, i.e. they are open interconnected systems, the nature of which is socio-cyber-physical (technical) [1]. In Europe, we use for their supervision the Total Quality Management (TQM) method [3], which is the basis of ISO standards of class 9000, 14000 and others. TQM's approach is that all employees, from ordinary employees to top managers, must be involved in the quality improvement process. This process is based on an impulse according to the needs of the customer / citizen. Since the highest quality for humans is their security and development, it is actually about the safety. TQM assumes that the lasting quality of products and services cannot be ensured by orders, control, sub-programs, organizational or economic measures, but by targeted search, measurement and evaluation of the reasons, why productivity and quality do not increase [3]. It is a way in which attention is focused on the processes taking place in the institution. When implementing the TQM for the management of critical elements, the specifics of critical elements are considered, because for the sake of efficiency, the measures must correspond to their structure.

2 Safety and Risk

Integral safety respects the systemic understanding the monitored element and changes in time and space [1]. It is based on a systemic, proactive and strategically targeted approach. It is understood as an emergent property of an element, on which the existence of an element depends; i.e. it is the most hierarchically determining property of an element. It is a set of measures and activities that, considering the nature of the critical element understood as a system of systems and all possible risks and threats, aim to ensure the functioning the elements, links and flows of critical infrastructure, so that under no

circumstances do they fail to endanger themselves or their surroundings.

Risk is the degree of probable losses and damages to the monitored assets in the event of a harmful phenomenon, which in terms of comparability, is normed per unit of time and unit of space [2]. It represents the degree of safety disruption of the monitored element in the event of a possible harmful phenomenon. Since the research of technical installations [1,4] showed that incidents, accidents, as well as failures of technical installations occur in about 80% when combining the harmful phenomena, it is necessary to monitor not only partial risks but also the integral risk. Therefore, the integral safety is associated with the management not only of large partial risks posed by beyond design natural disasters, but above all with the management of integral risk.

The quantities of risk and safety are not complementary quantities, since the safety of each entity can be increased through organizational measures, e.g. by introducing the warning systems and backup solutions, without reducing the risk size; an additional concept to safety is criticality [1,2].

Safety is understood as a system-level property that is shaped by a human's measures and actions and can only be ensured by high-quality anthropogenic management [1,2]. The integral safety is not limited to unilateral solutions to problems such as repression, but it deals with situations affecting a certain level of safety through the so-called safety chain, which consists of the following parts: proactivity (elimination of structural causes of uncertainties that undermine safety, i.e. threaten security and sustainable development); prevention (elimination of direct causes, if possible, of an uncertain situation violating the existing safety); preparedness (to deal with a situation in which safety is disrupted); response (to bring off safety disruption and stabilize the situation); and recovery (to ensure conditions for the restoration and growth of safety); Figure 1. On the basis of economy, it is necessary, above all, to reduce risks at the most critical points in the context of prevention, as well as to prepare a response and recovery to risks that are not dealt with either due to omissions or ignorance in the design and construction process, or preventive measures are very costly. This is a very costly activity, and therefore, it is necessary mutual communication among owners and operators of technical installations works, public administrations, the public and the media [1].

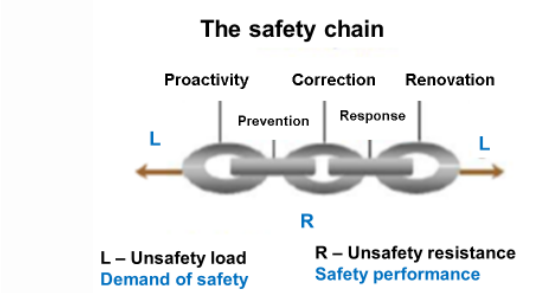

Fig. 1: Activities to ensure the safety of the critical element.

3 Summary of Knowledge on Working with the Technical Installations´ Risks

Risk is a quantity that is a measure of losses, damages and harms to protected assets (in the case of public assets under review, as well as assets of a technical installation). Its size depends on the specific disaster that is the source of the risk and on the vulnerabilities of the local monitored assets. In strategic management, the following variables are defined: hazard as the probable size of a disaster that occurs once per defined time interval (so-called design disaster) [2]; and risk as the probable size of losses, damages and harms to the monitored assets at a design disaster divided into a unit of time (most often 1 year) and a unit of territory [2]. The risk is, therefore, site and temporally specific because it depends on the amount and vulnerabilities of assets in a given territory and at a given time.

Due to the dynamic development of the world, the aging and wear and tear of parts of technical installations, and limited human knowledge, resources and possibilities, the technical installations´ management and the public administration must be prepared for the future occurrence of risks. This means to have the tools to reduce the realization of known sources of risks and mitigate new risks. The present knowledge promotes risk management in favour of safety. With regard to current knowledge, it is necessary to link existing norms and standards, because they contain previous knowledge and without their application there would be a repetition of past mistakes from the past and the results of risk management, as recommended now by a number of standards, e.g., ISO 31000, ISO 31010, ISO 9000, etc.; the method of linking is shown in the work [5].

Figure 1 shows the process of working with risks, the aim of which is to ensure technical installations safety, i.e. they perform the functions for which they were created in a high-quality and reliable manner, while not endangering themselves and

the environment. Therefore, in accordance with current knowledge and experience, humans must firstly identify the sources of risks (i.e. disasters – harmful phenomena of all kinds), appreciate their harmful potential (i.e. identify the hazards posed by phenomena and the distribution of their impacts) in individual locations, and determine the size of possible losses and damages depending on the distribution of public assets (i.e. determine the risk).

Depending on the specific possibilities of a given human society, then to divide the risks into acceptable, conditionally acceptable and unacceptable [2,4,6-19]; the basis for the division is:

- high risk is intolerable and cannot be justified even in extraordinary circumstances,
- ALARP risk is tolerable only if risk reduction is impracticable or if its cost is grossly in disproportion to the improved gained, i.e. if cost of reduction would exceed the improvements gained,
- acceptable risk – only check in time that risk maintains at this level.

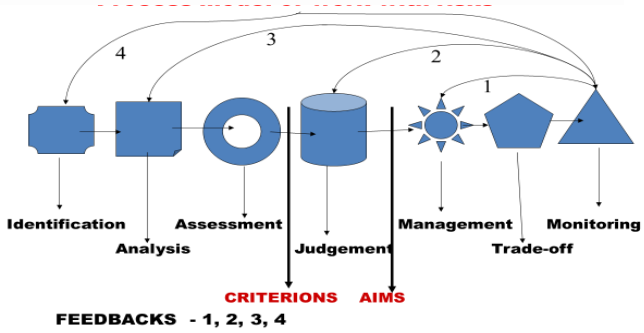

Fig. 2: Process model of working with risks. Criteria = conditions that determine when a risk is acceptable, conditionally acceptable or unacceptable. Aims indicate required conditions. The numbers 1,2,3,4 indicate the feedbacks that are used when monitoring shows that the specified safety requirements are not met [2].

In the case of risks that are: unacceptable, it is necessary to ensure the application of effective preventive measures against their sources; conditionally acceptable, mitigation, reactive and restorative measures should be prepared for the assets under review; and, for acceptable ones, to monitor whether there is an increase in the harmful potential of their causes over time. In this way, we carry out what we call "risk management".

3.1 Categories of Sources of Risks Monitored at the Critical Elements Risk Management

Based on the results of the research described in the works [2,4,20-25], the following selections of risk sources in conjunction with a specified entity (technical equipment, component, interconnection of components, etc.) are currently used in connection with critical elements:

1. Sources of risk determined either by legislation or by the experience of the worker, who solves the task in question.
2. Only the technical sources of risk in the given critical element. Most of them are sources of risk associated with: material (meeting the necessary parameters, supplier relationships – replacement material, etc.); the construction and interconnection of components and equipment (no established procedures, labile hazardous substances are present, etc.); manufacturing processes, e.g. in alloy production, welding, specific machining, etc.; and conditions that are necessary for a quality product, e.g. a certain pressure, a certain temperature or a certain humidity of the surrounding environment, etc.
3. Technical sources of risks and human factor. These are the sources listed in point 2 and the human´ poor execution of technical tasks in the operation of the critical element.
4. Technical sources of risks and human factor in the broadest concept. These are the sources listed in points 2 and 3 and the sources of organizational accidents in the operation of the critical element (i.e. manager´ wrong decisions, use of incorrect procedures, etc.).
5. The sources of risks referred to in points 2 to 4, complemented by sources of risk related to OSH and the working environment.
6. The risk sources referred to in points 2 to 5, supplemented by risk sources from the surroundings of the critical element, i.e. external sources of risk.
7. The risk sources referred to in points 2 to 6, complemented by risk sources associated with interconnections between sub-installations, components and systems (these are sources of risks that are related to technical integrity, automation, education and good skills, asset protection, data and information protection, protection of specific knowledge, protection of know-how, protection of good will, finances, competitiveness, continuity of operations under critical and extreme conditions, etc.).

It follows that in cases 1 to 6, many sources of risk for critical elements are neglected. This is due to the fact that in the listed cases:

- when determining risks, not all public assets and all assets of a critical element are considered (i.e. the All-Hazard Approach [2], which is very data-

intensive, methods, knowledge, experience and execution time, is not respected),
- the systemic nature of the critical element is neglected,
- the dynamic impacts of the external environment on the critical element are not considered, which in turn affect the competitiveness of the critical element and the provision of serviceability of the territory over a longer period of time (e.g. poor public administration practices are a source of risks for critical elements).

From the point of view of needs and economic use of resources, however, it is true that in a number of practical tasks it is sufficient to consider only some sources of risk, because the goal is a safe partial technical device, and not the entire critical element and its surroundings. Therefore, for each task involved in working with risks, the identification of the target is important (Figure 2).

Since some technical devices (safety valves, drain valves, etc.) or some components of a critical element (pressure equipment, air conditioning, control systems, etc.) are of fundamental importance for the safety of the critical element, it is not enough to work with risks only from the point of view of this entity itself, but it is necessary to work with risks that are also important from the point of view of the safety of the entire critical element. These are critical equipment, critical connections, critical components and critical systems of monitored critical element that require special work with risks in the sitting, manufacturing and operation [1,25].

3.2 Summary of the General Principles for Working with Risks

Based on a comprehensive analysis and critical assessment of several thousand professional works and results from practice, the results of which are in the works [1,2,4,6-25], it is necessary to use a systemic approach (i.e. focus on integral risk) when solving the problems of safety of critical objects and firstly to choose the right concept of working with risks (i.e. the context in which we monitor risks) and then respect the logical model of working with risks. The key concepts of safety-focused engineering are:

1. Risk-based approaches - the intensity of work and documentation is proportionate to the level of risk.
2. The professional approach is only based on considering the critical quality attributes and the critical process parameters.
3. Problem solving is focused on critical items – critical aspects of technical systems are monitored and managed to ensure the consistency of system operations.
4. Proven quality parameters must already appear in the critical element design.
5. Emphasis on high-quality engineering procedures – the correctness of the chosen procedures in the given conditions must be proven.
6. Focus on increasing the safety - continuous improvement of processes using the root cause analysis of accidents and failures.

Reducing any risk is associated with increasing the costs, lack of knowledge, technical means, etc., and therefore, in practice it is possible to reduce the risk so that the costs incurred are still reasonable. This level of risk (some optimization) is mostly the subject of top management and the result of political decision-making, in which it is necessary to use current scientific and technical knowledge and to consider economic, social and other conditions in order to ensure development.

Risks have been, are and will be, and new ones will continue to emerge. Managing and bringing over control the risks that cause harmful phenomena (disasters) requires a dimension and measurement of risks that considers not only physical damage, victims and the equivalent of economic losses, but also social, organizational and institutional factors. Most risk-determination techniques do not represent a holistic approach and do not respect that risk is divided into local, regional and national levels [2]. Therefore, a strategic management requires to use technique, which is correct for followed aim [26].

When working with risks, it is necessary to understand that the task of risk management is to find the optimal way to reduce the evaluated risks to the socially acceptable level, or to maintain them at this level. The basic principles when working with risks are: to be proactive; to imagine possible consequences; correctly to identify priorities of public interest; to think about coping with problems; to consider synergies; and to be vigilant.

According to the International Organization for Standardization (ISO), qualified risk management of a technical installation must: be part of the management system of the technical installation being pursued; be part of each decision-making process of the monitored technical installation; explicitly consider uncertainties and uncertainties in the processes and conditions of the monitored technical installation and its surroundings; be systematic and structured; be based on the best available information; be dynamic and respond appropriately to various changes; be adapted to local conditions and legislative requirements; respect the influence of man (human factor) on the technical installation; and have the ability to continuously improve.

3.3 Categories of Risk Handling Tools Broken Down by Critical Infrastructure Element Aim Pursued

When choosing tools for working with the risks of critical elements of infrastructure aimed at safety, according to the arguments summarized in the work [2], two factors are decisive:

1. The first factor is the recognition that risk is a quantity that is locally specific, i.e. it depends on both, the cause of damage to an asset or set of assets (i.e. on the nature and size of the harmful phenomenon / disaster) and the properties of the asset or set of assets (vulnerability) at the moment of occurrence of the disaster. For example, an unmaintained safety valve in the event of a boundary pressure surge usually fails to fulfil its function [4]. Since there are variables over time, both, the conditions of assets or the sets of assets, as well as the sizes of harmful phenomena or disasters, there are three categories of situations from the point of view of managing the impacts of the realized risks, namely situations: normal; emergency; and critical. With the growing the category, the professional, financial, organizational and personnel requirements for managing and settling the risks associated with these situations are growing. Therefore, the legislation that imposes requirements on owners and operators of critical elements and public administration requirements for safety supervision in the public interest plays a big role here [2].
2. The second factor is the selection of the type of risk to be monitored in the task under consideration, which depends on the determination: the number of assets and their enumeration, i.e. the consideration of which public assets and which specific assets of the critical element in the task are important; e.g., whether they include performance, competitiveness, profit, etc.; and whether the links and flows between the listed assets play a role in the given task, i.e. a mechanical concept is not enough, but a systemic concept must be considered.

To ensure the safety of a critical element in the short term (e.g. the safe condition of a simple technical device), it is sufficient to monitor the asset condition, i.e. the partial risk associated with the critical element. With regard to the humans´ security, the legislation in developed countries also requires monitoring the human safety in the workplace (OSH), i.e. it is already a matter of monitoring two assets (lives and health of humans in the workplace, quality of the working environment), using the integrated risk (i.e. the machine-human link is neglected). Since, the technical equipment, persons in the workplace and the working environment are interconnected, the links and flows among these subsystems, i.e. integral risk, should be monitored in order to ensure safety in the medium and long term.

Therefore, when choosing the tools for working with risks (identification, analysis, evaluation, assessment, management and settlement) aimed at the safety of the selected entity, it is necessary to distinguish the following tasks in the technical field in the case of critical elements: the selection of tools for working with the risk associated with the technical equipment condition (goal – safe technical equipment); the selection of tools for working with the risk associated with the technical component condition (goal – safe technical component); the selection of tools for working with the risk associated with the production process or operation (objective – safe production process or operation); the selection of tools for working with the risk associated with the set of processes condition in the entity (target – a safe set of processes in the entity); selection of tools for working with the risk associated with the entire critical element (target – safe critical element); and selection of tools for working with the risk associated with the critical element and its surroundings (target – safe critical element and its safe surroundings).

On the basis of the works [1,2,4,5-25], it is not enough to focus on technical installations and their equipment in order to ensure the humans´ safety, because the choice of tools for working with risks depends on: the nature of the entity being monitored (i.e. the selected technical equipment or higher systems of the technical installation, i.e. the critical element); the nature of the environment in which the monitored entity (i.e. the selected technical equipment or higher system of the technical installation) operates; the mode in which the monitored entity (i.e. the selected technical equipment or a higher system of the technical installation, i.e. the critical element) operates; requirements for the operation of the entity (i.e. selected technical equipment or higher systems of the technical installation); it also depends on whether short-, medium-term or strategic, i.e. long-term, solutions are required.

Instructions for choosing the right tool for each task are given in the works [4,26]. It is a fact that the higher the type of tool used, the higher the cost (knowledge, finance, time) of its use. It follows from the above that in order to ensure the safety of the monitored critical elements of the transport infrastructure, it is necessary to use decision support systems for risk decision-making.

3.4 Decision Support System (DSS) to Manage the Risks of Critical Elements during Operation

In general, when setting up a decision support system for critical elements (both composite and complex, SoS), based on an assessment of the level of work with risks of all kinds in favour of the safety of the critical element in operation, it is necessary to consider that the competencies and responsibilities that release the necessary resources for measures and activities to manage and settle risks in favour of security depend on the level of the organizational structure [4].

The organizational structure of critical elements in operation is a mechanism that serves to coordinate and control the operation of critical elements. According to [27], it represents a hierarchical arrangement of relations of superiority and subordination and resolves mutual powers (competences), ties and responsibilities. Of course, the release of large funds and other resources for the management and settlement of risks is only at the highest hierarchical level. According to practical experience [28], at creating the DSS, it is useful to consider the organizational structure of the critical element as follows: top management; senior management – responsible for projects (e.g. the result of a set of several processes); middle management – responsible for individual processes; technical management – responsible for the operation of individual technical facilities; and personnel (critical and supporting) – responsible for technical activities.

When compiling the DSS, the aspects they assess are taken into account: how risks and their sources are considered; the level of safety achieved in the given execution of the technical installation; the technical level of the measures introduced; material and energy performance; speed of implementation of measures; staff requirements; information requirements; demands on finances; liability claims; as well as the demands on the management of all involved (i.e. both, the management of the technical installation and the management of the territory).

3.5 Example of Processing the DSS Results for Critical Elements of Transport Infrastructure

Based on the requirements for working with the risks of technical installations, DSS has been compiled for critical elements of transport infrastructure during the operation to assess the risks associated with traffic with a philosophy, the higher the risk, the lower the safety of the critical element of the transport infrastructure during the operation, which also means a lower degree of coexistence of the technical installation with the surroundings. For application in practice, a scale was assigned to evaluate the entire checklist based on the principle that was introduced into the ČSN standards in the 80s of the last centuries [28].

Examples of DSS and risk assessment scales are for: bridges at work [20]; tunnels at work [21]; airport at work [22]; railway station at work [23]; transport control systems at work [24]; and roads at work [19]. These DSSs have more than 250 items, and therefore, they are not given here. Further, the way of integral risk determination and the way of integral risk acceptability judgement for critical element itself and for public are shown.

First of all, it is necessary to determine how and according to what it is necessary to evaluate the contributions of individual sources of risk to the integral (total) risk. In practice, according to [4], it has proven to be successful to use the classification scale (0-5) and the concept "the higher the value, the higher the risk [29], i.e. the lower the coexistence of the critical element at operation with the surroundings". The value scale for determining the level of risk that an accident or failure of a critical element entails for its surroundings, processed according to data at work [4], is in Table 1.

Table 1. A value scale to determine the level of risk that the operated critical element poses to its surroundings; proposed by analogy with the scales given and described in the work [4]; p – annual insurance, ABT – annual budget of the territory.

Domain	**Risk rate**	**Classification criterion**
Social	*By accident or failure of critical element, it is affected:*	
	0	less than 50 humans
	1	50 - 500 humans
	2	500 - 5000 humans
	3	5 000 – 50 000 humans
	4	50 000 – 500 000 humans
	5	more than 500 000 humans
Technical and Economic	*Accident or failure of critical element causes damages:*	
	0	less than 0.05 p
	1	equal to p
	2	between p and 0.05 ABT
	3	between 0.05 ABT and 0.075 ABT
	4	between 0.75 ABT and 0.1 ABT.
	5	higher than 0.1 ABT.
Environment	*Accident or failure of critical element causes:*	
	0	very low damages of environment
	1	damages of environment with which the nature cope during the acceptable time
	2	moderate damages of unrenewable resources

		of nature and natural reservations.
	3	medium damages of unrenewable resources of nature and natural reservations
	4	unreturnable damages of unrenewable resources of nature and natural reservations
	5	devastation of landscape, unrenewable resources of nature and natural reservations

The evaluation of a specific case, i.e. the evaluation of a set of expected variants of operation of a critical element according to the relevant DSS, must be carried out independently by a team of specialists from different departments; in practice, the team [4,19-25], which is composed of an employee: public administration officer responsible for the territory safety; the public administration officer responsible for supervising the operation of the critical element; the critical element manager responsible for risk management; officer of professional institutions for the safety assessment of a critical element – e.g. from a technical inspection; and the Integrated Rescue System responsible for responding to accidents and failures of critical elements of transport infrastructure.

The resulting value for each DSS criterion is the median, and in the event of a large variance of values for any criterion, the public administration officer responsible for territorial safety needs to provide further investigations, at which each evaluator communicates the justification for his assessment in the case in question and the resulting evaluation is determined on the basis of a panel discussion or [4,30].

Based on the modern approach [4,31-34], we consider in the given context the tolerable risk expressed by the ALARP principle (as low as reasonable possible) [2], i.e. the case where the critical element under investigation has benefits and at the same time there are impacts associated with it (losses, damages and harms to protected assets) that the organizations managing the critical element and its surroundings can handle through continuous risk management aimed at safety. The tolerance limit (i.e. the interface between tolerable and unacceptable risk) is defined as a quantitative property [35] used e.g. by the UN and Swiss Re, namely the limit of unacceptability is a tenth of the use value of the critical element.

Based on the above requirement in accordance with the works [36-43] using an integrated approach and other assumptions listed above, we get the condition for the highest possible annual losses of the critical element caused by the implementation of ***RZTD*** risks in the form of

$$\boldsymbol{RZTD} < 0.1 \sum_{i=1}^{n} \frac{k_i \, \boldsymbol{HTD}}{5 \, \boldsymbol{T}}, \qquad (1)$$

where ***HTD*** is the utility value of the critical element, $\boldsymbol{k_i}$ are the resulting risk sources assessments in the DSS, ***n*** is the number of risk sources in the DSS, and ***T*** is the lifetime of the critical element. If the condition given by equation (1) is not met, then the risk is not tolerable, i.e. coexistence is not ensured and the operation of the critical element should be changed, i.e. either a new option or additional risk reduction measures should be requested, followed by a further design assessment. If the requirement given by equation (1) is met, the evaluation can be continued.

When deciding on the critical element operation from the point of view of the requirement to ensure its coexistence with surroundings, it is necessary that the operation of the critical element is not loss-making for the territory. Therefore, another condition for assessing the degree of coexistence is given when evaluating the benefits of a critical element of transport infrastructure according to the table taken from [4], Table 2 and with the help of Tables 3 and 4.

Table 2. Checklist for assessing the contribution of a critical element to the surroundings. A - result of assessment (YES or NOT).

Critical element	**Criterion**	**A**	**Note**
	It increases education of the population in the territory		
	It increases the possibility of employment of the population in the territory		
	It increases the level of services in the territory		
	It increases welfare in territory		
	It contributes to the development of basic infrastructure in the territory.		
	It raises the prestige of the territory		
	It contributes to the cultural development of the territory		
	It improves the situation in the social sphere in the territory – Table 3		
	It improves situation in technical and economic spheres in territory - Table 3		
	It improves the situation in environment protection and welfares in territory - Table 3		

Table 3. A value scale to determine the degree of benefit that a critical element makes to its surroundings; proposed by analogy with the scales given in the work [4]; ABT – annual budget of the territory.

Domain	Benefit rate classification	Criterion
	Rate	*Critical element benefits:*
Social	0	less than 50 humans
	1	50 - 500 humans
	2	500 - 5000 humans
	3	5 000 – 50 000 humans
	4	50 000 – 500 000 humans
	5	more than 500 000 humans
	Rate	*Critical element gives to territory budget:*
Technical and economic	0	less than 0.005 ABT
	1	0.005-0.01 ABT
	2	0.01-0.025 ABT
	3	0.026-0.05 ABT
	4	0.05-0.075 ABT
	5	higher than 0.075 ABT
Environment	*Rate*	*Critical element contributes to environment protection and welfare increase per year by sum of money:*
	0	less than 50 EUR
	1	50 – 500 EUR
	2	500 – 5 000 EUR
	3	5 000 – 50 000 EUR
	4	50 000 – 500 000 EUR
	5	more than 500 000 EUR

Table 4. Value scale to determine the degree of contribution of the proposed critical element to its surroundings; N is a number equal to five times the number of criteria in Table 2, i.e. N = 50.

Level of critical element benefits for territory	Values in % N
Extremely high – 5	More than 95 %
Very high – 4	70 - 95 %
High – 3	45 - 70 %
Medium – 2	25 – 45 %
Low – 1	5 – 25 %
Negligible – 0	Less than 5 %

Based on practical experience and the knowledge of examples at work [44], using an integrated approach and assuming that all benefits listed in Table 2 have the same probability of occurrence, we get a relationship to determine the expected annual yield of a critical element of the ***PRZTD*** transport infrastructure in the form of

$$\boldsymbol{PRZTD} = \mathbf{0.7}\sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{n}} \frac{\boldsymbol{k_i}\,\boldsymbol{CPTD}}{\mathbf{5}\,\boldsymbol{T}}, \qquad (2)$$

in which ***CPTD*** is the total lifetime useful yield of a critical element, $\boldsymbol{k_i}$ are the individual ratings in Table 2, ***n*** is the number of benefit sources in Table 2 (i.e. n = 10 in this case) and ***T*** is the lifetime of the critical element. The expected annual net yield of the critical element ***RPTD*** for the territory is determined by the relation

$$\boldsymbol{RPTD} = \boldsymbol{PRZTD} - \boldsymbol{A} - \boldsymbol{RPNTD}, \qquad (3)$$

where ***A*** is the annuity and the ***RPNTD*** is the expected operating cost of the critical element. The basis for the decision is the result of the difference ***R*** between the permissible maximum annual losses of the critical element caused by realization, risks and expected net annual returns, i.e. the result of the difference ***R***.

$$\boldsymbol{R} = \boldsymbol{RZTD} - \boldsymbol{RPTD}. \qquad (4)$$

The assessment uses the thresholds of acceptability or unacceptability of risk, such as those used by the UN and Swiss Re, namely the amount of the annual premium for protected assets in the territory (***PRTD***) and a tenth of the annual budget of the territory (***ABT***) that ensures development in the territory. According to this rule, in practice we compare three variables: the difference between the annual losses of the critical element caused by the realization of risks and the expected annual net return from the operation of the critical element (***R***), the annual premium for the critical element (***PRTD***) and the annual budget of the territory (***ABT***). On the basis of the results of the scoring, the category to which the risk associated with the critical element belongs in a given case shall be determined according to the methodology described in [4] as follows:

$\boldsymbol{R < PRTD}$, thus, the risk of a critical element is acceptable for the territory,

$\boldsymbol{PRTD < R < 0.1\ ABT}$, thus, the risk of the critical element is conditionally acceptable (tolerable) for the territory,

$\boldsymbol{R > 0.1\ ABT}$, thus, the risk of a critical element is unacceptable for the territory.

In the first case (revenues are greater than losses), the advantages associated with the critical element outweighed the disadvantages, i.e. expected losses, and the critical element can be operated considering the coexistence of the critical element and its surroundings.

In the latter case, additional preventive measures in the management of the critical element

leading to risk reduction and mitigation, reactive and restorative measures shall be ensured [4] as part of continuous targeted risk management aimed at ensuring the safe critical element and its coexistence with its surroundings.

In the last case, i.e. in the case of an unacceptable risk, a thorough reflection on the conclusion is necessary – either risk avoidance, i.e. stopping the operation of the critical element, or requiring further preventive and mitigating measures to increase the safety of the critical element (application of: higher knowledge; better technical equipment; higher costs of protective systems; ensuring the higher readiness of human resources, etc. is necessary [4], and then conduct a new assessment of coexistence.

4 Generic Model of Safety Management of Critical Elements

Based on the above findings, the safety management structure, management actors, procedures, strategies and responsibilities are given.

4.1 Safety Management System

From the point of view of ensuring the critical elements safety and their coexistence with their surroundings throughout their lifetime, it is a matter of determining the size of the relevant risks and sorting them into categories: acceptable risk; a conditionally acceptable risk for which the necessary preventive, mitigating, reactive and restorative measures are proposed; and an unacceptable risk for which it is proposed either to avoid the activity, if possible, or to take other crisis management measures requiring the higher knowledge, higher technical equipment, higher costs, higher readiness of human resources [2]. Therefore, the risk of failure of a critical element of infrastructure must firstly be identified with the right tools.

In order to ensure the technical installations safety, we solve the problem of system safety [1,4], because a set of interconnected safe systems is not necessarily a safe system, since the safety of the system of systems also depends on the nature of the interconnections between the systems. The consequence of interdependencies is that a defect in one part of a technical installation causes the failure of other parts of the technical installation and a cascade of other impacts. This means that if we want to ensure the safety of the system of systems, in addition to the safety of the individual parts of the technical facility, we also have to pay special attention to the set of systems as a whole. We need to find out: types of system failures of systems; the system of systems operating conditions; internal links and their manifestations; and the characteristics of critical system of systems conditions.

Currently, several types of risk management are used in practice; their goals differ. The oldest type the management of technical installation reliability [1]. Continuity management is aimed at the safety of the technical installation and its surroundings under all possible conditions [4]. Flexible resilience management is a precursor to safety management and continuity management; it seeks to increase the toughness of the system and its surroundings in order to gain time to form an effective response [4]. Asset management prioritizes risk management in favour of production over the safety of the humans and surroundings of the technical installation [4]. Components of all types of management are specific types, which are emergency management and crisis management.

A comparison of types shows that: all types use the same methods and tools for working with risks, which, due to the different objectives of the procedures in question, do not give the same results in specific cases [1]; all types have the same objective, which is risk management and asset protection (but there is a difference in which risks and which assets consider); and are a superstructure of reliability management, which for many years was the royal discipline in the management of technical works [1].

Despite the different names of the types of management, their methodology is the same, namely to obtain: awareness of risk; understanding of risk and its relationship to assets and their safety; and apply relevant knowledge of what to do to achieve the goal. Risk management in favour of safety (i.e. safety management) is essential for the strategic development of human society and technical installations. In order to manage the risks of the technical installations in favour of safety, five key activities need to be carried out well [2], namely:

1. Definition of the objective and focus of safety management. It means: to identify the context; to identify priority objectives; and to identify areas and critical tasks. Selections are based on an evaluation of assets and targets. This will determine which risks have priorities in a given case.
2. Description. It means to give an objective understanding the probability of occurrence and size of impacts (in qualitative or better quantitative terms) of possible disasters and failures of the technical installation. It is a highly professional activity requiring the deep knowledge and quality data.
3. Decision. It means to evaluate the quality of the forecast of the development of the technical in-

stallation, if possible as an optimum when considering the benefits and losses in the operation of the technical installation in a dynamically variable surrounding; i.e. to do the decision-making, how to mitigate and manage risks and how to implement measures represents a key step in risk management.

4. Communication. It means a discussion of a set of measures and activities with the key actors in the process of operation of the technical installation and with other stakeholders. Legislation requires communication with the public, consultation, conflict resolution and the establishment of partnerships on important issues.
5. Monitoring and instruction. It means a monitoring of the specified quantities and their values that characterize the consequences of decisions and actions on the technical installation, and in case of detection of significant deviations that may interfere with the achievement of the goal, to apply corrections.

Risk management in the event that the risk is not acceptable consists, according to [1,2,4,5] in choosing one of the following alternatives: risk avoidance, i.e. not initiating or continuing the activities that are a source of risk when possible (human society can exists without a technical installation); eliminating the risk sources, i.e. preventing the disasters from occurring when possible (choosing an alternative to a technical installation that has fewer sources of risk or less risk); reducing the likelihood of risk occurring, i.e. the occurrence of major disasters when possible (application of the principles of safety culture); reducing the severity of the impacts of the risk, i.e. preparing the mitigation measures such as warning, response and recovery systems; risk sharing, i.e. risk allocation between the parties and the insurance undertakings; and risk retention.

Risk negotiation is based on the current possibilities of human society and consists, according to [1,2], in the division of risks into categories in which part of the risk is: reduced, i.e. preventive measures avert the realisation of risk; mitigated, i.e. through preventive measures and preparedness (warning systems and other emergency and crisis management measures) to reduce or avert unacceptable impacts; insured; ensured response and recovery measures for which reserves of all kinds shall be prepared; and for the part that is unmanageable or too expensive or infrequent, a contingency plan is prepared.

This is also accompanied by a distribution of risk management among all concerned. The breakdown in good management [27] is carried out by taking as a view to ensuring that all stakeholders (from politicians to administrative staff, technical management to technicians and citizens) are responsible for risk management and that the management of a particular risk is assigned to the entity best prepared for it; Figure 3.

When selecting the risk management measures and activities, it should be ensured that the cost of managing the risks, does not exceed the potential damage caused by the realisation of the risk. The safety management system (SMS) of the critical element shall include the tasks listed in Figure 4 [1,4].

According to current knowledge in connection with the safety of a technical equipment or technical installation, i.e. also a critical element of infrastructure, it is necessary to respect the following procedure when drawing up its concept, its sitting, design, construction and operation, which links standards and risk management results for the benefit of safety, i.e. using the risk-based design, the risk-based operation tools; the risk-based inspections, the risk-based maintenance, etc. [4,5], which link standards and risk management results. The actual methodological process of risk management in favour of safety (safety management) is shown in Figure 5.

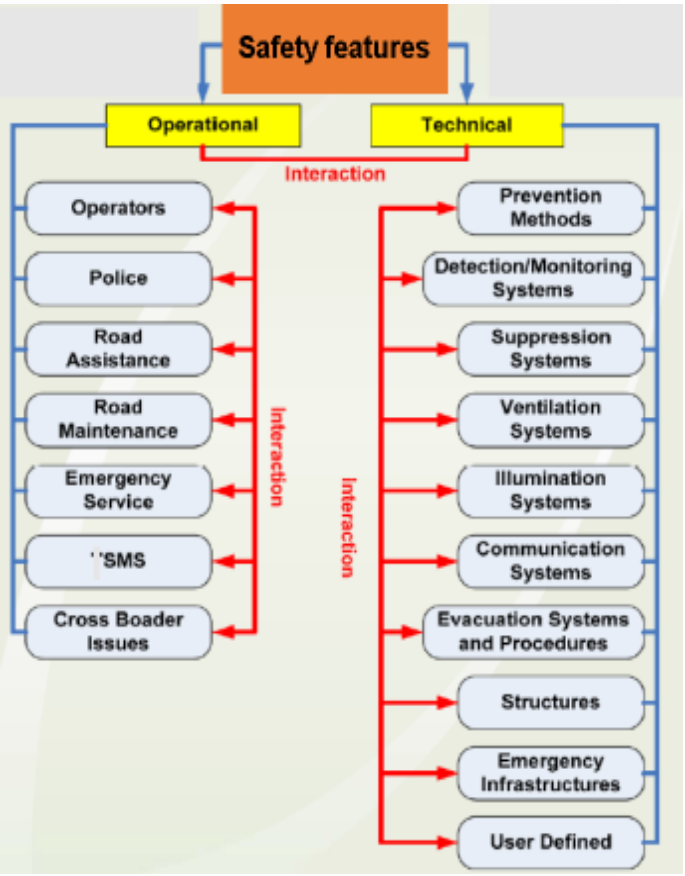

Fig. 3: The safety features of critical transport element; SMS is a safety management system.

Fig. 4: Tasks specified in the safety management system (SMS) of the critical element.

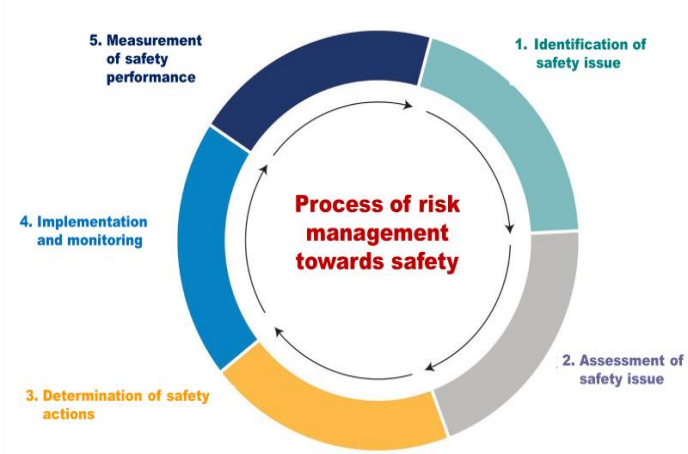

Fig. 5: Safety management of a critical entity.

4.2 Strategies for Increasing the Critical Elements Safety

The safety and security of critical elements is essential for the protection and development of humans and each State, so each State must have a strategy to maintain and possibly increase safety in integral concept. As the world evolves dynamically, conditions may arise for which critical element limits are not prepared, and therefore, the safety management systems (including the security management systems) must always be equipped with measures to minimize damages in the event that security measures and safety systems fail or an unidentified hazard occurs. Minimizing the damage can take the form of warning and warning signals, training, instructions and procedures for behaviour in dangerous situations, or isolation of hazardous facilities from populated centres etc. Measures prior to accidents, including the emergency planning, shall be drawn up before the equipment is put into operation, because in the event of an accident, there might not be enough time for this [4].

The safety management system has its roots in industrial safety engineering, which has been developing step by step since the 19th century. The relatively new discipline dealing with the safety management system is a response to the conditions that arose after the 2nd World War when its "parent" disciplines developed, namely systems ´ engineering and systems´ analysis, which developed to solve new and complex engineering problems. The scientific basis of all these new currents of engineering lies in the theory of systems, the development of which began in the thirties of the last century; at present, it is about the management of the safety of the whole and its surroundings (integral safety).

Critical elements are complex socio-cyber-physical systems with a high number of many different interconnections. According to the design, all elements, components and interconnections have their limits, which are set to certain conditions so that together they meet the specified goal (interoperability) [1,4]. As conditions change as a result of the dynamic development of the world, so also change the conditions for interoperability. Therefore, the critical elements safety varies depending on the conditions.

In accordance with OECD requirements [45] and results for technical installations [4,19-24], each critical element manager shall have a critical element safety management programme that is based on qualified risk management, from design to construction up to operation. Due to the present importance of the role of cyber infrastructure associated with an automated management system, the SMS must also ensure the cybersecurity; Figure 6 [11].

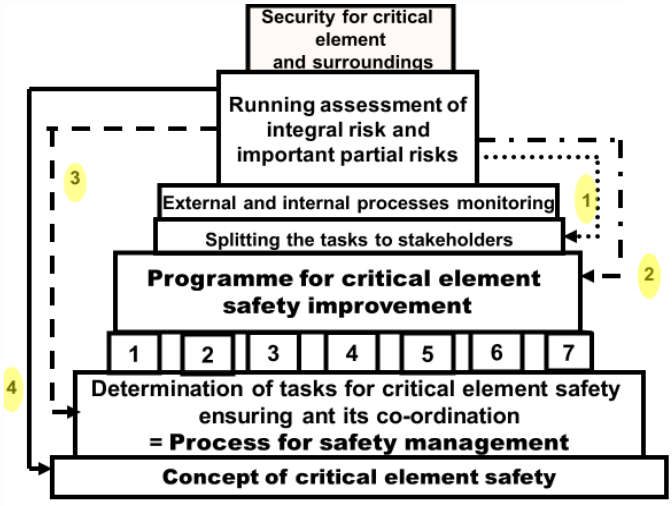

Fig. 6: Model of safety management of a critical element with automated control in time according to [11]. Processes: 1- conception and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; 6 - documentation and investigation of accidents; 7-

cyber security. Feedback: numbers 1-4 in a yellow circle.

The main goal of critical element security in automatic control is that the instructions for critical element control systems are clear and precise, i.e. not affected by phenomena that distort them.

4.3 Responsibility for the Safety of Critical Elements

Safety management is based on process management, which is based on the consistent use of knowledge about the problem in the system and its surroundings, which is why it is also called "knowledge management". The bearers of knowledge are humans, knowledge cannot be taken away from anyone, but can be expanded and multiplied indefinitely. In a knowledge society, it is precisely intellectual capital that dominates and has a completely different position than before. All this requires a different view of the management of departments and units. Process management based on the control of management and implementation processes differs from the operational approach, which is commonly used in the decision-making process of classical management. It is based on knowledge management and it does not focus on results, but on causes.

In each entity, we distinguish the basic levels of management that need to be aligned, namely: political, strategic, tactical, operational/functional and technical, Figure 7. The political level is often influenced by the ideas and power goals of the ruling political representations, and thus is sometimes far removed from the goals of knowledge-based process management. However, it is important because it is through it that the other levels are realized. It is greatly influenced by phenomena such as: corruption, power relations, abuse of power and lobbying.

In knowledge-based process management, the strategic level determines the basic directions of development, from which it follows which processes need to be modified or created, what organizational changes will need to be made, where to get know-how, financial resources, etc. The tactical level of process management helps to organize the activities necessary for the implementation of long-term goals. Answers to the questions of how to set up processes, in what condition to maintain them and how these processes must cooperate with each other are sought. Operational management decides on the specific distribution of resources in the process (human, technological, financial) and also on the performance of individual activities within the set processes (how to perform a specific operation). The aim is to ensure the of knowledge and skills among workers. At the technical level, specific problems are solved. It should be remembered that the most challenging negotiations with risks take place at this level; the resistance and resilience of elements, equipment, components and entire systems increases, and according to data from practice, the success rate of technical measures is between 40 and 80%. A significant effect and competitive advantage are achieved by the entity (territory, organization) only by harmonizing all levels of management. The aim is to achieve a condition where processes are defined and managed on the basis of strategy, operational management is not just extinguishing emergencies. The processes are improved on the basis of knowledge transferred from the operation. New knowledge stemming from process control is then quickly reflected back into the strategy and provokes another fundamental change or changes in the development of the subject.

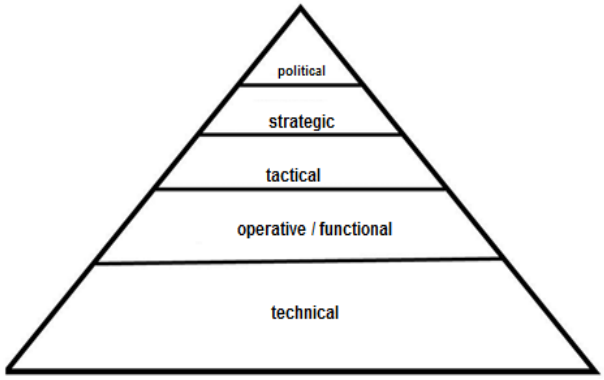

Fig. 7: Entity process management levels.

According to the TQM scientific theory [3] and according to the author's experience to date, in connection with problem solving, it is necessary to consider the possibilities that exist at each level of management when determining the division of tasks and responsibilities in ensuring safety. The possibilities are determined by both, the powers and the availability and amount of available resources, forces and means that are needed to solve:

- at the operational management level of a technical installation, well-structured problems can be successfully solved,
- at the middle management level of a technical installation, both, the structured problems and the poorly structured problems that are not associated with great risks to the technical installation can be successfully solved,
- at the top management level of a technical installation, complex and unstructured problems that have risks that can be controlled using the

tools that only the top management of the technical installation has at its disposal,
- only through mutual cooperation of public administration and top management of technical installation can complex and unstructured problems of large scale with great risks be solved.

In the case of technical installations of transnational scope, international cooperation is necessary. The highest responsibility is at the political level, where concepts are set and finances are decided.

5 Conclusion

The study of accidents and failures of technical equipment and technical installations [4,19-24,28] (*generally entities*) shows that these non-required phenomena occurred in a number of cases due to insufficient documentation of the processes shown in Figures 2, 5 and 6, and insufficiently determined responsibilities. Therefore, a number of supranational institutions (EU, IAEA, IATA, ICAO, OECD, etc.) require the preparation of documentation in the form of a safety report, which means that it is a document supporting the safety of the monitored entity. The document in question is intended for the management activities of the entity operator and for the needs of the relevant public administration bodies (state supervision) as well as for informing the public. In real case, this document describes the adaptation of generic model of safety management to real entity.

In general, a safety report is a set of documents that contain information about the monitored entity, its location and activities, the organization and control system with respect to the prevention of accidents and failures, a description of the entity's surroundings and the environment, a description of the equipment and an inventory of hazardous substances present in the entity, the identification and analysis of the risks of accidents and failures, their evaluation and preventive measures, measures related to preparedness for dealing with accidents and failures, and limiting their impacts, as well as map documentation. It monitors the processes shown in Figure 1 and is the basis of the integral safety management system of the monitored entity.

The safety report is processed already in the concept phase (preliminary), refined in the design and construction phase, and systematically updated during the operation of the entity. It provides a set of policies and rules for maintaining the safety and improving it. In practice, it is implemented by transposition into internal regulations, which are mandatory. It is the basic tool of the safety management system (SMS) in the entity; a detailed description is at work [4]. In terms of responsibilities, it is created hierarchically at different levels of details, and since the highest competencies are in top management [27], so the division of responsibilities is done from top to bottom.

An important document of the safety report for critical entities that are vital to ensuring the basic functions of the State is the continuity plan [4], which is the strategic plan for the management of safety and development of the entity anchored in the SMS. The plan is based on the way of integral safety management and it contains not only data important for the operation of the entity, but also a way of solving the problems that can seriously disrupt the operation and competitiveness of the entity. In accordance with [4], the entity continuity plan has higher goals than the risk management plan and it includes:
- how to deal with risks that have a source outside the entity and seriously affect the entity, with the appropriate responsibilities and procedures for resolving the conflicts between the public interest and the entity interests,
- procedures to ensure a safe entity for the planned lifetime so that the entity delivers quality products or services, it is competitive and does not endanger itself and its surroundings,
- due to the dynamic development of the entity and its surroundings, which are not necessarily synergistic, the response to the change of conditions, including the emergency and crisis management measures, which are elaborated in detail and ensured in all aspects for all levels of management of the entity, i.e. it is attached a crisis preparedness plan that contains measures and their provision for the State support.

To ensure the correctness and expertise of the safety report, it must be approved by the State authority, i.e. the State must have a safety oversight authority, which is codified by law. Due to reality that risk is site-specific, the generic model presented above must be adapted to site conditions.

References:

[1] PROCHÁZKOVÁ, D. *Principles of Risk Management for Complex Technological Installations.*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. http://hdl.handle.net/10467/72582

[2] PROCHÁZKOVÁ D. *Analysis, Management and Trade-off with Risks of Technical Installations.* ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. http://hdl.handle.net/10467/78442

[3] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.

[4] PROCHÁZKOVÁ, D., PROCHÁZKA, LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRAB- KA, L. *Risk management of Processes Associated with the Operation of a Technical Installation during its Lifetime*. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. doi:10.14311/BK.9788001066751.

[5] PROCHÁZKOVÁ D. Linking the Standards and Risk Management Results for Benefit of Safety. In: *Risk Management of Processes, Equipment and Safety of Complex Technical Installations.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 7-19. DSPACE. http://hdl.handle.net/10467/98461. doi.org/10.14311/ BK.9788001069066.

[6] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S. (eds). *Reliability, Risk and Safety. Theory and Applications.* ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.

[7] ALE, B., PAPAZOGLOU, I., ZIO, E. (eds). *Reliability, Risk and Safety.* ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.

[8] BÉRENGUER, C., GRALL, A., GUEDES SOARES, C. (eds). *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.

[9] IAPSAM (eds). *Probabilistic Safety Assessment and Management Conference. International PSAM 11th 2012. (and Annual European Safety and Reliability Conference).* ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889 p.

[10] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A. (eds). *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.

[11] NOWAKOWSKI, T., MLYŇCZAK, M., JODEJKO-PIETRUCZUK, A., WERBIŇSKA-WOJ CIECHOWSKA, S. (eds) *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.

[12] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W. (eds). *Safety and Reliability of Complex Engineered Systems: ESREL 2015.* ISBN 978-1-138-02879-1. London: CRC Press, 4560 p.

[13] WALLS, L., REVIE, M., BEDFORD, T. (eds). *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. ISBN 978-1-315-37498-7. London: CRC Press, 2942 p.

[14] CEPIN, M., BRIS, R. *Safety and Reliability – Theory and Applications.* ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.

[15] HAUGEN, S., VINNEM, J., E., BARROS, A., KONGSVIK, T., VAN GULIJK, C. (eds). *Safe Societies in a Changing World.* ISBN: 978-0-8153-8682-7 London: Taylor & Francis Group 2018, 3234 p.; ISBN: 978-1-351-17466-4; https: //www.ntnu.edu/esrel2018.

[16] BEER, M., ZIO, E. (eds). *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA 2019, Research Publishing 2019, 4315 p., e:enquiries@rp sonline.com.sg

[17] BARALDI, P., DI MAIO, F., ZIO, E. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (ESREL 2020 PSAM15). ISBN 978 -981-14-8593-0. Singapore: ESRA 2021, Research Publishing 2021, 5067 p., enquiries@rpsonline.com.sg

[18] CASTANIER, b., CEPIN, M., BIGAUD, D., BERENGUER, C. *Proceedings of the* 31st European Safety and Reliability Conference (ESREL 2021). I SBN 978-981-18-2016-8. Singapore: ESRA 2021, Research Publishing 2021, 3473 p., enquiries@rpsonline.com.sg

[19] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Risks Associated with Roads.* ISBN 978-8001-068 43-4. Praha: ČVUT 2021, 296 p., http://hdl.handle.net/10467/9 4283

[20] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Risks and Safety of Bridges. In: *Risk management of Processes and Safety of Technical Installations.* ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 107-179. http://hdl.handle.net/10467/91988; https://doi.org/10.14311/BK. 9788001067864

[21] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Risks and Safety of Tunnels on the Roads. In: *Risk management of Processes and Safety of Technical Installations.*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 268-318. http://hdl. handle.net/10467/91988; https://doi.org/10.14311/BK.9788001067864

[22] PROCHÁZKOVÁ D., PROCHÁZKA, J. Risks Associated with Air Travel. In: *Risk Management of Processes, Equipment and*

Safety of Complex Technical Installations. ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 70-136. DSPACE. http://hdl.handle.net/10467/98461. doi.org/10.14311/ BK.97880 01069066.

[23] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Risks Associated with Critical Train and Bus Stations. *Soudní inženýrství.* ISSN 1211-443X. 32 (2021), 3, pp. 33-46.

[24] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Risk Management of Traffic Management Systems.* Praha: ČVUT, *in print.*

[25] PROCHÁZKOVÁ, D. *Safety of Complex Technological Systems.* ISBN 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.

[26] PROCHAZKOVA, D., PROCHAZKA, J. Optimum Risk Engineering Tools Depend on Technical Facility Complexity. *International Journal of Computers,* ISSN 1998-4308.14 (2020), pp. 26-33. DOI: 10.46300/ 9108.2020.14.4

[27] BĚLOHLÁVEK, F, KOŠŤAN, P., ŠULEŘ, O. *Management.* ISBN 80-251-0396-X. Brno: Computer Press 2006. 724 p.

[28] ČVUT. *Archives of Disasters, Accidents, Failures and Results of Work with Risk.* Praha: ČVUT 2022.

[29] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569 p.

[30] PROCHÁZKOVÁ, D. Tool for Compiling the Documents for Safety management. In: *Occupational Health and safety 2011.* ISBN 978-80-248-2424-6. Ostrava: VŠB 2011, pp. 157-169.

[31] ISO/IEC. GUIDE 51:2014E. *Safety Aspects – Guidelines for Their Inclusion in Standards.* Genève: ISO 2014, 15 p.

[32] BOWLES, D. S. *L.1- How Safe Is Safe Enough? Acceptable and Tolerable Risk.* Utah: IDSRM 2008.

[33] ALE, B. Tolerable or Acceptable. A Comparison of Risk Regulation in the United Kingdom and in the Netherlands. *Risk Analysis*, 25 (2005),2, pp. 231-242.

[34] BOULDER, F., SLAVIN, D., RAGNAR, E. *The Tolerability of Risk: A New Framework for Risk Management.* ISBN 978-1-84407-398-6. London: Taylor & Francis 2007, 160 p.

[35] PROCHÁZKOVÁ, D. *Methods, Tools and Techniques for Risk Engineering.* ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.

[36] GAYLORD, E., GAYLORD, C. *Structural Engineering Handbook.* New York: McGraw-Hill Book Co 1979.

[37] TATUM, C., B. Innovation on Construction Project.: A Process View. *Project management Journal*, 18 (1987), 5, pp. 57-67.

[38] BERMAN, O., KRASS, D., MENEZES, M. B. C. Locating Facilities in the Presence of Disruption and Incomplete Information. *Decision Sciences.* 40 (2009), 4, pp. 845-868.

[39] BEN-GAL I., KATZ R. AND BUKCHIN J. Robust Eco-Design: A New Application for Quality Engineering. *IIE Transactions,* 40 (2015), 10, pp. 907-918.

[40] CHAPMAN, J. Design for Durability. *Design Issues*, 25 (2009), 4, pp. 29-35.

[41] FEMA. *Risk Management Series: Design Guide For Improving Critical Facility*. New York: FEMA 2007, 152 p.

[42] PORTNY, S. R. *Project Management for Dummies*. ISBN 978-0-470-24789-1 Indianapolis: Wiley Publishing 2007, 366 p.

[43] PRICE, B. *Active Directory: Optimal Procedures and Problem Solving*. ISBN 80-251-0602-0. Brno: CP Books 2005. 381 p.

[44] BRUCE, J. F. *Investment Performance Measurement.* ISBN 0-471-26849-9. New York: Wiley 2003, 748 p.

[45] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Com- munities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Re- sponse*. Paris: OECD 2002, p.191.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US