Tool for Management of Safety of Critical Technical Installations with Small Modular Reactor

DANA PROCHAZKOVA, JAN PROCHAZKA, VACLAV DOSTAL
Department OF Energy, Machinery Faculty
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6
CZECH REPUBLIC

Abstract: - Technical installations with small modular reactors (SMRs) are increasingly prepared to use in practice. They are critical installations due to content and work with dangerous substances because these are sources of fire, explosion and environment contamination. Therefore, for human society and its development, it is necessary to manage not only their nuclear safety, but also their integral (complex) safety, because just integral safety ensures the security and development of human society. The approach to safety and concept of safety management used by manufacturer, operator and regulator must be same. For this purpose, we give in article a tool showing the main features and requirements for management of the integral safety of such installations.

Key-Words: - Generic model of safety management; Integral safety; Risks; Small modular reactors (SMR); Systemic approach; Technical installations with SMR.

Received: April 16, 2022. Revised: December 11, 2022. Accepted: January 15, 2023. Published: February 8, 2023.

1 Introduction

Small modular reactors (SMR) have been in development for decades. The International Atomic Energy Agency [1] defines small, medium and large reactors according to output electrical performance; reactors up to 300 MWe are classified as small reactors. Small reactors are increasingly used in practice, as they are cheaper and their area of emergency planning is smaller compared to large nuclear power plants [2-4]. In spite of it, their safety must be on the first rank of designers, manufactures, operators and regulators. This big team of specialists from different professional fields must understand safety by same way.

In the Czech Republic , we work on the Energy Well reactor [5], which we want to use as energy sources in technical installations producing the energy for: train and ship drive [6,7]; operation of processes as reverse osmosis; hydrogen production and hydrogen storage [2]; and mining the minerals in remote regions [7]. From safety reasons, we create a tool that shows to all specialists the principles of risk management directed to safety in different domains that influence safety rate. Due to clear intelligibility we use a set of interconnected pictures, which we denote “generic model of safety management”. This tool for tutoring the specialists in same understanding the safety, we present in this article.

Technical installations with the SMR as other technical installations are threatened by risks caused by harmful phenomena: occurring in the locality, in which they are located [8,9]; originating at the operation by failure of technical fittings, components or their interconnection and their wear over time; associated with the human factor, in particular in the design and organization of operation management [10,11]; and, last but not least, by low possibilities of humans to anticipate sudden changes in the development of the world.

We further deal with technical installations with SMR that belong to critical infrastructure [12], which are critical objects, on which operation the region safety is dependent. Therefore, it is necessary to manage not only their nuclear safety, but also the integral safety, because they ensure the security and development of human society, however, costs on their operation must be acceptable to society.

Based on current knowledge and experience which are systematically enforced into practice by the IAEA and OECD and are permanently followed in the ESREL conferences, which are summarized in [10,11], a generic model for the management of integral safety of technical installations with the SMR is created, based on the principles of: risk-based design; and risk-based operation. It is also

shown way, how to adapt this general model to real site conditions.

Next paragraphs summarize main principles of model in question and process models for its construction.

2 Summary on Risk and Safety of Complex Technical Installations

Based on research of complex technical installations, the results of which are summarized in [10,11]:

1. 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. It represents the degree of safety disruption of the monitored set of assets in the event of a possible harmful phenomenon.
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.
3. Risk and safety are not complementary quantities because risks´ impacts might be reduced by organizational measures (warning systems, human training, backup solutions etc.); the complementary quantity to safety is criticality (marginal impacts which have been acceptable yet).
4. Safety is ensured by advanced risk management.

At complex technical installations we pay attention to safety of: individual fittings; components; personnel; processes; set of processes; whole installation; and whole installation and its surrounding (integral safety). Due to many interfaces among parts of complex technical installation, which moreover depend on dynamic changes of technical installation and its surroundings, the integral safety is not only set of safeties of mentioned parts [10,11].

Integral safety respects the systemic understanding the monitored technical installation and changes in time and space. It is based on a systemic, proactive and strategically targeted approach. It is understood as an emergent property of the monitored technical installation, 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 monitored technical installation understood as a system of systems and all possible risks and threats, aim to ensure the functioning the monitored technical installation elements, links and flows, so that under no circumstances do they fail to endanger themselves or their surroundings.

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 (Figure 1), 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); correction (to prepare to deal with a situation in which safety is disrupted); response (to bring off safety disruption and stabilize the situation); and renovation (to ensure conditions for the restoration and growth of safety).

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

Since the research of technical installations summarized in [10,11] 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. The integral risk is understood the aggregation of contributions from all risk sources that have capability to contribute to failure of technical installation if they appear; i.e. it includes also contributions from failures of joins of components and elements. 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 which also considers combination of partial harmful phenomena.

3 Sources of Risks of Technical Installations with SMR

On the basis of the analysis of 7829 accidents and failures of complex technical installations including the nuclear installations [10,11,13], the sources accidents and failures of the technical installations are mainly: natural disasters; defects and failures of technical equipment, components, production lines and systems; traffic accidents at transport spent fuel; accidents in storage of spent fuel; organizational accidents caused by a human factor, in particular by a poor safety culture in designing, manufacture and operation; and deliberate attacks. The world dynamically changes, and therefore, new data on risk sources will arise. For safety improvement , it is necessary to evaluate each failure or accident of technical installations and to determine lessons learned which is important for improving the prevention and response. Special attention must be given to technical installations with SMR because for them a low number of information.

4 Data for Compilation of Generic Model of Risk Management towards Safety

Real risk size depends on both, the hazard of specific disaster that is the source of the risk, and the vulnerabilities of the local monitored assets. It is site and temporally specific, because it depends on the amount and vulnerabilities of assets in a given territory and at a given time [10,11]. From this reason, a model of safety management of each entity (asset, fittings, technical installation etc.) needs to respect site conditions (set of disasters determined according to All-Hazard-Approach [8,9], local knowledge level, legislative and society possibilities).

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 31010, ISO 9000, etc.; the method of linking the standards and risk analysis results is e.g. in [14].

Depending on the specific possibilities of a given human society, the risks are divided into acceptable, conditionally acceptable and unacceptable [10,11,15]. Basis for risk management is:

1. High risk is intolerable and cannot be justified even in extraordinary circumstances.
2. 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.
3. Acceptable risk, at which it is necessary to check during time if risk maintains at this level.

In accordance with OECD requirements [15] and results for technical installations [10,11], each manager of technical installation shall have a safety management system (SMS) containing the safety management program 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 2 showing the model of safety management of technical installation with SMR is the analogy of model constructed in [16]. The main goal of technical installation security in automatic control is so that the instructions for control systems of technical installation may be clear and precise, i.e. not affected by phenomena that can distort them.

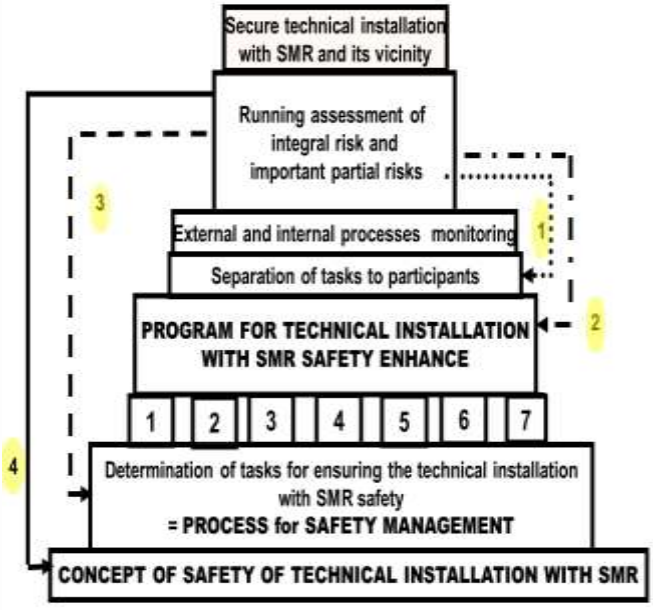

Fig. 2. Model of safety management of technical installation with SMR with automated control; pattern is in [16]. Processes: 1- conception and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; 6 - documentation and investigation of accidents; 7- cyber security. Feedbacks: numbers 1-4 in a yellow circle.

At technical installation with SMR as for each complex technical installation, it needs to be monitored, the partial risks connected with big disasters and the integral risk, which include contributions from elements and links and couplings among them. The tool for integral risk determination in the form of decision support system (DSS) was constructed by using the principles of decision with multiple objectives [17]. Its generic model determined for: designing the technical installation is given in [14]; and for operation of technical installations is given in [10]. Due to limited human possibilities and finances, the risk management measures costs may not exceed the human society sources [18]. The way of determination of acceptability of integral risk is described in details in [10,11].

5 Method Used at Compilation of Generic Model and Its Tasks

Generic model is a tool which describes a process how to work with risks towards safety. It solves tasks:

1. How to determine risk sources in locality according to All-Hazard-Approach [8,9].
2. How to determine important external and internal risk sources for technical installations with SMR by critical analysis of qualified data sets (how historical data on big events need to be considered).
3. How to evaluate sizes of hazards for all important risk sources [10,11].
4. How to propose concept of technical installations with SMR which copes with all important risks´ sources; namely either in design or in operation (by response).

For construction of generic model of safety of technical installations with SMR we consider requirements of [1,19,20], recommendations of Perrow [21] and procedure used by OECD [15] which was elaborated in [10] and tested in practice [13].

6 Features of Tool for Safety Management

The approach to safety and concept of safety management used by designer, manufacturer, operator and regulator must be same. For this purpose, we construct a generic model of safety management showing the main features and requirements for management of the integral safety of such installations. Background features of generic model of safety management are shown in Figures 1 and 2. Further features go out from knowledge summarized in works [10,14] and they are described by figures:

- Figure 3 shows the way of planning the safe technical installation with SMR.
- Figure 4 shows way of creation of technical installation with SMR risk-based design.
- Figure 5 shows way of comparison of technical installation with SMR important parameters.
- Figure 6 shows technical installation with SMR safety features at operation.

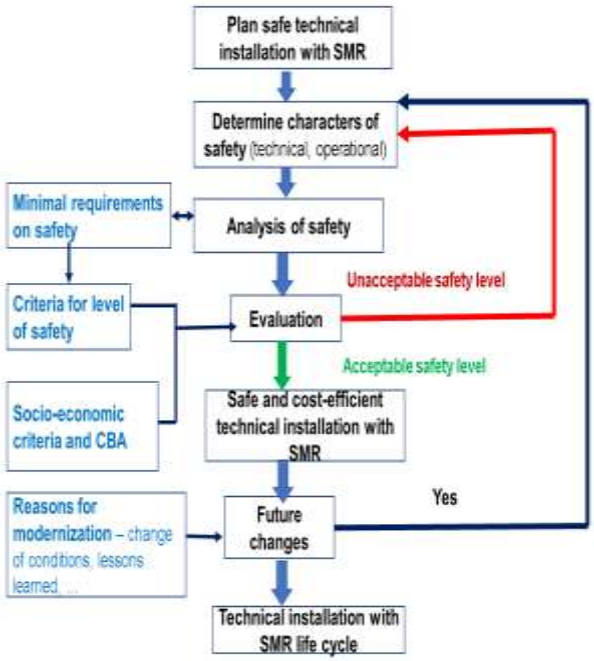

Fig. 3. Way of planning the safe technical installation with SMR.

Fig. 4. Risk-based design flowchart.

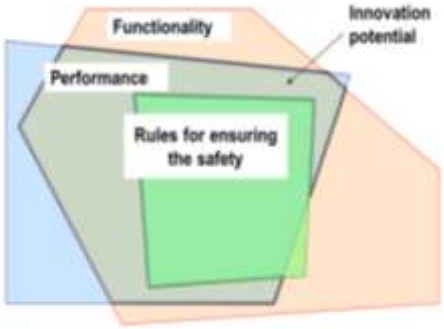

Fig. 5. Way for comparison of technical installation with SMR important parameters.

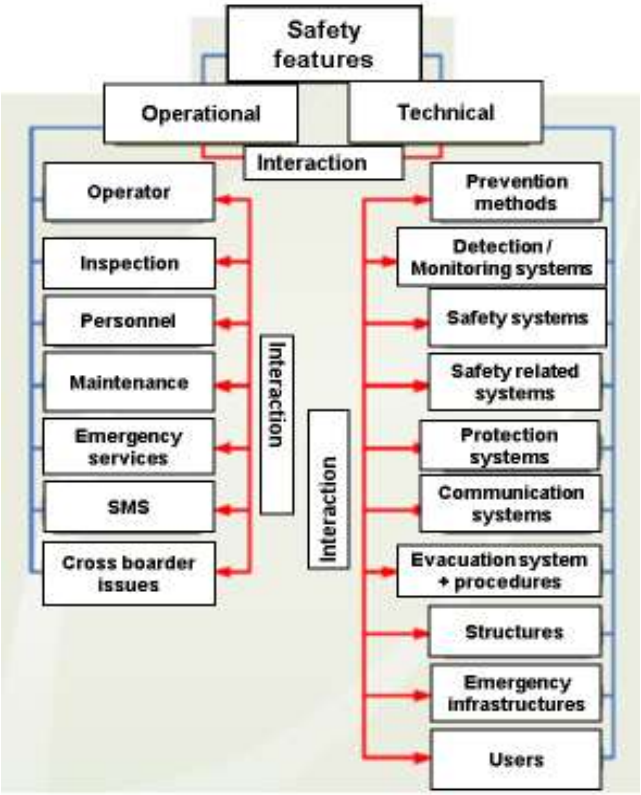

Fig. 6. Safety features of technical installation with SMR.

Considering the knowledge summarized in foregoing chapters, the other important parts of generic model of safety management of technical installation with SMR at operation are:

- Process of technical installation with SMR risk management towards safety during the operation, which is shown in Figure 7.

Fig. 7. Safety management of technical installation with SMR at operation.

- Tasks, which need to be specified in technical installation with SMR safety management system (SMS), are shown in Figure 8.

Fig. 8. Tasks specified in the safety management system (SMS) of technical installation with SMR.

At technical installation with SMR safety management, we distinguish the basic levels of management that need to be aligned, namely: political, strategic, tactical, operational/functional and technical, Figure 9.

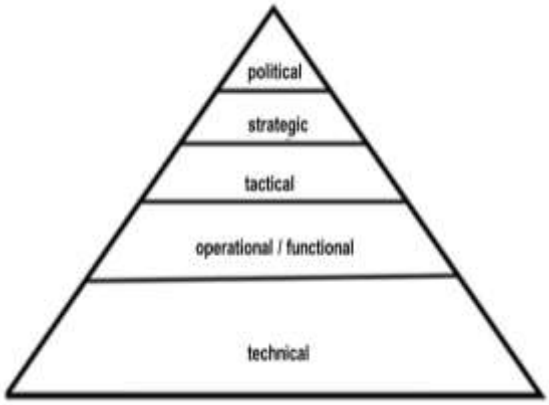

Fig. 9. Technical installation with SMR process management levels.

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.

According to the TQM scientific theory [21] and according to the authors´ 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:

1. At the operational management level of technical installation with SMR, well-structured problems can be successfully solved.
2. At the middle management level of technical installation with SMR both, the structured problems and the poorly structured problems that are not associated with great risks to the technical installation with SMR can be successfully solved.
3. At the top management level of technical installation with SMR, complex and unstructured problems that have risks that can be controlled using the tools that only the top management of the power plant with SMR has at its disposal.
4. Only through mutual cooperation of public administration and top management of technical installation with SMR can complex and unstructured problems of large scale with great risks be solved.

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

A number of supranational institutions (EU, IAEA, IATA, ICAO, OECD, etc.) require for critical technical installations (those with SMR belongs to them) the preparation of documentation on safety 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 technical installation with SMR of 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 technical installation with SMR.

In general, a safety report of technical installation with SMR. 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 technical installation with SMR surroundings and the environment, a description of the equipment and an inventory of hazardous substances present in the technical installation with SMR, 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 2 and is the basis of the integral safety management system of the monitored entity.

The safety report of technical installation with SMR needs to be processed already in the concept phase (preliminary), refined in the design and construction phase, and systematically updated during the operation. It provides a set of policies and rules for maintaining the safety and improving it. In practice, it is implemented by its transposition into internal regulations, which are mandatory. It is the basic tool of the safety management system (SMS) of entity [10,11]. In terms of responsibilities, it is created hierarchically at different levels of details, and since the highest competencies are in top management [23], so the division of responsibilities is done from top to bottom.

An important document of the safety report for technical installation with SMR as important critical facility, which is vital to ensuring the basic functions of the State is the continuity plan [10], which is the strategic plan for the management of safety and development of technical installation with SMR, which is 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 technical installation with SMR, but also a way of solving the problems that can seriously disrupt the operation and competitiveness of technical installation with SMR. In accordance with [10], the entity continuity plan has higher goals than the risk management plan and it includes procedures:

1. How to deal with risks that have a source outside the technical installation with SMR and seriously affect it. It contains clearly determined responsibilities and procedures for resolving the conflicts between the public interest and the technical installation with SMR operator.
2. How to ensure a safe technical installation with SMR for the planned lifetime, so that technical installation with SMR may deliver quality products and services, it is competitive and does not endanger itself and its surroundings.
3. How to coordinate changes caused by dynamic development of technical installation with SMR. 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 technical installation with SMR., i.e. it is attached a crisis preparedness plan that contains measures and their ensuring, and way for support the State in critical situations.

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 risks are site-specific, the generic model presented above must be adapted to site conditions and legislation which is in force in a given region.

7 Conclusion

The article summarizes the knowledge on complex technical installations safety management during their lifecycles (i.e. from sitting to decommissioning). The safety management is based on continuous risks´ management, namely partial ones and integral one. For determination of integral risk, the special decision support system is used and for decision-making on its acceptability, the general principles used by the UN, WB, Swiss Re etc. are recommended [10].

Because technical installation with SMR belongs to complex technical installations , it is made the technology transfer, and on the base of analogy method, it is constructed the generic model for management of safety for it. All figures (1-8) show the solution of main parts of safety management of technical installation with SMR. Its safety report needs to be processed already in the concept phase (preliminary), refined in the design and construction phase, and systematically updated during the operation of this technical installation. This safety report provides a set of policies and rules for maintaining the safety and improving it. In practice, these demands are implemented by transposition into internal regulations, which are mandatory in the given country.

The generic model of technical installation with SMR includes: definition of the objective and focus of safety management; description of accidents and failures; proposals for risk management decision-making; discussing the package of measures and activities with key actors; monitoring principles and lessons learned for correction applications.

The safety management of technical installation with SMR includes: the concept of increasing safety; the definition of safety-related roles and their tasks; a risk management process for the benefit of safety; a system for operational risk management decision support, including a value scale to determine the level of risk that technical installation with SMR poses to its surroundings and a value

scale to determine the degree of contribution of technical installation with SMR to its surroundings; division of responsibilities; and safety documentation.

Acknowledgement: Authors thank for the TACR project TK02030125.

References:

[1] IAEA, *Considerations for Environmental Impacts Assessment for Small Modular Reactors. IAEA-TECDOC-2915*. Vienna: IAEA 2020, 48 p.

[2] C. P. Pannier, R. Skoda, Comparison of Small Modular Reactor and Large Nuclear Reactor Fuel Costs. *Energy and Power engineering.* Vol. 6, No 4, pp. 82-94. 2014. doi: 10.4236/epe.2014.65009.

[3] R. Rosner, S. Goldberg, *Small Modular Reactors – Key to Future Nuclear Power Generation in the U.S.* Chicago: EPIC 2018, 81 p.

[4] C. Stenberg, *Energy Transitions and the Future of Nuclear Energy: A Case for Small Modular Reactors. Washington Journal of Environmental Law & Policy*. 2020. https://digitalcommons.law.uw.edu/wjelp /vol11/iss1/3

[5] UJV, *Design of the* Active *Zone and* F*easibility* S*tudy of a Small* Modular *Reactor Cooled* b*y Molten Salt.* Řež: Centrum výzkumu 2017, 48 p.

[6] L. Myšák, *Proposal of Marine Shipment wit Use of Hydrogen and SMR*. Praha: ČVUT 2022; manuscript.

[7] UJV, *Plan of Use of Constructed Energy Well Reactor in Practice.* Řež: Centrum výzkumu 2022, 205 p.

[8] EU, *FOCUS Project Study – FOCUS*. Brussels: EU 2012. http://www. focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c469 59712 f8a

[9] FEMA, *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996, 96 p.

[10] D. Procházková, J. Procházka, J. Lukavský, V.Dostál, Z. Procházka, L, Ouhrabka, *Management of Risks of Processes Associated with Operation of Technical Facilities during Their Lifetime.* Praha: ČVUT 2019, 465 p. Doi: 10.14311 /BK.9788001066751

[11] D. Procházková, J. Procházka, J. Riha, V. Beran, Z. Procházka, DSS for Ensuring the Coexistence of Technical Facility with Its Vicinity during the Type Selection and Sitting. *Proceedings of the 29th European Safety and Reliability Conference*. Research Publishing: Singapore 2019. Doi: 10.3850/978-981-11-2724-3_0096-cd,

[12] EU, *Green Paper on a European Program for Critical Infrastructure Protection*. Brussels: EU 1005. https://eur-lex.europa.eu

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

[14] D. Procházková , „Risk-Based Design of Technical Facilities," *JUFOS 2021*. Brno: VUT 2021, pp. 40-51.

[15] 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 Response*. Paris: OECD 2002, 191 p.

[16] J. Procházka, D. Procházková, *Risk Management of Traffic Management Systems.* Praha: ČVUT 2022,129 p. doi: 10.14311/BK.97880010 69950

[17] R. L. Keeney, H. Raiffa, *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1993, 569 p.

[18] R. H. Coase, R. H. „The Problem of Social Cost". *Journal of Law and Economics,* Vol. 3, No. 1, pp. 1-44, 1960.

[19] IAEA, *Safety of Nuclear Power Plants. No. SSR-2/1.* Vienna: IAEA 2016, 67 p.

[20] IAEA, *Safety of Nuclear Power Plants. No. NS-R-1.* Vienna: IAEA 2000, 99 p.

[21] Ch. Perrow, *Normal Accidents: Living with High-Risk Technologies.* Princeton: Princeton University Press 1999, 196 p.

[22] M. Zairi, *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd.1991, 192 p.

[23] B. Delongu, *Risk Analysis and Governance in EU Policy Making and Regulation.* ISBN 978-3-319-30822-1. Sprin-ger 2016, 288 p.