Generic Model for Management of Safety of Technical Installations with Small Modular Reactors

DANA PROCHAZKOVA
Department of Energy, Faculty of Machinery
Czech Technical University
Technicka 4, 166 00 Praha 6
CZCH REPUBLIC

Abstract: - Technical installations with small modular reactors (SMRs) are perspective industrial complexes due to high need of energy of new technologies. 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: - Small modular reactors (SMR), technical installations with SMR, systemic approach, risks, integral safety, generic model of safety management.

Received: ….. Revised: …….. Accepted: ……. Published: ….

1 Introduction

Due to the ever-increasing consumption of energy, we need to apply new energy sources to ensure safe and stable operation of industry and services. Therefore, we deal with industrial complexes with small modular reactors that are stable energy sources. Because, a lot of open problems exists, we construct generic model for management of safety of such complexes.

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.

Technical installations with the SMR as other technical installations are complex facilities of system of systems type with nature socio-cyber-physical [5,6]. They are threatened by risks caused by harmful phenomena: occurring in the locality, in which they are located; 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 [7,8]; and, last but not least, by low possibilities of humans to anticipate sudden changes in the development of the world. 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 [5,6], 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.

2 Risk and Safety of Complex Installations

Manifestation of complexity means that the behavior of the whole cannot be inferred from the behavior of individual parts, and under certain conditions there

are unexpected phenomena that lead to the destruction or failure of the functionality of a given of a technical facility [5,6]. It is about: suddenly emerging features of behavior that cannot be derived from knowledge about the behavior of components (it is so-called emergence); hierarchy; self-organization; and a diversity of management structures that together resembles chaos. Integral safety is understood as the attribute of the highest quality of installations and organizations; the principles of total quality management are in [10].

Technical Installations with the SMR are complex technical installations, the type of which are system of systems; Figure 1. They contain different technologies, different elements and their interfaces from different fields. To be safe and profitable, they must have specific property – interoperability at conditions normal abnormal and critical [11]. Interoperability is the ability for the equipment and systems of the whole to work together in an efficient manner, i.e. performing the tasks assigned to them so that the system of systems meets the target within the required time and to the required extent

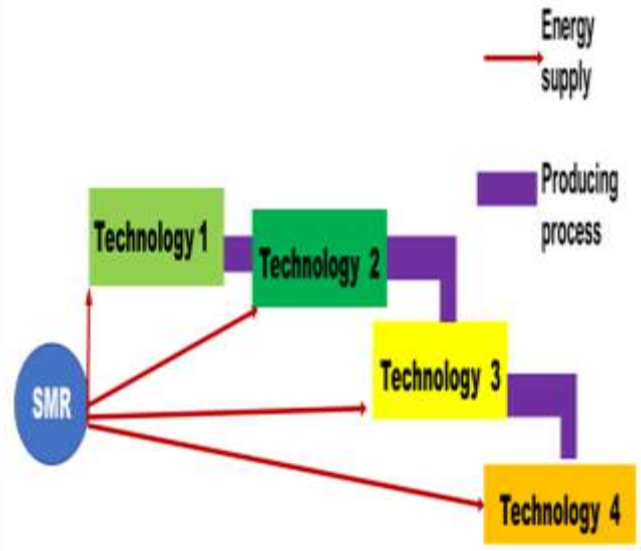

Fig. 1. Simple scheme of set of technologies having the SMR as energy source.

To ensure the safety of complex technical facilities, many branches and interdisciplinary approaches [5,6] are required to ensure their: existence (ability to ensure balance); efficiency (ability to cope with resource shortages); freedom (ability to handle challenges from around); security (ability to protect yourself from phenomena inside and outside); adaptation (ability to adapt to external changes); and safety which ensures the coexistence (the ability to change its behavior so that the behavior responds to the behavior and orientation of other systems and that the system does not endanger them and they do not endanger it).

The basic principle of such technical facility safety management is a qualified interconnection of technical, organizational, financial, personnel, social and knowledge areas and clearly defined roles and responsibilities of all involved [5,6]. The safety management system (SMS) thus covers a number of areas, namely technical, military, legislative, financial, economic, social, environmental, educational, research, etc. The SMS is inserted into technical facility by so called risk-based design and its capability to manage risks towards integral safety during the operation must be permanently monitored and kept on required level.

The integral safety concept at operation [5] requires to: monitor priority risks and conditions of critical fittings, components and personnel; keep rules for safe operation at all organization levels; permanently increase safety by help of special strategic program; perform risk base inspections on critical fittings, components and systems; realize condition-based maintenance; systematically improve safety culture; be prepared for response to all expected emergencies in all aspects connected with response and for ensuring the operation continuity under abnormal and critical conditions; use optimal working modes; motivate personnel; have necessary reserves in all important items; systematically co-operate with public administration, organizations using the same technology and research organizations; and be able to install technological changes if necessary.

3 Risk Sources of Complex Installations

Research of accidents and failures of 7829 technical installations [5] showed that their sources 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.

Results of research [12] showed the causes of organizational accidents in technical facilities; Table 1; and results of research of technical facilities [5] showed internal sources of risk in technical facilities; their examples are in Table 2.

Table 1. Phenomena which cause the organizational accidents in technical facilities.

Area	Defects leading to critical situations
Top management domain	Management of the area: it is predetermined by the political and military aspects; it lacks the human dimension and gives a little support to residents of the EU; it is not carried out on the basis of the data processed by qualified skilled methods; it is often determined by fixed ideas without real assessment of their feasibility; it is based on the idea that everything is stationary and it does not respect the dynamic development of the world, which requires the preparation of a possible extreme scenarios of situations and measures for the survival of the people; and it is not realized on the basis of the principle of the safety management of system of systems in dynamically varying world.
Technical domain	In the field it is missing: standards and norms for the construction of a particularly large underground and above-ground structures with regard to the safety of people and the public welfare; basic services for the population; scenarios for decision making – those used are prepared only on the basis of simulations without validation on real data – sometimes they are used scenarios that were derived for different conditions, i.e. they are not met the conditions for the technology transfer; the norms and standards for interoperability and cooperation of diverse systems; coordinated emergency plans at all levels (it is necessary to have a professional level and respect knowledge and experience), the continuity plans and plans for response to unforeseen situations.
Organisational domain	In the field it is missing: the efforts aimed at the reduction of weaknesses (few sources, contaminated the environment, do not consider the value of work, unemployment) and use the strengths (qualified technical population); an effective tool against corruption, abuse of power, suppressing the influence of lobbyists, etc.; support for cooperation on mutual partnership principle; a basis for mutual understanding and mutual coexistence; effective international teams for the first response; the basis for the cooperation of the members of the first response and norms and standards for their interoperability.
Knowledge domain	In the knowledge base used for decision making it is missing: a systematic respect for the essence of the world – a dynamic open system of systems; sufficient effort focused on collecting qualified data on disasters and lessons learned from the responses to extreme disasters; reliable management of disasters; considering the creeping disasters such as the depletion of groundwater, contamination of the human food chain, etc.; qualified disaster scenarios for decision making.

Table 2. Areas of sources of risk of technical facilities.

Category of disasters	Examples of sources of risks of technical facilities
Technical	Aging - Corrosion – internal and external - Quality of welds - Wear and tear of fittings - Specific phenomena connected with critical fittings – e.g. turbines: mechanical vibration, aging, load, etc.
Procedural	They relate to the production process – leaks, explosive or flammable material, dust, emissions, etc.
Working activity	Danger activities – work at heights, driving vehicles or excavators, underwater work, work in solitary confinement, etc.
Working environment	Floor adjustment – slipping, tripping and falling; rough surface, hot / frosty surface, cramped space, etc.
External	Natural disasters, external crashes, plane crashes, terrorist attacks
Employees´ behaviour	Non-compliance with rules.
Organizational	Poor organisation of work, heavy workload, inadequate training, poor change management.
Working environment contamination	Noise, hazardous emissions, pools, puddles, spills, etc.
Finance	Pay outs, contract payments, taxes, material availability, inventory management, etc.
Project management	Availability of human resources, project implementation, lifetime management, contract management, etc.

4 Purpose of Generic Model for Safety Management

Because a lot of problems that led to accidents and failures were in many cases in interconnections of safe elements, which was caused by bad co-operation of specialists from different fields at designing and operation [5], a tool for unification of understanding the safety by all specialists is important. We denote this tool "generic model for safety management". For safety preservation and improvement, it is also necessary to consider that the world dynamically changes, which leads to origin of new risk sources. Therefore, 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 [5].

Generic model of complex installations, the simple scheme of which is shown in Figure 1, is nonlinear description of process of designing and operation of set of many open interconnected systems of different nature and location, which ensure certain operations and activities with considering that interconnections also cause unacceptable interdependences at certain conditions. The role plays a reality that each partial system has certain 'limits and conditions', which set its safety, and these are not always the same for all systems. The limits and conditions for the whole technical installations are determined by the current configuration of the partial systems, i.e. they depend on both, on the quantity and properties of the subsystems and on the diversity of their interconnections, i.e. their relationships and flows among them and also across them [5].

At occurrence of conditions, which are beyond conditions of one or more critical systems of technical installation, the cascade failure of whole usually origins. To prevent this, it is needed robust architecture and mainly robust interconnections [5,6]. To ensure robust interconnections, which have diverse nature, professionals from different specializations need to: understand safety in the same way; and communicate. Therefore, generic model for safety management of technical installation with SMR needs to show interconnected domains: activities for ensuring the safety; way of management of technical installation safety, which considers seven processes (i.e. processes connected with: conception and management; administrative procedures; technical matters; external cooperation; emergency preparedness; documentation and investigation of accidents; and cyber security); way of planning, risk-based designing and risk-based operating, which lead to safety; and duties and responsibilities connected with safety on management levels, which must be codified. Further, we mostly concentrate to integral safety, because nuclear safety is covered by the IAEA standard [9].

x

5 Generic Model for Management of Safety of Technical Installations with SMR

Generic model for management of safety of technical installations with SMR shows how to: deal with risk towards safety; create robust design that is realistic and economically acceptable; operate safely and economically acceptable; manage ALARA phenomena ; and respond unacceptable phenomena. Analogically to [5,6] the safety management procedure consists of: identification of strategic goals of this complex; identification of critical activities, functions or services that rely on this complex or which this complex provides; identification of external context: legal / regulatory requirements, stakeholder perceptions and expectations, and any relevant social, political, economic, financial, technological or market factors; collection of data on risk sources and their impacts on technical facility – external, internal, organizational etc.; investigation of this complex opportunities and specially at occurrence of cascading or cumulative impacts; risk identification – process of finding, recognizing and describing the risk; risk management – sources, events (conditions for realization), causes, impacts / consequences; and risk owner solutions – person with accountability and authority to manage a risk.

The following figures show main features of generic model:

- Figure 2 shows way of planning of the safe technical installation with SMR.
- Figure 3 shows way of creation of technical installation with SMR.
- Figure 4 shows way of comparison of risk-based design of technical installation with SMR important parameters.
- Figure 5 shows safety features of technical installation with SMR at operation.
- Process of risk management of technical installation with SMR towards safety during the operation, which is shown in Figure 6.
- Tasks, which need to be specified in safety management system (SMS) of technical installation with SMR, are shown in Figure 7.
- Figure 8 showing the model of safety management of technical installation with SMR in time.

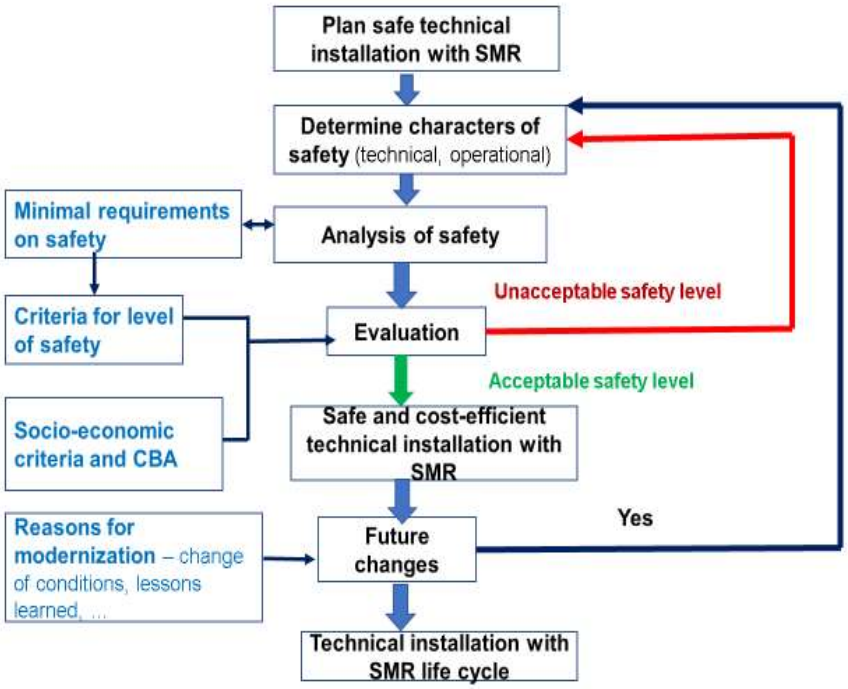

Fig. 2. Generic model of planning the safe technical installation with SMR.

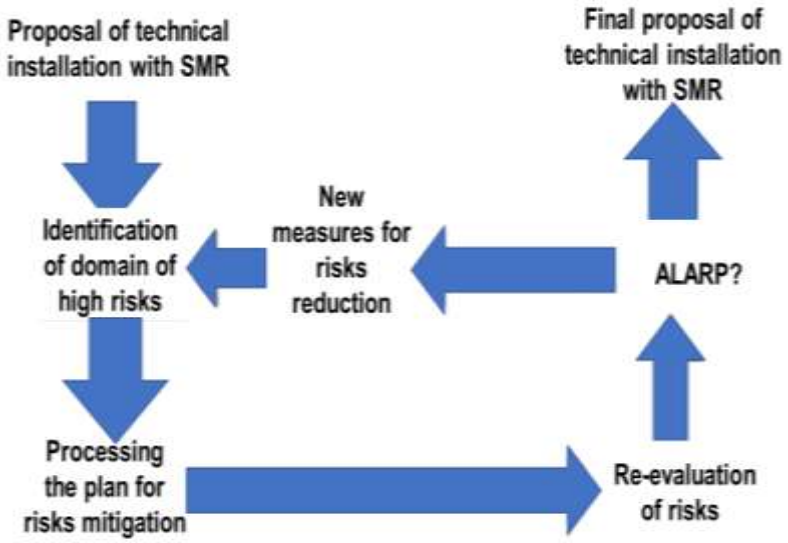

Fig. 3. Risk-based design flowchart.

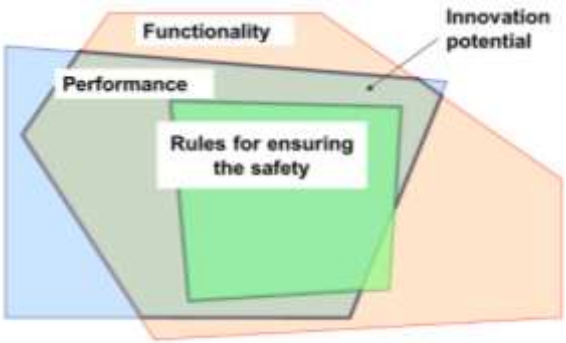

Fig. 4. Way for comparison of technical installation with SMR important parameters.

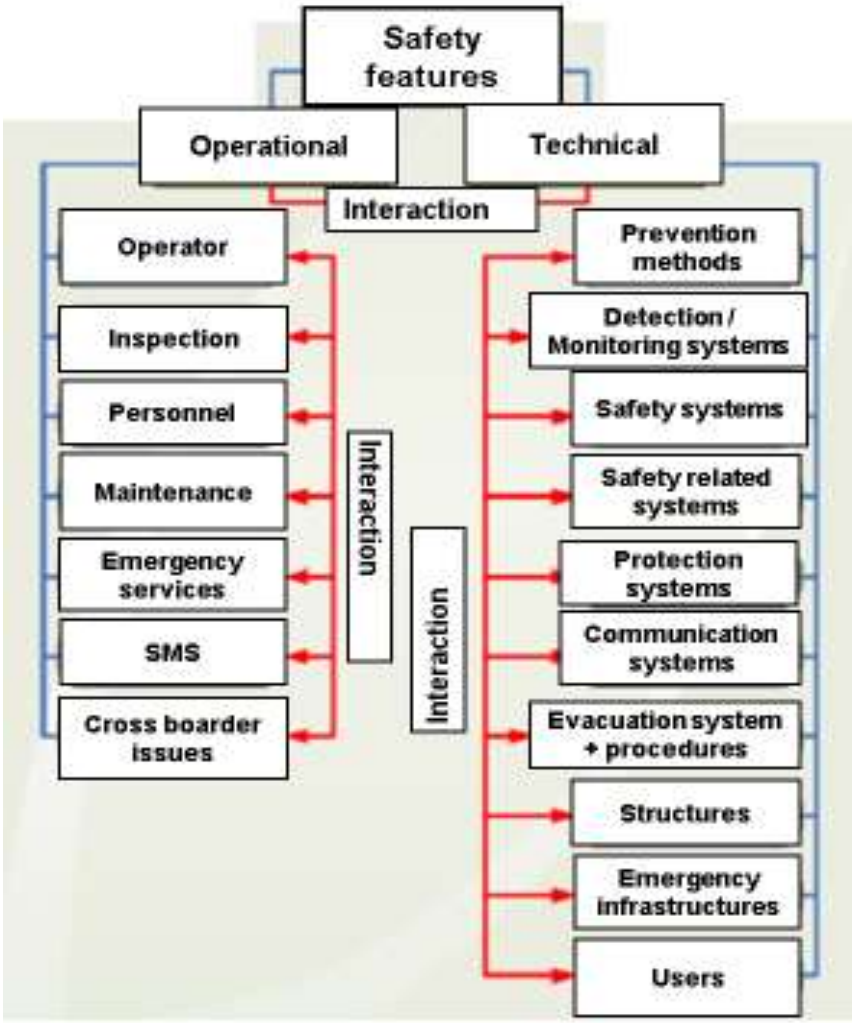

Fig. 5. Safety features of technical installation with SMR.

Fig. 6. Safety management of technical installation with SMR at operation.

Fig. 7. Tasks specified in the safety management system (SMS) of technical installation with SMR.

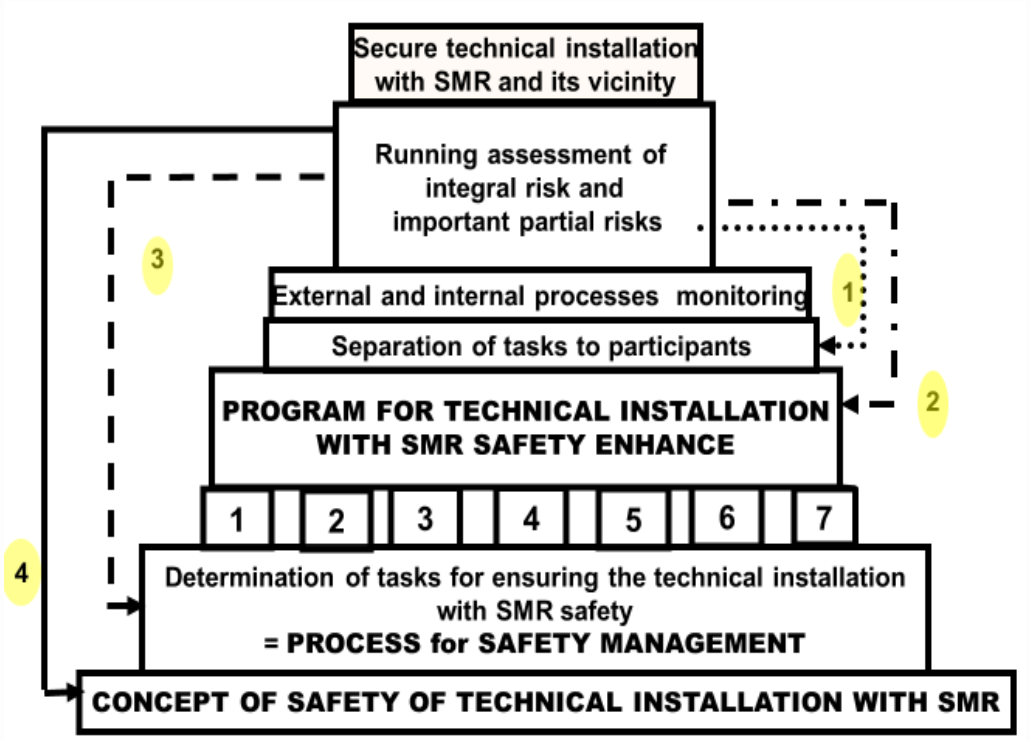

Fig. 8. Model of safety management of technical installation with SMR with automated control. Processes: 1- conception and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; 6 - documentation and investigation of accidents; 7- cyber security. Feedbacks: numbers 1-4 in a yellow circle.

6 Tool for Determination of Integral Risk

Because of 80% of failures is caused by combination of several risk sources, it is necessary to manage both, the important partial risks and the integral risk [5]. Since, causes of individual contributing sources are incommensurable, it is necessary to determine the integral risk by help decision support system (DSS) which is judged by numbers from 0 to 5 with using the principles proposed by [13], the higher, the worse. The general shape of such DSS for technical installations with the SMR shown in Figure 1 is in Table 3.

In Table 3, the individual criterions are the results of assessment of individual DSSs for partial technological facilities. The procedure for construction of individual DSS is described in [5]. At their assessment, it is planned to use the auxiliary scale for judgement of sources of risk from domains: technical; environmental; legal, economic; and organi-

zational, which will be judged by auxiliary scale for ensuring the commensuration is e.g. in [5].

Table 3. General DSS for integral risk assessment.

Criterion	Assessment
Rate of integral risk of occurrence of organization accident of complex technical installation	
Rate of integral risk of technology 1 - DSS1	
Rate of integral risk of technology 2 - DSS2	
Rate of integral risk of technology 3 - DSS3	
Rate of integral risk of technology 4 - DSS4	
Rate of integral risk of SMR - DSS for SMR	
Total integral risk of complex technical installation	

The proposed scale for judgement of integral risk of complex to Table 3 is given in Table 4.

Table 4. Scale for determining the integral risk rate; N = 30.

The level of risk	Values in % N
Extremely high – 5	More than 95 %
Very high – 4	70 - 95 %
High – 3	45 - 70 %
Medium – 2	25 – 45 %
Negligible – 0	Low than 5 %

According to the risk values identified by Table 3, the results of the risk assessment will be classified into three groups:

- risk acceptable – category 0 and 1;
- ALARA risk, i.e. conditionally acceptable – category 2 and 3;
- risk unacceptable – category 4 and 5.

If the risk is acceptable, then no further risk mitigation measures need to be taken. If the risk is ALARA, it is necessary to build technical elements into the project that will allow a response in the event of risk realization. In the event of an unacceptable risk, corrections must be made, e.g. in the material, structure or method of interconnection, and the risk reassessed.

7. Conclusion

The results are based on 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 and for decision-making on its acceptability, the special decision support system is used [5]. From the safety point of view [6], the design of complex requires to follow: durability; manageability of equipment, components and processes; lifespan; human resources; costs; technical services; additional ser-vices; safety of employees; and safety of humans in surroundings and safety of environment. Consideration and good provision of requirements in question determines the future costs of ensuring the safety.

In terms of current knowledge [5,6], we follow two tasks: solving the functionality of set of interconnected (i.e. dependent) elements and their interfaces under normal, abnormal and critical conditions; and searching the critical conditions of complex fitting, equipment or facility that are unpredictable or are result of serious operator´ error, and that may, under certain conditions, go to highly non-demanded, i.e. highly unacceptable conditions, i.e. situations in which the very existence of facility or even humans is threatened, and which we usually refer to as crisis. Therefore, at design and operation they need to be followed specific characteristics such as: interoperability (i.e. ability of technical facility as a whole to perform quality tasks under normal, abnormal and critical conditions); safety integrity, which is mostly tracked in conjunction with human errors (at specification, design, installation, maintenance, modification, etc.); criticality (i.e. extent to which personal injury, material destruction, damage or other asset losses may occur – threshold below which monitored equipment condition is demanded and vice versa); dependability (operational reliability), which ensures that system meets specified requirements and its operation complies with specified conditions.

The generic model for safety management 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 concept of preserving and 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.

Based on recent experience from practice [5], it can be said that the use of generic model for management of safety come in useful at education of specialists, who construct technical installations with SMR for mining, transport, production etc. It improves cooperation of specialists from different fields in solving the problems connected with safety.

Acknowledgement:

Author thanks 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] PANNIER, C. P., SKODA, R. Comparison of Small Modular Reactor and Large Nuclear Reactor Fuel Costs. *Energy and Power engineering.* 6 (2014), 4, pp. 82-94. doi: 10.4236/epe. 2014.65009.

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

[4] STENBERG, C. *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] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZ-KA, Z., OUHRABKA, L. *Management of Risks of Processes Associated with Operation of Technical Facilities during Their Lifetime.* Praha: ČVUR 2019. Doi:10.14311 /BK.9788001066 751

[6] PROCHÁZKOVÁ, D., PROCHÁZKA, J., RIHA, J., BERAN, V., PROCHÁZKA, Z. *DSS for Ensuring the Coexistence of Technical Facility with Its Vicinity during the Type Selection and Sitting*. Praha: ČVUT 2019. Doi: 10.3850/ 978-981-11-2724-3_0096-cd,

[7] EU. *FOCUS Project Study – FOCUS.* http://www.focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c46959712 f8a

[8] FEMA. *Guide for All-Hazard Emergency Opeations Planning.* State and Local Guide (SLG) 101. Washinton: FEMA: 1996.

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

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

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

[12] PROCHAZKOVA, D. *Safety of Complex Technological Facilities.* ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244 p.

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