Tool for Technical Instllations Safety Based on Interconnection of Standards and Risk Management

DANA PROCHAZKOVA

Czech Technical University in Prague, Technicka 4, 166 00 Praha 6. Czech Republic
danuse.prochazkova@fs.cvut.cz

Abstract: The article deals with the reliability, security and safety of complex technical installations. It shows the role of technical standards and the role of risk management at ensuring the complex technical installations safety. Based on present knowledge and experiences from practice, it proposes a principle for linking the provisions of standards and the results of risk management. It introduces an example of such interconnection at designing.

Key words: Complex technical installations; safety; risk; technical standards; risk management; tool for linking; risk-based design; risk-based operation.

1. Introduction

Complex technical facilities, both object and network, are essential for the life, protection and development of human society. They are currently socio-cyber-physical in nature, as they are made up and operated by humans, and are composed of technical and cyber elements and their interconnections. A targeted analysis of their accidents and failures [1-14] has shown that despite the great amount of knowledge about technical installations, their equipment, structures, interconnections, risks and safety, which are contained in the technical standards for their design and operation, accidents and failures of technical installations still occur. There are several reasons for this: the dynamic variability of the world; insufficient human knowledge and abilities; slow application of knowledge and experience gained in practice; and unsatisfactory awareness of the risks and their consequences for technical installations and the public interest.

As the world changes dynamically, so there are also change the processes that trigger the phenomena (commonly called disasters) that cause risks. Therefore, the harmful potential of disasters changes over time, i.e. the size of the hazard changes and with it the sizes of the risks, to which the changes in the distribution of public assets in the area of interest or the monitored technical installation that occur over time contribute [1,15]. Therefore, the safety of technical installations and the safety of their surroundings must be monitored from the concept, through the design, construction, operation to decommissioning and revitalization of the occupied area.

2. Risk

Risk is a quantity that is a measure of loss, damage and harm 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 vulnerability of the local monitored assets. In strategic management, the following variables are defined: hazard as the probable size of a disaster that occurs once in a given place once per defined time interval (so-called design disaster [15]; and risk as the probable size of losses, damages and damage to the monitored assets in a design disaster divided into a unit of time (most often 1 year) and a unit of territory [15]. The risk is ,therefore, locally and temporally specific because it depends on the amount and vulnera-

bility 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 management of the technical installations and the public administration must prepare for the future implementation of risks. This means having the tools to reduce the realisation of known sources of risk and to limit the emergence of new risks. The paper follows risk management in favour of safety. With regard to current knowledge, the article does not call into question existing standards, since they contain earlier knowledge. Without their application, past errors would be repeated. The aim of the article is to show how to connect the knowledge included in the valid standards with the results of risk management, which is now recommended by a number of standards. E.g. ISO 31010, ISO 31010, ISO 9000, etc.

3. Technical Standards

A technical standard is an established norm or requirement for a repeatable technical task which is applied to a common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices. A technical standard includes definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength [16-18].

It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices. In contrast, a custom, convention, company product, corporate standard, and so forth that becomes generally accepted and dominant is often called a de facto standard. The term formal standard refers specifically to a specification that has been approved by a standard´s setting organization. The term de jure standard refers to a standard mandated by legal requirements or refers generally to any formal standard.
When an organization develops standards that may be used openly, it is common to have formal rules published regarding the process. This may include: who is allowed to vote and provide input on new or revised standards; what is the formal step-by-step process; how are bias and commercial interests handled; how negative votes or ballots are handled; and what type of consensus is required. The Expert Group of such organization assesses the proposal from the perspective of: uniformity and mutual compliance of standards with legal regulations; the use of the achieved degree of development of science and technology; the application of the protection of a legitimate interest; fulfilling the obligations arising from international treaties and exploiting the results of international cooperation; and discussion of the draft standard, its amendment or repeal.

Following the recommendation of the approval group, the standard shall be drawn up in the form of a proposal to be put to the vote. In case of acceptance, the norm shall be approved and printed. Draft European standards are approved by a weighted vote expressing the economic importance of CEN and CENELEC member countries. For example, the Czech Republic has 12 votes in this system, as do Belgium, Hungary, Portugal and Greece. Once approved, member countries are obliged to introduce the standards into their national standards within 6 months. In ISO and IEC, 75% of the positive opinions of voting members are required for approval [16,18].

What is important, it is the fact above that standards are a "consensus-based document". Since the environment is dynamically evolving, draft standard provisions include the results of a certain interval, which we refer to as the "median ± σ“, where σ is the standard deviation that is determined by probability theory. In this case, however, we must be aware of the fact that in no case does the selected solu-

tion cover all possible variants of the monitored issue. For normal distribution, the interval (-σ, +σ) covers 68.5% of cases; the interval (-2σ,+2σ) covers 95.4% of cases; the interval (-3σ,+3σ) covers 99.8% of cases [19]. This means that standards cover 68.5% of cases. This means in practice that the objective of the standards is limited by the so-called 'red tape' - limits and conditions; i.e. the solution applies only to certain conditions (and when they are exceeded, the target is not met, which leads to the failure or failure of the element, object or process) [1,19].

4. Risk and Safety

The aim of people is that technical installations would be safe, i.e. they perform the functions for which they were created in a quality and reliable way, while not endangering themselves and their surroundings, i.e. people and the environment, which is essential for the life and development of human society. Therefore, in accordance with current knowledge and experience, humans must first identify the sources of risk (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 magnitude 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 divide the risks into acceptable, conditionally acceptable and unacceptable [15].

In the case of risks which are: unacceptable is the need to ensure the application of effective preventive measures against their sources; conditionally acceptable, i.e. ALARA, mitigation, reactive and restorative measures should be prepared for the monitored assets; 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".

Safety is understood as a property at the level of the system, which is formed by human by their measures and actions [1,15]. The quantities, risk and safety are not complementary quantities, since the safety of the environment and of each technical installation can be increased through organizational measures, e.g. by introducing the warning systems and back-up solutions, without reducing the size of the risk; an additional concept to safety is criticality [1,15].

The safety of a technical installations and its surroundings can only be ensured by high-quality anthropogenic management [1,15,20]. At operation, 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 requires mutual communication between owners and operators of technical installations, public administrations, the public and the media [20].

5. Safety-oriented Risk Manage-ment of Technical Installations

Management is the type of activity that triggers and ensures the functioning the monitored systems. It is a conscious way of applying the theoretical and practical knowledge of a person (manager) focused on identifying and recognizing the problems and goals in the monitored system, ways of coping with problems, setting procedures to achieve required goals and on the implementation of procedures associated with control mechanisms aimed at achieving the required goals optimally. Its first task is to correctly diagnose or specify each problem, make a rational decision, accept the decision and implement it in the given specific conditions. Management has a predisposition to be successful when it is based on knowledge and experience and when the individual decisions that make up management, or better the management process, are qualified. Acquiring the relevant knowledge and experience means constantly collecting, evaluating

and verifying the data and conducting the qualified assessments.

Total Quality Management (TQM) [21] is the type of management that helped European industry to recover from the slump caused by the World War II. To be successful, it was introduced into the public sector in the EU by the Treaty of Maastricht in 1989. It 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. The quality improvement process is based on an impulse according to the needs of the customer / citizen. TQM is based on the recognition 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. It is a way in which attention is focused on the processes taking place in the institution. When implementing TQM, the specifics of the institution are considered, since for reasons of efficiency it must correspond to the structure of the institution. TQM is used in the management of enterprises (technical works), municipalities and regions.

The outputs from the risk management process towards safety in the application according to TQM are as follows:

1. Risk assessment document - all information about the relevant risks is recorded here.
2. Top risks list – it contains a list of selected risks, the solution of which has the highest demands on resources and time (for technical installations, these are risks that need to be constantly monitored and, according to the results of monitoring, apply measures and activities leading to security [20]).
3. Retired risk list – it serves as a historical reference for future decision-making during changes and modernizations (e.g. to avoid removing barriers that have been inserted into the system for prevention or mitigation [22]).

According to the data summarized in the work [1], different types of management are used for technical installations. Currently, the following ones are used: reliability management; security management; safety management; continuity management; resiliency management; and asset management. Each of these types has certain specifics. The first type of management is the oldest and is regulated by technical norms and standards. In addition to reliability management, the second type of management focuses on the protection of technical installations from internal and external harmful phenomena (disasters), including the behaviour of the humans who create and operate them [15]. Security in connection with a certain object generally means a set of measures and activities to ensure that the monitored object does not suffer losses, damage and harms in the presence of internal and external harmful phenomena. Physical and cyber protection of the object [1,20] is used for its implementation, not only against attacks from the outside, but also from the inside.

The rules for the security of technical installations are elaborated in the work [23], in which there are also definitions as opposed to the safety of technical installations [24]; the distinction between security and safety is also in IAEA documents [25]. Although logically a safe object is also a secured object [20], there is still conjecture as to what is more important. The consensus is that a secure technical installation, as well as a safe technical installation, flawlessly performs the set tasks for a set period of time under certain conditions, while being protected against all internal and external disasters, including the human factor. The difference is that the secured technical installation does not have built-in protection of the surroundings.

In order to ensure the safety of technical facilities, we solve the problem of system safety od systems of systems [1,20], because a set of interconnected safe open systems is not necessarily a safe system, since the safety of the system of systems also depends on the nature

of the interconnections among 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 partial parts of the technical installation, we also have to pay special attention to the set of systems as a whole. We need to find out:

- types of system of systems failures,
- operating conditions of the system of systems,
- internal links and their manifestations,
- characteristics of critical conditions of system systems.

Continuity management is aimed at the safety of the technical installations and its surroundings under all possible conditions [1]. Resilience management is a precursor to safety management and continuity management; it tries to increase the toughness of the system and its surroundings in order to gain time to form an effective response of the object in the event of a harmful phenomenon occurrence [1]. Asset management prioritises risk management in favour of production over the security of the humans and surroundings of the technical installation [1], i.e. it does not favour the public interest.

Components of all mentioned 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 dealing with risks which, due to the different objectives of the procedures in question, do not usually give the same results [20],
- 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),
- starting with the second type, they are the superstructure of reliability management, which for many years was the royal discipline in the management of technical works [20].

Despite the different names of the types of management, their methodology is the same, namely to obtain: awareness of risk; understanding the risk and its relationship to assets and their security; and apply relevant knowledge of what to do to achieve the goal. For the strategic development of human society and technical installations, the risk management in favour of safety, which is aimed at the whole (i.e. safety management), is essential.

In order to manage the risks of the technical installation in favour of safety, five key activities need to be carried out well [15], namely:

1. Definition of the objective and focus of safety management: 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 risk is a priority in a given case.
2. Description: it aims at 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: evaluation of the quality of the forecast of the development of the technical installation, if possible as an optimum when considering the benefits and losses in the operation of the technical installation in dynamically variable surroundings. Deciding how to mitigate and manage risks and how to implement measures represents a key step in risk management.
4. Communication: 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 lessons learned: monitoring 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, apply corrections.

Risk management in the event that the risk is not acceptable consists, according to [15,20], in the choice of one of the following alternatives:

- risk avoidance, i.e. not to initiate or continue activities that are a source of risk when possible (e.g., human society can do without a technical installation),
- elimination of sources of risk, i.e. avoiding the occurrence of disasters when possible (choosing an alternative to a technical installation that will have 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. the allocation of risk between the participants and insurance undertakings,
- risk retention.

Negotiation with risk is based on the current possibilities of human society and consists, according to [15,20], in the division of risks into categories:

- part of the risk is reduced, i.e. preventive measures avert the realisation of the risk,
- part of the risk is mitigated, i.e. mitigating measures and preparedness (warning systems and other emergency and crisis management measures) reduce or avert unacceptable impacts,
- part of the risk is insured,
- the part of the risk for which response and recovery reserves is be prepared,
- the part of the risk that is unmanageable or too costly or infrequent, for which a Contingency plan is prepared.

This is also accompanied by a distribution of risk management among all concerned. The distribution in good management [15] is carried out by taking as a view to ensuring that all stakeholders (from politicians to administrative staff, technical installation 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. When selecting the risk management measures, it should be ensured that the costs of managing the risk does not exceed the potential damage caused by the realisation of the risk.

6. Example of Tool for Designing

It follows from the above that when drawing up the concept of a technical installation, as well as in its sitting, design, construction and operation, both the standards and the risk management results are important in favour of the objective pursued, which today is overall (integral) safety. Therefore, in accordance with knowledge, risk-based design [22] and risk-based operation [1] tools are created that link standards and risk management results.

According to [26], firstly, a decision support system is set up for the given technical installation to support decision-making on the risks of individual components and their interconnection, a scale for the assessment of the level of risk is determined – Table 1. According to the risk values identified, the results of the risk assessment are classified into three groups: risk acceptable – category 0 and 1; ALARA risk, i.e. conditionally acceptable – category 2 and 3; and 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.

Table 1. Value scale for determining the level of risk; N is number of items that influences the risk of a given entity.

Risk level	**Risk category**	**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	Low than 5 %

An example of the link of standards and risk management results in designing process is shown in Figure 1. The progress of building the technical installation shall be determined. The further procedure is the following:

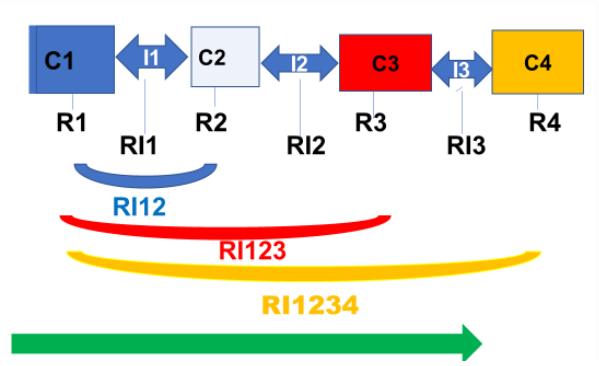

Fig. 1. Scheme of risk-based design. The green arrow shows how to create a project.

- design of components (C1, C2, C3, C4) and their interconnections according to standards,
- according to disasters´ scenarios, the risks of the components (R1, R2, R3, R4) and their interconnections (RI1, RI2, RI3) are determined and after assessed according to Table 1 and, if the risks are not acceptable, corrections are made, e.g. in the material or method of interconnection,
- according to the DSS, the risk of the RI12 linkage set shall be determined and assessed according to Table 1 and, if the risks are not acceptable, corrections shall be made, e.g. in the material or method of interconnection,
- according to the DSS, the risk of the RI123 link file shall be determined and assessed according to Table 1 and, if the risks are not acceptable, corrections shall be made, e.g. in the material or method of interconnection,
- according to the DSS, the risk of the RI1234 link set shall be determined and assessed according to Table 1 and, if the risks are not acceptable, corrections shall be made, e.g. in the material or method of interconnection.

7. Conclusion

The findings presented in the works [22,26] show that the designer must have very important competences for: applying the results of methods of risk analysis and assessment; implementation of a methodology for the analysis and assessment of risks adapted to the problem; solution of problems at emergency and crisis management; analysis of situations / activities / accidents; turning the policy into real action; transforming the accident statistics into action plans; strategic planning; establishing a hierarchy of problems; finding the right information and knowledge; performing the critical analyses; designing the right solutions; communication; synthesizing and adapting the wording intended for the public; and adherence to ethics. When deciding in favour of safety, it is necessary to keep in mind: all the factors and processes that can be dangerous and how often they can occur; how big their

impacts can be; how the size of impacts or the frequency of occurrence can be reduced; whether the proposed measures may be a source of new hazards; and which technical and control systems can control threats that cannot be prevented.

Finally, it should be noted that, in line with the results in [20,22], it is necessary what the political will is to create a system to protect against the unacceptable impacts of harmful phenomena. Research has shown that:

- every design of a technical installation or equipment has certain dangers. The art of designer lies in the fact that he can choose the optimal solution, i.e. a solution sufficiently safe and feasible with regard to the possibilities of the investor and public administration,
- impressive and not very robust structures with insufficient safety margins often fail sooner or later,
- erroneously set limits and conditions for critical parts of a technical installations or equipment lead to frequent failures and even serious accidents; such technical installations are not capable of responding to changes in condition.

An analysis of the available legislation [27] revealed that, according to the applicable rules, it is not required to monitor the safety of processes and the safety of whole installation during the operation at the design phase, which sometimes leads to problems in operation [1]. Another error in the legislation is the fact that it does not require measures to reduce the risks that occur when a sudden time combination of a number of harmful phenomena occurs. According to recent experience, it is necessary to introduce into legislation an obligation to consider higher values of project disasters, at least for critical infrastructure objects.

The procedure for risk management in the operation of a technical installation is described in the work [1] and its effective tools are: risk-based inspections, risk-based maintenance and a risk management plan.

References

[1] PROCHÁZKOVÁ, D., PROCHÁZKA, LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., a L. OUHRABKA. *Management of Risks of Processes Connected with Operation of Technical Installation during Lifecycle.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. doi:10.14311/BK.9788001066751.

[2] 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.

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

[4] 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, 3035p.

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

[6] 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.

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

[8] 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.

[9] 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.

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

[11] 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 (Handbook). London: Taylor & Francis Group 2018, 3234 p.; ISBN: 978-1-351-17466-4 (eBook); https://www.ntnu.edu/esrel2018.

[12] 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 Publis- hing 2019, 4315 p., e:enquiries@rpsonline.com.sg

[13] BARALDI, P., DI MAIO, F., ZIO, E. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (ESREL2020 PSAM15). ISBN 978 -981-14-8593-0. Singapore: ESRA 2021, Research Publishing 2021, 5067 p., enquiries@rpsonline.com.sg

[14] 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

[15] 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 /10 467/78442

[16] ISO. *ISO Strategy2030.* Geneve: ISO 2021, 25 p.

[17] CELLUCCI, T. A. *Developing Operational Requirements.* Washington: Homeland Se- curity 2008, 353 p.

[18] IEC. *Statutes and Rules of Procedure.* Geneve: IEC 2011, 25 p.

[19] PROCHÁZKOVÁ, D. *Grounds of Management of Safety of Critical Infrastructure.* ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.

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

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

[22] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Management of Risks connected of Processes Connected with Their Designing, Manufacturing and Commissioning.* ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p.

[23] ANDERSON, R. *Security Engineering- A Guide to Building Dependable Distributed Systems.* ISBN 978-0-470-068552-6. J. Willey, 2008, 1001p.

[24] ROLAND, H. E., MORIARITY, B. *System Safety Engineering and Management.* ISBN 0-471-6186-0. J. Willey, 1990, 321p.

[25] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2021.

[26] PROCHÁZKOVÁ, D. Risk-based Design of Technical facilities. In: *JUFOS 2021*. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 40-51.

[27] ČVUT. *Database pf Disasters, Accidents and Failures of technical Installations, Their Causes, Lessons Learned and Measures of Response.* Praha: CVUT 2021.