Risk Management Plan for Technical Facility Designing, Manufacturing and Commissioning

PROCHAZKOVA DANA, PROCHAZKA JAN
Department of Energy
Czech Technical University in Prague
Technicka 4, 160 00 Praha 6
CZECH REPUBLIC
prochdana7@seznam.cz, japro2am@seznam.cz, http://www.cvut.cz

Abstract: - Human society needs for security and development such technical facilities that ensure products and services, which are safe, i.e. they fulfil well their functions and do not threaten themselves and their surroundings not under their critical conditions. To ensure the coexistence between technical facility and its surrounding, it is necessary to begin with measures against relevant risk at preparation of terms of references, designing, building, testing and commissioning. The article deals with risk management plan for complex technical facilities during the life cycle stage involving the design, construction, outfit by technology equipment, testing and commissioning. Its aim is to make resilient ground for the co-existence of technical facilities with their surroundings during their existences.

Key-Words: - Risk, technical facility, designing, construction, testing, commissioning, safety, risk management plan.

1 Introduction

The human system is composed of three basic systems: environmental one; social one, which is related to human society; and technological one, which is represented by technical facilities that humans consistently create for their lives quality improvement. These systems are open and mutually interconnected, and therefore, they are interdependent. Some systems´ interactions are beneficial for humans and other ones adverse and highly unacceptable [1,2].

In research, the results of which we describe in paper, we concentrate to technical facilities, which are created by human activities and provide products or services relevant to human life. Important stage of each technical facility life cycle is its designing, construction, outfit by technology equipment, testing and commissioning. The aim of this stage is to make resilient ground for co-existence of technical facilities with their surroundings during their existences. Therefore, it is given strong emphasis on risk management with regard to all possible disasters, and the concept, in which safety is preferred over reliability. It is considered the integral technical facility safety management because due to interconnections among different parts, the set of safe parts is generally not safe; and expected changes of parts with time at given space. The paper aim is to show the proactive tool in which it is prepared solution of both, the possible emergency situations induced by serious risks origination and the possible conflicts at response to emergency situations that can occur [3].

2 Summary of Knowledge on Technical Facilities Designing, Construction and Commissioning

Technical facilities have form of objects or networks, and complex technical facilities represent a system of systems – SoS [2-14]. They include physical, cyber, organizational and social systems, i.e., individual devices, machines, components, systems, or entire production or service units. Knowledge and experience show that technical facilities are put in a certain environment, which in any case react to located technical facility. From safety reasons, these reactions need to be revealed in advance and considered in design to ensure human security.

The followed technical facility stage of life is covered by a wide range of problems, e.g.: theoretical analysis of critical processes, equipment and places and design of practical implementation of technically and financially available countermeasures; selection of: materials, technical principles, construction procedures, determination of critical construction and mounting processes etc., experimental verification of installed fittings and their operability under normal, abnormal and critical

conditions; ensuring: durability, tractability of equipment and processes, required service life; quality and sufficient human resources, costs in the required amount, technical services; services etc.; and realization of buildings, structures and equipment under given conditions, etc. [15].

For human security, it is needed, so environment reactions throughout technical facility lifetime may be adequate and during the technical facility life cycle the coexistence with its surrounding may exist. Ground needs to be inserted in initial technical facility life stage, i.e. at designing, construction, outfit by technology equipment, testing and commissioning. Firstly, it is necessary to consider sources of all risks – All-Hazard-Approach [16]. To this set they also belong destructive phenomena that are results of all mutual reactions inside and outside technical facilities under, normal, abnormal and critical conditions [15].

The identification of internal technical facilities sources of risks associated on the one hand with individual technical equipment, their arrangement into components and systems, and on the other hand with production processes and their management, is a site specific activity which requires the risk identification at several levels, namely: technical equipment; components; systems; technical, organizational and cyber interconnections under normal operating conditions; technical, organizational and cyber interconnections under abnormal operating conditions; technical, organizational and cyber interconnections under critical operating conditions; and for high-important technical facilities such as nuclear power plants, dams, etc., technical, organizational and cyber-operation interconnections under extreme operating conditions [2,17,18].

When identifying the technical facilities risk sources, it is very important to consider all stable and mobile sources inside and outside the technical facility: fires (flash, pool, jet, fireball), explosions (mechanical, electrical, chemical, explosion of a cloud of gases – BLEVE or VCE, dust and, or nuclear), leakage of hazardous substances, because the damage will cause both, their impacts and their possible domino effects [3].

Each dangerous phenomenon can have different sizes and different occurrence probabilities, and therefore, it is important the hazard determination for each one. Because extreme dangerous phenomena occur rarely and irregularly, the hazard determination is one of principal steps at risk determination [3]. The hazard determination is technical-methodological method of determining the maximum expected disasters sizes. Because severe events occur randomly and irregularly and world dynamically develop in space and time (which also leads to changes in conditions that lead to disasters, and, of course, to changes in the very disasters´ characteristics), simple statistical methods cannot be used (their assumptions requiring stable processes are not fully fulfilled). Since we do not have enough knowledge of this area, we must consider existence of uncertainties, both random and knowledge-based, and to use methods based on the theory of extremes, e.g. [19].

According to hazards curves we determine so call the design disaster, which is dangerous phenomenon size, the occurrence probability of which is once during the time interval determined by legislation [3]. The parameters of design disasters are used at technical facility project, construction, outfit by fittings, equipment components, systems and system of systems design. They create the technical facilities terms of references. Their respecting ensures that technical facility has incorporate measures to prevent, mitigate and respond to unacceptable situations caused by internal, external and organizational sources of accidents and failures of elements, components and systems, namely for disasters´ sizes lower than design disasters. They are key part of technical facility design documentation containing the technical, financial, time and other data determining the safe, reliable and functional technical facility. They create so called limits and conditions for safe technical facility operation [15].

According to data in [3,9], it is necessary to have in terms of references creation: knowledge of: regulations; risks in the site to which the technical facility is placed; technical system, which constitutes a technical facility; models and theories associated with accidents; methods of analysis, management and settlement of risks; and management of enterprise (finance, human resources, organization, technology, innovation...); competencies for: the application of results of methods of risk analysis and evaluation; implementation of methodology of analysing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; transformation of policy into real actions; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; capability to find right information and lesson learned; critical analysis; designing the right solutions; communication; carrying out the synthesis and adapting the wording intended for the public; and ethics.

In terms of reference creation, in the light of possible disasters in site and in connection with coexistence of technical facility with surroundings, it is necessary to specify: for each relevant disaster,

size of threat according to given standards; identify critical tasks of technical facility from integral safety viewpoint; understand tasks and causes of their criticality; identified possible human failures; and propose measures for safety ensuring with regard to variable conditions.

Critical technical facility tasks from integral safety viewpoint are physical activities, by which operator contributes to: triggering the non-committed and unacceptable phenomenon; detection and prevention of phenomenon in question; management and mitigation of phenomenon in question; and response to emergency situation. At terms of references creating, it is necessary to consider that to criticality they also contribute: lack of communication (errors and interruptions in the flow of information); routine approach (certainty resulting from long-term practice in combination with risk awareness loss caused by frequent repetitive activities and tired work); lack of knowledge (ambiguity or misunderstanding); distraction (confusion, mental chaos); lack of team collaboration (inconsistent efforts of a group of people due to a lack of belonging, fear of other mistakes, inappropriate leadership style or inappropriate communication); fatigue (it is ignored because people perceive it after it is excessive); lack of means (lack of resources, tools and materials, outdated documentation, inappropriate working conditions); coercion (from superiors or colleagues, lack of time, incorrect task settings); lack of self-esteem (inability to refuse to perform tasks resulting from lack of self-esteem, anxiety or complexes); stress (nervousness caused e.g.: time pressure, new methodology, change in the range of tasks, competitions or private factors); negligence (incorrect assessment of the possible consequences of action caused by e.g.: coercion, lack of experience or lack of knowledge); acceptability of a large number of deviations from instructions and standards in order to facilitate work.

The aim of technical facility project is to create a production process that is profitable, economic, safe and does not threaten public assets, especially humans and environment. This can be achieved by optimizing the safeguard, economic and functional criteria. Technical facility project covers a wide range of problems, e.g. selection of: materials; technical principles; construction procedures; framework procedures; determination of critical construction and framework processes; protection ways in domains physical, cyber etc. It, therefore, requires the participation of many different knowledge fields, i.e. the participation of a number of specialists from different fields. It should be remembered that here the human factor manifests. The low cooperation of experts leads to errors that will occur later at operation, e.g. they lead to: occurrence of organizational accidents [20]; maintenance problems [2,17]; impossibility to repair important parts [21] etc.

In each technical facility project from safety perspective, it is necessary to follow the requirements for: durability; manageability of equipment and processes; lifespan; human resources; costs; technical services; service; safety of employees, humans in surroundings and environment. Consideration and good provision of requirements in question determines the future costs of ensuring the safety and coexistence of technical facility with surrounding area. E.g., non-provision of human resources for operation leads to limitation of production or service that is provided by the technical facility [15].

Designing the technical facilities is a very complex activity, and in each country is regulated by national legislation (e.g. in the Czech Republic - the Act No. 183/2006 Coll.) and in some cases by international ones [22,23]. Research results [15] show: from safety viewpoint, the main goal is to avert unwanted combinations of incidents that have potential to cause accidents accompanied by major damages. To do this, proactive indicators or safety functions are used to control safety under border conditions, thereby reducing the possibility of unlikely severe accident.

Seven principles of resilience are used: backup; to insert ability of sleek and controlled degradation; to insert ability to return from degraded state; flexibility in both, the system and the organization; to insert ability to control limit conditions close to the performance interface; to insert optimal management models; to reduce complexity; and to reduce possible undesirable couplings.

It is necessary to have program for safety increase that ensures: safety and functionality of all fittings that corresponds to their missions; identification, evaluation, elimination or regulation of potential risks at acceptable level for important installations, systems and their various parts; risk management, which includes all possible disasters with resources inside and outside the technical facility that cannot be eliminated; protection of personnel, people in the vicinity, facilities and property; use of new materials or products and test techniques only in a way that is associated only with minimal risk; insertion of safety factors that ensure corrective measures that lead to improvement; consideration of all appropriate historical data on ensuring the safety generated by similar safety-enhancing programs.

From engineering viewpoint, conditions and limits of operation are established, safety systems (active, passive and hybrid) are installed and appropriate backups are ensured; it is solved: what safety systems are appropriate and what must be their backup; where / in which places safety systems operate most effectively; why they must be used just there and not elsewhere, in what limits they work reliably.

It is a fact that, at technical facility designing there are often used software based on tree models. Based on the current knowledge summarized in [3], it should be remembered that tree models do not create a basis for mastering all possible disasters that affect the technical facility, because they start on one point in the technical facility, i.e. they do not consider impacts of external disasters, attacks and human factor.

According to [2,17,22-25], for the technical facility safety during the lifetime, it is necessary at designing to consider at each critical process the problems connected with: given process; designing a process; process management; operational staff and signalling its condition; safety management system; other technical systems promoting the safety; external active and passive systems for mitigating the risks leaded to process failure; technical facility emergency response; technical facility surrounding response.

According to knowledge summarized in [2], it is important so that the processes risk management strategy may use: principles of inherent safety, e.g. [26,27]; and passive safety systems, active safety systems and different barriers types, procedural procedures that are proven or thoroughly tested in such a way that they do not contain latent sources of danger under possible conditions [15].

To ensure the important technical facility safety, the Defence-In-Depth principle is used [28]. The principle in question is implemented using a combination of several subsequent dearly independent levels of protection. The basic condition is - when one level of protection or barrier fails, the subsequent level must be available. When approach is well applied, so individual technical, human or organizational failure should not lead to devastating impacts, and a combination of several failures leading to devastating impacts should have a low occurrence probability. Special attention must be paid to pressure equipment with dangerous substances [15,21].

The technical facility manufacturing means the complete and impeccable implementation of all construction and assembly works and structures, including the supplies of necessary materials and equipment, necessary for facility proper completion, as well as execution of all activities related to supply construction works and structures, the design of which is necessary for proper facility completion (e.g. site equipment, security measures and site safeguard against access of third parties), provision of communication, provision and design of engineering networks, routing network establishment, control measurements during the construction, focus of actual implementation, drawing up the geometric plans of completed construction, transport engineering measures, all revisions, tests, certifications and declarations of conformity related to the subject matter selection procedure, payment of local and administrative fees, provision of further discussions and operations related to the production of the subject of performance, etc.).

The requirements for technical facility commissioning are set out in legislation. The applicant for the commissioning must demonstrate that technical facility was carried out in accordance with all applicable technical norms and standards, acts, follow-up decrees, regulations of manufacturers of individual designed materials or equipment, regulations on the buildings and technical equipment safety. It needs to be demonstrated that all hygiene and fire protection rules as well as OSH (personnel health and safety) requirements have been complied with during implementation. From safety viewpoint, specific safety documentation provided for by the laws cited must be processed.

From a professional viewpoint, safety document shall contain answers to questions: what may break down; what may not work (hazard identification and its analysis); how serious consequences (risk assessment) can be; what measures need to be taken to avoid this (risk management); what needs to be done when this occurs (emergency measures).

3. Coexistence

Coexistence generally means a common existence. In the reference case, it goes on ensuring such conditions in the human system at technical facility designing, construction, outfit by technology equipment, testing and commissioning. The need for and the importance of coexistence is now under consideration in many technical fields [4-14]; the problem was discussed in detail in work [15].

4. Data and Methods Used in Research

For research, the original database of technical facilities accidents and failures from world data was compiled [21] and several case studies were analysed in great details in [15]. The database contains

7829 events from the whole world sources that were accessible in last 35 years to authors; 521 events originated due to mistakes in designing, construction and commissioning (we denote them as stage specific). To reveal the event causes (risk realized), the collected data were processed by risk engineering methods: e.g. What, If; Checklist; Fishbone diagram; Case studies; Event Tree; FMECA; etc. [29]. Their results were critically assessed and separated into classes according similarity of causes and create the basis for Decision Support System enabling to multicriterial assessment of possible technical facility risks [15]. The obtained results on lessons learned from the risk impacts suppressions were also critically assessed and separated into classes according similarity of response tools and create the basis for Risk Management Plan.

The risk management plan is based on the TQM management method [30], i.e. in given entity, they are considered priority risks that could not be get over and which have the potential to significantly damage the technical facility and its surrounding (e.g. beyond design disaster occurrence, human error, intent attack etc.). The plan itself is processed in the form of a table that considers risks from the following areas: technical facility management; internal sources of risks in technical facility related to its design, construction, outfit by equipment and commissioning; technical staff; external sources of risks linked to natural disasters; external sources of risks related to the supervision of public administration, competition, market, etc.; terrorist attacks; cyber sources of network-related risks; war.

For each risk area, the table shall state: causes of risk; occurrence risk probability and expected risk impact size on protected assets (based on the legislation requirements basic public assets should also be considered); and measures to get over or at least mitigate the risk impacts that are clearly identified and at each one responsible person for its implementation is given. The risk management plan is also recommended by ISO [31].

5. Causes of Technical Facilities Accidents and Failures and Lessons Learned from Responses to Them

The causes of stage specific technical facilities failures and accidents in database [21] were split up into categories: matter of facts issues connected with technical facilities at designing, building, outfit by technology equipment, testing and commissioning; public administration supervision; legislation deficit; and other. These categories were further subdivided; e.g.: the first one was designated into: errors in terms of references (e.g. omitting the critical disaster); errors in design (e.g. mistakes in concept of barriers; omitting of important norms and standards etc.); or legislation deficits into: low authority of public administration supervision; very general requirements on design, construction, outfit by technology equipment, testing and commissioning, etc.

The specific identified causes of technical facilities failures and accidents found in a process involving design, construction and commissioning are omissions, errors and deficiencies in:

1. Technical facility design - factual area:
   - errors in terms of references (e.g. not used the All Hazard Approach procedure; incorrectly determined hazard sizes of disasters; not applied Defence-In-Depth principle etc. – further ones in [15],
   - errors in the project (an inappropriate building model used for calculations with regard to the conditions in the site, either too theoretical or general or not to settle uncertainty and uncertainty; not properly used principle Defence-In-Depth principle),
   - omitting the site vulnerabilities as e.g. large populations, existence of objects such as hospitals, schools, etc.,
   - insufficient capacity sources of energy, water and sewerage,
   - insufficient capacity of transport routes, lack of staff to operate, etc.,
   - the non-determination of critical building sites, which led to omission of measures for risk management towards safety at normal operation – as barriers, on the basis of an assessment of the risks to their safety, i.e. barriers, backups – further ones in [15],
   - the non-determination of critical building sites, which lead to omission of measures for risk management towards safety at abnormal operation conditions, – on the basis of an assessment of the risks to their safety, i.e. the risk assessment of their safety, i.e. barriers, backups – further ones in [15],
   - the non-determination of critical points of technology and production processes, which led to omission of measures for risks management to safety, protection and dependability under abnormal and critical conditions - barriers, advances, principles to increase safety,
   - they have not been considered and adequately addressed critical points of technology (pressure vessels and their equipment in which

dangerous substances are or carry out hazardous reactions or pressured pipes, mainly those with hazardous substances) and places in which there is a risk of operator failure from the point of view of potential risks,
- failure to comply with good practice standards or the application of erroneous standards (which has led to the project being designed: inappropriate materials; inappropriate technical principles; inappropriate construction procedures; inappropriate design procedures; critical construction and construction processes have not been established and specific measures have been proposed for their quality design; equipment, machines, components and systems did not meet the safety, reliability and long-term functionality requirements, i.e. the safety, reliability and long-term functionality of the equipment, machinery, components and systems. durability and easy handling of equipment and processes; ergonomic requirements of the operator, service requirements, maintenance and financial costs associated with them are not respected; inappropriate placement of protective equipment and safety support systems; inappropriate technologies of construction, construction and assembly),
- in creation of design of automatic and semi-automatic control systems, there were deficiencies caused by insufficient knowledge or lack of cooperation of specialists from different disciplines or the use of faulty or imperfect IT tools,
- non-incorporation of technical measures for the basic physical and cyber protection of technical facility,
- not considering the possibilities of changes in: laws during construction; system of taxation during the construction; interest system during construction; market situation – inflation, deflation, demand changes, etc.; support for technical facility by the State (e.g. when changing political representation); supplies of essential materials and technologies and relied on only one supplier, leading to problems in construction and operation – e.g. due to the lack of finance or unavailability of the material, some buildings and equipment were then ripped off.

2. Technical facility manufacturing and construction - factual area:
   - construction started without sufficient preparation,
   - failure to comply with standards and approaches of good practice, which caused the choice of faulty construction technology (inappropriate material, inappropriate schedule of work, which led to frequent work breaks, lengthening the construction and increasing financial costs,
   - chaos in the workplace,
   - poor execution of construction works in critical buildings caused by lack of resources such as: lack of tools and materials; obsolete documentation or inappropriate working conditions.
3. Outfit and assembly of technical facility - factual area:
   - assembly started without sufficient preparation (e.g. the distribution of cable heads on the wall was not intended),
   - failure to comply with standards and approaches of good practice (which allowed faulty or defective procedures to be caused by: faulty designs of pressure vessels, valves and connections; poor design of tight connection screws; faulty welds),
   - false work schedule of works, which led to frequent breaks, the extension of outfit and assembly, financial costs increase and workplace chaos.
4. Testing of buildings and technology - factual area:
   - not to draw up an accurate works schedule,
   - not to drawn up scale to criticality assessment of critical equipment,
   - not specifying the precise conditions for starting and switching off the critical equipment, such as pressure equipment, safety support systems, safety systems, etc.,
   - poorly performed tests of critical machines, equipment, components and systems, e.g. omissions of leak tests for pressure equipment or pipe systems pressurized by hazardous substances,
   - use of erroneous or inappropriate methods for tests necessary for reliability and safety verification (e.g. selection of incorrect methods for non-destructive testing; failure to comply with standards and approaches of good practice (lack of knowledge, omissions, human failure),
   - the use of faulty or imperfect IT tools in verifying test results (e.g. tree models that do not have the ability to assess the size of specific risks, e.g. failure of the technological process due to simultaneous multiple failures several

critical components e.g. as a result of external disasters).

5. Trial operation of technical facility - factual area:
   - the use of erroneous procedures,
   - not to draw up accurate work schedule (chaos, haste),
   - failure to comply with standards and approaches of good practice (lack of knowledge, hastiness), i.e. poorly performed test operation of machinery, equipment, components and systems,
   - missing the safety certificates, i.e. it was not verified that measures of all critical equipment for expected failures management are functional and effective sufficiently.
6. Start-up (commissioning) - factual area:
   - failure to comply with standards and approaches of good practice (lack of knowledge, hastiness),
   - not to draw up accurate work schedule (chaos, haste).
7. Supervision of public administration over technical facility design and production - organizational area:
   - lack of public administration supervision, e.g. it did not ask for documentation on certification of technical facility safety in all important six stages of the technical facility referred to above,
   - neglecting the solution of sufficient capacity of local sources of energy, water and sewerage, transport routes and personnel in technical facility sitting and design,
   - permission of significant environmental contamination and long-term disruption of local residents´ lives during the construction,
   - neglecting the assessment of investor financial capacity in granting the relevant authorizations.
8. Supervision of contractor and investor over design and production - organizational area:
   - lack of supervision, i.e. failure to draw up safety documentation proof in all important six stages followed above,
   - underestimating the safety management,
   - underestimating the economic factors (finances),
   - underestimating the environmental factors,
   - underestimation of social factors (the needs of the local population).
9. Inadequate legislation:
   - insufficient public administration supervisory power,
   - insufficient legislation governing the design, construction and commissioning requirements of technical facilities (too general, incomplete, allows for several interpretations,
   - insufficient enforceability of the right to safety, employee protection, public protection and the environment.
10. Other:
   - the State has not professional institution which has been able to professionally assess the process of making the technical facility in all aspects,
   - haste in design and construction due to pressure from politicians,
   - the State has not developed a system of supervision under design and construction of technical facilities,
   - the State did not have criteria for assessing the accuracy of the design and production of technical facilities,
   - contractor and investor did not cooperate with the public administration during the design and production of the technical facility,
   - natural disaster occurrence as: earthquake; landslide; flood; fire,
   - occurrence of phenomena as: corruption; insider´ attack; hackers´ attack; terrorist attack.

6. Risk Management Plan

For creating this top-quality safety management tool, they are considered both, the current knowledge and experience on risks associated with technical facilities and their surroundings summarized in [15], and the new real knowledge, which were obtained from study of compiled original database of technical facilities failures and accidents, among the causes of which they were found defects in the area of design, building, construction, testing and commissioning; totally 521 cases were identified.

The aim of risk management plan is to ensure the technical facility coexistence with surroundings. Two actors are considered - public administration, which supervises activities in the territory with aim to ensure the safety of territory and citizens, and maker (contractor), who is responsible for the safety of the manufactured technical facility, which also includes the protection of the surroundings and inhabitants. It is prepared in the form of table as it is given in chapter 4; Table1 shows example for designing and Table 2 shows example for construction, mounting, testing a commissioning; complete tables are in [15].

Table 1. Risk management plan for technical facility designing directed to coexistence of operated technical facility with its surrounding.

Risk area	**Risk description**	**Probability of occurrence Risk impacts size**	**Risk mitigation measures**
Public administration	As a result of absence of a State strategy on technical facilities design focused on safety, it is possible to enforce current political interests, requirements of coercive groups or the failure to cope with extreme political situations (war, terrorist attacks), which in turn leads to reduction in human living standard and safety of citizens, economic instability, etc.	Probability: Large Impacts: Large	***Measures:*** To develop the relevant State strategy and adapt the Building Act ***Execute:*** Prime minister ***Responsibility:*** Parliament chairman
	Due to lack of competence of public authority in overseeing the technical facilities design there is an extension of construction, problems in commissioning, accidents accompanied by enormous expenditure from the public budget, disruption of citizens security.	Probability: Large Impacts: Large	***Measures:*** To adapt the Competence Act and the laws associated with it. ***Execute:*** Prime Minister ***Responsibility:*** Parliament chairman
	……..		
	As a result of errors in the authorized designer selection, the project is of poor quality, which sooner or later will disrupt the construction or operation and lead to accidents accompanied by enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	*Measures:* Change of designer *Execute:* Authorized investor worker *Responsibility:* Investor director
Future operator	…….		
	As a result of a poor estimate in the field of supplier – customer relations, the project is based on unrealistic data, which sooner or later will lead to disrupts the construction or operation of a technical facility, enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	*Measures:* To force investor to perform remedy *Execute:* Authorized future operator worker *Responsibility:* Future operator director
Authorized designer	…….		
	As a result of a poor quality or non-cooperative team of project processors, the project is of poor quality and it leads sooner or later to disruption of construction or operation, enormous expenditure, citizens safety and problems with public administration. …….	Probability: Medium Impacts: Large	***Measures:*** To introduce rules for team cooperation ***Execute:*** Authorized designer team worker ***Responsibility:*** Authorized designer team director

Table 2. Risk management plan for technical facility construction, mounting and commissioning directed to coexistence of operated technical facility with its surrounding.

Risk area	Risk description	Probability of occurrence / Risk impacts size	Risk mitigation measures
Public administration	As a result of poor-quality technical education aimed at quality production and commissioning of technical facilities (it does not consider existence of possible risks), it is construction prolonging, problems in commissioning or origin of accidents, which is accompanied by enormous expenditure from the public budget, the disruption of citizens safety and the State stability, which leads to a reduction in living standards, economic instability, etc.	Probability: Large Impacts: Large	***Measures:*** Correction of acts on education ***Execute:*** Minister for education ***Responsibility:*** Prime Minister
	……..		
Investor	As a result of errors in authorized builder selection, the technical facility is of poor quality, which sooner or later will disrupt the operation, lead to accidents accompanied by enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	*Measures:* Change of builder *Execute:* Authorized investor worker *Responsibility:* Investor director
	As a result of not considering cross-cutting risks (associated with equipment, IT and man-machine connections) in building, testing and commissioning, the operation will be disrupted sooner or later and will lead to accidents accompanied by enormous expenditure, disruption citizens' safety and problems with public	Probability: Large Impacts: Large	***Measures:*** To ensure so builder makes remedy ***Execute:*** Authorized investor worker ***Responsibility:*** Investor director
	……..		
· :	……		

Both risk management plans were tested with success at six medium enterprises [21]; their site-specific compilation and application in practice are ambitious on experts´ knowledge and time, and it requires the access to detail enterprise and public administration documents, which is connected with respecting the certain legal rules. Table 1 serves for protection against problems that impede to building permit issue. Table 2 serves for protection against problems that impede to operation permit issue. Both tables show that big role plays the human factor, namely at way of execution of critical tasks of designing (terms of references compilation, use of knowledge on compilation of safe design etc.) and at professionality of supervision performed by the public administration directed to public interest.

7. Conclusion

The quality of project and construction of technical facility predetermines its safety throughout the life-time. Examples from practice show that some errors, such as underestimation of foundation conditions or some errors in terms of references, cannot be removed after the construction completion and commissioning. They pose a danger under certain conditions (e.g. at flood or earthquake) and can only be mitigated by organizational measures that entail additional costs and do not have the ability to ensure safety level as correct measures at design stage.

The above-summarized knowledge and results of study of technical facilities accidents and failures show that basis for ensuring the facilities safety at required life cycle is knowledge of: regulations; risks in the site to which the technical facility is placed; technical system, which constitutes a technical facility; models and theories associated with accidents; methods of analysis, management and settlement of risks; way of management that operator might use after commissioning (finance, human resources, organization, technology, innovation...).

Furthermore, it is necessary for all those involved to respect the public interest, to participate in building the safety culture and for managers to motivate employees to do quality work, even by their own example, as shown by the so-called "golden rules of safety" [25].

An analysis of environmental development as well as development of political, social and economic situation in the world shows the need to be prepared for the resolution of cases and actions that will cause critical situations with impacts intensities higher than these today. In order to manage realization of risks which are inherent in present world using the adequate forces, resources and means, it should be had: principles for managing the emergencies and critical situations, especially those of a large range; allocation of resources; and allocation of responsibilities. The risk management plan is tool that gives overview on measures, the person who execute them and the responsible person.

Acknowledgement
Authors thank for the EU grant; project RIRIZIBE-CZ.02.2.69/0.0/0.0/16-018/0002649.

References:

[1] BOSSEL, H., *System, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme. Books on Demand.* Norderstedt/Germany, 2004, www.libri.de

[2] PROCHAZKOVA, D., *Principles of Management of Risks of Complex Technological Facilities*. Praha: CVUT 2017, 364p., http://hdl.handle. net/10467/72582

[3] PROCHAZKOVA, D., *Analysis and Coping with Risks Connected with Technical Facilities*. Praha: CVUT 2018, 222p. http://hdl. handle.net/10467/78442

[4] ALE, B., I. PAPAZOGLOU and E. ZIO, *Reliability, Risk and Safety.* London: Taylor & Francis Group 2010, 2448p.

[5] BEER, M. and E. ZIO, *Proceedings of the 29th European Safety and Reliability Conference.* Singapore: ESRA 2019, e:enquiries@ rpsonline. com.sg

[6] BÉRENGUER, C., A. GRALL and C. GUEDES SOARES, *Advances in Safety, Reliability and Risk Management*. London: Taylor & Francis Group 2011, 3035p.

[7] BRIŠ, R., C. GUEDES SOARES and S. MARTORELL, *Reliability, Risk and Safety. Theory and Applications.* London: CRC Press 2009, 2362p.

[8] CEPIN, M. and R. BRIS, *Safety and Reliability – Theory and Applications.* London: Taylor & Francis Group 2017, 3627p.

[9] HAUGEN, S., J. VINNEM, A. BARROS, T. KONGSVIK and A. VAN GULIJK, *Safe Societies in a Changing World.* London: Taylor & Francis Group 2018, 3234p.; https://www.ntnu. edu/esrel2018.

[10] IAPSAM, *Probabilistic Safety Assessment and Management Conference.* Helsinki: IPSAM & ESRA 2012, 6889p.

[11] NOWAKOWSKI, T., M. MLYŇCZAK, A. JODEJKO-PIETRUCZUK and S. WERBIŃSKA -WOJCIECHOWSKA, Safety *and Reliability: Methodology and Application*. London: Taylor & Francis Group 2014, 2453p.

[12] PODOFILLINI, L., B. SUDRET, B. STOJADINOVIC, E. ZIO and W. KRÖGER, S*afety and Reliability of Complex Engineered systems: ESREL 2015.* London: CRC press 2015, 4560p.

[13] STEENBERGEN, R., P. VAN GELDER, S. MIRAGLIA and A. TON VROUWENVELDER, *Safety Reliability and Risk Analysis: Beyond the Horizon*. London: Taylor & Francis Group 2013, 3387p.

[14] WALLS, L., M. REVIE and T. BEDFORD, *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. London: CRC Press 2016, 2942p.

[15] PROCHAZKOVA, D., J. PROCHAZKA, J. LUKAVSKY, V. BERAN and V. SINDLEROVA, Management of Risks of Processes Connected with Manufacturing and Commissioning Technical Facility. Praha: ČVUT 2019, 207p. http://hdl.handle.net/ 10467/84466

[16] FEMA, *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA 1996.

[17] PROCHAZKOVA, D., *Safety of Complex Technological Facilities.* Saarbruecken Lambert Academic Publishing 2015, 232p.

[18] RAUSAND, M., *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons 2014.

[19] EPSTEIN, W., Not Losing to the Rain: What I Learned when I Learned about Onagawa. In: *Safety and Reliability of Complex Systems*. London: Taylor &Francis Group 2015, pp. 365-371.

[20] REASON, J., *Human Error*. Cambridge: University Press 1990.

[21] CVUT, *Database on World Disasters, Technical Entities Accidents and Failures – Causes,*

Impacts and Lessons Learned. Praha: CVUT 2020.

[22] EU, *Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities*. Brussels: EU 1982.

[23] IAEA, *Safety Guides and Technical Documents*. Vienna: IAEA 1954–2020. www.ns.iaea.org/ standards

[24] COMAH, *Safety Report Assessment Manual: COMAH*. London: UK – HID CD2 London 2002, 570 p.

[25] OECD, *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191p.

[26] HEIKKILÄ, A., M. *Inherent Safety in Process Plant Design. An Index-Based Approach*. Helsinki: VIT 1999, 132 p.

[27] KLETZ, T., *Process Plants: A Handbook for Inherently Safer Design* CRC. London: Taylor &Francis Group 1998.

[28] INSAG, Defence in Depth in Nuclear Safety. *INSAG-10*. Vienna: IAEA 1996.

[29] PROCHAZKOVA, D., *Methods, Tools and Techniques for Risk Engineering*. Praha: CVUT 2011, 369p.

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

[31] ISO, *Risk Management – Principles and Guidelines.* ISO 31000:2009.