RISK MANAGEMENT AT TECHNICAL FACILITIES DESIGNING, BUILDING AND COMMISSIONING

Dana Prochazkova, Jan Prochazka

PRAHA 2020

Reviewers:

Prof. Ing. Tomáš Čechák, CSc.

Doc. Ing. Jaromír Novák, CSc.

Doc. RNDr. Dana Procházková, DrSc., RNDr. Jan Procházka, Ph.D.

ISBN 978-80-01-06716-1

CONTENT

LIST OF ABBREVIATIONS

Abbreviation	Title
BLEVE	Boiling Liquid Expanding Vapour Explosion
CBA	Cost Benefit Analysis
ČVUT	Czech Technical University
DSS	Decision Support System
ESRA	European Safety and Reliability Association
ESREL	European Safety and Reliability Conference
EU	European Union
FEMA	Federal Emergency Management Agency
GIS	Geographical Information System
IAEA	International Atomic Energy Agency
I & C	Information and Control System
ISO	International Organization for Standardization
IT	Information Technologies
OECD	Organisation for Economic Co-operation and Development
SMS	Safety Management System
SoS	System of Systems
TQM	Total Quality Management
UN	United Nations
VCE	Vapour Cloud Explosion

ABSTRACT

The publication subject is to show the risk management of complex technical facilities at a stage involving the design, construction, outfit by technology equipment, testing and commissioning. In harmony with the present knowledge, it is respected the "Sendai Framework", in which there is a strong emphasis on risk management from all possible disasters connected with technical facilities and their surroundings. Technical facilities belong to the administration of the various sectors and include physical, cyber, organizational and social systems, i.e. individual devices, machines, components, systems, or the entire production or the service units. Their character is socio-cyber-technical (physical). Large technical facilities represent the systems of systems, i.e. a number of open and mutually interconnected systems. From this reason, their behaviour is dynamic and depends on a number of factors. The problems´ solution way is based on the simultaneously preferred concept, in which the safety is preferred over the reliability.

The safety of a technical facility is related to the entire technical facility because, as a result of the interconnections among different parts, the set of the safe parts is generally not safe. The safety also considers the dynamic evolution of the world. Therefore, it is going on managing the risks caused by all possible causes in time and space. Management of technical facility safety is not easy and requires the application of specific engineering tools for coping with the expected risks. Due to complex architecture of majority of present technical facilities, their behaviours are sometimes unforeseeable, and therefore, the special engineering tools need to be used at their designing, manufacturing and commissioning.

For creating the top-quality safety management tools, they are firstly summarised the current knowledge and experience and they are given proven tools by which it is possible to identify, analyse, manage and control the risks associated with technical facilities and their surroundings. Based on the original database of failures and accidents of technical facilities, which also included weaknesses in the area of design, building, construction, testing and commissioning, they are determined the basic categories of risk causes. Through the procedures of advanced risk disciplines, there are developed the tools for working with risks in the monitored stage of the technical facility aimed at ensuring the technical facility safety throughout its life time, namely: decision support system; and risk management plan. Both tools are in two versions. The first one is connected with the process, the result of which is building permit. The other one is connected with whole process including designing, manufacturing and testing, the result of which is operation permit. Tools are determined for both, the investor (manufacturer), who is responsible for the safety of the manufactured technical facility, which also includes the protection of the surroundings and inhabitants, and the public administration, which supervises activities in the territory with aim to ensure the safety of territory and citizens. To increase the book validity, three attachments are added; the first one explains the integral safety; the second one describes the risk sources for technical facilities; and the third one shows advanced hazard assessment procedure.

The book shortly summarizes results of specific research performed in project "***Řízení rizik a bezpečnost složitých technologických objektů (RIRIZIBE)" CZ.02.2.69/0.0/0.0/16_018/000***". The detail results are in original Czech monograph, which is cited.

1. INTRODUCTION

In research, the results of which we will hereafter describe, we concentrated to technical facilities, which have been created by human activities and have been provided 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 grounds for co-existence of technical facilities with their surroundings during their operations.

From human society security and development, they are necessary such technical facilities that ensure products and services and are safe, i.e. they fulfil well their functions and do not threaten themselves and their surroundings, namely 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. To consider all possible risk sources, the decision support system is created on the basis of present knowledge and known risk sources.

Due to world dynamic development, each technical facility needs to be during the life cycle also prepared for possible non-demanded situations. In face of it, the risk management plan for complex technical facilities during the life cycle stage involving the design, construction, outfit by technology equipment, testing and commissioning is prepared.

The publication deals with the risk management of complex technical facilities in a phase that includes designing, construction, outfit by technology equipment, testing and commissioning. In line with the knowledge, the currently acknowledged “Sendai Framework” is respected, with a strong emphasis on risk management from all possible disasters. It is about ensuring the safe technical facilities, which also ensures the coexistence of the technical facilities with the surrounding throughout their lifetimes. The way of solving the problem [1] is based on the currently preferred concept in which safety is superior to reliability.

With regard to publication extent, all technical, legal, organizational, personnel and financial issues are not subject to a thorough analysis; details are in [2] and in its citations. This publication aim is to show verified tools for risk management in the followed technical facility stage. The technical facility is considered as a part of territory in which it is inserted, and the model of which is the human system. This 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 [3,4].

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 are not synergic due to development. The aim is to show the proactive tools, which ensure the sufficient level of technical facility prevention and are prepared for solution of both, the possible emergency situations induced by serious risks origination and the possible conflicts at response to

emergency situations that can occur [5]. Figure 1 shows the basic idea of problem understanding, the target of which is the human security and development during whole life cycle, and especially at designing, manufacturing and commissioning.

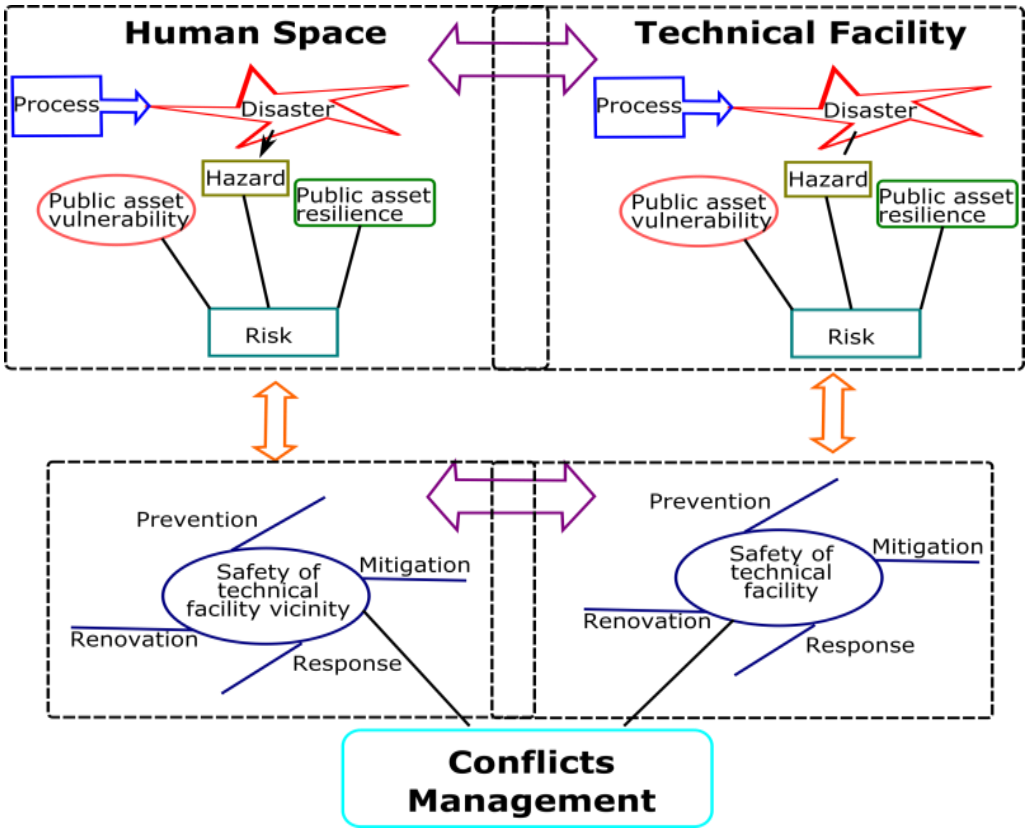

Figure 1. Idea of risk management that needs to be considered during the technical facility designing, manufacturing and the commissioning.

As it was given above, this publication focuses on the early stages of the technical facility life cycle, namely: project; fabrication; tests; trial operation; and commissioning. It should be noted that the process in question [4,6,7] is significantly affected by:

- knowledge and experience of designers, investors and contractors (manufacturers),
- the characteristics of the territory in which the technical facility is located,
- the financial capacity of the technical facility investor,
- the level of public administration supervision under the technical facility safety in sense of public interest during this phase.

In next chapters, we show:

- the current situation in knowledge and experiences in the followed domain, i.e. at the stage involving the technical facility design, construction and commissioning,

- the causes of the risks that led to the failure of the technical facility due to design or construction errors, namely immediately during the manufacturing or later at operation,
- the appropriate tools from the toolbox used by disciplines that work with risks that ensure the quality work with the risks associated with the design, construction and start of operation of the technical facility.

As information technology is now increasingly affecting the humans´ lives, the risks involved need also to be considered. Therefore, the problems presented are followed in the book and references are provided for detailed understanding and deeper study.

As mentioned above, the present work focuses on the design, construction and commissioning of a technical facility. Therefore, attention is focused on the dominant risks in this phase of the life cycle of a technical facility. In the light of current knowledge [4,5,7,8], it holds that the particulars given hereafter do not:

- deconstruct existing norms and standards because the authors have both, the knowledge and the experience of practice, from which it implies that without standards and legislation, the professionals and the professional community would be doomed to repeat mistakes from the past,
- debar to use in designing models and software that facilitate and speed up work. However, on the basis of the experience and practical experiences summarized in [5,9], it is apparent that by their application they can be neglected some uncertainties, i.e. knowledge uncertainties due to the fact that the real conditions are replaced by idealized conditions that do not respect the inhomogeneities of the environment and material, anisotropy of environment and material, and temporal changes of environment and material. Therefore, where important facilities or their important elements are concerned, the results of models and simulations need to be complemented by expert studies, so the result technical facility may be provided by sufficient safety margin.

With the proposed risk management procedures, the authors demonstrate their conviction that without proper safety-related risk management we do not have the capability to sustainably respond to unexpected events, i.e. we will not be prepared for the future because real conditions are not normative and change over time, which is in accordance with current knowledge.

The monograph is the summary of results of research project „Řízení rizik a bezpečnost složitých technologických objektů (Management of risks and safety of complex technological facilities - RIRIZIBE)“ CZ.02.2.69/0.0/0.0/16 _018/000. It summarizes the most important present facts. Detail data and lists of all used references are in book [2] and in given cited sources. It is necessary to give that some new facts followed from research are more stressed than in [2] due to lessons learned from discussions with specialists to this book. The terms used are explain in [1,5].

For recommendations and comments authors thank to reviewers Prof. Ing. Tomáš Čechák, PhD. and Assoc. Prof. Jaromír Novák, PhD. For working condition creating, the authors thank to the Czech Technical University in Prague, the Faculty of Mechanical Engineering, namely to the Energy Department.

2. FINDINGS ON TECHNICAL FACILITIES PLANNING, DESIGNING, BUILDING AND COMMISSIONING

Technical facilities are created by objects or networks, and complex technical facilities are represented by a model called “system of systems – SoS” [1,2,4,10-20]. They include physical, cyber, organizational and social systems (i.e. they are socio-cyber-technical SoS), i.e., individual devices, machines, components, systems, or entire production or service units, organizational systems, personnel.

Knowledge and experience show that technical facilities are put in a certain environment, which in any case reacts to located technical facility, namely immediately or later. From safety and coexistence reasons, these reactions need to be revealed in advance and considered in design to ensure human security and technical facility safety.

2.1. Technical facility design concept

Each technical facility is located in an area in which there are many sources of risk, the manifestation of which may damage both, the technical facility and its surroundings. In strategic management, the risk is a measure of losses, damages and injuries [1,5]. The size of the risk depends on the real disaster that is the source of the risk and on the vulnerability of the site-specific assets under review, namely both, the public ones and the technical facility ones [1,5,8].

The strategic management [1,5,21] defines to basic quantities:

- the hazard, which is defined as normative quantity expressing the probable size of a disaster occurring once in a given time interval (a so-called project or design disaster) [1,5,7,8],
- the risk, which is defined as the probable size of losses, damages and harms to the assets under review at a design disaster, calculated per unit of time (typically 1 year) and unit of territory [1,5,7,8].

The public interest is the security and development of humans, and for its fulfilment, both, the safe environment and the safe technical facilities located there, are important. From this reason, the safety is understood to be a system-level characteristic that humans form through their actions and activities [1,5-8,21,22]; safe system is a system that, under its critical conditions, does not endanger itself or its surroundings. The safety of the territory and its subparts in the above-described context is specifically monitored in the work [21]. The safety of the technical facilities is monitored in the works [4,7,23,24].

It is true that the risk and safety variables are not complementary variables, because the safety of both, the territory and each technical facility can be also increased by organizational measures, e.g. by introduction of warning systems and backup solutions without reducing the size of the risk; An additional term to safety is the criticality [1,5,7,8].

Current knowledge shows that the world in which humans live (the human system) needs to be in such condition that the interconnected systems as the environment, the social system and the technological system coexist.

Coexistence generally means common existence and its concept is followed for example in the work [25]. It is about ensuring such conditions in the human system in the design and construction of a technical facility that ensures the coexistence of interconnected systems, i.e. social, environmental and technological [26]. The need and importance of coexistence is today considered in many technical fields; e.g. telecommunications work [27-33]. The works in question show that technical facilities cannot be designed as closed systems, but their surroundings needs always to be considered, which confirms the requirements gathered in the works [4,7,24,34].

The safety of each technical facility is determined by many factors. At the design stage, it is a question of setting the right terms of references (tender conditions), which need to respect the characteristics of the territory in which the technical facility is inserted. Furthermore, they are important measures inserted into the project to facilitate the technical facility safety management at operation. Since the late 1970s, we have been talking about introducing the principles of inherent safety [7]; the inherent safety will be characterized later. The principles in question need to be followed at designing the buildings, construction and installation of buildings, networks and equipment.

In line with current knowledge, the “Sendai Framework” [35] is respected in developing tools for practice, with a strong emphasis on risk management from all possible disasters. From the public interest viewpoint, the variants of project and the construction of a technical facility that have a risk lower than a specified level of risk can be accepted. However, each selected variant needs to be a subject to regular monitoring of the level of risk in the light of the dynamic development of the world during the manufacturing and operation [4,7,21].

When deciding whether or not to issue a building permit to manufacture a technical facility, the other options need either to be excluded or their parameters adjusted and, if necessary, measures should be taken to mitigate the worst impacts on public protected assets in the case of a risk realization [4,7,8]. According to the data in works [2,5,7,8], in the design and implementation of the optimal variant of the technical facility in the real case, the role plays:

- the achieved level of safety of the technical facility and its surroundings,
- the technical feasibility of measures to ensure a safe technical facility, considering the suitability of the measures for the given system, i.e. the technical facility and its surroundings,
- material demandingness and energy demandingness of the technical facility,
- speed of implementation of the technical facility,
- claims of operation of the technical facility on qualified personnel,
- technical facility demands on transport and information provisions, i.e. communication networks,
- claims of the technical facility for finance during the construction and operation,
- claims of a technical facility for safety responsibility,
- management / organization requirements in the territory associated with the technical facility.

The first important aspect associated with the design of a technical facility is the choice of the concept of itself technical facility and its economic framework. According to current knowledge, there are today used two concepts, namely: reliability management; and safety management.

Safety and reliability are important features of technical facilities. Both are associated with risk and use the same risk management methods and procedures [4,5]. Their interrelationship has changed as a result of major-accident analyses of technical facilities performed in the late 1970s and early 1980s [4,6,7,36-38]. The consistent application of systems theory and the introduction of the concept of integral safety in 1994 [39] also contributed significantly to this; a more detailed interpretation is given in Annex 1.

It is true that level of safety and level of reliability depend on the work with risks [4]. The aims of work with risks in mentioned concepts are different, and therefore, their results of work with risks are not the same. It should be borne in mind that there are currently three distinct concepts that work with risks:

- reliability management and engineering, where risk management for technical facility is aimed at reliability, e.g. [40],
- security management and engineering, where the risk management of technical facility is targeted to a secured technical facility, e.g. [41],
- safety management and engineering where risk management is aimed at safe technical facility, e.g. [42].

All three concepts use the same procedures, methods, tools and techniques. Practice shows that there are sometimes conflicts between them. In accordance with the “Sendai Framework” [35], the solution below focuses on the overall (integral) safety of the technical facility; and it can be only ensured by safety management and engineering [4,6,7].

2.2. Risk sources for technical facilities

For human security and development, it is needed, so surroundings 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 according to generally accepted concept “All-Hazard-Approach” defined in [43] and derived for Europe in work [44]; details are in Annex 2. To this set they belong destructive phenomena that are results of all mutual reactions inside and outside technical facilities under, normal, abnormal and critical conditions and manifestations of human factors [2,4,7].

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 [2,4,7,45,46], namely:

- technical conditions of equipment, components and systems,

- behaviour of technical, organizational and cyber interconnections under normal operating conditions,
- behaviour of technical, organizational and cyber interconnections under abnormal operating conditions,
- behaviour of technical, organizational and cyber interconnections under critical operating conditions,
- and for high-important technical facilities such as nuclear power plants, dams, etc., behaviour of technical, organizational and cyber-operation interconnections under extreme operating conditions.

When identifying the technical facilities risk sources, it is very important to consider all stable and mobile sources of risk inside and outside the technical facility [2,4,5,7] as:

- 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.

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 [5]; details are in Annex 3.

To reveal all internal sources of technical facility, the followed technical facility time cycle needs to follow a wide range of problems in which the risk sources are contained [2], e.g.:

- theoretical analysis of critical processes, equipment and their locations, and to design the 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: the durability, tractability of equipment and processes, required service life,
- quality and sufficient human resources, costs in the required amount, technical services,
- necessary services,
- and realization of buildings, structures and equipment under given conditions, etc.

2.3. Hazard determination

As it was given above, the hazard is the probable size of a disaster occurring once in a given time interval (a so-called project or design disaster) [1,5,7,8]. The hazard

determination is technical-methodological method of determining the maximum expected disaster´ size. 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 could not be used (their assumptions requiring stable processes are not fully fulfilled). Since we do not have enough knowledge of this area, we need to consider existence of uncertainties, both random and knowledge-based, and to use methods based on the theory of extremes, e.g. [5,8,47]. The verified procedure for hazard determination is shown in Annex 3.

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 [5].

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 base for technical facilities terms of references.

2.4. Terms of references

Technical facilities terms of references are key part of technical facility´ design documentation. They contain the technical, financial, time and other data determining the safe, reliable and functional technical facility. 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. The terms of references of the technical facility specifying it and they are a document that reflects the risk management process shown in Figure 2.

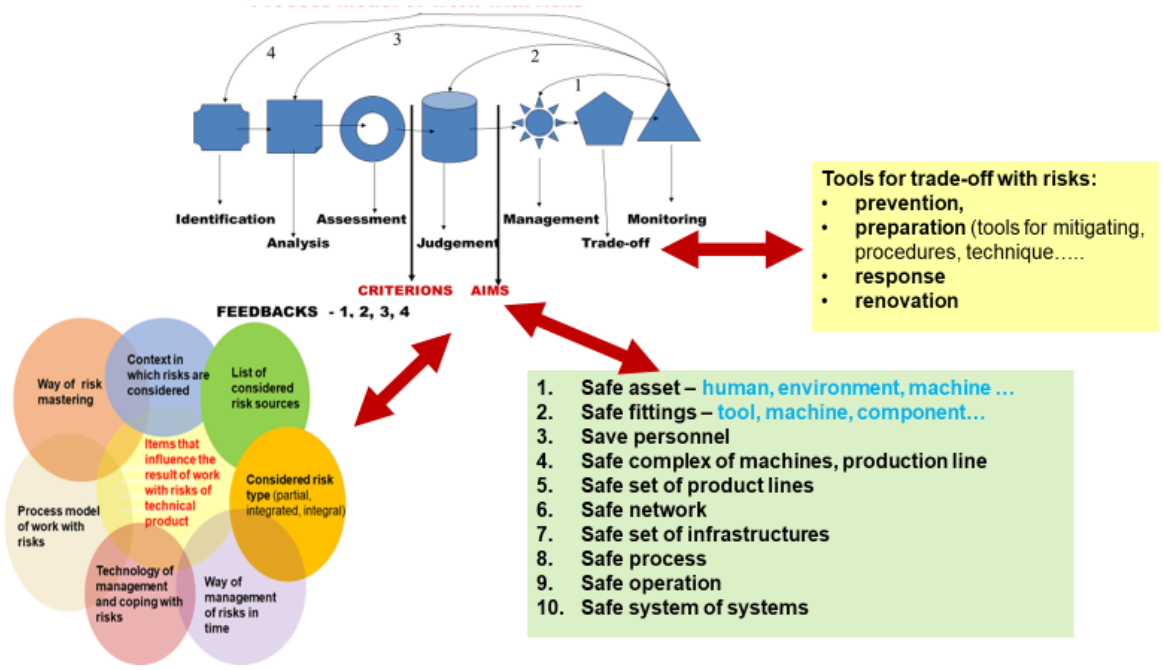

Figure 2. Process model for risk management - 1,2,3,4 = feedbacks used when monitoring indicates that the specified safety requirements are not met [1,2,5].

According to data in [5,15], it is necessary to have in terms of references creation:

1. Knowledge of:
    - regulations, norms and standards,
    - risks in the site to which the technical facility is placed,
    - technical system, which constitutes a technical facility,
    - models and theories associated with expected accidents,
    - methods of analysis, management and settlement of risks,
    - management of enterprise (finance, human resources, organization, technology, innovation...).
2. 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,
    - determination of hierarchy of problems,
    - capability to find right information and apply lessons learned,
    - execution of critical analyses,
    - 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 [7,45] to specify:

- for each relevant disaster, size of threat (expected impacts) according to given standards,
- critical tasks of technical facility from integral safety viewpoint,
- tasks and causes of their criticalities and to understand them,
- possible human failures,
- 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.

From these reasons, at terms of references creating, it is necessary to consider that to technical facility criticality [2,4,6,7,45] 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.

From above, it follows that technical facility terms of reference are result of expert team that selects parameters, which ensure the sufficient safety margin for technical facility operation.

In total, the terms of reference need to include documentation of how the risks associated with both, the territory, where the facility is located, and the facility itself, and the expected reactions and conflicts in given territory in the manufacturing and operation of technical facility.

2.5. Technical facility project

Project preparation, project design, construction and commissioning of a technical facility is a complex area, with constantly changing processes and activities. It involves many actors, who are interdependent, and therefore, they should work together. At the same time, it is also influenced by a number of external factors [2,4,7], such as:

- market situation,

- other engineering projects in same area,
- size of the technical facility,
- availability of resources,
- competence and experience of designer, managers and employees.

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 [2,4,7,45], 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 in great rate. The low cooperation of experts leads to errors that will occur later at operation, e.g. they lead to:

- occurrence of organizational accidents [48],
- maintenance problems [2,4,45],
- impossibility to repair important parts [2,49] etc.

From the particulars in [49], it follows that impressive and low robust designs often fail sooner or later. The same holds for design that suits for very narrow interval of conditions.

2.5.1. Technical facility project requirements for design disasters withstanding

To increase the safety of technical facilities, the results of analytical and heuristic processes are increasingly interconnected - and experience databases are being created. In practice, it is necessary to apply the interconnection of principles [2,4,5]:

- All-Hazard-Approach,
- Defence-In-Depth,
- inherent safety,
- passive safety,
- active safety,
- and those for a safety management system over time.

The basic principle of safety management is a qualified interconnection of technical, organizational, financial, personnel, social and knowledge areas; and clear roles and responsibilities of all involved. The safety management system of critical facilities

(SMS) thus covers a number of areas, namely technical, military, legislative, financial, economic, social, environmental, educational, research, etc. The roles of individual stakeholders and their interconnection in different situations need to be determined by law, moral and other standards and norms.

Since the fact is that we are unable to identify knowledge uncertainties, we need at management of technical facility safety to rely heavily on the response; i.e. the drafting the operating rules in the event of significant changes in conditions and, if unsuccessful, on the response applying the safeguards to essential public assets. Therefore, to ensure the safety of complex objects and to protect people, we are looking for a response solution also for possible cases that cannot be detected by probabilistic approaches [1,5], and we need to build alternative water and energy sources, specific response systems and specific rescue training for them [4].

Options for performing a good response need to be already created in the technical facility project. E.g. the arrangement of the equipment and its interconnections shall make it possible in critical items to set up:

- a program to continuously improve the safety of critical items,
- measures for assessing the level of safety in terms of the effectiveness of the safety system (indicators),
- a program for continuous safety improvement consisting of interconnected projects,
- and projects that are filled with interrelated processes.

As with the terms of reference, so at the project development, the models are used, i.e. preferably in the form of available software. These tools are usually based on tree models and use linearized relationships. According to the data summarized in [5], these instruments do not consider external disasters, attacks and the human factor which usually affect many fittings and system in one stroke. Therefore, when designing the critical elements, equipment and systems of a technical facility for safety reasons, they need to be pursued impact assessments of the mentioned disasters and into the project, the measures for prevention, mitigation and response need to be implemented; e.g. IEC requirements [50].

The point is that already in the technical facility project itself [2], there would be measures for:

- ensuring the inherent safety,
- technical protection,
- ensuring that fittings and components fail safely,
- activity of quality reserves (backups),
- ensuring the integrity of measures for risk management,
- informing the operator about the condition of the equipment, especially on its big sudden change.

There are now a number of safety standards; for machinery e.g. standards ISO 16090, ISO 12100, ISO 1384911 [51-53] are important. The standards´ analyses [49] show that they concentrated to equipment safety and not to operation safety (and also not to whole (integral) technical facility safety). Due to changes in time, the critical equipment monitoring is necessary inserted in project. In the project itself, equipment and

tools need also to be built to enable the response to major failures and accidents, such as the requirements of the EU Directive [54].

2.5.2. Requirements on project

Designing the technical facilities is a very complex activity, and in each country is regulated by national legislation and in some cases by international ones [55-58]. The real design of a technical facility depends on the complexity of the proposed technical facility and the requirements laid down in the public interest. From the safety point of view, the design of each technical facility [2] requires to follow:

- durability,
- manageability of equipment, components and processes,
- lifespan,
- human resources,
- costs,
- technical services,
- additional services,
- safety of employees,
- 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 and coexistence of technical facility with surrounding area. For example, non-provision of human resources for operation leads to limitation of production or service that is provided by the technical facility [2].

The consideration and good assurance of the requirements in question determine the future costs of ensuring the safety and coexistence of the technical facility with the surrounding. For example, failure to provide human resources for operators leads, for example, to a reduction in production or service to be provided by the technical facility.

The primary task of the designer is to identify all possible hazards by application of the All-Hazard-Approach approach, which has been explained above and to divide them into acceptable, conditionally acceptable (tolerable) and unacceptable. In the case of the second and third, the designer needs to think in the following way:

1. Can I eliminate the hazard? In case yet, how?
2. Can I reduce the size of this hazard? In case yet, how?
3. Cannot I create a new hazard by the measures proposed to deal with the hazard? In case yet, what measures are better?
4. What technical and control systems are required to manage the residual hazard?

According to [2,4,45,55-60], for the technical facility safety during the lifetime, it is necessary at designing to consider at each critical process the problems connected with:

- a given process,
- designing the process,
- process management,

- operating personnel and its condition indication,
- safety management system,
- other technical systems promoting the safety,
- external active and passive systems to mitigate the risk of process failure,
- emergency response of the technical facility,
- the emergency response of the site where the technical facility is located.

Research results summarized in [2] show:

1. 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 the 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.
2. It is necessary to ground for program for safety increase that ensures:
   - safety and functionality of all fittings that correspond 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, humans in the vicinity, fittings, equipment and property,
   - use of new materials or products and test techniques only in a way that is only associated with minimal risk,
   - insertion of safety factors that ensure the corrective measures that lead to improvement,
   - consideration of all appropriate historical data on ensuring the safety generated by similar safety-enhancing programs.
3. From engineering viewpoint, the 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 need to be their backups,
   - where / in which places safety systems operate most effectively,
   - why they need to 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. As it was said above, based on the current knowledge summarized in [5], 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.

Due to dynamic development of technical facility and its surroundings, it is necessary for ensuring the integral safety and coexistence to insert into project sufficient safety margin. This safety margin enables to overcome expected risks.

It is a fact that an engineering project with high safety is costly and that the aspiration of every investor or operator for the least possible cost of a technical facility leads to a reduction in safety, i.e. the costs of the technical facility. to narrow the interval of conditions that a technical facility can handle. Figure 3 shows that, in reality, the cost of reducing the risk and the costs of the measures taken, i.e. the cost of reducing the risk, should be compared. application of the CBA method [61] with compliance with safety requirements. Because each entity has only limited sources, the optimum solution from safety viewpoint (sufficient safety margin) is such, in which total costs are round the total costs curve minimum.

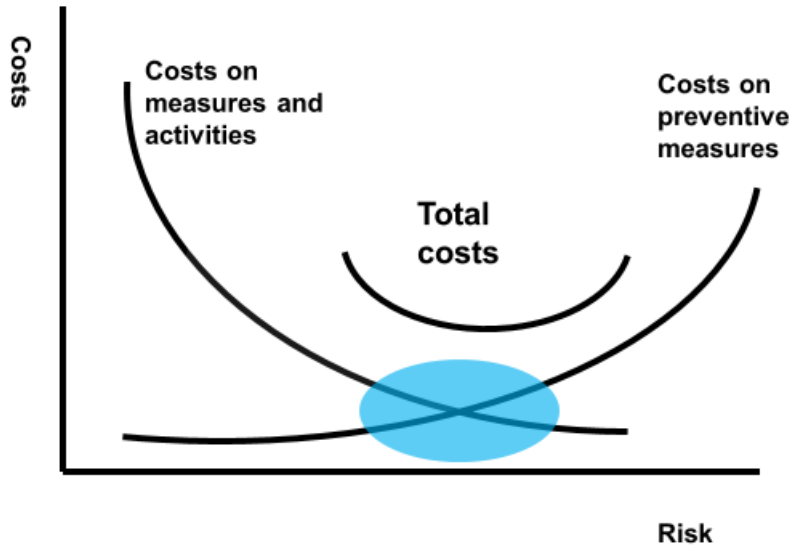

Figure 3. The total cost interval in which safety is ensured; processed in [62]; the area of optimal costs for safety margins is marked in blue.

The outputs from the risk management process to ensure safety according to [63], based on total quality management, are as follows:

1. Risk assessment document - all information on the risks involved is recorded here.
2. Top risks list, i.e. the list of risks, the solution of which has the highest demands on resources and time (for technical facilities these are risks that need to be monitored and, according to the results of the monitoring, the measures and activities leading to safety [4,6,7] applied. ***These risks need to be given in the project documentation and need to be systematically managed during the operation by help of operating rules and tools for maintenance and improvement safety of technical facility in time.***

3. Retired risk list - serves as a historical reference for future decision-making in changes and upgrades (e.g. not to remove barriers, which have been placed in the system for prevention or mitigation [2,4,6,7].

According to knowledge summarized in [2,4], it is important so that the processes for risk management strategy use: principles of inherent safety; passive safety systems; active safety systems; 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.

2.5.3. Inherent safety

The term "inherent safety" was introduced in 1977 by the English engineer Kletz in the chemical industry. This is a fundamental approach to managing the hazards from harmful phenomena (i.e. disasters of all kinds) by reducing its size, thereby reducing their danger. It is the way in which the hazard is managed, i.e. the risk is precluded. Of course, it is not possible in natural disasters, because they are not yet controlled by humans.

Inherent safety is a specific feature of components and processes of technical facility, which is determined by physical and chemical laws and characteristics, i.e. not by human measures. It is a principle that allows the self-regulation of dangerous processes. This means that the inherent (inner, own) safety of the device or system is the approach to which the device or system acquires the capability to have a low level of danger even under unacceptable conditions. It is a way of thinking when designing a technical solution that seeks a principle that reduces risk in a different way than risk management.

Based on the data in [2,64-69], the incorporation of inherent safety into a technical facility is carried out, for example by:

- reducing the amount of hazardous substances (use of hazardous substances in smaller quantities),
- using a less dangerous substance instead of the very dangerous one (substituting substances, if possible, e.g. cleaning not with a flammable solvent but with water and possibly scrubbing),
- use of the substance in another state or at a different temperature,
- the use of equipment to reduce the impact of a dangerous substance,
- reducing the number of unsafe operating processes - reducing the complexity of equipment,
- application of the principle of error tolerance (e.g. design of a device to withstand the maximum pressure possible),
- limiting the impacts (e.g. setting the traps for hazardous substances),
- special operating the equipment to ensure:
    - avoiding the shocks,
    - impossibility of moving the device to an unstable position,
    - a clearly defined position and condition of the equipment; easy operation of the device,

- flawless control instructions and software.

The concept of inherent safety is a dynamic, subjective and holistic concept. It requires thinking and experience from the designer. For example, it is necessary to decide whether it is better to have large stocks of dangerous substances or often to import dangerous substances by train (in both cases they are dangers, i.e. in the particular case it is necessary to choose the one with lower risk). The problem with the implementation of inherent safety is that the principles are descriptive and not prescriptive.

Since the insertion of inherent safety can also be a cause of destruction [49], for example, using one refrigerant in a refrigerator suffices less than another refrigerant, but the use of the former is harmful to the environment, so one should always think about what is worse.

2.5.4. Elements and systems of passive safety

Passive safety elements are physical elements or devices that operate only at the moment of the accident. This is a design device designed to minimize the consequences of an accident. Examples are the safe construction of the vehicle body or steering column, head restraints, seat belts, belt pretensioners, airbags, etc.

Passive safety systems are physical systems that control the hazards of a process or device by means of device elements without intervention from the control centre. The best-known applications of passive safety are:

- protective walls,
- protective nets; etc.

2.5.5. Elements and systems of active safety

Active elements for ensuring the safety are technical devices, systems and features of a technical facility that help to prevent and to avert incidents and accidents. E.g. for vehicles, the most important elements of active safety are:

- effective brakes allowing for safe deceleration or stopping of the vehicle,
- good visibility from the vehicle,
- good tires,
- precise and reliable steering,
- good quality shock absorbers ensuring the sufficient contact between the tires and the road,
- and lighting.

Other elements of active safety include modern electronic systems such as ABS, ESP, TCS, EBA, ACC and others. For other machines and equipment, active safety means especially:

- significant marking of dangerous places,
- covering the dangerous parts of the machine (uninsulated electrical conductors, rotating parts,…),
- significant light and sound signalling of the machine operation,

- and safety fuses stopping the machine operation after opening the cover.

Active safety systems control the hazards of a process or device by means of device elements based on a command from the control centre, which is realized based on monitoring data. An example is the fall of safety rods in a nuclear reactor in the event of a rapid reactor shutdown. The control and safety rods contain neutron absorbing material (e.g. boron or cadmium compounds). The inserted rods absorb neutrons and the fission reaction is inhibited. The rods in the upper position hold the electromagnets. If the control system evaluates the need for rapid insertion of the rods into the core, it disconnects the power supply to the electromagnets, and the absorption rods are gravitationally attracted to the earth's surface and thereby slide into the core. Other examples are:

- early warning systems,
- fire alarms,
- sensors,
- equipment condition control and / or reaction systems.

2.5.6. Selection of elements, procedures and fittings

From a safety point of view, it is good practice to select elements, procedures and equipment that are proven or thoroughly tested so that they do not contain latent sources of danger under possible conditions. In cases, where there is a high risk, care should be taken accent on prevention, for example, to install pressure relief valves, sprinklers, walls to absorb pressure waves, etc., even if they are costly.

In practice, there is often a reference to BAT (Best Available Technology), which refers to the best available technique that is codified or standards-based to reduce unacceptable impacts on public and corporate assets. The concept was introduced in 1984 in European Economic Community law by Directive 84/360 / EEC, which was aimed at reducing emissions to air from large industrial installations. An overview of current BAT in the EU is at work [70]; for details see [70-72].

In accordance with European legislation, the term BAT denotes:

- technique means both, the technology used and the way in which the equipment is designed, built, operated, maintained and decommissioned,
- available technique means technique developed to the extent that they can be implemented in the relevant industry under economically and technically acceptable conditions, considering the costs and benefits, provided that they are available to the operator of the equipment under reasonable conditions, without in which country they are manufactured,
- best techniques are the most efficient techniques to achieve a high level of protection for the environment as a whole.

At selection of equipment, procedures and fittings it is necessary to consider their robustness with regard to working conditions and their variability. From the particulars in [49], it follows that impressive and low robust designs often fail sooner or later. It is evident that low robust equipment, procedures and fittings may not be used for critical ones. The same holds for design that suits for very narrow interval of conditions; interface “limits and conditions” determines safety margins of each entity.

2.5.7. Princip Defence-In-Depth

In order to ensure the protection (under concept directed to safety or to reliability or to security) of important technical facilities, it is used the principle of Defence-In-Depth, which is described, for example, in [2,6,7,73]. The principle was already used in the military in the Middle Ages, and therefore in the English text is used the word "defence". It is a comprehensive approach that ensures that humans and the environment are protected even under critical conditions in a technical facility. It is a comprehensive philosophy of safety that began systematically in technical domain to apply in the 1980s. Today, it is very broadly used in different technical domains, e.g. energy, transport, protection of workers, medicine etc.

The principle in question for critical complex facilities having five protection degrees is shown in Figure 4 [4,7]. It is implemented by 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 needs to be available to fulfil its function. 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.

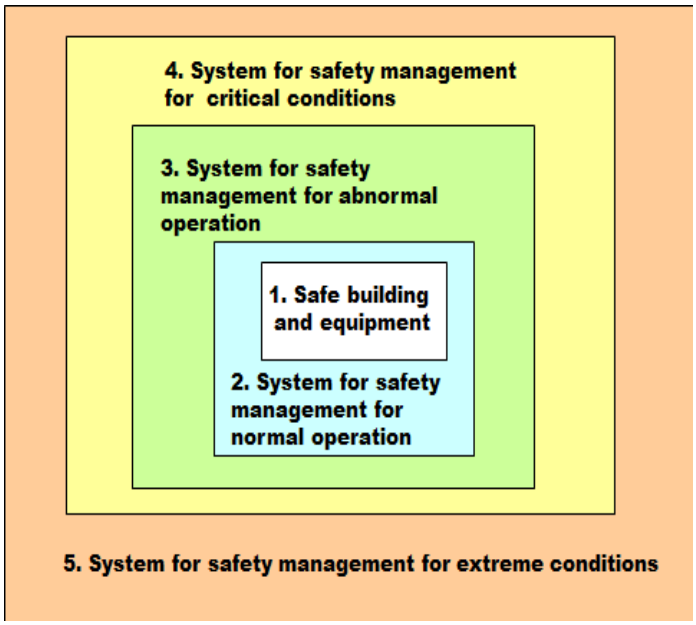

Figure 4. Five steps model for complex critical technical facility safety management.

It is understandable that it would be good if the individual layers of safety management would be independent, which is de facto impossible because there are physical linkages. Therefore, it is necessary to pay attention to these linkages and either to limit them or to treat them so that they cannot cause failure or an accident of important components of the technical facility. For example, the “fail safe” principle is used to ensure that the equipment is safely stopped quickly when dangerous conditions are detected, i.e. the equipment is brought into a stable state that does not dangerously disrupt other systems and notifies the operator.

The principle in question needs to be correctly inserted into the technical facility safety management system (SMS) and it has very special requirements of the information and control system (I & C) designing and execution. Due to knowledge and experience from practice, a special attention needs to be paid to pressure equipment with dangerous substances [2,7,45,49,56]. The execution of followed principle uses the systems of barriers and regime measures to ensure a safe technical facility (understood as a system of systems).

Barriers are devices that have different purposes and different characteristics [73,74]. These are devices that are always designed to prevent any risk, i.e. to protect human lives, the environment or to ensure operation continuity. The aim of barriers is:

- to compensate human and technological failures,
- to maintain effective barriers that to prevent damage to equipment and barriers themselves,
- to protect humans and the environment when barriers do not fulfil their tasks.

It is true that barriers are a measure that in many cases also contributes to the safety of a technical facility. In line with the work [38], it should be pointed out that the application of barriers in complex technical facilities is being contested among engineers, who advocate reliability theory (they claiming that the safety of the engineering work can be assured by continuously increasing reliability by adding barriers) and engineers who prefer to focus on the safety of the technical facility (they argue that barriers increase the complexity, which is the cause of unexpected behaviour at conditions that were not considered in design, which in many cases leads to unacceptable impacts).

The concept of barriers has several interpretations that depend on the sector or state in which they are used. Details are, for example, in standards and standards, such as IEC 61508 (2002), IEC 61511 (2003), Seveso II Directive (1996) and Machinery Directive (1998), etc. These standards imply that when considering the safety barriers, a distinction should be made between safety management function and safety management system function.

Barriers having a function in safety management are intended to prevent the development of an accident [2]. Barriers having a function in the safety management system consist of one or more different elements and are designed to ensure that an activity is performed. This means that for each barrier, the purpose and action need to be specified. The purpose is either to prevent unwanted phenomena such as technical failures, human errors, external phenomena or combinations thereof that may lead to potential hazards, or to the development of accidents that result in damage to people, the environment or equipment. Therefore, we divide the barriers into two types:

1. Barriers used for prevention. They are built into the fittings and they need to be in continuous operation.
2. Barriers aimed at protection. They are triggered only after the occurrence of non-demanded phenomenon.

The quality and safety of barriers is assessed according to:

- efficiency, i.e. how well the barrier fulfils its intended function for safety,
- the resources required, i.e. what costs are necessary for designing, developing and maintaining the barrier for ensuring the safety,

- robustness, i.e. how the barrier is related to reliability (how the barrier can withstand the variability of operating conditions),
- start-up delay, i.e. how much time does the barrier require to start the activity,
- accessibility, i.e. whether it can fulfil its role whenever it is needed,
- assessing how easy it is to determine that the barrier is working as expected,
- independence, i.e. whether or not its activity is dependent on human intervention.

The ARAMIS procedure [75] proposes 3 criteria for assessing the barriers:

- efficiency – the capability of the safety barrier to perform a safety-oriented function under specified conditions for a specified period of time in good quality; it is measured as a percentage or probability of failure,
- response time – it refers to the time taken by the barrier work to achieve the required safety level,
- the level of barrier confidentiality – it depends on:
    - the independence of the barriers from regulatory systems,
    - barriers´ architecture,
    - concept and periodic tests of barriers.

For the operation of barriers in the project of technical facilities, sufficient capacity spare electricity and refrigerant sources needs to be built into the project.

Due to the safety of the technical facility and its surroundings, in particular its reliability and resilience, in many critical systems according to the works [4,7,76,77], barriers are inserted, i.e. they are inserted devices or systems with aim to prevent or mitigate harmful impacts; for example, various means of signalling. At their proposals is according to the work [76] to proceed cautiously, because poorly selected barriers can under certain conditions more harm technical facility.

Figure 5, borrowed from work [76], shows the basis for placing and assessing the barriers. Where it is possible to insert barriers into a technical facility and it is cost-effective in terms of resources and means needed, barriers to ensure prevention are applied. Otherwise, safeguards are applied to protect both, the public and the technical assets. For reasons of economy, a combination of the two barrier types, which is optimal in terms of purpose and cost, is logically sought. The division and method of classification of barriers by work [77] is shown in Figure 6.

In the project processing, they are determined the regime measures for operation, i.e. a management mode is established which ensures:

- method of controlling the socio-cyber-technical system under normal conditions, i.e. the method of preventing the abnormal operation and failure,
- method of controlling the socio-cyber-technical system under abnormal conditions, i.e. the method of controlling the abnormal operation and failure detection,
- the way of controlling the socio-cyber-technical system under critical conditions, i.e. the control of accidents by means of project measures,
- method of controlling the socio-cyber-technical system in extreme (beyond design) accidents, including prevention of further development of the accident and mitigation of the impacts of the accident outside.

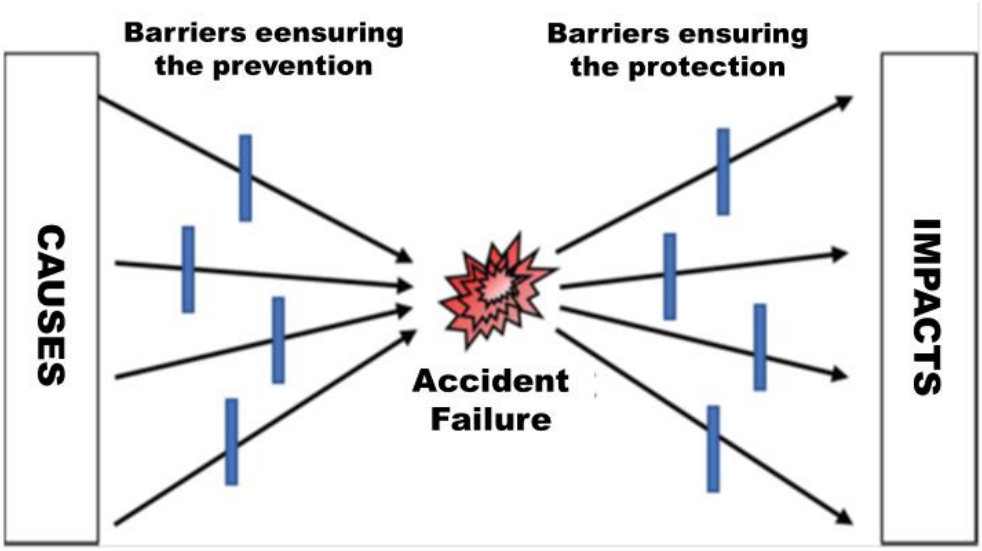

Figure 5. Bowtie diagram for the assessment of activity of barriers at major hazards; processed according to [76].

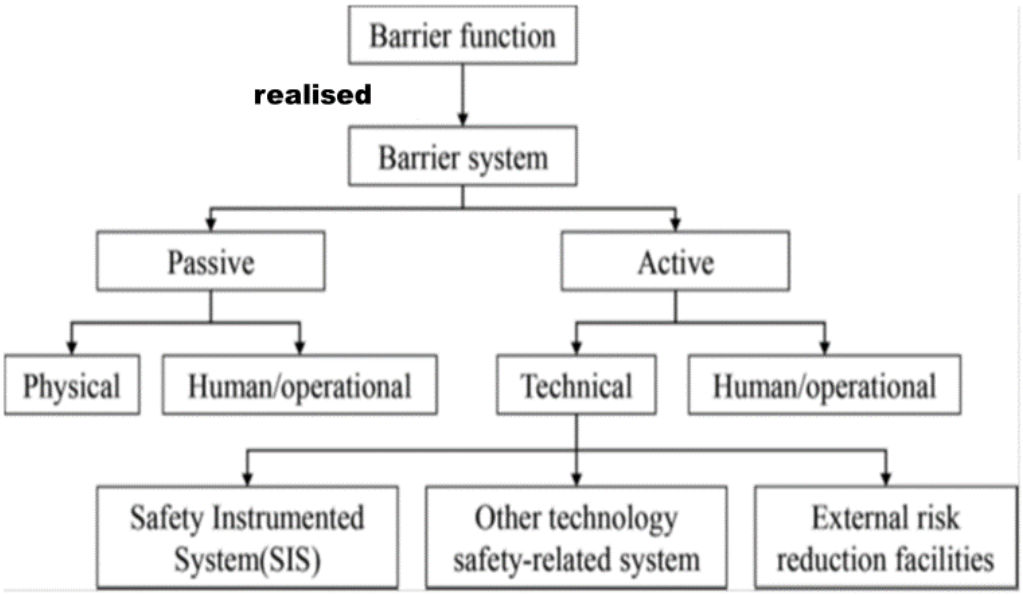

Figure 6 Classification of barriers to ensure the safety of a technical facility; processed according to [77].

2.5.8. Coexistence

Coexistence generally means a common existence. The importance of coexistence is now under consideration in many technical fields [10-20,26-33]; the problem was discussed in detail in previous work [25,78]. In the reference case, it goes on ensuring such conditions at technical facility designing, construction, outfit by technology equipment, testing and commissioning that enable continuously to control the reactions

between conditions of technical facility and its surroundings (Figure 1) and immediately solve originated conflicts .

The coexistence of technical facility with its surrounding is ensured by the way that in the technical facility design are included special elements and systems. These items are interconnected into safety management system, which enables the continuous management of integral safety of technical facility. The scheme for such procedure is shown in Annex 1. In practice, this concept is realized by I & C systems of technical facility [4].

The technical facility I & C system main part is the safety management system (SMS). The SMS ensures data for safety management in time by the way shown in Figures 7 [4,7]. The safety management system (the so-called SMS) based on the process management includes the organizational structure, responsibilities, practices, rules, procedures, and resources for determining and implementing the prevention of disasters, or at least mitigating their unacceptable impact in the territory.

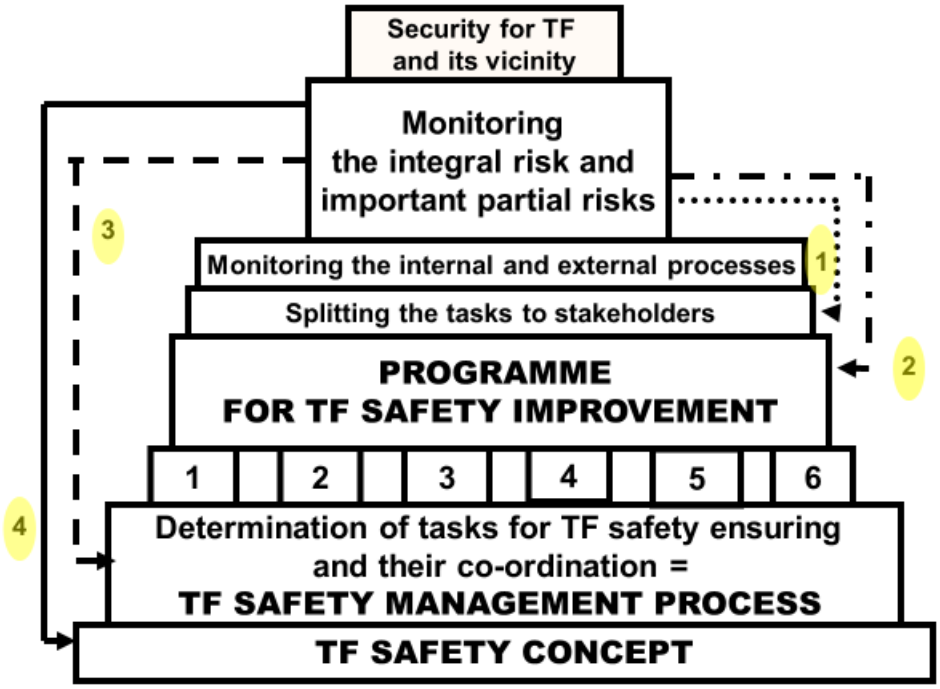

Figure 7. Model of the technical facility (TF) safety management in time. Processes: 1 - concept and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. Feedbacks that are used to control when the risk is unacceptable - the numbers in the yellow circle.

In Figure 7 the black block indicates basic decisions to ensure a safe entity (i.e. the technical facility) – specification of the essential processes of a technical facility, that predispose a safe technical facility, i.e. its existence, safe operation and development. Then there follow the sequential steps aimed at the security and development of the technical facility.

As the technical facility and its surrounding dynamically develop it considers corrections and changes. In case of the need for corrective measures there are indicated the basic feedbacks, by which it is corrected the set of measures and activities; the dotted line — feedback 1, dash-dot line — feedback 2 dashed line-feedback 3, full line – feedback 3. From Figure 7 it is evident the vital role of monitoring the internal and external processes and phenomena, which is followed by an assessment of the impacts of processes on a critical facility and by determination of optimal measures and actions to ensure safe critical facilities. In the event that the limits and conditions are not complied with, it is necessary to make changes, as indicated on the feedbacks in Figure 7. Because the changes require resources, forces and means, on the basis of ensuring the cost-effectiveness, there is realized in the first the feedback 1, and only when not desirable, it realizes the feedback 2; after the feedback 3, and when, even after it is not a desirable outcome, so feedback 4. In the case of the occurrence of extreme phenomena with disastrous impacts, it is immediately implemented the feedback 4.

The SMS refers to a number of questions, inter alia, the organization, workers, the identification and assessment of hazards and risks resulting from hazards, the management of the organization, the management of changes in the organization, emergency and crisis planning, monitoring the safety, audits and reviews [4-7,56,58]. On the basis of the cited works, the SMS of critical facility consists of six main processes that have sub-processes:

1. Process of concept and management, which is further divided into sub-processes, which ensure: the overall concept; partial safety objectives; leadership / management of safety; the safety management system; the staff, which is further divided into sections: human resources management, training and education, internal communication/awareness, working environment; and review and evaluation of the implementation of the objectives in the safety.
2. Process of administrative procedures, which are further divided into sub-processes, which ensures: identification of hazards from potential disasters and risk assessment; documentation; procedures (including work permits); the changes; safety in conjunction with the contractors; and supervision under safety of products.
3. Process of technical issues, which are further divided into sub-processes, which ensures: research and development; design and assembling; inherently safer technical and technological processes; industry standards; storage of dangerous substances; maintenance of the integrity and maintenance of equipment and buildings.
4. Process for external cooperation, which is further divided into sub-processes, which ensures: cooperation with the administrative authorities; cooperation with the public and other stakeholders (including academic institutions); and cooperation with other enterprises.
5. Process of the emergency preparedness and response, which is further divided into sub-processes, which ensures: planning of internal (on-site) preparedness; facilitating the planning of external (off-site) preparedness (to which the public administration corresponds); the coordination of the activities of the departmental organizations at emergency preparedness and response.
6. Process of reporting and investigation of accidents / accidents almost, which is further divided into sub-processes, which ensures: reports on accidents, incidents, near-misses and other lessons learned; investigation of near-misses, incidents and

accidents; and responses and follow-up after the incidents and accidents, including the application of lessons learned and information sharing.

Processes need to be coordinated so that they are targeted to the objectives set, i.e. the safe operation of critical facilities.

The safety management system (SMS) of a technical facility is based on the concept of prevention of disasters, or at least their serious impacts, which includes the obligation to establish and maintain a management system in which they are considered the following issues:

- roles and responsibilities of persons participating in important hazards management on all organising levels and in ensuring the training,
- plans for systematic identification of important hazards and risks connected with them that are connected with normal, abnormal and critical conditions, and for assessment of their occurrence probability and severity; plans and procedures for ensuring the safety of all components and functions, namely including the object and facilities maintenance,
- plans for implementation of changes in territory, objects and facilities,
- plans for identification of foreseeable emergency situations by systematic analysis including preparation, tests and judgement of emergency plans for response to such emergency situations,
- plans for continuous evaluation of harmony with targets given in safety concept and in the SMS, and mechanisms for examination and performance of corrective activities in case of failure with aim to reach determined targets,
- plans for periodic systematic assessment of safety concept, effectiveness and convenience of the SMS and of criterions for judgement of safety level by top workers group.

The SMS design needs to ensure the coordination of processes targeted to the safe technical facility under the conditions of normal, abnormal and critical by the way shown in Figures 8 [4,7].

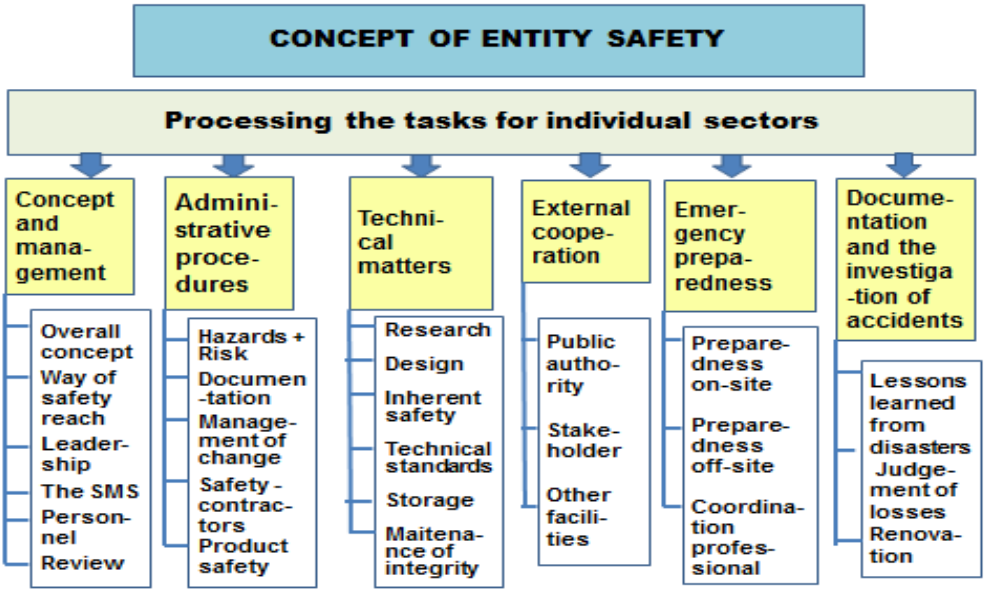

Figure 8. Concept of entity safety and its main parts.

The quality of the I & C systems depends on quality of parley of behaviours of critical interfaces at different conditions; especially those which are connected by sudden big dynamic changes either in the technical facility or in its surrounding. It goes on collection of quality particulars from monitoring (correct prompt information) and on quality principles for decision-making which are included in the I & C system.

2.5.9. Resilience engineering

Resilience is the potential of the system, which is in a specific arrangement of the system, which keeps the functions and feedbacks of system, which include the capability of system to reorganize itself on the basis of changes induced by disorders. Its relations with other technical facility characteristics [23,79] are shown in Figure 9. From this it follows that the management of sustainability needs to be based on management of resilience, which has two objectives:

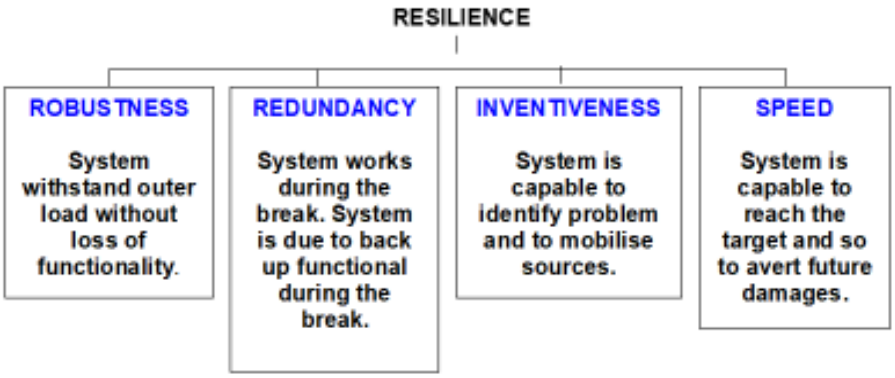

Figure 9. Context of resilience of system with robustness, redundancy, inventiveness and speed.

1. To avert the non-demanded system conditions in the consequences of external disturbances and external load.
2. To keep the elements that trigger system reorganization and reconstruction in the wake of massive changes.

Resilience management process takes place in three steps, namely:

Step 1: Resilience who, what? It proposes a conceptual model of system based on specific questions:

- what are the spatial boundaries of the system?
- what are the key system services used in the system?
- what are the stakeholder groups?
- what are the key components of the system, how to characterize what is their importance and dynamism?
- what is the historical profile system?
- what environment variables act as driving forces key system products and services?

- which factors are controllable and manageable?

Step 2: Resilience in relation to what? (scenarios). They are analysed the external and development processes (processes of sustainable development) and described the demanded arrangements, which are resilient. The scenarios need to avoid primarily uncontrollable and ambiguous external driving forces.

Step 3: Analysis of resilience. There are exploring the interactions among the external exposure and resilient folders and finding the processes in the system, that control the dynamics of the system. A key element of the analysis of resilience is the determination of ***the threshold values.***

It is a fact that ensuring the integral (overall) safety of a technical facility is very difficult because there is:

- either limited knowledge of all possible conditions in which the technical facility may be, causing unacceptable temporary links or unacceptable temporary couplings leading to an accident or failure,
- or measures are too costly or unavailable for other reasons (e.g. embargo, political intentions, etc.), which means that they are not applicable.

Therefore, a completely specific field, i.e. resilience engineering, has evolved over time [80,81]. It is about creating the internal capability of the system to adapt its function to changed conditions, so that the operation is maintained. The feature in question has to be introduced into the system at the time of its design, and therefore, in system design it is ensured [78] the system capability to:

- anticipate,
- monitor,
- respond,
- and learn.

System resilience depends on:

- the capability of the system to sense and respond to a major change in conditions before losses and damage occur, i.e. system:
    - has procedures in place to handle with non-normal conditions,
    - includes human factor, human-machine linkage, training, safety culture and experience,
    - has the capability to recognize that:
        - adaptation is deteriorating,
        - the silencer or reserve is depleted,
        - a compromise or change of priorities is needed,
        - roles, activities or goals need to be changed,
        - and it is needed to look for a new method for customization,
- robustness, i.e. how the system is able to detect deviations from the expected state (conditions) and adjust its operation,
- adaptation, i.e. how the system is able to detect deviations from the expected state (conditions) and adjust its operation appropriately.

The safety of critical systems is affected by new technologies such as the Internet of Things based on the interconnection of various technical devices over the Internet [82]. The technology in question has a number of advantages, but also disadvantages, which have the potential to significantly undermine the safety of technical facilities, and therefore, the safety of technical facilities needs to be carefully considered in their use; their non-use is conservative and provides greater security, but it means that their advantages are not used.

Safety and resilience of the I & C systems is present problem, the solution of which has been searched; only sector-specific standards are to disposal.

2.5.10. Summary of requirements on project ensuring the technical facility safety

The basic means for ensuring the technical facility safety during the designing, are:

- conservative design for the building and high quality of construction and operation,
- installation of control, restriction and protection systems and other typical features of surveillance under operation,
- insertion of (inherent) safety-enhancing properties,
- alternative measures and accident management for internal response (in-site) plan,
- means for external response (off-site) plan.

Since the monitored SoS are the basis for the life and development of humans, it is necessary to ensure that the objects can be put into operation in the foreseeable future, even under beyond design conditions.

In the design, building and construction it is necessary to use safe design principles, i.e.:

- All-Hazard Approach,
- proactive approach,
- Defence-In Depth principle,
- systemic approach based on application of integral risk, as well as significant partial risks associated with material, energy, financial and information linkages and flows in and across subsystems,
- correct risk management,
- monitoring, in which corrective measures and actions are inserted.

It is important to draw up the technical facility terms of reference associated with the territory in question, which express the way in which local vulnerabilities to all relevant disasters that may affect the site are valued, as well as the valuation of all site-specific features that may cause specific impacts. Based on recent knowledge summarized in the works [4,7,24], critical and complex objects need to consider random and knowledge uncertainties, i.e. vagueness in data for prevention of atypical accidents that are resulted from unpredictable phenomena that cannot be detected by common stochastic methods.

The technical facility information and control system (I & C) shall have basic operator functions, alarms and operator responses processed to maintain the technical facility in a normal (stable) state under normal conditions.

The technical facility needs to have special safety-oriented control systems and protective barriers to keep it safe even when the operating conditions change significantly (i.e. abnormal conditions) and prevent the occurrence of non-demanded effects, which means that it has good resilience. These systems maintain the safe operation even under changing conditions or have the ability to ensure normal operation after applying remedial measures (cleaning, repairing…).

In the event that critical conditions occur that result in the loss of control of the facility, the facility shall have a system of internal emergency response, mitigation of impacts, and return to normal operation (continuity and internal emergency / in-site plan) .

In the event that the impacts of the loss of control of the system affect the surroundings of the technical facility, the facility shall also have measures for external response, mitigating measures to prevent losses in the facility; and the capacity to overcome the difficulties to be able to restore the object.

In the technical field, the above-mentioned layers are considered as protective barriers (so-called defence-in-depth protection) and when distinguishing technical facilities from the safety point of view, the safety characteristic is used that the object facility has one- or five-level depth protection. Individual systems of control of safety ensure the application of technical, operational and organizational measures and actions that are designed to either prevent or stop the initiation of a chain of harmful phenomena [83].

Since the deterministic approach to defence in depth does not explicitly consider the probability of occurrence of challenges or mechanisms, nor does it include quantification of the probability of success associated with the implementation of elements and systems at each defence level in depth, the deterministic approach is complemented by probabilistic safety analysis (PSA) in the area system reliability, probable targets etc. in order to ensure an adequate level of safety that ensures a well-balanced project.

Because of the knowledge uncertainties that cannot be captured by the stochastic approach [80], stochastic procedures are currently combined with expert data obtained by evaluating a number of case studies [24].

For the successful management of risks in complex technological systems, according to [84]:

- to maintain technical facility operation in moderate operating conditions, which can be ensured by measures that operating personnel:
    - is properly trained,
    - has the necessary skills,
    - and understands the essence of managing basic operational functions,
- to ensure safe technical facility operation under variable conditions, which can be ensured by the measures that operating personnel:
    - is properly trained,
    - knows operating rules under variable conditions,
    - and respects the requirements of a safety culture,
- to control the critical state of equipment through preventive mechanisms (e.g. critical safety systems), which can be ensured by:

- applying the working procedures to certain accepted standards,
- and personnel training to deal with deviations from normal operations,

- in the event of loss of control, it is necessary again to obtain control under the system with the training of staff to be able to:
  - gain awareness of the situation,
  - understand the nature of the problem,
  - understand the limitations of basic as well as preventive control functions,
  - improvise,
- in the event of inability to handle equipment, staff needs to be educated in order to be able to:
  - shut down the technology by ensuring the least possible loss of technology,
  - and activate an external emergency plan (i.e. apply protective measures and actions, release reserves, evacuate).

Grounds for application of this procedure need to be inserted in the technical facility project; especially in designing the I & C system as a part of the SMS.

It follows from the above that the higher the design disasters we choose for the design (i.e. by other way we ensure passive protection), the higher technical facility safety we reach, because the effectiveness of organizational measures in the field of management is always lower than for technical measures, for which it reaches up to 80% [7] .

The recommendation to all designers is to consider the following knowledge:

- a critical analysis of data in [49,83,85-87] shows that the requirements for equipment, systems and components of critical facilities do not systematically consider cascading failures,
- not an application of the best current concept (system of systems safety management) for ensuring the safety of facilities has not negligible criticality (i.e. some sources of risk remain after its application) due to cascading failures caused by knowledge uncertainties [24],
- too much reliance on the PSA efficiency, which assesses the risks associated with the production process model and does not consider the failure of safety features, i.e. protective barriers show that despite all the measures applied so far, there are sources of risks that can have extreme impacts. In addition, many examples show that many experts are affected by operational blindness, they are relieved of meeting the requirements of standards and standards, and do not see the risks associated with various linkages and couplings with the surrounding. Again, a simple comparison of the intervals used in probabilistic assessments shows that according to the findings in the paper [24]: the interval $(\mu-\sigma, \mu+\sigma)$ covers 68.5% of cases; the interval $(\mu-2\sigma, \mu+2\sigma)$ covers 95.4% of cases; and the interval $(\mu-3\sigma, \mu+3\sigma)$ covers 99.8% of cases - where μ is the median and σ the standard deviation.

Considering these recommendations means to favour conservative and robust designs of technical facilities and their critical fittings, components and systems, and pay attention to their sufficient safety margins.

2.6. Technical facility manufacturing

The technical facility manufacturing [2,55] means:

- to 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,
- to carry out all activities related to supply construction works and structures, which are necessary for proper facility completion, e.g.:
  - construction of 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.).

Legal requirements are governed by the Building Law and other laws, because these are financial, relationship, liability, environmental, insurance, information protection, etc.

At technical facility manufacturing the great attention needs to be given to all technical works quality (to respects valid norms, standards and rules of good engineering practice). Special attention needs to be concentrated to critical technical operations [2] as:

- construction and location of pressure vessels and their fittings,
- connections of structural and machinery parts,
- connections of different machinery parts, especially to quality of welding, gasket, screwing etc.
- connections of structural and machinery parts with cyber elements enabling the quality of control,
- etc.

To archive safe, i.e. reliable and functionable installations (elements, machines, fittings, components, systems etc.) and safety of their interfaces, the regular tests and inspections need to be carried out. Their aims are judgement of fulfilment of demands

of standards and norms in harmony with the project and rules of good practice. They are used the non-destructive tests methods [2,55,57,88,89].

2.7. Trial operation

The aim of trial operation of the technical facilities is to verified the functionality and properties of the executed construction and structure according to the project documentation [2,55,57]. The attention is concentrated not only to whole operation process but also to behaviour of critical fittings, components and systems (especially pressure vessels, sealing, welds etc.) and their interfaces of all kinds. Especially, there are followed behaviours of critical fittings, components and systems in relation to particulars on limits and conditions given in project documentation (from the safety reasons, their robustness's are verified). Special attention is also concentrated to the I & C behaviour and to quality of its reactions to conditions´ changes.

Testing operations shall be authorized by the building authority at the reasoned request of the investor / manufacturer or ordered at the request of the authority concerned or in another justified case. The decision shall specify, in particular, the duration of the trial operation of the technical facility and, if necessary, lay down the conditions, or conditions for the smooth transition of the trial operation to the use of the technical facility.

The investor / manufacturer shall attach the evaluation of the results of the trial operation to the application for the final building approval. Trial operations may only be authorized on the basis of a favourable binding opinion or, where appropriate, a decision by the authority concerned [2,55,57].

2.8. Technical facility commissioning

The requirements for technical facility commissioning are set out in legislation [2]. The applicant for the commissioning needs to 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.

The final safety document needs to contain:

- basic information about the technical facility,
- technical description of the technical facility,
- information about environmental components in the vicinity of the technical facility,
- assessment of the risks of major accidents,
- a description of the principles, objectives and policies for the prevention of major accidents,

- a description of the safety management system,
- a description of the preventive safety measures to limit the occurrence and consequences of major accidents,
- a final summary for safety management,
- namely those legal and natural persons who participated in the preparation of the safety report.

From a professional viewpoint [2,55,57], the 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).

The structure of the safety report is determined by the legislation in force. The safety certificate is summarized in the safety documentation of the technical facility, which we call the safety report for complex technical facility [2,55,57]. It is base document for operation permit issue.

2.9. Summary of important matters

Legal requirements related to the authorisation of final approval decision are codified by the Building Act and related legislation. Because of the focus of the book, they are not the subject of analysis here. We only briefly present important facts:

- the decision on the location of the facility defines the building plot, places the proposed construction, lays down its type and purpose, the conditions for its location, for the processing of project documentation for the issue of a building permit, for the declaration of the building and for connection to public transport and technical infrastructure,
- for technical facilities, a territorial decision with an environmental impact assessment is required for a construction project subject to environmental impact assessment under the Environmental Impact Assessment Act. In a joint permit, the Building Authority approves the construction plan, defines the land for its implementation and lays down the conditions for the location and execution of the building, where appropriate, laydown the conditions for the division or coaling of the land, and, if necessary, also for its use. In the case of a set of buildings, common or specific conditions are laid down for the location and authorisation of the construction of main and secondary buildings in the set of buildings. The conditions shall ensure the protection of public interests and provide, in particular, for other conditional buildings and installations, compliance with general construction requirements or technical standards. As necessary, it shall determine which stages of construction the builder shall notify for the purpose of carrying out inspections of the building site.
- by issuing a building permit, the Building authority lays down the conditions for the construction and, if necessary, for its use. The conditions shall ensure the

protection of public interests and provide, in particular, for other conditional buildings and installations, compliance with general construction requirements, including requirements for barrier-free use of the building or, where appropriate, technical standards. It shall determine, as appropriate, which phases of construction the builder shall notify for the purpose of carrying out inspections of the building; may also provide that the construction can only be used on the basis of final approval. For facilities containing technological equipment for which eligibility for safe use must be verified, compliance with the conditions of a building permit or integrated permit under the specific legislation, the Building authority may impose in a building permit the test operation. In such a case, the period of the test operation shall be discussed with the builder in advance,

- by issuing the final approval decision (operation permit), the building authority shall authorise the operation.

The legislative analysis shows that the Building authority has professional and legal supervision of the safety of the technical facility during the design, construction, construction and testing operation. After the final approval of a technical facility, the State exercises continuous supervision of safety only for technical facilities falling under special laws, namely: Atomic Act, Act on the prevention of major accidents caused by selected hazardous substances or chemical mixtures. In other cases, it addresses the safety of technical facilities only after an accident or failure; no supervision by the State is yet to be carried out on technical facilities falling within critical infrastructure [23].

Due to the complexity of the problem of technical facilities in views of the needs of human society, i.e. the public interest, it is not ideal for human society, so that technical facilities, object and network oriented only on their performance. If public assets and critical assets of a technical facilities are not taken into account, and accidents of failures of technical facilities occur, so the examples in the works [4,7,24] show that there are often losses on human lives inside and outside the technical facility, losses on property, environmental damages and, in the case of critical technical facilities also large economic losses in the territory of a smaller or greater dimension, which are often medium to long-term, i.e. significantly influence the development of human society and the affected territory. Therefore, the management of technical facilities should be taken primarily into account for the prevention of losses [7], which can only be achieved through targeted qualifying risk management.

The principles for quality of technical facility risks´ management need to be inserted in terms of references and in project. They need to be respected during the manufacturing, testing and commissioning. Only by this way it may be ensured safe operation of created technical facility. The work [5] sets out the factors to be monitored in the strategic management of the safety of technical facilities; Figure 9.

Furthermore, the area of production and services depends on technical equipment, operators, conditions and production processes, which are again interconnected open systems. The very condition of the technical equipment depends on the material from which the equipment was made, the method of manufacture and construction, the operating conditions and the way in which it is treated, i.e. the type of equipment. quality and method of maintenance and repair. Figure 10 shows that technical facility management cannot be focused solely on the performance of technical equipment, but it is also necessary to ensure the management of risks in public interest.

In the case of technical fittings, components and whole technical facilities, this is about ensuring their safety in an integral sense, which can only be achieved by purposefully managing all priority risks, including:

- the risks associated with the material from which they were made,
- risks associated with the architecture of technical equipment, their control, etc., whose resources are diverse, and therefore, they are required specific methods and approaches at work aimed at managing risks [4,5,7,24].

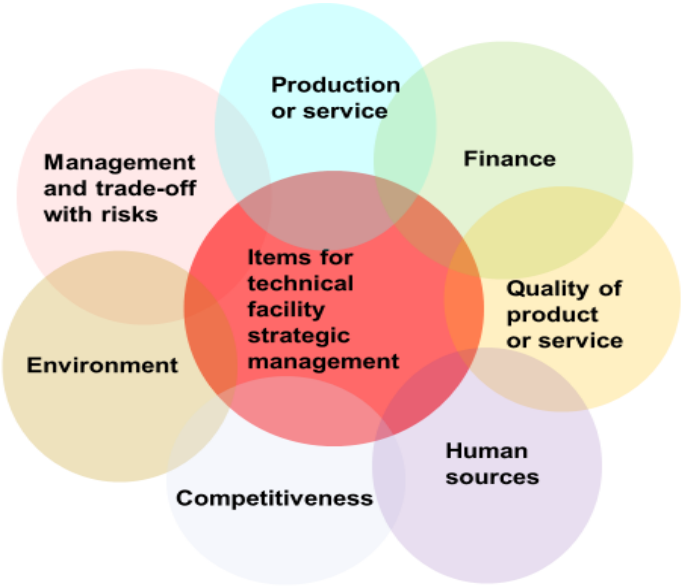

Figure 10. Items that need to be followed in strategy management targeted to technical facility safety.

In order to ensure the integral safety (i.e. overall safety of the technical facility), the care needs to be also paid to the safety of sub-parts, i.e. risks of subparts need to be also managed. The principles need to be inserted into technical facility project and in instructions for technical facility operations; according to legislation the designer is forced for very detail and precise technical description of ways of mastery of equipment, components, systems and whole technical facility at normal, abnormal and critical conditions.

According to [7,24] and experience from practice, it is advisable to use a five-step scale when assessing the criticality of a technical fitting:

- very good condition of technical equipment: the technical equipment is in perfect physical condition and performs thoughtful functions. Maintenance costs are in line with norms and standards. The technical equipment is new or has recently been restored. The requirements for the operation of the technical equipment correspond to the project, the operational problems of the technical equipment are not. All program is implemented efficiently and efficiently,
- good condition of technical equipment: the technical equipment is physically in good condition and performs thoughtful functions. The maintenance costs of technical equipment are in line with norms and standards, but they are growing. The technical equipment is about half its service life. The requirements for the operation of the technical equipment correspond to the project, the operational problems of

the technical equipment are only occasionally. All programme is implemented in an acceptable way,

- acceptable condition of the technical equipment: the technical equipment shows signs of wear and lower performance than thought. Some parts of the technical equipment are inadequate. The maintenance costs of technical equipment exceed the amounts set by norms and standards and increase. The technical equipment has long been used or worked in adverse conditions and is therefore at the last stage of its service life. The requirements for the operation of the technical equipment correspond to the project, the operational problems of the technical equipment are common. All programme is mostly implemented, but there are ineffective and inefficient,
- poor condition of technical equipment: the technical equipment shows significant signs of wear and performs thoughtful functions at a low level. Many parts of the technical equipment are inadequate. The maintenance costs of technical equipment significantly exceed the amounts of norms and standards. The technical equipment is close to the end of its life. The requirements for the operation of the technical equipment exceed the data in the project, the operational problems of the technical equipment are obvious. All programme is implemented only to a very limited extent,
- critical condition of technical equipment: the technical equipment is in poor condition and does not work as it should. There is a high probability of failure. The cost of maintaining technical equipment is highly unacceptable compared to norms and standards, the reconstruction of technical equipment is not cost-effective. An exchange is required. The requirements for the operation of the technical equipment are significantly higher than those in the project; operational problems of the technical equipment are serious and permanent. The specified programme is not fulfilled.

When working with risks, the risk should be identified, analysed, evaluated, assessed, managed and dealt with in favour of the stated objective; there are a number of factors in a complex world that determine the size of the risk [5]; Figure 7 above shows the factors that decide on the relationship between risk and safety of the technical facility.

An essential role in working with risks plays risk assessment, and mostly available data for its implementation [90] plays. The risk assessment is a process that is an essential component of management and regulation of technical facilities and an important component of decision-making, and therefore, its accuracy and credibility are important. Its feasibility needs to be inserted in the project and critical fittings, components and systems need to have sufficiently robustness, redundancy, inventiveness and speed (Figure 6), so expected priority risks might be mastered by professional ways, i.e. without dangerous impacts on assets of technical facility and public assets.

3. RISK ENGINEERING METHODS

Both logical methods, i.e. analysis, synthesis, deduction, evaluation and assessment, as well as the specific heuristic methods described in [1,5,61] are used to obtain the results of the presented monograph. At this point we will give only the methods on which the following results are based. These are: what, if, checklist, fishbone graph; case study; decision support system; and a risk management plan.

3.1. What, If

The What, If method is the most general method for detecting the impacts of a disaster by which the risk of a disaster can be determined. We use it in the form of filling the table; Table 1 [1,5,61] using the data from experts obtained by brainstorming or panel discussion.

Table 1. Standard model for applying the What, If method.

Asset		**The potential impact of a disaster on an asset**
Human lives and health		
Human security		
Property		
Welfare		
Environment		
Infrastructures and technologies		
	Energy supply sector	
	Water supply sector	
	Sewerage sector	
	Transport sector	
	Communication and information sector	
	Bank and finance sector	
	Emergency services	
	Basic territory services (industry, agriculture, supply service, health service, waste	

	management, social services, funereal services)	
	Public administration	
Technical facility: - critical fittings - critical components - critical links - critical infrastructures - critical couplings - critical stocks - critical personnel - critical processes management - ……..		

3.2. Checklist

The checklist is an engineering discipline tool that allows a multi-criteria assessment of the nature of the problem being observed [1,5,61]. Checklists are aimed at risk or safety of a technical facility and they are an essential tool for managers because they clearly identify risks in areas that are well-known and for which the development of knowledge and experience are defined by the limits of individual activities, actions, behaviours, etc. To ensure safety and development, it is necessary to eliminate the immediate, evident and recognizable risks. For their identification, the checklists serve very well. Then, it is necessary to reveal and to cope with the risks that are hidden in the chains of possible events, delayed in time using the specific methods and specific and qualified data.

3.3. Ishikawa (Fishbone) diagram

Fishbone diagram (Ishikawa diagram) is a tool used at causal analysis of the observed problem [1,5,61]. The cause-and-consequences analysis helps to thoroughly understand the nature of the problem by forcing us to address all possible disaster causes. The procedure for its application is:

- identification of the problem (it means to answers to the questions:
  - where does the problem occur?
  - what is the nature of the problem?
  - when did it occur?

- how often did it occur?

- enumeration of significant problem factors (factors are fish bones),
- identification of possible causes (small lines on 'fish' bones),
- diagram analysis.

To create a diagram, it is necessary to collect and organize data about the causes that cause the problem and their impacts. This means that the processes associated with the problem to be solved need to be described in detail by data, while the random and knowledge uncertainties [1,5,61] need to be clarified. Collecting the data is a first step and is time and knowledge consuming, as many resources need to be used to make the data files representative [1,5,61,90], i.e.:

- to be complete,
- to contain the correct particulars,
- to have sufficient particulars number,
- particulars need to be spread homogeneously throughout the observed interval and to be validated.

The tool under review supports the analysis of the causes and consequences of a particular process, phenomenon, objects and facilitates the search for solutions to the problems that have arisen. The aim of the method is to identify all possible causes or sources of the problem (or areas that affect the problem) and to structure them graphically.

The problem-solving organizer draws a "fish skeleton". In a group discussion, the consequences are placed on the respective skeleton sites according to their kinship and then causal chains of causes and consequences are searched for on the basis of discussion (brainstorming). The method can be used, for example, in the creation of objects or department concepts, in identifying the starting state (condition) and in defining the starting points. Data that can be detected with considerable effort by routine data collection or measurement can also be quickly obtained. However, the knowledge and experience (i.e. qualifications) of the discussers is a drawback of the method; further details are in [61].

3.4. Case study

A case study that relates to a specific decision, is associated with certain work models or simulations of processes that take place over time and territory or in an entity. The case study describes and justifies the real experience gained from life in the subject area, thus broadening the knowledge of the problem and its aspects. The quality of the case study, i.e. the quality of the results presented in the case study, is based on the knowledge and life experience of the case study processor [61].

The case studies are based on both qualitative and quantitative data. Their result is a qualified locally and time-specific solution to a particular problem / case, and therefore, they are a suitable tool to support decision-making and management at the site. They are used when the knowledge of the problem in the system conception is unstructured, i.e. in connection with the problem in which for a number of elements, links and flows

of the assessed system there are not only uncertainties that can be assessed by mathematical statistics, but also vagueness (epistemic / knowledge uncertainties), the estimation of which requires highly qualified data sets and demanding theoretical procedures. In other words, the problem and context data in the system in question do not meet the requirements for a generally valid solution. Therefore, either expert methods or case studies are used in these cases [61].

The case study methodology is, according to the knowledge gathered in [1,5,61], a tool to obtain a set of knowledge about the problem. It combines theory with practice while requiring the practical skills: identifying and recognizing the problem; understanding and interpreting the data and information; distinguishing the facts from the assumptions; analytical and critical thinking; understanding the random and epistemic uncertainties (data is never complete); improving the judgment; ability to communicate issues with experts with a different opinion. It is a problem-solving technique under various conditions (therefore, multi-criteria analysis of the system and its surroundings is important). It allows to solve unstructured problems, which are almost all failures and all complex systems accidents. It does not assume random distribution of solution variants [61].

It is de facto a historical scenario of a process, i.e. a model of the course of a certain process that takes place under specific conditions, i.e. at a certain place and at a certain time. From a methodological point of view, it is a process model that is compiled on the basis of real data. It is used in project and process management, if the knowledge of the problem in the system conception is unstructured, i.e. in connection with a problem in which many elements, links and flows of the assessed system are not only random uncertainties that can be assessed by mathematical apparatus. statistics, but also knowledge uncertainties, which require highly qualified data sets and demanding theoretical procedures. In other words, the problem and context data in the system in question do not meet the requirements for a generally valid solution.

The processing of a case study, as well as the processing of an expert opinion, requires both, the multidisciplinary and the interdisciplinary theoretical and practical knowledge, at least in the field of management and systems safety management, as well as considerable practical experience. In addition, it teaches justifying decisions to solve a problem.

In original monograph [2], they are used two forms, namely the evaluation case study and the prognostic case study. The evaluation study evaluates the potential risks and their impacts on the safety of the technical facility being prepared in a specific territory. When compiling it, the following questions are used:

1. What is the problem of the proposed technical facility and its surroundings?
2. What are the aspects and impacts of the problem on the conditions and development of the proposed technical facility and its surroundings?
3. What is the root cause of the safety damage of the proposed technical facility and its surroundings?
4. How could be averted the accident or failure of proposed technical facility and its surroundings?
5. What should be done to prevent a proposed technical facility and its surroundings from occurring safety the damage of during the lifetime?

Process of case study compilation is in Figure 11.

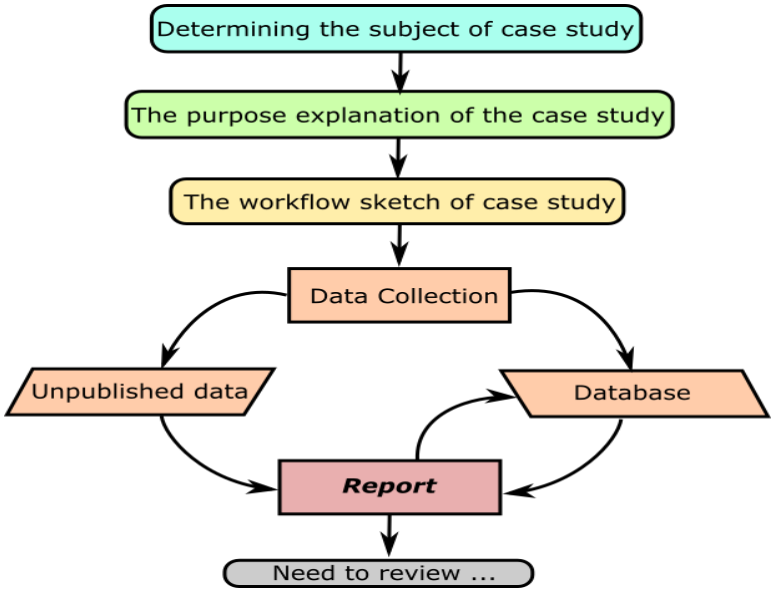

Figure 11. Process of case study compilation.

3.5. Decision support System

The Decision Support System (DSS) [1,5,61] is a special technique for obtaining data for deciding the complex problems. It generally consists of the following components: data management module; model of management modules (model library); module for management of dialogue with user; and knowledge core (Knowledge engine). There are different DSSs, or they have different conceptual starting points:

- model-based DSS (it using statistical simulation),
- communication DSS (it is for cooperation on a number of decisions),
- document DSS (it uses different types of documents to support decisions),
- knowledge DSS (it contains defined rules).

The decision support system (DSS) helps to solve the problem by supporting an analytical style of decision making against heuristic decision making. This means that:

- it organizes information for decision-making situations,
- it interacts with the decision-maker at various stages of decision-making,
- it extends the information horizon of the decision-making body,
- it facilitates multi-criteria evaluation, because it has built-in multi-criteria methods without the user knowing their mathematical structure.

Decision support systems use a general model for the certain case, reflecting the real situation. When specific parameter variables are substituted, they provide results for the given problem. The aim is to ensure that the result corresponds to the optimal solution. In their creation and application are used:

- knowledge and data from experts who know the technical parameters, limits and conditions of the technical facility and the local vulnerabilities,
- the principle of maximum utility theory [91], i.e. "the greater, the better" or "the greater, the worse".

Decision support systems are divided into special ones that provide support for solving the specific problems; and general, which are based on adaptive and flexible decision-making models. Obviously, the use of a specific DSS is only possible when verification establishes that the conditions for technology transfer are met [92]. Otherwise, the method needs to be adapted to local conditions. It should be noted that the adaptation of the method to specific conditions cannot be done by IT specialists, but by technical experts, who know the technical parameters, limits and conditions of the technical facility and local vulnerabilities.

Applications of sophisticated DSS based on multi-criteria evaluation give good solutions. In our case, we will compile a DSS in the form of a checklist [1,5,61] supplemented by a rule for evaluating questions in terms of [92] and assigning a logical value scale.

DSS application aims are:

- identifying, managing, eliminating or minimizing the unforeseen events that have adverse impacts on critical elements, critical components, critical processes, critical functions, critical infrastructure and critical technologies in the technical facility,
- the process of comparing the estimated risks against the benefit and / or cost of possible countermeasures and establishing an implementation strategy in the context of integral (systemic, overall) safety,
- determining:
    - to which disasters (harmful phenomena) is the technical facility exposed,
    - what are the risks from individual harmful phenomena,
    - what damage may arise,
    - which measures will eliminate or minimize the occurrence of harmful events,
- the procedure consists of:
    - the assets are defined and their safety requirements are defined,
    - identification of vulnerabilities, potential impacts and risks,
    - estimated: the amount of potentially caused damage; and the cost of appropriate safety measures,
    - adequate safety measures are selected.

For critical items, limit values (limits) shall be established to ensure acceptable security. This means that the task of their managing is to ensure compliance with the limits, and therefore, the basis is thorough monitoring and qualified DSS.

3.6. Scoring the variables using the decision matrix

The method of scoring the variables according to [1,5,61] makes it possible to classify the problem described by two mutually incommensurable variables into several categories according to established preferences. The method itself does not set or recommend classification criteria. In practice, it is very often used to classify risks into acceptable, conditionally acceptable and unacceptable risk [1,5,61] or to categorize objects according to their criticality [4,21,34]. The method will be further used to assess the benefits and risks of the proposed technical facility.

3.7. Risk management plan

The risk management plan is based on the TQM facility management method [63], i.e. in the monitored facility they are considered priority risks that could not be settled and that have the potential to significantly damage a technical facility at their realization. The plan itself is drawn up in the form of a table [1,5] that considers the risks of:

- technical facility,
- internal sources of risk of the technical facility related to its construction, construction, equipment and operation,
- technical facility personnel,
- external sources of risk of technical facility associated with natural disasters,
- external sources of technical facility risks related to public administration behaviour, competition, market, etc.,
- attacks on technical facility,
- cybernetic risk sources associated with networks,
- war.

For each risk area, the table shall indicate:

- causes of risk,
- the probability of risk realization occurrence and the expected sizes of the impacts of the risk on the protected assets (basic public assets should also be considered based on legislative requirements),
- risk management measures, or at least for risk mitigation, which are clearly identified, and at each of them it is given responsible person for their implementation.

The risk management plan is also recommended by ISO 31000 [93].

To develop a risk management plan that meets the management requirements required by the TQM, it is necessary to know in detail:

- disasters, i.e. sources of risks,
- local vulnerabilities that determine the severity (criticality, relevance) of critical situations,
- and ways and possibilities of response to critical situations.

As is has been shown, that the risks are associated with itself work with the risks, a checklist (Table 2) for assessing the criticality of the risk management plan has been developed and tested in practice; the scale of which was used to assess each item:

0 point - fulfilment of the criterion has negligible shortcomings in the monitored area (less than 5%), i.e. it has negligible criticality,

1 point - fulfilment of the criterion has low deficiencies in the monitored area (5-25%), i.e. it has low criticality,

2 points - fulfilment of the criterion has medium deficiencies in the monitored area (25-45%), i.e. it has medium criticality,

3 points - fulfilment of the criterion has high shortcomings in the monitored area (45-70%), i.e. it has a high criticality,

4 points - fulfilment of the criterion has very high deficiencies in the monitored area (70-95%), i.e. it has a very high criticality,

5 points - fulfilment of the criterion has extremely high deficiencies in the monitored area (higher than 95%), i.e. it has extremely high criticality.

Table 2. Checklist for judgement of quality of risk management plan.

Question	**Rating**
Is the risk management plan guided by a clear vision and the objectives pursued?	
Does the risk management plan apply the principle of integrity (i.e. consideration of the welfare of the social, ecological and economic subsystem; expression of costs and benefits; impacts and benefits of economic activity using the both, the monetary and the non-monetary values)?	
Are substantial elements considered in the risk management plan (e.g. fair distribution of resource use between present and future generations; over-consumption and poverty; human rights; environmental conditions conditional on life; prosperity permitted by economic development and off-market activities)?	
Is the risk management plan adequate in scope (e.g. appropriate time and space measure)?	
Is the risk management plan practically focused (e.g. explicitly defined categories that link the idea with indicators and criteria; a limited number of key objectives; a limited number of indicators; a standardized way of measuring and benchmarking; benchmark values, thresholds, development trends)?	
Is the risk management plan open (e.g. generally accepted methods and databases; explicit plausibility, elimination of uncertainty)?	
Is effective risk management communication included in the risk management plan?	

Is the general public involved in the risk management plan?	
Does the risk management plan provide for a follow-up assessment (e.g. specifying the progressive targets due to system development)?	
Are the institutions' capacities ensured in the risk management plan (e.g. identification of responsibility for meeting the decision-making process objectives, data collection and storage, documentation)?	
TOTAL	

The scale for overall criticality of the risk management plan is determined in analogy to the principles used since the 1980s in technical standards. The resulting criticality rate, assuming all criteria have the same weight, can range from 0 to 50; the thresholds for the criticality level of the risk management plan corresponding to the scale used are given in Table 3.

Table 3. Value scale to determine the level of criticality of the risk management plan.

Criticality rate of the risk management plan	**Values in %**	**Number of points for all criteria**
Extremely high– 5	Over 95 %	Over 47.5
Very high – 4	70 - 95 %	35 – 47.5
High – 3	45 - 70 %	22.5 – 35
Medium – 2	25 – 45 %	12.5 – 22.5
Low – 1	5 – 25 %	2.5 – 12.5
Negligible – 0	Less than 5 %	Less than 2.5

4. RISK SOURCES

For research, it was compiled the original database of technical facilities accidents and failures [49] from world data collecting from sources given in [2]. In last cited publication several case studies are shown in great details. 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. [61]. Their results were critically assessed and separated into classes according similarity of causes. By this way we create the basis for Decision Support System enabling to multicriterial assessment of possible technical facility risks [2]. 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 causes of stage specific technical facilities failures and accidents in database [49] 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 the design, manufacturing and commissioning are omissions, errors and deficiencies in:

1. Designing the technical facility:
    - errors in terms of references, e.g.:
        - not used the All Hazard Approach,
        - incorrectly determined hazard sizes of disasters,
        - not applied defence-In-Depth principle,
        - further ones in [2],
    - errors in the project, e.g.:
        - 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,
        - wrongly used principles of inherent safety,

  - further ones in [2],
- 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,
  - further ones in [2],
- the non-determination of critical building sites, which led to omission of measures for risk management towards safety at:
  - normal operation conditions – as barriers, on the basis of an assessment of the risks to their safety, i.e. barriers, backups,
  - 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, back-ups,
  - critical operation conditions – as barriers, on the basis of an assessment of the risks to their safety, i.e. barriers, backups,
- not to identify 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,
- not 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 building, construction and assembly, etc.
    - 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;
    - and 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 construction of technical facility - 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,
    - used poor design of tight connection screws,

- faulty welds,
- false work schedule, 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),
   - 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 manufacturing - 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 or investor over design and manufacturing - 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 respects,
   - 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,
   - during phase realization the occurrence of disasters as: earthquake; landslide; flood; fire; corruption; insider.

The causes of the coexistence disruption caused by a technical facility by a faulty implementation of the design, construction and commissioning process of the technical facility are illustrated in Figure 12.

Above listing the causes of accidents and failures and Figure 12 show that great role in risk sources plays the human factor manifestation, namely at organization and management (i.e. it goes on organizational accidents). The human errors at designing, commissioning and manufacturing were summarized in Chapter 2; the heaviest errors are some errors in designing or in terms of references; e.g. selection of bad ground conditions or low robust concrete fundament under heavy rotative machine or weak anchor of heavy tall machines and tall narrow buildings [49].

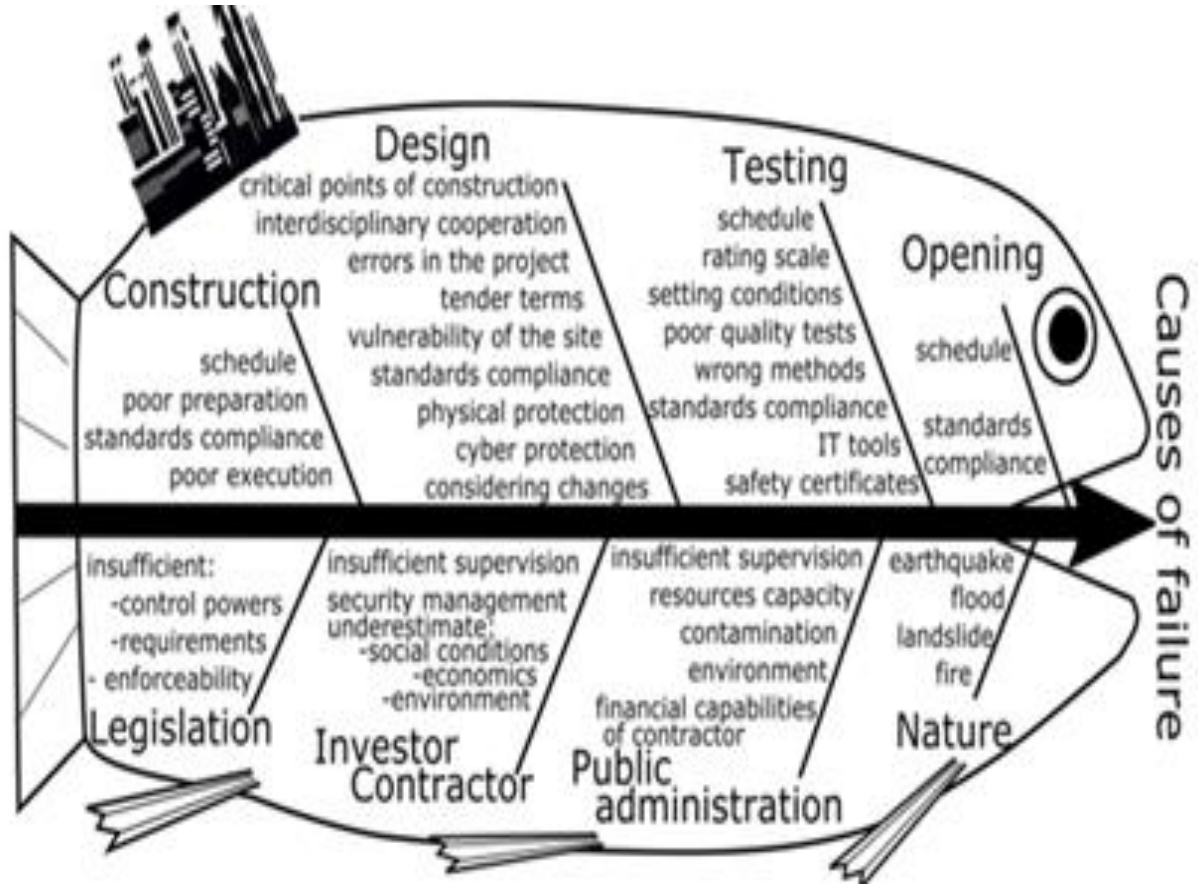

Figure 12. Basic categories of risk sources associated with the technical facilities design, building, construction, testing and commissioning which lead to the failures of coexistence of technical facilities with surrounding areas during their operation.

5. TOOL - DECISION SUPPORT SYSTEM FOR ENSURING THE COEXISTENCE AT TECHNICAL FACILITY DESIGNING, BUILDING AND COMMISSIONING

In order to ensure the safe technical facilities during their design, construction and commissioning, it is, therefore, necessary to assess the possible risks for the technical facilities also from the perspective of the dynamic development of the technical facility and its surroundings including the material wear and tear due to working load and conditions Therefore, to this task solution, it is necessary to use both, the historical data and the models of possible processes based on predictive case studies or analogies in similar technical facilities and expected working conditions [4,7,45].

From the point of view of knowledge for projected and manufactured technical facilities, it goes on:

- determining the size of the priority risks, which can be properly influenced in the given phase from the point of view of safety and coexistence of the technical facility with its surroundings throughout the lifetime of the technical facility,
- categorization:
    - acceptable risk,
    - conditionally acceptable risks for which the necessary preventive, mitigating, reactive and recovery measures need to be proposed,
    - and unacceptable risks that need to be either removed, where possible (e.g. selection of other material, other technology, etc.) or reduced by other measures that mitigate their occurrence frequencies or their impacts as insertion of:
        - inherent safety principles, safeguards, barriers, etc.,
        - systems and equipment that ensure effective response to critical situations (e.g. shower systems, fire extinguishers etc.),
        - requirements that they need to be respected during the operation, and therefore, they need to be properly given in technical facility safety documentation. During the operation they will create the ground for emergency and continuity plans [7]. Due to problem complexness, it is adjured to apply higher knowledge, higher technical equipment, higher costs, higher human resources readiness, so to reach safe operation.

When establishing the criteria for assessing the risk associated with a technical facility, provided that the coexistence of the technical facility with the surroundings needs to be ensured throughout the lifetime of the technical facility, as shown in Figure 1, we consider both, the risk management principles outlined in the work [4] and the responsibility principles, which are common in Europe [94], which means that responsibility for the safety of a technical facility, i.e. for the level of work with risks associated with a technical facility safety, lies at the time of design, construction, testing and commissioning on both, the investor (including the designer and manufacturer) and the public administration that is obligated for supervision in the frame of public interest. This requirement is logical also because the problems of the technical facility mean not only

the loss of products or services, but also the loss of taxes for public administration, expenditures caused by unemployment and other social problems, e.g. also increased crime.

With regard to the requirement of the most legislations, which considers two milestones:

- granting a building permit on the basis of project documentation of a technical facility,
- issuance of the final permit or operation permit allowing the permanent operation based on the documentation for the technical facility operation,

we divide the coexistence level assessment based on safety assessment (or risk assessment) into two cases. The first one is kept as a basis for granting a building permit and the second one as a basis for final approval of operation – i.e. the operation permit. In both cases, tools are designed so that both, the investor (i.e. also the designer and the manufacturer) and the public administration can use them. In the face of facilitating the reader understanding the procedure, some of tables are repeated.

5.1. DSS for building permit

Based on the collected knowledge, it was constructed the Decision Support System – DSS for the evaluation of risks associated with the proposed technical facility [2]; Table 4. The criterions are evaluated by scale (0-5) with the philosophy “the higher number, the higher risk, i.e. the lower technical facility coexistence with the surroundings” [91]. For the DSS application in practice, they are processed two scales, namely the auxiliary scale in Table 5 derived in [95], and the second scale for the evaluation of the entire checklist based on the principle that was introduced into technical standards in the 1980s, Table 6.

The assessment of Table 4, hereafter given, assumes that all criteria have the same weight. Practical examples [49] show that in many cases some criteria are more important than others, and therefore, it is necessary to assign them higher weight, and to change data in Table 6 by appurtenant way. It means that the procedure is site and sector specific.

Table 4. Checklist for assessing the risk connected with coexistence of the proposed technical facility and its surroundings for needs of Building permit; A – assessment; number of criteria n = 32; N – note.

Criterion	**A**	**N**
The rate in which the terms of references of the technical facility are processed by a legal entity which has: - 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 and failures; methods of analysis, management and settlement of risks;		

management of the enterprise (finance, human resources, organization, technology, innovations...), - knowledge and capabilities for: the application of the results of methods of risk analysis and evaluation; implementation of the methodology for analysing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; the transformation of policy into actual action; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; finding the right information and learning; critical analysis; designing the right solutions; written and spoken communication; carrying out the synthesis; and adapting the wording intended for the public, - ethic.		
The rate in which the terms of references of the technical facility have clearly defined assets and include public assets.		
The rate in which the terms of references of the technical facility consider the impacts of disasters that are possible in the territory under the All-Hazard-Approach.		
The rate in which the terms of references of the technical facility are based on well-defined hazards to all disasters that are possible in the territory and have harmful potential; e.g. in the case of natural disasters due to the sparse and irregular occurrence of large phenomena, historical data need also to be used. In particularly serious disasters, it is not only limited to probabilistic approaches and it is complemented by the results of appropriate methods that have the ability to detect extreme phenomena.		
The rate in which the terms of references of the technical facility consider local vulnerabilities and, where is necessary also regional ones: - anomalies and non-homogeneity of geological structure, - large number of inhabitants, - reality that in territory there are hospitals, schools or other public buildings nearby, - reality that in territory there are sources of domino effects, i.e. warehouses or product lines with hazardous substances, fuel stations, etc. - reality that in territory it is insufficient capacity of energy sources, - reality that in territory it is insufficient capacity of water sources, - reality that in territory it is insufficient capacity of wastewater drainage (sewerage), - reality that in territory it is lack of transport service, - reality that in territory it is protected nature reserve.		

The rate in which the terms of references of the technical facility consider all risks associated with major disasters and all vulnerabilities in the territory.		
The rate in which the terms of references of the technical facility clearly define the fittings and systems for which risks need to be addressed in order to ensure: - reliability, - security - safety. According to the specified objective, they set the limits and conditions for the operation of the fittings and systems and their reserves in sufficient number.		
The rate in which the terms of references of the technical facility are assessed by qualified experts.		
The rate in which the technical facility project considers the results of the expert assessment of the terms of references.		
The rate in which the technical facility project is organized clearly so that it would be possible to simply control the technical facility and have a safety management system.		
The rate in which the technical facility project respects the size of the criticality associated with priority disasters (a combination of hazard size, vulnerability and sizes of impacts on assets), including the human failures, and proposes measures to ensure safety; at the same time it is based on an assessment of whether the proposed measures cannot be a source of new dangers and where they cannot be dealt with (e.g. ignorance or too much costs), it proposes technical measures, in management systems organizational ones.		
The rate in which the technical facility project considers protecting the public assets and technical facility assets.		
The rate in which the technical facility project is based on valid legislation and standards. It goes on a selection of materials, selection of computational methods, design of technical principles and procedures in building, construction and assembly, as well as commissioning.		
The rate in which the technical facility project used in cases that are not codified by standards approaches of good practice in building, construction and assembly.		
The rate in which the technical facility project when selecting and joining equipment with regard to safety, follows the requirements of: durability; manageability; service life; human resources; costs; technical utilities; and service.		
The rate in which the technical facility project with regard to safety uses: principles of inherent safety; passive safety systems; active safety systems; procedural procedures that are proven or thoroughly		

tested in such a way that they do not contain latent sources of danger under possible conditions.		
The rate in which the technical facility project with regard to safety has measures that triggers the emergency shutdown of critical devices and it reassign to a safe state, e.g. systems with emergency disconnection or stopping the reaction.		
The rate in which the technical facility project establishes critical processes of building or construction and proposes measures to reduce their criticality. It contains technical and organisational measures to ensure sufficient resilience.		
The rate in which the technical facility project proposes, in accordance with the terms of references, requirements for equipment and systems for which risks need to be addressed in order to ensure: - reliability, - security, - safety.		
The rate in which the technical facility project is based on a proper assessment of the risks targeted at the safety of the entire technical facility.		
The rate in which the technical facility project is based on the system concept of technical facility and its surroundings, and therefore, in ensuring the safety of all assets, it considers linkages and couplings between assets, both in demand and not-demanded and in the light of the management of unacceptable interconnections that can be expected when conditions are very different from normal ones, has an arranged architecture to allow Defence-In-Depth protection access to be applied in control.		
The rate in which the technical facility project considers critical sites of building structure and includes the right measures based on an assessment of the risks targeted to their safety, i.e. to ensuring the reliability and operation ability under abnormal and critical conditions (barriers, reserves, back-up).		
The rate in which the technical facility project considers the critical sites of technology and production processes, and shall take measures on the basis of an assessment of the risks directed to their safety, i.e. to ensuring the reliability and operation ability under abnormal and critical conditions (barriers, reserves, back-up and principles for safety upgrade).		
The rate in which the technical facility project considers highly critical fittings (pressure vessels, pressured pipes – especially those with highly hazardous substances) and for ensuring their safety it uses special measures, special protection systems (safety systems and safety related systems) and proposes specific limits and conditions for operation.		

The rate in which the technical facility project considers all risks associated with major disasters and all vulnerabilities in the territory in the systemic concept (i.e. the risks associated with the interconnections demanded, both permanent and temporary, and even non-demanded, which may occur only under certain conditions (e.g. at external disasters or operator errors or insider attacks). It contents appropriate technical and organisational measures to reduce the potential impacts.		
The rate in which the technical facility project pays from ensuring the safety and performance reasons special attention of the management system. The control system in the form of manual, semi-automatic and automatic based on IT is hierarchical and risk-based, possibly under normal, abnormal and critical conditions – it is more level-level and respects the Principle of Defence-In-Depth. It also includes proposals for measures to manage emergency and critical situations.		
The rate in which the technical facility project contains technical measures for physical and cyber protection of the technical facility.		
The rate in which the technical facility project considers the property rights of third parties; possible changes in the laws or system of taxes and market situations (e.g. it is dangerous to rely on the supply of critical items by only one supplier) during the making of a technical facility, and for these cases it contains reserves to reduce any causes thus created future losses and damages.		
The rate in which the technical facility project contains financial costs of the production of the technical facility are adequate.		
The rate in which the public administration has ensured an assessment of the technical facility project required by the legislation in force.		
The rate in which the technical facility project considers the results of professional assessment of the technical facility project by experts.		
The rate in which the technical facility project considers results of the public's comments on the technical facility project.		

Table 5. Auxiliary scale for determination of rate of risk that planned technical facility means for its surroundings (rate of coexistence disruption); by analogy to scales in [95]; p – annual insurance, ABT-the annual budget of territory governance.

Domain	**Risk rate**	**Classification criterion**
Social	*By accident or failure of technical facility, it is affected:*	
	0	less than 50 humans
	1	50 - 500 humans
	2	500 - 5000 humans
	3	5 000 – 50 000 humans
	4	50 000 – 500 000 humans

	5	more than 500 000 humans
Technical and Economic	*Accident or failure of technical facility causes damages:*	
	0	less than 0.05 p
	1	equal to p
	2	between p and 0.05 ABT
	3	between 0.05 ABT and 0.075 ABT
	4	between 0.75 ABT and 0.1 ABT.
	5	higher than 0.1 ABT.
Environment	*Accident or failure of technical facility causes:*	
	0	very low damages of environment
	1	damages of environment with which the nature cope during the acceptable time
	2	moderate damages of unrenewable resources of nature and natural reservations.
	3	medium damages of unrenewable resources of nature and natural reservations
	4	unreturnable damages of unrenewable resources of nature and natural reservations
	5	devastation of landscape, unrenewable resources of nature and natural reservations

Table 6. Value scale for determining the rate of the coexistence of the planned technical facility and its surroundings; N = five times the number of criteria in Table 4; N = 160.

The level of coexistence disruption (risk) between technical facility and surrounding	**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 %

The evaluation of real cases according to the Table 4 needs to be performed by a team of specialists from the different fields independently; in practice, according to [23,95], it works the team consisting of:

- worker of public administration responsible for the land use planning,
- worker of public administration responsible for the territory development,
- representative of planned technical facility,
- competent representative of the professional institution for the technical facility safety assessment, for example from the state technical inspection,
- and representative of the Integrated rescue system.

The resulting value is the median for each criterion, and in cases of great variance of the individual values in the one criterion it is necessary, so that the worker of public administration responsible for land use planning may ensure further investigation, on which each assessor shall communicate the grounds for his / her review in the present case, and on the basis of panel discussions or brainstorming session, the final value is determined.

The appreciation of the benefits of a technical facility for the territory is done again using a checklist. On the basis of the knowledge gathered above, a checklist is drawn up to assess the contribution of the technical facility to the territory [2], Table 7. The criterions are evaluated by scale (0-5) with the philosophy “the higher number, the higher risk, i.e. the lower technical facility coexistence with the surroundings” [91]. For application in practice they are processed two scales, namely the auxiliary scale in Table 8 derived in [95], and the second scale for the evaluation of the entire checklist based on the principle that was introduced into technical standards in the 1980s, Table 9.

Table 7. Checklist for assessment of the technical facility return for territory. A- result of assessment; number of criteria n = 10; N - note.

Planned technical facility	**Criterion**	**A**	**Note**
	It increases education of the population in the territory		
	It increases the possibility of employment of the population in the territory		
	It increases the level of services in the territory		
	It increases welfare in territory		
	It contributes to the development of basic infrastructure in the territory.		
	It raises the prestige of the territory		
	It contributes to the cultural development of the territory		
	It improves the situation in the social sphere in the territory – Table 8		

	It improves situation in technical and economic spheres in territory - Table 8		
	It improves the situation in environment protection and welfares in territory - Table 8		

Table 8. Value scale for determining the rate of benefits that the technical facility means for the territory; it is designed by analogy to the scales set out in the work [95], ABT – the annual budget of the territory.

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

Table 9. Value scale for determining the rate of return of the technical facility for its surroundings; N is quintuple of criteria in Table 7 (N=50).

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

At the technical facility risk management based on data in Table 9 we consider the responsibility principle that is general in Europe [94]. It means that in the followed technical facility phase both, the developer and the public administration are responsible for the technical facility safety.

Considering:

- the ALARP principle as in works [94,96-98],
- the integrated approach as in works [99,100],
- and the assumption that all risk sources have the same occurrence probability, we obtain the requirement for tolerable risk (with respect to the UN and the Swiss Re [24] limits) measured by the technical facility maximum annual losses ***RZTD***

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

where ***HTD*** is the technical facility utility value given in technical facility document (official approved budget for designing, manufacturing and commissioning), $\boldsymbol{k_i}$ are result evaluations of risk sources in Table 4, *n* is the number of risk sources (in our case 32) and ***T*** is the technical facility lifetime in years. When this condition is not fulfilled, so the proposed technical facility may not be accepted for realisation because the coexistence will be violated. It means that either a new option or other risk reduction measures should be requested, followed by a further assessment of the proposal. In other case the evaluation process continues.

In order that the losses caused by the technical facility at its operation might be also acceptable for the territory, it is calculated the benefit that the technical facility operation gives rise to territory. Using the data in Tables 7 - 9 and the principles for expected return [101] and the same assumptions on data processing as in the previous case, the expected annual technical facility return caused by the technical facility operation ***PRZTD*** is

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

where ***CPTD*** is the total utility technical facility return during the lifetime ***T***, $\boldsymbol{k_i}$ are result evaluations of return sources in Table 7 (assessed by experts with help of data in Tables 8 and 9) and ***n*** is the number of benefit sources (in our case 10). The expected pure annual technical facility return ***RPTD*** is given by

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

where ***A*** is annuity and ***RPNTD*** is operating costs. Difference ***R*** of allowed maximum annual technical facility losses ***RZTD***, Eq. (1), and of expected pure annual technical facility return ***RPTD***, Eq. (3)

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

is used as the quantitative property for decision-making. They are used the boundaries of acceptability of risk that used the UN and the Swiss Re [24], namely:

- amount of annual premium for protected assets in territory (***PRTD***),
- one-tenth of annual territory budget (***ABT***).

On the basis of results of scoring, they are determined the categories to which in a given case, the risk associated with technical facility belongs:

R is less than PRTD, risk is acceptable,

R is between PRTD and 0.1 ABT, risk is conditionally acceptable,

R is higher than 0.1 ABT, risk is unacceptable.

In the first case, the technical facility benefits will outweigh the technical facility disadvantages, it means the expected losses are acceptable and the coexistence of the technical facility with its vicinity is ensured. It can be done building permit for the technical facility realization.

In the second case, the effective technical facility safety management is required; it means to include additional preventive measures in the technical facility design and to ensure the mitigation, reaction and renovation measures for coping with risk realization.

In the latter case, unacceptable risk, it should be thorough reflection on conclusion – either to reject the proposed technical facility variant, or to ask for further measures associated with an increase of technical facility safety (it is necessary to require application of: higher knowledge; a better technical equipment; the higher costs for protective systems; ensuring the greater human resources readiness, etc.) and after this new coexistence judgement.

The tool was tested in five real cases with success. The tests showed that it is pernickety on expert knowledge and moral, however, it ensures the coexistence the technical facility with its vicinity during the technical facility lifetime.

5.2. DSS for operation permit

Based on the collected knowledge, it was constructed the Decision Support System – DSS for the evaluation of risks associated with the proposed technical facility [2]; Table 10. The criterions are evaluated by scale (0-5) with the philosophy “the higher number, the higher risk, i.e. the lower technical facility coexistence with the surroundings” [91]. For DSS application, the auxiliary scale Table 11 derived in [95], and the second scale for the evaluation of the entire checklist based on the principle that was introduced into standards in the 1980s, Table 12.

The assessment of Table 10, hereafter given, assumes that all criteria have the same weight. Practical examples [49] show that in many cases some criteria are more important than others, and therefore, it is necessary to assign them higher weight, and to change data in Table 12 by appurtenant way.

Table 10. Checklist for assessing the risk connected with coexistence of the proposed technical facility and its surroundings; A – assessment; number of criteria n = 90; N - note.

Criterion	**A**	**N**
Designing		
The rate in which the terms of references of the technical facility are processed by a legal entity which has: - 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 and failures; methods of analysis, management and settlement of risks; management of the enterprise (finance, human resources, organization, technology, innovations...), - knowledge and capabilities for: the application of the results of methods of risk analysis and evaluation; implementation of the methodology for analysing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; the transformation of policy into actual action; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; finding the right information and learning; critical analysis; designing the right solutions; written and spoken communication; carrying out the synthesis; and adapting the wording intended for the public, - ethic.		

The rate in which the terms of references of the technical facility have clearly defined assets and include public assets.		
The rate in which the terms of references of the technical facility consider the impacts of disasters that are possible in the territory under the All-Hazard-Approach.		
The rate in which the terms of references of the technical facility are based on well-defined hazards to all disasters that are possible in the territory and have harmful potential; e.g. in the case of natural disasters due to the sparse and irregular occurrence of large phenomena, historical data need also to be used. In particularly serious disasters, it is not only limited to probabilistic approaches and it is complemented by the results of appropriate methods that have the ability to detect extreme phenomena.		
The rate in which the terms of references of the technical facility consider local vulnerabilities and, where is necessary also regional ones: - anomalies and non-homogeneity of geological structure, - large number of inhabitants, - reality that in territory there are hospitals, schools or other public buildings nearby, - reality that in territory there are sources of domino effects, i.e. warehouses or product lines with hazardous substances, fuel stations, etc. - reality that in territory it is insufficient capacity of energy sources, - reality that in territory it is insufficient capacity of water sources, - reality that in territory it is insufficient capacity of wastewater drainage (sewerage), - reality that in territory it is lack of transport service, - reality that in territory it is protected nature reserve.		
The rate in which the terms of references of the technical facility consider all risks associated with major disasters and all vulnerabilities in the territory.		
The rate in which the terms of references of the technical facility clearly define the fittings and systems for which risks need to be addressed in order to ensure: - reliability, - security - safety. According to the specified objective, they set the limits and conditions for the operation of the fittings and systems and their reserves in sufficient number.		

The rate in which the terms of references of the technical facility are assessed by qualified experts.		
The rate in which the technical facility project considers the results of the expert assessment of the terms of references.		
The rate in which the technical facility project is organized clearly so that it would be possible to simply control the technical facility and have a safety management system.		
The rate in which the technical facility project respects the size of the criticality associated with priority disasters (a combination of hazard size, vulnerability and sizes of impacts on assets), including the human failures, and proposes measures to ensure safety; at the same time it is based on an assessment of whether the proposed measures cannot be a source of new dangers and where they cannot be dealt with (e.g. ignorance or too much costs), it proposes technical measures, in management systems organizational ones.		
The rate in which the technical facility project considers protecting the public assets and technical facility assets.		
The rate in which the technical facility project is based on valid legislation and standards. It goes on a selection of materials, selection of computational methods, design of technical principles and procedures in building, construction and assembly, as well as commissioning.		
The rate in which the technical facility project used in cases that are not codified by standards approaches of good practice in building, construction and assembly.		
The rate in which the technical facility project when selecting and joining equipment with regard to safety, follows the requirements of: durability; manageability; service life; human resources; costs; technical utilities; and service.		
The rate in which the technical facility project with regard to safety uses: principles of inherent safety; passive safety systems; active safety systems; procedural procedures that are proven or thoroughly tested in such a way that they do not contain latent sources of danger under possible conditions.		
The rate in which the technical facility project with regard to safety has measures that trigger the emergency shutdown of critical devices and it reassign to a safe state, e.g. systems with emergency disconnection or stopping the reaction.		
The rate in which the technical facility project establishes critical processes of building or construction and proposes measures to reduce their criticality. It contains technical and organisational measures to ensure sufficient resilience.		
The rate in which the technical facility project proposes, in accordance with the terms of references, requirements for equipment and systems for which risks need to be addressed in order to ensure:		

- reliability, - security, - safety.		
The rate in which the technical facility project is based on a proper assessment of the risks targeted at the safety of the entire technical facility.		
The rate in which the technical facility project is based on the system concept of technical facility and its surroundings, and therefore, in ensuring the safety of all assets, it considers linkages and couplings between assets, both in demand and not-demanded and in the light of the management of unacceptable interconnections that can be expected when conditions are very different from normal ones, has an arranged architecture to allow Defence-In-Depth protection access to be applied in control.		
The rate in which the technical facility project considers critical sites of building structure and includes the right measures based on an assessment of the risks targeted to their safety, i.e. to ensuring the reliability and operation ability under abnormal and critical conditions (barriers, reserves, back-up).		
The rate in which the technical facility project considers the critical sites of technology and production processes, and shall take measures on the basis of an assessment of the risks directed to their safety, i.e. to ensuring the reliability and operation ability under abnormal and critical conditions (barriers, reserves, back-up and principles for safety upgrade).		
The rate in which the technical facility project considers highly critical fittings (pressure vessels, pressured pipes – especially those with highly hazardous substances) and for ensuring their safety it uses special measures, special protection systems (safety systems and safety related systems) and proposes specific limits and conditions for operation.		
The rate in which the technical facility project considers all risks associated with major disasters and all vulnerabilities in the territory in the systemic concept (i.e. the risks associated with the interconnections demanded, both permanent and temporary, and even non-demanded, which may occur only under certain conditions (e.g. at external disasters or operator errors or insider attacks). It contents appropriate technical and organisational measures to reduce the potential impacts.		
The rate in which the technical facility project pays from ensuring the safety and performance reasons special attention of the management system. The control system in the form of manual, semi-automatic and automatic based on IT is hierarchical and risk-based, possibly under normal, abnormal and critical conditions – it is more level-level and respects the Principle of Defence-In-Depth. It also includes proposals for measures to manage emergency and critical situations.		

The rate in which the technical facility project contains technical measures for physical and cyber protection of the technical facility.		
The rate in which the technical facility project considers the property rights of third parties; possible changes in the laws or system of taxes and market situations (e.g. it is dangerous to rely on the supply of critical items by only one supplier) during the making of a technical facility, and for these cases it contains reserves to reduce any causes thus created future losses and damages.		
The rate in which the technical facility project contains financial costs of the production of the technical facility are adequate.		
The rate in which the public administration has ensured an assessment of the technical facility project required by the legislation in force.		
The rate in which the technical facility project considers the results of professional assessment of the technical facility project by experts.		
The rate in which the technical facility project considers results of the public's comments on the technical facility project.		
Manufacturing		
The rate in which the building structure of the technical facility was started after sufficient preparation – documentation, material, technical equipment, sufficient quality staff were available.		
The rate in which the timetable of building structure of the technical facility is complete, clear and sufficiently detailed.		
The rate in which the building works on the technical facility respects standards setting out material, working procedures, protection of employees and contractors.		
The rate in which the contractor regularly follows financing during building activities and in case of deficiencies (e.g. jump in prices of important items) or substantial changes in legislation or taxes or interest rates the contractor takes effective measures to reduce these possible causes of future losses and damages; and with the reserves set out in the project shall be treated economically.		
The rate in which at the building works on the technical facility, safety procedures are respected.		
The rate in which at the building works on the technical facility is used only qualified staff.		
The rate in which the building structure supervision of the contractor and the investor perform regular checks of material, technical design of buildings, compliance with OSH.		
The rate in which public authorities carry out regular supervision of the construction of buildings from the point of view of OSH, environmental protection and, where in the case of, use of public money.		
The rate in which public administration (including supervisory inspections) comments on construction gaps are settled.		

Construction and assembly		
The rate in which the construction and assembly in the technical facility were started after sufficient preparation – documentation (e.g. precise distribution of the technical elements used), material, technical equipment, sufficient quality staff are available.		
The rate in which the schedule of construction and assembly in the technical facility was complete, clear and sufficiently detailed.		
The rate in which standards setting materials, working procedures, protection of employees and contractors are respected in construction and assembly works in the technical facility.		
The rate in which the contractor regularly follows financing during the installation of equipment and, in the event of deficiencies (e.g. jump in prices of important items) or substantial changes in legislation or taxes or interest rates, takes effective measures on reduction of any causes of future losses and damages; reserves are handled economically.		
The rate in which safety procedures are followed during the constructions and assembly works in the technical facility.		
The rate in which only qualified personnel are used in construction and assembly works on critical objects of technical facility (pressure vessels, dangerous substances storage tanks, product pipes).		
The rate in which, with regard to the safety of the technical facility, special attention is paid to the installation of equipment to trigger an emergency shutdown and transfer to a safe state, e.g. systems for emergency disconnection or stopping the reaction.		
The rate in which the supervision of the contractor and the investor carries out regular checks of material, technical design, OSH compliance.		
The rate in which quality changes in the material used, technical equipment due to market shortages, price increases, etc. have been made.		
The rate in which an assessment of the technical suitability of the changes applied is carried out in the case of critical installations.		
The rate in which public authorities carry out regular supervision of the installation of critical equipment, from the point of view of OSH, environmental protection and use of public money.		
The rate in which public administration comments on construction and assembly deficiencies are settled.		
Testing		
The rate in which in the technical facility was started after sufficient preparation – there is documentation, which defines e.g. methods of non-destructive testing, scale of criticality for assessing the method results, computational procedures, technical equipment, sufficiently qualified personnel.		

The rate in which the test schedule in the technical facility is complete, clear and sufficiently detailed.		
The rate in which norms and standards setting the materials, work-flows, protection of employees and contractors are respected when testing in a technical facility.		
The rate in which special attention is paid to tests of critical elements, critical equipment, critical components (e.g. pressure vessels), critical networks (energy, water, product lines with hazardous substances, IT), safety systems, safety related systems and protective systems (e.g. emergency shutdown equipment and systems, shower systems, power supply systems for own consumption – need for control, emergency coolant supply).		
The rate in which safety procedures are followed when tested in a technical facility.		
The rate in which only qualified personnel are used in testing critical equipment of a technical facility (pressure vessels, dangerous sub-stances storage tanks, pipelines).		
The rate in which the supervision of the contractor and the investor carries out regular checks on the technical execution of tests, the cor-rectness of the calculations carried out, the OSH compliance.		
The rate in which quality, the changes are made based on the test re-sults.		
The rate in which quality, the draft of new measures and the assess-ment of their technical suitability are in the case of critical installations.		
The rate in which quality, a test of the effectiveness of physical and cyber protection of a technical facility is conducted.		
The rate in which the public authorities carry out regular supervision of testing, from the point of view of OSH, environmental protection and, use of public money.		
The rate in which public administration comments on testing deficien-cies are settled.		
Trial operation		
The rate in which the trial operation of the technical facility is started after sufficient preparation – documentation, technical equipment, suffi-ciently qualified personnel are available.		
The rate in which the trial schedule in the technical facility is complete, clear and sufficiently detailed.		
The rate in which at trial operation the norms and standards setting the working procedures, protection of employees and contractors are re-spected.		
The rate in which with technical facility safety, it is special attention paid to tests of fittings and systems connected with safety function		

(they are disconnected or overwhelmed and the eligibility of organisational measures to cope with the situation is verified).		
The rate in which, with regard to the technical facility safety, it is verified the functionality of the equipment, detecting the disturbances of important equipment or systems, noise level, temperature level, fire, leakage of dangerous substances, large vibrations of the equipment, external disasters or disturbances.		
The rate in which the special attention is paid to the operation of critical elements, critical equipment, critical components (e.g. pressure equipment including joints of all kinds), critical networks (energy, water, product lines with hazardous substances, IT), safety systems, safety related systems and protection systems.		
The rate in which safety procedures are followed during the trial operation of a technical facility.		
The rate in which only qualified personnel are used in the trial operation of critical equipment of a technical work (pressure equipment, hazardous substances tanks, pipelines).		
The rate in which the supervision of the contractor and the investor carries out the control of the technical performance of the trial operation, the correctness of the measures taken, the OSH performance.		
The rate in which quality, the changes are made based on the trial operation results.		
The rate in which the draft of new measures and the assessment of their technical suitability are made in the case of critical installations based on results of trial operation.		
The rate in which the verification of the effectiveness of physical and cyber protection of the technical facility is carried out at trial operation.		
The rate in which public authorities carry out regular supervision of the installation of trial operation critical, from the point of view of correct function of critical fittings, OSH , environmental protection and use of public money.		
The rate in which public administration comments on trial operation deficiencies are settled.		
Commissioning		
The rate in which the technical facility commissioning is started after sufficient preparation – it is to disposal documentation (aimed to integral safety during the life cycle), technical equipment, sufficiently qualified personnel are available.		
The rate in which quality, the documentation of the technical facility for commissioning from a safety point of view includes: - answers to the following questions: • what can break down, • what may not work (identification and analysis of danger),		

• how serious the consequences can be (result of risk assessment), • what measures have been taken to avoid this (risk management), • what needs to be done when this occurs (disaster response and failure response measures), - in the case of complex technical facilities, the proof of safety is the result of extensive theoretical analyses and evaluation of tests. Safety certificate contains: • references to previous use, • references to validated procedures, • compliance data with standards, • certification, • calculations, • test results, • simulation results, • results of analytical methods (e.g. HAZOP, FMECA, FTA, etc.), • the results of expert examinations.		
The rate in which the commissioning schedule in the technical facility is complete, clear and sufficiently detailed.		
The rate in which at technical facility commissioning the norms and standards setting the working procedures, protection of employees and contractors are respected.		
The rate in which at technical facility commissioning is special attention paid to operation of critical elements, critical components (e.g. pressure vessels), critical networks (energy, water, product lines with dangerous substances), safety systems, safety related systems and protection systems.		
The rate in which safety procedures are followed during the technical facility commissioning.		
The rate in which only qualified personnel are used in the technical facility commissioning trial at critical equipment (pressure equipment, hazardous substances tanks, product lines).		
The rate in which the supervision of the contractor and the investor carries out the control of the technical performance of the commissioning, the correctness of the measures taken, the OSH performance.		
The rate in which at technical facility commissioning, the physical and cyber protection means are carried out in operation.		
The rate in which public authorities carry out regular supervision of the technical facility commissioning, from the point of view of correct		

function of critical fittings, OSH , environmental protection and use of public money.		
The rate in which public administration comments on technical facility commissioning deficiencies are settled.		

Table 11. Scale for determination of rate of risk that planned technical facility means for its surroundings (rate of coexistence disruption); by analogy to scales in [95]; p – annual insurance, ABT- the annual budget of territory governance.

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

	5	devastation of landscape, unrenewable resources of nature and natural reservations

Table 12. Value scale for determining the rate of the coexistence of the planned technical facility and its surroundings; N = five times the number of criteria in Table 10; N = 270.

The level of coexistence disruption (risk) between technical facility and surrounding	**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 %

The evaluation of real cases according to the Table 10 needs to be performed by a team of specialists from the different fields independently; in practice, according to [23,95], it works the team consisting of:

- worker of public administration responsible for the land use planning,
- worker of public administration responsible for the territory development,
- representative of planned technical facility,
- competent representative of the professional institution for the technical facility safety assessment, for example from the state technical inspection,
- and representative of the Integrated rescue system.

The resulting value is the median for each criterion, and in cases of great variance of the individual values in the one criterion it is necessary, so that the worker of public administration responsible for land use planning may ensure further investigation, on which each assessor shall communicate the grounds for his / her review in the present case, and on the basis of panel discussions or brainstorming session, the final value is determined.

The appreciation of the benefits of a technical facility for the territory is done again using a checklist. On the basis of the knowledge gathered above, a checklist is drawn up to assess the contribution of the technical facility to the territory [2], Table 13. The criterions are evaluated by scale (0-5) with the philosophy “the higher number, the higher risk, i.e. the lower technical facility coexistence with the surroundings” [89]. For the DSS application in practice, two scales are assigned to the checklist: the auxiliary scale Table 14 derived in [95], and the second scale for the evaluation of the entire

checklist based on the principle that was introduced into standards in the 1980s, Table 15.

Table 13. Checklist for assessment of the technical facility return for territory. A- result of assessment; N – note.

Planned technical facility	**Criterion**	**A**	**Note**
	It increases education of the population in the territory		
	It increases the possibility of employment of the population in the territory		
	It increases the level of services in the territory		
	It increases welfare in territory		
	It contributes to the development of basic infrastructure in the territory.		
	It raises the prestige of the territory		
	It contributes to the cultural development of the territory		
	It improves the situation in the social sphere in the territory – Table 14		
	It improves situation in technical and economic spheres in territory - Table 14		
	It improves the situation in environment protection and welfares in territory - Table 14		

Table 14. Value scale for determining the rate of benefits that the technical facility means for the territory; it is designed by analogy to the scales set out in the work [23,95], ABT – the annual budget of the territory.

Domain	**Benefit rate classification**	**Criterion**
	Rate	*Technical facility benefits:*
Social	0	less than 50 humans
	1	50 - 500 humans
	2	500 - 5000 humans
	3	5 000 – 50 000 humans
	4	50 000 – 500 000 humans
	5	more than 500 000 humans

	Rate	*Technical facility gives to territory budget:*
Technical and eco-nomic	0	less than 0.005 ABT
	1	0.005-0.01 ABT
	2	0.01-0.025 ABT
	3	0.026-0.05 ABT
	4	0.05-0.075 ABT
	5	higher than 0.075 ABT
	Rate	Technical facility contributes to environ-ment protection and welfare increase per year by sum of money:
Environment	0	less than 50 EUR
	1	50 – 500 EUR
	2	500 – 5 000 EUR
	3	5 000 – 50 000 EUR
	4	50 000 – 500 000 EUR
	5	more than 500 000 EUR

Table 15. Value scale for determining the rate of return of the technical facility for its surroundings; N is quintuple of criteria in Table 13 (N=50).

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

At the technical facility risk management based on data in Table 10 we consider the responsibility principle that is general in Europe [94]. It means that in the followed technical facility phase both, the developer and the public administration are responsible for the technical facility safety.

Considering:

- the ALARP principle as in works [94,96-98],

- the integrated approach as in works [99,100],
- and the assumption that all risk sources have the same occurrence probability, we obtain the requirement for tolerable risk measured by the technical facility maximum annual losses ***RZTD***

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

where ***HTD*** is the technical facility utility value given in technical facility document (official approved budget for designing, manufacturing and commissioning), $\boldsymbol{k_i}$ are result evaluations of risk sources in Table 10, *n* is the number of risk sources (in our case 90) and ***T*** is the technical facility lifetime in years. When this condition is not fulfilled, so the proposed technical facility may not be accepted for realisation because the coexistence will be violated. It means that either a new option or other risk reduction measures should be requested, followed by a further assessment of the proposal. In other case the evaluation process continues.

In order that the losses caused by the technical facility at its operation might be also acceptable for the territory, it is calculated the benefit that the technical facility operation gives rise to territory. Using the data in Tables 11 – 13 and the principles for expected return [101] and the same assumptions on data processing as in the previous case, the expected annual technical facility return caused by the technical facility operation ***PRZTD*** is

$$\boldsymbol{PRZTD = 0.7 \sum_{i=1}^{n} \frac{k_i\, CPTD}{5\, T}} \quad (6)$$

where ***CPTD*** is the total utility technical facility return during the lifetime ***T,*** $\boldsymbol{k_i}$ are result evaluations of return sources in Table 11 (assessed by experts with help of data in Tables 12 and 13) and ***n*** is the number of benefit sources (in our case 10). The expected pure annual technical facility return ***RPTD*** is given by

$$\boldsymbol{RPTD = PRZTD - A - RPNTD} \quad (7)$$

where ***A*** is annuity and ***RPNTD*** is operating costs. Difference ***R*** of allowed maximum annual technical facility losses ***RZTD,*** Eq. (5), and of expected pure annual technical facility return ***RPTD,*** Eq. (7)

$$\boldsymbol{R = RZTD - RPTD} \quad (8)$$

is used as the quantitative property for decision-making. They are used the boundaries of acceptability of risk that used the UN and the Swiss Re [24], namely:

- amount of annual premium for protected assets in territory (***PRTD),***

- one-tenth of annual territory budget (***ABT***).

On the basis of results of scoring, they are determined the categories to which in a given case, the risk associated with technical facility belongs:

R is less than PRTD, risk is acceptable,

R is between PRTD and 0.1 ABT, risk is conditionally acceptable,

R is higher than 0.1 ABT, risk is unacceptable.

In the first case, the technical facility benefits will outweigh the technical facility disadvantages, it means the expected losses are acceptable and the coexistence of the technical facility with its vicinity is ensured. It can be done permit for the technical facility realization.

In the second case, the effective technical facility safety management is required; it means to include additional preventive measures in the technical facility design and to ensure the mitigation, reaction and renovation measures for coping with risk realization.

In the latter case, unacceptable risk, it should be thorough reflection on conclusion – either to reject the proposed technical facility variant, or to ask for further measures associated with an increase of technical facility safety (it is necessary to require application of: higher knowledge; a better technical equipment; the higher costs for protective systems; ensuring the greater human resources readiness, etc.) and after this new coexistence judgement.

The tool was tested in five real cases with success. The tests showed that it is pernickety on expert knowledge and moral, however, it ensures the coexistence the technical facility with its vicinity during the technical facility lifetime.

6. TOOL - RISK MANAGEMENT PLAN FOR ENSURING THE COEXISTENCE AT TECHNICAL FACILITY DESIGNING, BUILDING AND COMMISSIONING

The risk management plan is based on the TQM management method [63], 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 [93].

The facts in works [1,2,4,5,10-20,24,45,49] imply that each technical facility needs to have a plan to increase the safety of the technical facility over time in order to ensure that it fulfils the specified tasks in the required quality and time and it is competitive; on-side plan; data for off-side plan in the event of an accident or failure of the technical facility; a technical facility continuity plan to overcome critical conditions; crisis plan; and a disaster recovery plan. A very effective plan for rapid problem management is the priority risk management plan [93].

The risk management plan is based on identified sources of the causes of accidents or failures of technical facilities, the results of which were losses of human lives, financial and other damage, and therefore, they need to be considered as priority. In the interest of safety, they need to be monitored and timely response and recovery need to be ensured. This plan helps to resolve conflicts because, in the event of an expected conflict of interest, the objectives of addressing the problem caused by the realization of the risk can be agreed in advance. It can be also determined in advance the respective responsibilities and codified the procedures for responding to the problem. As it was given above, the risk management plan contains four basic items, namely:

- domain of risk causes (technical, organizational, internal, external, cyber),
- description of the causes of the risk,
- probability of occurrence and evaluation of risk impacts,
- risk and liability mitigation measures.

In Europe, it is promoted the good governance [21]. The governance type in question is based on the openness, accountability and efficiency of institutions and public participation in decision-making and other processes. In practice, it means transparency,

accountability, integrity, appropriate type of governance, efficient and affordable services, a commitment to partnership and the continuous development of public administration institutions. The adopted territorial management strategies need to have a clear link with the specific activities of the authorities. Good governance has five basic features: openness; public involvement in decision-making; responsibility; efficiency; and the coherence of strategies and real activities. In other words, states, regions or cities, the political and institutional governance of which does not show the mentioned five basic features cannot achieve the sustainable development.

Each entity management has certain hierarch. In every case it holds that the manager (officer) on higher position has higher power and also higher responsibility on solving the problems connected with the organizational and public matters.

Good governance means applying an optimal management system based on problem diagnosis and problem-solving measures. The essence of good governance lies in the combination of different levels of decision-making as opposed to the almost exclusive role of the State. As a result, decision-making shifts to multi-level structures, i.e. to regional structures. Another stage of good governance is the application of project and process management, which is based on the strategic development plan [24].

In book [4] summarizing the principles for managing the risks of complex technical facilities, it is shown that, in addressing tasks in the division of tasks and establishing responsibilities, the account needs to be taken of the possibilities that exist at the management level in question. The possibilities are determined by both, the powers and the availability and amount of available resources, forces and means that needed for problem solution:

- well-structured problems can be successfully solved at the operational level of technical facility management.
- structured and poorly structured problems that are not associated with high risks for the technical facility can be successfully solved at the middle level of technical facility management,
- at the top level of technical facility management, both complex and unstructured problems that have risks that can be controlled using the tools available only to the top management of the technical facility can be successfully addressed,
- only the mutual cooperation of the public administration and the top management of the technical facility can solve complex and unstructured large-scale problems with high risks.

For transnational technical facilities, international cooperation is still necessary.

In complex world, the technical facility management represents the hierarchical interconnected system. According to [94], the responsibility principle paid in Europe means that for risk management are responsible both, the technical facility management and the public administration that gives permit and supervise the provision of public interest.

Results of research given in [4] has shown that in terms of humans´ safety and development, risk management of complex technical facilities is important in two areas:

A. Domain connecting the public administration and management of complex technical facility.

B. Domain of technical facility dealing with data, methods, material and technical matters, organizational, legal, financial and personnel matters directly in a complex technical work.

The model risk management model plan is drawn up by analogy to the situation in the developed countries [2]. When designing, manufacturing and commissioning the technical facility, responsibilities are considered for the following functions:

- mayor of the municipality,
- chairman of the Building Authority,
- responsible public administration officer for the territory safety,
- responsible public administration officer for the territory development,
- the responsible representative of the investor of the technical facility,
- responsible representative of the future operator,
- responsible representative of the relevant professional institution responsible for the safety of technical facilities (Technical Inspection, Environmental Inspection, Nuclear Inspection, State Office for Occupational Safety, etc.),
- responsible representative of civil protection (the Integrated Rescue System),
- Parliament chairman.

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 [2], 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 3:

1. Table 16 shows the risk management plan for designing.
2. Table 17 shows the risk management plan for construction, mounting, testing a commissioning; complete tables are in [2].

There is no distinction between the risk management plan for technical facility of local to regional importance, and for technical facility of national to transnational importance, since building documents in both cases are issued by the locally competent municipal authority, which has the authority of the building authority.

Table 16. Risk management plan for technical facility designing directed to coexistence of operated technical facility with its surrounding.

Risk domain	**Risk description**	**Occurrence probability**	**Measures for risk mitigation**

		Impacts	
Public administration	As a result of the absence of a state strategy on the management of the design of technical facilities focused on safety, priority of current political interests, the promotion of the requirements of coercive groups or the failure to cope with extreme political situations (war, terrorist attacks), which in turn leads to a reduction in the standard of living and security of citizens, economic instability, etc.	Probability: great Impacts: great	***Measures:*** To develop new strategy and modify building law ***Execute:*** Government chairman ***Responsibility:*** Parliament chairman
	As a result of the weak state support aimed at quality design of technical facilities, construction is being extended and the costs of construction are being increased, which in turn leads to a reduction in living standards, economic instability, etc.	Probability: great Impacts: great	***Measures:*** To modify legislative, especially building law ***Execute:*** Minister of interior + minister of economy ***Responsibility:*** Government chairman
	As a result of poor-quality technical education aimed at quality design of technical facilities, which considers not only standards, but also possible risks, it goes on prolongation of construction, problems in commissioning or accidents accompanied by enormous expenditure from public budget, disruption of citizens' security and state stability, which in turn leads to a reduction in living standards, economic instability, etc.	Probability: great Impacts: great	***Measures:*** Modify education system ***Execute:*** Minister of education ***Responsibility:*** Government chairman
	As a result of erroneous legislation (e.g. inaccurate requirements for a technical facility project with a view to ensuring the coexistence of a technical facility with the surroundings (it is possible to use faulty or unverified technologies; there is no emphasis on the use of quality equipment and their connection over a lifetime; it is the absence of a requirement for the inclusion of	Probability: great Impacts: great	***Measures:*** Modify laws on technical facilities safety ***Execute:*** Minister for economy ***Responsibility:*** Government chairman

	inherent safety measures for hazardous technologies; it is not processing of operating regulations for normal, abnormal and critical conditions and ensuring response to accidents and accidents) there is an extension of construction, commissioning problems or accidents accompanied by enormous expenditure from the public budget, disruption security of citizens and the stability of the state.		
	Due to the lack of competence of the public authority in supervision of the design of technical facilities, there is an extension of construction, problems in commissioning or accidents accompanied by enormous expenditure from the public budget, disruption of the security of citizens	Probability: great Impacts: great	***Measures:*** Modify law on competences and responsibilities ***Execute:*** Government chairman ***Responsibility:*** Parliament chairman
	When large technical facilities do not provide a professional body with sufficient competences to ensure a quality project and the construction of a technical facility, the construction is prolonged, problems in commissioning or accidents accompanied by enormous public budget expenditure, disruption of citizens' security and national stability.	Probability: medium Impacts: great	***Measures:*** Modify building law ***Execute:*** Minister of economy ***Responsibility:*** Government chairman
	When there is a lack of a data base on properties and phenomena in the territory, the project is built on general knowledge and does not respect local conditions, which sooner or later will disrupt the construction or operation of the technical facility and lead to accidents accompanied by enormous expenditure from public budget, disruption of citizens' security and state stability.	Probability: great Impacts: great	***Measures:*** Modify strategy of research – include duty to ensure data and their processing for public needs ***Execute:*** Government chairman ***Responsibility:*** Parliament chairman

	As a result of the finding that the technical facility project is based on poor quality of the terms of references, documentation and technologies used, which sooner or later will disrupt the construction or operation of the technical work and lead to accidents accompanied by enormous expenditure from public budget, disruption of citizens' security and state stability.	Probability: medium Impacts: great	***Measures:*** Ask investor for terms of references correction according to building law ***Execute:*** Building office chairman ***Responsibility:*** Mayor or at specific technical facilities minister of economy
	As a result of not finding that the technical facility project has not considered whether the technical facilities' claims to critical infrastructure capacities and personnel correspond to the conditions in the site, it will be sooner or later disrupted the construction or operation of the technical facility with enormous expenditure from the public budget, the disruption of the security of citizens and the stability of the state.	Probability: medium Impacts: great	***Measures:*** Ask investor for project correction according to building law ***Execute:*** Building office chairman ***Responsibility:*** Mayor or at specific technical facilities minister of economy
	Failure to find that the technical facility project has neglected to consider the impact of a technical facility on the safety of the territory (not considering or underestimating the impacts of accidents and failures) will occur sooner or later in the construction or operation of the technical facility and lead to accidents accompanied by disruption of citizens' security, expenses on response and recovery expenses, including expenses from the public budget.	Probability: medium Impacts: great	***Measures:*** Ask investor for project correction according to building law ***Execute:*** Building office chairman ***Responsibility:*** Mayor or at specific technical facilities minister of economy
	As a result of not finding that the technical facility project is not of good quality in terms of financing (underfinancing) and the construction schedule, construction will be	Probability: great Impacts: great	***Measures:*** Ask investor for project correction according to building law

	extended and the costs originally determined will increase.		***Execute:*** Building office chairman ***Responsibility:*** Mayor or at specific technical facilities minister of economy
investor of technical facility	Due to the lack of investor competence in the field of design of technical facilities, it comes: construction is being extended; commissioning problems, enormous expenditure and later other problems in operation, financing, safety, etc.	Probability: medium Impacts: great	***Measures:*** Modify building law ***Execute:*** Minister of economy ***Responsibility:*** Government chairman
	As a result of errors in the selection of an authorised designer (insufficient knowledge and experience from all disciplines that must be considered in the project), the project is of poor quality, which sooner or later will disrupt the construction or operation of the technical facility and lead to accidents accompanied by enormous expenditure, disruption of the security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Change of authorized designer ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	As a result of the lack of quality of technical facility terms of references and requirements for the protection of the surrounding territory, the project does not consider the local specificities and local risks, which sooner or later will disrupt the construction or operation of the technical facility and lead to accidents accompanied by enormous expenditure, disruption of the security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Modify terms of references ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	As a result of wrong supervision on the design of the technical facility (it did not find that there were used: inappropriate methods, incorrect data on the territory, incomplete data on	Probability: medium Impacts: great	***Measures:*** Change of investor check and inspection system ***Execute:***

	technology, incomplete set of standards, principles and procedures ensuring safety; experts from technical, IT, legal, OSH did not cooperate with each other; etc.), which sooner or later disrupts the construction or operation of a technical facility and will lead to accidents accompanied by enormous expenditure, disruption of citizens' security and problems with public administration.		Competent investor worker ***Responsibility:*** Investor director
	Due to not ensuring an expert assessment of the technical facility terms of references submitted by the designer will occur sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Execute correction on the basis of expert judgement of terms of references ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-detection that the technical facility project has overestimated or underestimated the claims of a technical facility on critical infrastructure capacities and the staff at the site will occur sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Execute correction and negotiate with public administration ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-detection that the technical facility project is not clear enough to ensure simple manageability of the technical facility and a well-organised safety management system will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:***

			Investor director
	Due to non-detection that at selection of fittings and their interfaces in the technical facility, there were not considered requirements on: durability; fittings and process manageability; service life; human resources; costs; technical utilities; and service will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-existence of proof on the technical facility project feasibility will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-ensuring the complete technical facility technical documentation, e.g. an accurate description of all the fittings and the modes of their operation will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: great Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director

	Due to non-consideration of cross-sectional risks (connected with interfaces of fittings, IT and man-machine) in the safety analyses will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: great Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-monitoring changes in legislative, norms, standards, taxes etc., it will occur finance problems which lead to prolongation of building, loss of public administration support and may be to non-finishing the building.	Probability: medium Impacts: great	***Measures:*** Order to authorized designer to ensure corrections on its costs and in fix time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
Future operator	Due to incorrectly assigned requirements on the technical facility, the project poorly resolves the local specificities, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask to investor to ensure corrections ***Execute:*** Competent future operator worker ***Responsibility:*** future operator director

	Due to wrong co-operation of investor, public administration and designer, the technical facility project may not resolve possible conflicts of the technical facility with the surroundings, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask to investor to ensure corrections; pertinently ask the building office chairman of director of technical inspections for help ***Execute:*** Competent future operator worker ***Responsibility:*** future operator director
	Due to wrong estimation in domain oh relation supplier- subscriber, the technical facility project is based on unrealistic data, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask to investor to ensure corrections ***Execute:*** Competent future operator worker ***Responsibility:*** future operator director
	Due to wrong estimation of demands of the technical facility on energy, transport, water supply, sewerage, waste liquidation, the technical facility project is based on unrealistic data, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask to investor to ensure corrections and to negotiate with public administration with aim to solve problem ***Execute:*** Competent future operator worker ***Responsibility:*** future operator director

	Due to wrong estimation on personnel needs, the technical facility project is based on unrealistic data, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask to investor to ensure corrections and to negotiate with public administration with aim to solve problem ***Execute:*** Competent future operator worker ***Responsibility:*** future operator director
Approved designer of technical facility	Due to designer insufficient knowledge, it will occur sooner or later disruption of the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Refuse commission or to take on experts ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to low-class or non-cooperating team of the technical facility project processors, the project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. to create rules for working team cooperation ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to ignorance or non-ensuring the quality data, the technical facility project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. to ensure correct data or ask investor for their delivery ***Execute:*** Competent designer worker ***Responsibility:***

			Designer director
	Due to ignorance or non-ensuring the quality methods mainly from domain of work with risks, the technical facility project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. either use correct methods or ensure appropriate expert, who does it ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to ignorance or non-ensuring the postulated legislative, norms, standards and modus-operandi principles of good engineering practice, the technical facility project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. either by own resources or by special commission ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to short time interval or limited finances on project processing, non-detection that the technical facility project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask investor for correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to unclear and uncomplete schedule of works on project in form modus-operandi checklist, the technical facility project has bad quality, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by	Probability: medium Impacts: great	***Measures:*** Create clear schedule of works, their quality, aims and deadlines ***Execute:***

	enormous expenditure, disruption of security of citizens and the problems with public administration.		Competent designer worker ***Responsibility:*** Designer director
	Due to insufficient knowledge or finances, specific survey of site-specific conditions was ignored, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask investor for correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to insufficient legislative, the technical facility project does not contain measures for protecting the public assets, limits and conditions for critical fittings operation, reserve resources for pulling off the emergency and critical situations, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask investor for correction, pertinently ask public administration for support ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to insufficient knowledge of the technical facility project processor and wrong supervision of investor and public administration, it was used the bad technology, which will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: medium Impacts: great	***Measures:*** To top up team by specialists and in cooperation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to incomplete documentation on allowable operation modes, it will occur sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of	Probability: medium Impacts: great	***Measures:*** To top up team by specialists and in cooperation with investor to do correction ***Execute:***

	citizens and the problems with public administration.		Competent designer worker ***Responsibility:*** Designer director
	Ignorance of technical facilities being in surrounding the designed technical facility which can be sources of domino-effects, will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: great Impacts: great	***Measures:*** To top up team by specialists and in co-operation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Ignorance of occurrence of situations which can require higher costs (e.g. increase of taxes, change of public administration support, occurrence of natural or other disaster) will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: great Impacts: great	***Measures:*** To top up team by specialists and in co-operation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Wrong separation of invest complex into stages will lead sooner or later to disruption the construction or operation of the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.	Probability: great Impacts: great	***Measures:*** In co-operation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
	Due to unclearly defined the technical facility safety objectives and tools for ensuring the safety, the project does not obtain instruction for correct risk management, which will lead sooner or later to disruption the construction or operation of	Probability: great Impacts: medium	***Measures:*** In co-operation with investor to do correction ***Execute:***

	the technical facility that lead to accidents accompanied by enormous expenditure, disruption of security of citizens and the problems with public administration.		Competent designer worker ***Responsibility:*** Designer director
Natural disaster, fire in facility	Due to natural disaster or fire occurrence, the works on project will be disrupted, which will lead to disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and will lead to extension of manufacturing deadline and with this connected additional costs and additional works (e.g. maintenance and physical protection of occupied territory).	Probability: low Impacts: medium	***Measures:*** In co-operation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
Failure of technique, accident, failure of critical infrastructures	Due to occurrence, the works on project will be disrupted, which will lead to disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and will lead to extension of manufacturing deadline and with this connected additional costs and additional works (e.g. maintenance and physical protection of occupied territory).	Probability: low Impacts: great	***Measures:*** In co-operation with investor to do correction ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
Insider	Due to occurrence, the errors in project will occur, which will lead to disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and even technical facility operation, will lead to extension of manufacturing deadline and with this connected additional costs and cause disruption of security of citizens, harms on environment and damages on employee health's or humans in technical facility surrounding, and also problems with public administration.	Probability: low Impacts: medium to great	***Measures:*** To build the safety culture and to motivate workers for work targeted to fulfilment of tasks ***Execute:*** Competent designer worker ***Responsibility:*** Designer director

Terrorist attack	Due to occurrence, the errors in project will occur, which will lead to disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and even technical facility operation, will lead to extension of manufacturing deadline and with this connected additional costs and cause disruption of security of citizens, harms on environment and damages on employee health's or humans in technical facility surrounding, and also problems with public administration.	Probability: low Impacts: medium to great	***Measures:*** In co-operation with investor to do correction; i.e. to ensure response and renovation and to improve the physical protection and guard of workplace ***Execute:*** Competent designer worker ***Responsibility:*** Designer director
Finance crisis	Due to occurrence, the lacks of finances which will lead to project works stop, disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and even technical facility operation, will lead to extension of manufacturing deadline and with this connected additional costs and cause social problem (unemployment, disruption of security of citizens), harms on environment and problems of public administration (costs on social allowances, fight against criminality etc.).	Probability: low Impacts: medium to great	***Measures:*** In co-operation with investor and public administrative to carry out protective measures and ensure the acceptable solution of tasks ***Execute:*** Competent designer worker ***Responsibility:*** Designer director

War	Due to occurrence, the lacks of finances, personnel, change in state priorities (e.g. finance and other support of investors) which will lead to project works stop, disruption deadline or to reduction of project quality, which will disrupt further stages of technical facility manufacturing and even technical facility operation, will lead to extension of manufacturing deadline and with this connected additional costs and cause social problem (unemployment, disruption of security of citizens), harms on environment and problems of public administration (costs on social allowances, fight against criminality etc.).	Probability: low Impacts: great	***Measures:*** In co-operation with investor and public administrative to carry out protective measures and ensure the acceptable solution of tasks ***Execute:*** Competent designer worker ***Responsibility:*** Designer director

Table 17. Risk management plan for technical facility construction, mounting and commissioning directed to coexistence of operated technical facility with its surrounding.

Risk domain	**Risk description**	**Occurrence probability** **Impacts**	**Measures for risk mitigation**
Public administration	Due to absence of a state strategy on the domain of management of the construction and commissioning of technical facilities focused on safety, it is possible preference of current political interests, enforcement of the requirements of coercive groups or failure to cope with extreme political situations (war, terrorist attacks), which in turn leads to a reduction in living standards, economic instability, etc.	Probability: great Impacts: great	***Measures:*** To develop new strategy and modify building law ***Execute:*** Government chairman ***Responsibility:*** Parliament chairman
	Due to weak support of a state strategy targeted to quality manufacturing and commissioning the technical facilities, it goes to	Probability: great Impacts: great	***Measures:*** Modify competence law and building law ***Execute:***

	prolongation of construction and to enormous costs on the manufacturing, which in turn leads to a reduction in living standards, economic instability, etc.		Government chairman ***Responsibility:*** Parliament chairman
	Due to absence of quality technical education targeted to quality construction and commissioning, which would consider not only norms but also possible risks; it comes up to prolongation of construction, problems at commissioning or to accidents accompanied by enormous expenses from public budget, disruption of security of citizens, economic instability, etc.	Probability: great Impacts: great	***Measures:*** Modify laws on education ***Execute:*** Minister for education ***Responsibility:*** Government chairman
	Due to wrong legislative in the domain of management of the construction and commissioning the technical facilities (it is possible to use wrong or non-verified technologies at construction or commissioning) it goes to prolongation of construction and to enormous costs on the manufacturing, which in turn leads to a reduction in living standards, economic instability, etc.	Probability: great Impacts: great	***Measures:*** Modify laws on technical facilities and law on education ***Execute:*** Minister for education Minister for economy ***Responsibility:*** Government chairman
	Due to insufficient authority of public administration at supervision under the technical facilities, it comes to prolongation of construction and to problems at commissioning or operation or to accidents accompanied by enormous expenses from public budged and to disruption of security of citizens.	Probability: great Impacts: great	***Measures:*** Modify laws on competence, laws on state administration ***Execute:*** Minister for interior ***Responsibility:*** Parliament chairman
	When large technical works do not provide a professional body with sufficient	Probability: medium Impacts: great	***Measures:*** Modify building law

	competences to ensure quality construction and the commissioning the technical facility, it will origin prolongation of construction, problems in commissioning or accidents accompanied by enormous expenditure from the public budget, disruption of the security of citizens and the stability of the territory.		***Execute:*** Minister for economy ***Responsibility:*** Government chairman
	Non-detection of reality that the construction and commissioning of the technical facility is not good quality in terms of financing (underfinancing) and the construction schedule will increase construction time and increase the costs originally set.	Probability: great Impacts: great	***Measures:*** Ask investor for correction according to building law ***Execute:*** Building office chairman ***Responsibility:*** Mayor or at specific technical facilities minister of economy
Technical facility investor	Due to insufficient investor competence in the field of construction and commissioning of technical facilities, it goes to prolongation of construction, commissioning problems, enormous expenditure and later to other problems in operation, financing, safety, etc.	Probability: medium Impacts: great	***Measures:*** Correct building law ***Execute:*** Minister of economy ***Responsibility:*** Government chairman
	As a result of errors in the selection of an authorised builder (insufficient knowledge and experience from all disciplines, which must be considered in the manufacturing and commissioning), the technical facility is of poor quality, which sooner or later will disrupt the operation of the technical facilities and lead to accidents accompanied by enormous expenditure, disruption of the	Probability: medium Impacts: great	***Measures:*** Change of manufacturer or building site manager ***Execute:*** Competent investor worker ***Responsibility:*** Investor director

	security of citizens and problems with public administration.		
	Due to neglection of the requirements for the protection of the surrounding territory during construction and commissioning, it will result in a disruption of the security of citizens and problems with public administration.	Probability: great Impacts: great	***Measures:*** Ensuring correction according to building law ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to wrong supervision under the construction and commissioning of the technical facility (it did not detect that: inappropriate methods were used in the construction, construction, testing of equipment, trial operation and commissioning), it leads sooner or later to problems at technical facility operation or to accidents accompanied by enormous expenditure, disruption of the security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ask manufacturer and building site manager for correction ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to neglection of expert assessment of the schedule of works and works carrying out at manufacturing and commissioning the technical facility, they will occur sooner or later in accidents accompanied by enormous expenditure, disruption of citizens' security and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. to ensure expert judgements of documents and force manufacturer and building site manager to carry out appropriate changes ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Due to non-detection that the manufacturing and	Probability: medium	***Measures:***

	commissioning the technical facility does not comply with the project, the requirements for equipment quality, OSH and environmental protection, it will lead sooner or later to disruption of the operation of the technical facility or to accidents accompanied by accidents accompanied by enormous expenditure, disruption of the security of citizens and problems with public administration	Impacts: great	Ensure correction and at negotiation with public administration to find suitable solution ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Non-execution of high-quality non-destructive tests of critical technical equipment, high-quality tests of operational processes and quality trial operation will lead sooner or later to disruption of the operation of the technical facility or to accidents accompanied by enormous expenditure, disruption of citizens' security and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction and at negotiation with public administration to find suitable solution ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	Non-execution of complete final technical documentation after trial operation (containing an accurate description of all equipment, their functions, limits and conditions, operation modes and procedures for overcome the emergency and critical situations, including the necessary technical provision, and necessary personnel requirements) will lead sooner or later to disruption of the operation of the technical facility or to accidents accompanied by enormous expenditure, disruption of citizens' security and problems with public administration.	Probability: great Impacts: great	***Measures:*** Ensure so that manufacturer performs corrections on its expenses and in determined time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director

	As a result of non-considering the cross-cutting risks (associated with equipment, IT and man-machine connections) in the manufacturing, tests and commissioning, the operation of the technical facility will be disrupted sooner or later or they origin accidents accompanied by enormous expenditure, disruption citizens' security and problems with public administration.	Probability: great Impacts: great	***Measures:*** Ensure so that manufacturer and building site manager perform corrections on its expenses and in determined time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
	As a result of not monitoring the changes in legislation, norms, taxes, etc. at manufacturing and commissioning the technical facility, financial problems will occur, which will lead to an extension of construction, loss of public administration support and, to not complete a project or construction.	Probability: medium Impacts: great	***Measures:*** Ensure so that manufacturer performs corrections on its expenses and in determined time interval ***Execute:*** Competent investor worker ***Responsibility:*** Investor director
Future operator	Due to poor cooperation of the investor, public administration and construction manager, the conflicts can occur at manufacturing and commissioning the technical facility, namely internal or between technical work facility and surrounding area, which sooner or later will lead to a disruption of the operation of the technical facility and accidents accompanied by enormous expenditure, disruption of citizens' security and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure so that investor will perform corrections, pertinently ask for help Building office director or Technical Inspection director ***Execute:*** Competent future operator worker ***Responsibility:*** Future operator director

	Due to the poor estimation of the demands of the technical facility for energy, transport, water supply, sewerage, waste disposal, delays occur sooner or later at manufacturing and commissioning, failures of the future operation of the technical facility, resulting in enormous expenditure, disruption of citizens' security and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure so that investor will perform corrections, and negotiate with public administration on problem solving ***Execute:*** Competent future operator worker ***Responsibility:*** Future operator director
Manufacturer – authorized approved building site manager	Due to the lack of knowledge of the contractor/building site manager, it will occur sooner or later to the disruption of manufacturing and commissioning the technical facility, which lead to enormous expenditure, disruption of the security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Refuse commission, change building site manager, or to take on experts ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Due to wrong and non-collaborating teams ensuring the manufacturing and commissioning the technical facility, it will occur sooner or later to the disruption of manufacturing and commissioning the technical facility, which lead to enormous expenditure, disruption of the security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, i.e. to create rules foe team co-operation ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	As a result of ignorance or carelessness, the construction and commissioning are carried out poorly, which sooner or later will lead to disruption of the operation of	Probability: medium Impacts: great	***Measures:*** Ensure correction ***Execute:*** Competent manufacturer worker

	the technical facility, and the associated enormous expenditure, the disruption of the security of citizens and problems with public administration.		***Responsibility:*** Manufacturer director
	Due to ignorance the required legislation, OSH requirements, standards and modus operandi principles of good engineering practice and all possible measures against risks at manufacturing and commissioning, it will come up to workers' injuries, enormous expenses and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction, to create safety culture ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Due to short time interval or lack of finances on manufacturing the technical facility, it will occur sooner or later to disruption of manufacturing or late operation of technical facility, which will lead to enormous expenses, disruption of security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Ensure correction dealing with technical facility safety with negotiation with investor ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Due to unclear and incomplete work schedule at manufacturing and commissioning, it will occur sooner or later to disruption of manufacturing or late operation of technical facility, which will lead to enormous expenses, disruption of security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** Determine clear work schedule, clear quality targets, works deadlines ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Due to insufficient knowledge of building site manager and wrong supervision of investor,	Probability: medium Impacts: great	***Measures:*** To fill experts into team in co-operation

	future operator and public administration at manufacturing and commissioning the technical facility, it will occur sooner or later the disruption of manufacturing or late operation of technical facility, which will lead to enormous expenses, disruption of security of citizens and problems with public administration.		with investor and perform correction ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Default in registration of real technical solutions at manufacturing or commissioning the technical facility into complete technical documentation lead sooner or later to disruption of manufacturing or later operation of technical facility, which will lead to enormous expenses, disruption of security of citizens and problems with public administration.	Probability: medium Impacts: great	***Measures:*** To fill experts into team in co-operation with investor and perform correction ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	Default in preparation of solution of situations that can require extra costs (e.g. increase of taxes, change of public administration support, natural or other disaster occurrence etc.) lead sooner or later to disruption of manufacturing or later operation of technical facility, which will lead to enormous expenses, disruption of security of citizens and problems with public administration.	Probability: great Impacts: great	***Measures:*** To fill experts into team in co-operation with investor and perform correction ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
	As a result of unclearly defined objective of the safety of the technical facility and the tools to ensure the safety at manufacturing and commissioning the technical work, it is not ensured the correct management of possible risks, which sooner or later will lead to disruption of construction or operation	Probability: great Impacts: medium	***Measures:*** To ensure correction in co-operation with investor ***Execute:*** Competent manufacturer worker ***Responsibility:***

	technical work and will lead to accidents accompanied by enormous expenditure, disruption of citizens' safety and problems with public administration.		Manufacturer director
Natural disaster, fire	Due to natural disaster or fire occurrence, works on technical facility manufacturing will be disrupted, which will lead to delay in completion or to quality reduction, which will lead to delay in operation start, additional expenses (including the expenses on response and renovation of damaged parts of damaged buildings and fittings) and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: medium	***Measures:*** To ensure correction in co-operation with investor ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
Failure of technique, accident , failure of critical infrastructure	Due to occurrence such phenomenon it gets to disruption on technical facility manufacturing, which will lead to delay in operation start, additional expenses (including expenses on response and renovation of damaged buildings and fittings) and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: great	***Measures:*** To ensure correction in co-operation with investor ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director

Insider	Due to insider occurrence it gets to disruption on technical facility manufacturing, which will lead to delay in operation start, additional expenses (including expenses on response and renovation of damaged buildings and fittings) and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: great	***Measures:*** To build safety culture and to motivate workers to work targeted to tasks fulfilment ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
Terrorist attack	Due to occurrence such phenomenon it gets to disruption on technical facility manufacturing, which will lead to delay in operation start, accident of failure of facility, additional expenses (including expenses on response and renovation of damaged buildings and fittings), environmental damages and damages on health's of employee and humans in technical facility surrounding and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: great	***Measures:*** To ensure correction in co-operation with investor; i.e. response and renovation, and improve physical protection and guarding the workplace ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director

Financial crisis	Due to occurrence such phenomenon it gets to lack of finances, which will lead to delay in operation start, accident of failure of facility, additional expenses (including expenses on response and renovation of damaged buildings and fittings), environmental damages and damages on health's of employee and humans in technical facility surrounding and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: medium to great	***Measures:*** To ensure protection measures and way of works in co-operation with investor and public administration ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director
War	Due to occurrence such phenomenon it gets to change of priorities of public administration, disruption on technical facility manufacturing, which will lead to delay in operation start, accident of failure of facility, additional expenses (including expenses on response and renovation of damaged buildings and fittings), environmental damages and damages on health's of employee and humans in technical facility surrounding and to reduction of welfare (disruption of security of citizens, unemployment and connected non-demanded social phenomena), i.e. to problems of public administration.	Probability: low Impacts: great	***Measures:*** To ensure protection measures and way of works in co-operation with investor and public administration ***Execute:*** Competent manufacturer worker ***Responsibility:*** Manufacturer director

In order to ensure the security and development of citizens and the whole of the State, it is necessary for the public administration to take proper care of citizens, property, finance and the environment, i.e. correctly fulfil the basic functions of the State. Since this is not a simple matter, as the dynamic evolution of the complex system of the world (the human system) brings more and more sources of risk, it is important not to overlook the risks and to work with them at the level of current knowledge and experience.

Good management of the State, based on quality data, their quality processing, well-established competences and well-fulfilled responsibilities, needs a quality tool for management. One well-proven tool is a well-designed risk management plan.

In order to the risk management plan may fulfil its role, it needs to be based on quality data processed by experts using the quality methods and be backed by legislation that ensures well-divided competences and enforces responsibilities, thereby contributing to building a safety culture in society.

7. CONCLUSION

The quality of technical facility project and manufacturing predetermines its safety throughout the operation. 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 [4,7,49].

The monitored phase of the technical facility lifetime covers a wide range of problems, e.g.:

- deep analysis and judgement of risks in territory to which technical facility is inserted,
- theoretical analyses of critical processes, fittings, equipment and sites and a proposal for practical implementation of technically and financially available countermeasures,
- selection of:
  - materials,
  - technical principles,
  - design and building procedures,
  - construction procedures,
  - identification of critical building and construction processes,
  - etc.,
- experimental verification of installed equipment and its operability under normal, abnormal and critical conditions,
- ensuring:
  - the durability,
  - the manageability of equipment and processes,
  - the required service life,
  - the quality and sufficient human resources,
  - the costs required,
  - the technical utilities,
  - the service,
  - etc.
- realization of buildings, structures and equipment in given conditions, etc.

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 (legislation, norms, standards) in context,
- 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" [58]. The grounds need to be inserted into the design.

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 for execution.

Since the design and construction of a technical facility is complex, the Process Safety Management (PSM) should be required for rational management of each process and for complete management is required the Safety Management System (SMS) [4,7,45,58) for rational management of each process. For practice, twelve methodologies for public administration are presented at work [102]:

1. Methodology for the determination of relevant natural and other disasters in the territory. The output is in the form of a matrix on the basis of which a qualified and transparent decision can be made on which disasters can cause a critical situation.
2. Methodology for determining the largest expected size of the disaster in the territory for the corresponding time intervals, i.e. for natural disasters for 50, 100, 200, 500, 1000 and 10000 years (i.e. 50 years, centenary ... disaster). The output for each disaster is in the form of a matrix on the basis of which a qualified and transparent decision can be made on which size the disaster can cause a critical situation.
3. M22ethodology for determining the decrease in the disaster impacts sizes with the growth of the distance from the disaster site origin. The output for each disaster is in the form of a scenario, map or graph, on the basis of which a qualified and transparent decision can be made on which distance (measured from the disaster origin site) and in which the azimuths, the disaster impacts no longer causing harm and damage to protected assets.
4. Methodology for the determination of anomalies in the territorial disaster impacts distribution. The output for each disaster is in the form of a scenario, a map on the basis of which qualified and transparent decisions can be made on the existence

of vulnerabilities where the disaster impacts may escalate, in which, unlike the surroundings, a disaster can cause a critical situation.

5. Methodology for the selection of unacceptable impacts in the territory. The output is in the form of a matrix in which the disaster´ return period and the overall impact of each disaster are considered.
6. Methodology for the assessment of potential damages to property caused by unacceptable impacts of disasters. The output is in the form of a sequential (flowchart) to determine asset damage. The basis is to sort assets in the territory into categories according to vulnerability.
7. Methodology for determining appropriate corrective actions for expected disasters. The outcome is a set of corrective measures against a particular disaster aimed at withstanding property in a territory that may be affected by the disaster.
8. Methodology for the selection of optimal corrective measures for the restoration of assets for expected disasters. The output is a set of optimal corrective measures against a particular disaster aimed at withstanding property in the territory that may be affected by the disaster. Optimisation is understood to be a selection of such corrective measures, which at the same time:
   - effectively and fast ensure the minimisation of losses on critical assets, i.e. on property without which the quality and safe life of people in the territory is not possible and further losses are incurred in the sections of the human system,
   - reduce assets vulnerability to a particular disaster,
   - are sufficiently effective,
   - they can be implemented in gradual steps at a certain time interval with regard to the sources of public administration, the state, legal and natural persons and citizens,
   - do not increase the vulnerability of property and territory to other potential disasters,
   - do not increase the vulnerability of other protected assets to potential specific disasters
   - effective to reduce the vulnerability of property to other disasters.
9. Methodology of implementation of corrective measures to ensure the restoration of assets. The result is the implementation of the project, which is selected and implemented in such a way as to meet all the requirements for the restoration of assets in the territory affected by the elemental or other
10. Methodology for establishing a database of corrective measures. The output is a structured database containing specified data on corrective measures for the restoration of assets in the area affected by the disaster, which is assembled for the territory.
11. Methodology for determining the relationship “costs of recovery vs. expected size of the disaster”. The result is the relationship between the costs on asset recovery and the size of the disaster for each individual disaster that may affect the area under review.
12. Methodology for determining the financial reserve. The output is to determine the size of the reserve according to the Swiss reinsurance company procedure for each

specific or critical disaster for the territory concerned and to propose how to ensure existing risks to property from disasters, i.e. the amount corresponding to the total damage is allocated by transferring part to an appropriate insurance undertaking and part of it moves to the Fund, with a regular contribution to the Fund set at 3 - 5 % of the value (damage) determined in the prescribed manner from the risk size, provided that the exact value is determines the annual political decisions.

Most of these methodologies can also be used for technical facilities in the event of external risk sources. For internal sources of risk, specific investigations should always be carried out or procedures should always be applied to analogue technical facilities where the conditions for technology transfer are met [92].

The results of the study show that designer´ competences are very important for:

- the application of the results of methods of risk analysis and evaluation,
- implementation of the methodology for analysing and assessing the risks adapted to the problem,
- emergency and crisis management,
- analysis of situations / activities / accidents,
- the transformation of policy into a real action,
- the conversion of accident statistics into action plans,
- strategic planning,
- hierarchy of problems,
- finding the right information and learning,
- critical analysis,
- designing the right solutions,
- communication,
- carrying out synthesis and adapting the wording intended for the public,
- ethics.

At each decision in favour of safety it should be remembered: all factors and processes that can be dangerous and how often they can occur; how large their impacts can be; how the size of the impacts or frequency of occurrence can be reduced; whether the proposed measures cannot be a source of new hazards; and which technical and control systems can be controlled by hazards that cannot be prevented.

Finally, it should be noted that, in line with the results at work [4], it is essential what is the political will to create a system to protect against unacceptable impacts of harmful phenomena, i.e. natural and other disasters. An analysis of environmental development as well as the development of the political, social and economic situation in the world shows the need to prepare for the resolution of cases and actions that will cause critical situations by the intensity of impacts, and these are phenomena that do not today have such cruelty (severity) in the followed territory. Therefore, in terms of human security, the development of the human system, the existence, stability and development of the State, the concept of human safety and the subsequent concept of development must be codified and implemented through the management of safety

into practice. In order to manage the realisation of the risks, which are inherent in the present world using adequate forces, resources and means, it should be had:

- management principles for managing emergencies and critical situations, especially those of a large range,
- allocation of resources,
- and allocation of responsibilities.

The research showed that:

- each technical facility design has a certain danger. The designer art is to select such solution that is optimal, i.e. it is sufficiently safe and it is possible to realize with regard to investor and public administration options. The near the same holds for manufacturer´ skill (craftsmanship) at realization,
- impressive and low robust designs with insufficient safety margins often fail sooner or later,
- wrongly determined limits and conditions for critical technical facility parts lead to frequent disturbances up to serious accidents; they are not able to react to condition changes.

The analysis of accessible legislations [49] revealed that rules in force do not require to follow operation process safety in designing, and this occasionally leads to problems at operation, which is revealed e.g. in [103].

REFERENCES

[1] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Analysis, Management and Trade-off with Risks of Technical Facilities.* ISBN 978-80-01-06714-7. Praha: CVUT 2020, 172p. http://hdl.handle.net/10467/87451

[2] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Management of Risks of Processes Connected with Technical Facility Manufacturing and Commissioning* (in Czech). ISBN 978-80-01-06609. Praha: ČVUT 2019, 207p. http://hdl.handle.net/10467/84466

[3] BOSSEL, H., *System, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme.* ISBN 3-8334-0984-3. Norderstedt / Germany, 2004, www.libri.de

[4] PROCHAZKOVA, D. *Principles of Management of Risks of Complex Technological Facilities* (in Czech). ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/ 10467/72582

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

[6] PROCHÁZKOVÁ, D., PROCHAZKA, J. Concept of Safety of Complex Technological Facilities and Tools for Facility Safety Management. In: *Safety and Reliability – Theory and Applications.* ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, pp. 3559-3567. www.crc.press.com, www.taylorandfrancis.com

[7] PROCHÁZKOVÁ, D. *Complex Technological Systems Safety* (in Czech). ISBN 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.

[8] PROCHÁZKOVÁ, D. *Risk Analysis and Management* (in Czech). ISBN 978-80-01-04841-2. Praha: ČVUT 2011, 405 p.

[9] PROCHAZKOVA, D., PROCHAZKA, J. Alternatives of Work with Risks Used at Technological Facilities Safety Management. *International Journal of Economics and Statistics.* ISSN 2309-0685. 6 (2018), 3, pp. 1-7; http://naun.org/ cms.action? id=18790.

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

[11] 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.

[12] BEER, M., ZIO, E. *Proceedings of the 29th European Safety and Reliability Conference.* ISBN 978-981-11-2724-3. Singapore: ESRA 2019, doi:10.3850/978-981-11-2724-3_0095-cd. e:enquiries@ rpsonline.com.sg

[13] 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, 2362p.

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

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

[16] 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, 2453p.

[17] 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, 4560p.

[18] 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, 3387p.

[19] 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, 2942p.

[20] 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, 6889p.

[21] PROCHÁZKOVÁ, D. *Strategic Management of Safety and Organization* (in Czech). ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.

[22] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Trade-off with Them* (in Czech). ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234 p.

[23] PROCHÁZKOVÁ, D. *Critical Infrastructure Safety* (in Czech). ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[24] PROCHÁZKOVÁ, D. *Principles of Management of Critical Infrastructure Safety* (in Czech). ISBN 978-80-01-05245-7. ČVUT, Praha 2013, 223 p.

[25] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Risk Management at Technical Facilities Type and Site Selection.* ISBN 978-80-01-06718-5. Praha: ČVUT 2020, 86p. http://hdl.handle.net/10467/87352.

[26] KHAMINWA, A. N. *Coexistence." Beyond Intractability*. In: *Conflict Information Consortium*. Boulder: University of Colorado 2003. http://www.beyondintractability.org/essay/coexistence

[27] KOEPKE, G., YOUNG, W., LADBURY, J., CODER, J. *Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure*. NIST Technical Note 1885. http://dx.doi.org/10.6028/NIST.TN.1885

[28] LADBURY, J. M., KOEPKE, G. H., CAMELL, D. G. *Evaluation of the NASA Langley Research Center Mode-Stirred Chamber Facility*. NIST Technical Note 1508. 1999.

[29] IEC. IEC 61000-4-3 ed3.2, Electromagnetic Compatibility (EMC) - Part 4-3: Testing and Measurement Techniques – Radiated, Radio-Frequency, Electromagnetic Field Immunity Test. http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/43958

[30] IYER, A., ROSENBERG, C., KARNIK, A. What is the Right Model for Wireless Channel Interference? *IEEE Transactions on Wireless Communications*, 8 (2009), 5.

[31] MA, R., MENG, W., CHEN, H., HUANG, Y. Coexistence of Smart Utility Networks and WLAN/ZigBee in Smart Grid. In: *IEEE Third International Conference on Smart Grid Communications (SmartGridComm),* 2012, pp. 510-520.

[32] IEEE. IEEE Std 1900.2TM - 2008, Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence between Radio Systems.

[33] OECD. Machine-to-Machine Communications: Connecting Billions of Devices. *OECD Digital Economy Papers*, No. 192, Paris: OECD 2012. http://dx.doi.org/10.1787/5k9gsh2gp043-en

[34] PROCHÁZKOVÁ, D. ET AL. *Risk of Processes and Their Management*. ISBN 978-80-01-06144-2; e – ISBN 978-80-01-06186-2. Praha: ČVUT 2017, 295 p.

[35] UNISDR. *Sendai Framework for Disaster Risk Reduction 2015-2030*. United Nations Office for Disaster Risk Reduction: Geneva UN 2015. http://www.unisdr.org/we/inform/publications/43291

[36] TURNER, B. *Man-made Disasters.* New York: Wykeham Science Press 1978.

[37] PERROW, CH. *Normal Accidents: Living with High-Risk Technologies.* Princeton: Princeton University Press 1999.

[38] SAGAN, S. *The Limits of Safety.* Princeton: Princeton University 1993.

[39] UN. *Human Development Report*. New York… UN, 1994, www.un.org.

[40] KECECIOGLU, D. *Reliability Engineering Handbook.* Englewood Cliffs, New Jersey: Prentice-Hall 1991.

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

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

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

[44] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a

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

[46] RAUSAND, M. *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons 2014, 421p.

[47] EPSTEIN, W. Not Losing to the Rain: What I Learned when I Learned about Onagawa. In: *Safety and Reliability of Complex Systems*. ISBN 978-1-138-02879-1. London: Taylor &Francis Group 2015, pp. 365-371.

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

[49] CVUT. *Database on World Disasters, Technical Entities Accidents and Failures – Causes, Impacts and Lessons Learned.* Praha: CVUT 2020.

[50] IEC. *IEC 61511:2016 Functional Safety—Safety Instrumented Systems for the Process Industry Sector*.

[51] ISO. *ISO 12100. Safety of Machinery—General Principles for Design—Risk Assessment and Risk Reduction.* Berlin: Beuth Verlag GmbH 2010.

[52] ISO. ISO 13849-1, 2015. *Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design.* Berlin 2015.

[53] ISO. *ISO 16090-1: Machine Tools Safety—Machining Centres, Milling Machines, Transfer Machines—Part 1: Safety Requirements.* Berlin 2016.

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

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

[56] OECD. Guiding Principles on Chemical Accident Prevention, Preparedness and Response. Paris: OECD 2003, 192 p.

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

[58] 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.

[59] LEVESON, N., DULAC, N., MARAIS, K., CARROLL, J. *Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems*. https://doi.org/10.1177/0170840608101478

[60] TEICHOLZ, E. *Facility Design and Management Handbook.* ISBN 978 007 135 3946. London: McGRAW-HILL; https://www.accessengineeringlibrary.com

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

[62] COASE, R. H. The Problem of Social Cost. *Journal of Law and Economics,* 3 (1960), pp. 1-44.

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

[64] KLETZ, T. *Process Plants: A Handbook for Inherently Safer Design* CRC. ISBN 1-56032-619-0. London 1998.

[65] HEIKKILÄ, A.-M. *Inherent Safety in Process Plant Design. An Index-Based Approach*. ISBN 951-38-5371-3. Helsinki: VIT 1999, 132 p.

[66] KLETZ, T. A., *Plant Design for Safety – A User-Friendly Approach*. New York: Hemisphere 1991.

[67] *PAPADAKIS, G. A., AMENDOLA, A., eds. Guidance on the Preparation of a Safety Report to Meet the Requirements of Council Directive 96/82/EC (Seveso II.* ISBN 92-828-1451-3*. Archived from the Original on 2008-05-11.*Technical Research Centre of Finland 1997, VTT Publications 384. ISBN 951-38-5371-3.

[68] HENDERSHOT, D. C. *Inherently Safer Design: An Overview of Key Elements*. 2011. http://www.allbusiness.com/safety-accidents-disasters/accidents-chemical/ 15519792-1.html#ixzz1Y7Tswa3b

[69] MANSFELD, D., POULTER, L., KLETZ, T. *Improving Inherent Safety* OTH 96 521. London: HSE 1996. ISBN 0-7176-1307-0, 85 p.

[70] http://eippcb.jrc.ec.europa.eu/reference/

[71] OECD. *Best Available Techniques for Preventing and Controlling Industrial Pollution, Activity 2: Approaches to Establishing Best Available Techniques (BAT) Around the World, Environment*. Paris: OECD 2018, 151 p.

[72] THOMSEN, P. *10 Schritte zur optimalen, auf Dauer technisch Dichten Dichtverbindung.* ISBN 3-934736-27-0. Bremen: GmbH, 2015, No 2.

[73] IAEA. *Assessment of Defence in Depth for Nuclear Power Plants*. ISBN:92–0–114004–5. Safety report series No. 46. Vienna: IAEA 2005, 119 p.

[74] IAEA. Safety of Critical Power Plants: Design. *Safety Standards Series No. NS-R-1*. Vienna: IAEA 2000.

[75] EU. *Accidental Risk Assessment Methodology for Industries in the Framework of the SEVESO II Directive. EVG1-CT-2001-00036* (ARAMIS). http://aramis.jrc.it

[76] ZIO, E. Some Challenges and Opportunities in Reliability Engineering. *IEEE Transactions on Reliability.* 65 (2016), 4, pp.1769–1782.

[77] SKLET, S. Safety Barriers: Definition, Classification, and Performance. *Journal of Loss Prevention in the Process Industries.* 19 (2006), 5, pp. 494–506.

[78] PROCHÁZKOVÁ, D., PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z. *Management of Risks of Processes Connected with Specification and Location of Technical Facility in Territory* (in Czech). ISBN 978-80-01-06467-2. Praha: ČVUT 2018, 134 p., http://hdl.handle.net/10467/78522

[79] PROCHAZKOVA, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.

[80] HOLLNAGEL, E., WOODS, D., LEVESON, N. *Resilience Engineering*. Ashgate 2006.

[81] HOLLNAGEL, E., NEMETH, C., DEKKER, S. Remaining Sensitive to the Possibility of Failure*. Resilience Engineering*, 2008 v. 1. Aldershot, Ashgate.

[82] https://phys.org/news/2017-05-world-cyber-specialists.html

[83] VATN, J. Structuring Contributors to Successful Operation. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group, 2014.

[84] SEVCIK, A., GUDMESTADO, T. Solutions and Safety Barriers: The Holistic Approach to Risk-Reducing Measures. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014.

[85] EM-DAT: *The OFDA/CRED International Disaster Database* – www.emdat.net – Université catholique de Louvain – Brussels – Belgium. www.emdat.be

[86] PROCHÁZKOVÁ, D. Real Problems of Critical Infrastructure Threatening the Region Safety. In: *Reliability, Risk and Safety* . ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, pp 2387-2394.

[87] PROCHÁZKOVÁ, D. Critical Infrastructure and Principles for Its safety (in Czech). In: *Technologies and Prosperity*, Praha 2009, CD ROM, ISBN 978-80-87205-09-9, 84p.

[88] KUDĚLKA, V. AT Al. *Technical Requirements on Construction, Products, technical and Technological Equipment and Structures* (in Czech). ISBN 978-80-87102-19-0. Brno: TESYDO, s.r.o. 2018, 720p.

[89] KREINDL, M., ŠMÍD, R. *Technical Diagnostics* (in Czech). ISBN 80-7300-158-6. Praha: BEN 20006, 466p.

[90] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data and Methods for Their Processing for Engineering Disciplines Needs* (in Czech). ISBN 978-80-01-05792-6. Praha: ČVUT 2015, 186p.

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

[92] PROCHÁZKOVÁ, D. Examination of Core of Complaints and Conflicts Concerning Technical Solutions (in Czech). *Kontrola MSK ČR 1992*. MSK ČR Praha, 95p.

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

[94] DELONGU, B. *Risk Analysis and Governance in EU Policy Making and Regulation.* ISBN 978-3-319-30822-1. Springer 2016, 288p.

[95] PROCHÁZKOVÁ, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.

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

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

[98] EU. *Land Use Planning Guidelines in the Context of Article 12 of the SEVESO II DIRECTIVE 96/82/EC as Amended by DIRECTIVE 105/2003/EC*. Brussels: Joint Research Centre 2006.

[99] CUI, T., OUYANG, Y., SHEN, Z. J. M. Reliable Facility Location Design under the Risk of Disruptions. *Operations Research,* 58 (2010),1, pp.998-1011.

[100] LEVITT, R. E., LOGCHER, R. D., QUADDUMI, N. H. Impact of Owner-Engineer Risk Sharing on Design Conservatism. *ASCE Journal of Professional Issue in Engineering.* 110 (1984), pp. 157-167.

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

[102] PROCHÁZKOVÁ, D. *Methodology for Estimation of Costs for Property renovation in Territories Affected by Natural or Other Disaster* (in Czech). Ostrava: SPBI SPEKTRUM XI 2007, ISBN 978-80-86634-98-2, 251p.

[103] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Management of Risks of Processes Connected with Technical Facility Operation at Life Cycle* (in Czech). ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465p. http://hdl.handle.net/10467/85867. doi:10.14311/BK.9788001066751

ANNEX 1 – Integral safety

Globalisation, on the one hand, and regionalisation or decentralisation (e.g. the idea of 'Europe of the regions') on the other hand mean mutually complementary processes that are often expressed by the slogan "think globally, act locally". However, their implementation requires that the attitude to security and safety might be reconsidered, on the one hand in the context of the growing complexity and vulnerability of contemporary society (critical processes, critical elements, critical objects, critical infrastructure and its functions) and on the other hand in the context of the undeniable changes that we observe (and may expect) in the human system, e.g.: in the environment, it goes on climate changes, landscape changes, etc.; and in the human society, it goes on dehumanization, great dependence of individuals on property, loss of such values as friendship, etc.

Considering these contexts, it is clear that security and safety need to have a wider social dimension, i.e. they need to express social, economic, cultural and ethno-political factors, and all government offices need to deal with them. This pays not only for central public authorities, but also for local public authorities and, in fact, for all those involved [1]. The public administration's position on security and safety for the citizen legitimizes its activity. The public administration is responsible for security and safety in the entrusted territory, namely for all facilities inserted in it, i.e. the safety should be continually a public service that does not deregulate or privatise. Thus, the starting points for the present concept of safety have a much broader basis than previously formulated safety on the state level.

At present, the division of safety into external and internal is no longer sufficient, but safety needs to be understood from a systemic point of view [1]. From the system viewpoint, ensuring the safety is the basic requirements on system as a whole, not only demands on its components; system scheme of safety management at certain situation is shown in Figure 1. From the process model of building the safety and security in Figure 1, it is clear relation between safety and security; their often-discussed conflict is removed.

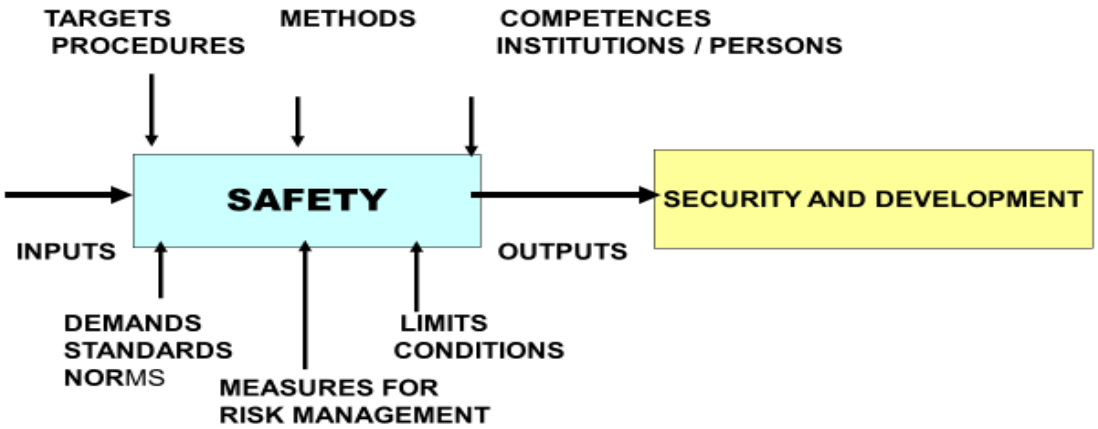

Figure 1. Process model for ensuring the security and development of entity.

The requirement for a systemic concept of safety complies with the concept of integral safety introduced by the United Nations in 1994 [2]. Wever [3] supported the introduction of the term in 1995 for the following reasons:

1. A way of perceiving the safety by a citizen. Unlike the central public administration institutions, the citizens see the safety primarily as a local problem, and therefore, they expect the local solutions that may vary from case to case. In other words, the citizens are particularly interested in their security, i.e. in security in the place where they live.
2. Security policy should cover a causal chain that solves the safety issues. The integral safety is not limited to unilateral solutions in the event of problems such as repression, but it deals with situations affecting a certain level of safety through so-called "the safety chain", which consists of the following parts:
   - proactivity (it eliminates the structural causes of uncertainty that undermines the safety, i.e. which they threaten security and sustainable development),
   - prevention (it eliminates direct causes of precarious situations infringing the present safety, if possible),
   - preparedness (it addresses to situations in which safety is impaired),
   - repression - response (it manages faults of safety, stabilises the situation and ensures conditions for recovery and growth of safety).
3. The level of danger is territorially dispersed, and this dispersion is not even. Some safety problems are concentrated in certain areas, with types of safety problems (i.e. in terms of work [1] (disasters)) may not be and in practice are usually not the same.
4. Public administration often faces ineffective and inefficient solutions to safety problems. This fact is the result of the so-called "safety bureaucracy", which does not deal at all with the causal chain of safety. It is the result of a lack of understanding the concept of safety in reality (in a given case), i.e. it is the consequence of misunderstanding the links associated with the creation of safety and security as shown in Figure 1, which shows that the level of safety predetermines the level of security of the system (i.e. the territory or technical facility which we monitor).

However, the concept of integral safety is slowly expanding in practice for the reasons set out in [1]:

1. Integrity is understood more as an organizational aspect with horizontal and vertical connection among components / organs, i.e. not in the concept of a system with components, linkages and flows, and its understanding is mainly associated with police forces or the military.
2. There is still no satisfactory and generally accepted definition of integral safety in legislation.
3. Implementation of the concept of integral safety is in practice time-consuming (especially in domain of data collection and their analyses).
4. Local public authorities do not know "to deal with safety problems" because they focus too much on local problems.

However, the safety as a quantity / measure expressing the certain system behaviour, is not and cannot be isolated from its background. Each system and its surroundings are in interdependent relationship, which is due to the fact that each system is open system. The relationship in question can be characterized by some attribute of the system, such as adaptability, durability, flexibility and reliability [4].

To the concept of integral safety, they belong life-supporting functions, the risks of which with regard to human health, ecosystems and system safety are minimized. These are, in particular, possible non-demanded and unacceptable impacts, e.g.:

- industrial agriculture with regard to food safety,
- contamination of the environment,
- climate changes,
- lack of natural resources, energy and water,
- poverty and migration of humans,
- social discrimination,
- industrialisation and misuse of technologies,
- and gene manipulation.

It is, therefore, apparent that the security (in other words the system condition and its protected assets conditions) in relation to the environment needs to be specified in the context of sustainable development, i.e. to ensure its provision, the disasters should be monitored in the concept defined at work [1].

The Johannesburg World Summit on Sustainable Development has pointed out that the development in question needs to be carried out primarily at local level and should be focused on the following objectives:

- environmental quality protection,
- quality of human life (health and human security, social justice),
- resilience to disasters,
- and economic vitality.

Sustainable development is not a static state (conditions) of harmony of society and the environment, but it is a process of changes in resources use, technologies' focuses and institutional transformations in order to avoid possible irreversible difficulties. It is just one of the possible dynamic models of the development of the human system. However, in practice, especially in public administration decisions, the concept of sustainable development is not more pronounced. Intuitively, however, it can be assumed that development requires a certain degree of sureness and stability, which are significant attributes of safety and security.

Integral safety is directly linked to the concept of sustainable development, as it can be characterised as a set of conditions under which humans are protected. By these conditions, it is strengthened the humans´ ability to cope with serious and sudden threats to their survival (biological and social) and existence (health and housing), namely including the access to society's resources and the respect of human dignity [1]. Pillars of sustainable development are:

- environmental protection being related to environmental, technological and health safety,
- economic development being in relation to social, economic and technological safety,
- social development being linked to social, cultural, legislative and political safety.

Integral safety is measured using the indicators that already have a large number [1]. Indicators relevant to technical facilities were introduced by the OECD in 1992 [5]. In practice, it is always necessary to select indicators that are relevant to the objective of the task addressed; choice is a critical activity and the success of the solution is dependent on it. It should be noted that in practice the following types of indicators are used:

- contextual (input and output relationship),
- causal,
- trending,
- and stative (measuring the conditions).

According to the works [1,5] for the assessment of indicators, they are used the criteria for assessing:

- the validity, where there are evaluated aspects such as:
  - relevance and importance,
  - appropriate measuring scale,
  - correctness (relation to the system examined),
  - sensitivity (how system responds to changes),
  - distinguishability (resolution of natural variability from mand-made changes),
- the clarity, when there are evaluated aspects such as:
  - understanding (appropriateness of indicators for decision-making),
  - simplicity,
  - compliance with the interests of the public,
  - the possibility of presentation and documentation,
- the interpretation, when there are evaluated aspects such as:
  - robustness (the calculation is transparent and defensible),
  - interpretability (to current status, changes and trends),
  - credibility (the direction of change reflects certain experiences),
  - trend evaluation,
- the information richness,
- the data availability, when there are evaluated aspects such as:
  - sources for immediate use,
  - time series,

- the possibility of updating,
- updating,
- topicality,¨
- anticipation and symptoms of warning,
- cost-check and feasibility,
- comparison of the costs and benefits of the indicator,
- ease of quantification
- the cost of collecting data,
- the ease of calculations

- the procedure of work with indicators.

This overview may be supplemented by a selection of appropriate measuring and evaluation scales and a description of the data type: time series, spatial data from GIS, relative or aggregated data, average, median, percentile, distribution function, etc.

In the main text, the procedure of integral safety classification is based on multicriterial approach using the theory of utility [6] – it is constructed the decision support system for determination of criticality rate and the relation [7] is used:

rate of safety = 1 – rate of criticality.

References

[1] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organisation* (in Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.

[2] UN. *Human Development Report*. New York: UN, 1994, www.un.org.

[3] WEVER, J. *Integral Safety in Netherland*. Paper presented at the Australian Institute of Criminology in 2000, www.aic.gov.au/conference.

[4] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Analysis, Management and Trade-off with Risks of Technical Facilities.* ISBN 978-80-01-06714-7. Praha: ČVUT 2020, 172p. http://hdl.handle.net/10467/87451

[5] 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.

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

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

ANNEX 2 – Risk sources for technical facilities

The world and its parts are dynamically developed in time and space. This development is manifested by different processes that are inside and across of world´s structural systems that create them. These processes product different phenomena, and some of them damage humans and other public assets, i.e. including the technical facilities (we call them as disasters). The originated phenomena have the various sizes and cause the changes that have often highly unacceptable impacts on humans, namely directly or indirectly over the public assets that humans need for quality life and development. This reality causes that the accent is put on the management type called "disaster management" in which considering all disasters is denoted as „All Hazards Approach" [1]; its definition for Europe is in [2].

Among the disasters, we classify the phenomena that cause damage, losses and harms to humans and other public assets on which the humans are dependent. These phenomena are the results of five different processes in the human system that represents the world [3]. The results of processes:

- running in and out of the Earth are: *natural disasters* (earthquake, floods, drought, strong wind, volcanic activity, land slide, rock slide etc.); *epiphyte; epizootic; land erosion; desertification; fundament liquefaction; sea floor spreading etc*.
- running in the human body and in human society are: *unintentional:* illnesses; epidemic; involuntary human errors etc.; and *intentional*: robbery; killing; victimization; religious and other intolerance; criminal acts; terrorist attacks; local and other armed conflicts, bullying; religious and other intolerance; criminal acts such as: vandalism and illegal business, robbery and attacking, illegal entry, unauthorized use of property or services, theft and fraud, intimidation and blackmail, sabotage and destruction, intentional disuse of technologies, such as: improper application of CBRNE substances; data mining from social networks and other cyber networks used for psychological pressure on a human individual etc.
- connected with the human activities are: *incidents; near misses; accidents; infrastructure failures; technology failures; loss of utilities; etc*.
- that are reactions of the Planet or environment to the human activities are: man-made earthquakes; disruption of ozone level / layer; greenhouse effect; fast climate variations; contaminations of air, water, soil and rock; desertification caused by human bad river regulation; drop of the diversity of flora and fauna (animal and vegetal) variety; fast human population explosion; migration of great human groups; fast drawing off the renewable sources; erosion of soil and rock; land uniformity etc.
- connected with inside dependences in the human society and its surrounding separated to: *natural*: changes in stress and movements of territorial plates; changes in water circulation in the nature (environment); changes in substance circulation in the nature (environment); changes in the human food chain; changes in the planet processes; changes in the interactions of solar and galactic processes; *and human established*: the failure of human society management (organizational accidents caused by: mutual improper behaviour of an individual or groups of individuals as illegal migration of great groups of people; incorrect governance of public affairs - as: corruption, abuse of authority, the disintegration of human society into intolerant

communities; and failures in organization of education and upbringing etc.); the failure of correct flows of raw materials and products; the failure of correct flows of energies (harmful is e.g. blackout); the failure of correct flows of information; the failure of correct flows of finances etc.;*{word "correct" means the way in benefit of human interest, i.e. given by legislation}*.

The disaster sources are shown in Figure 1.

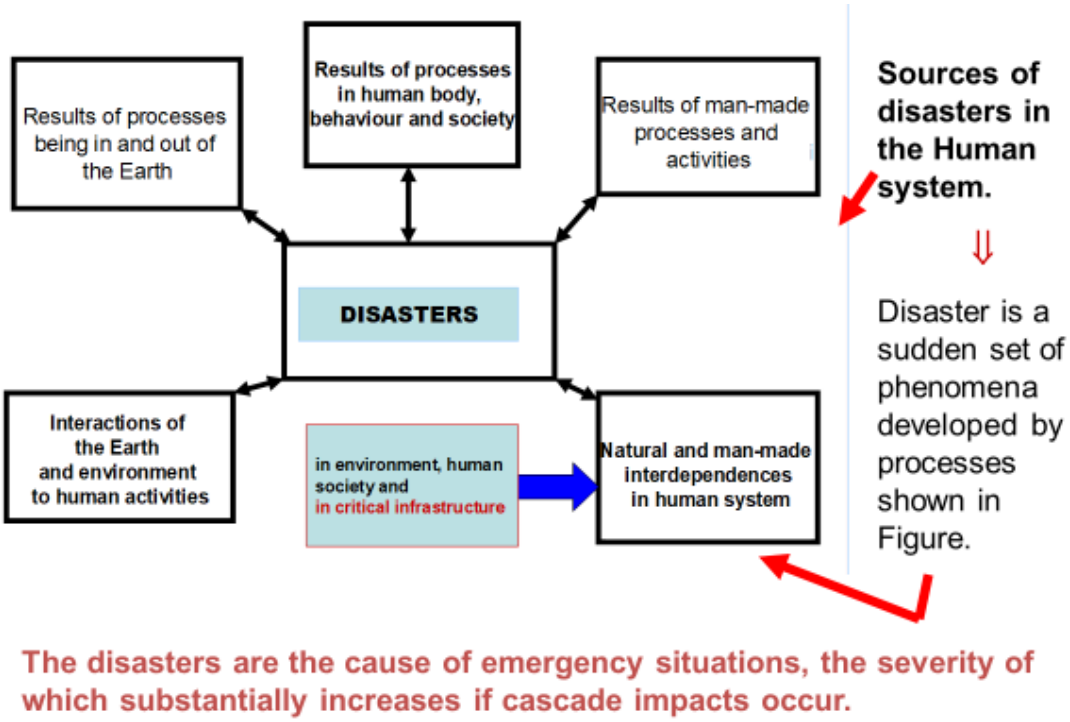

Figure 1. Sources of disasters.

Above facts show that disasters, according to the process, the product of which they are, have very mixed physical, chemical, economical, biological, social or cybernetic nature/basis. This mentioned fact is a clincher from the view of safety, because the preventive measures need to be targeted to the nature of disaster for the sake of being effective.

Definitions, features and impacts of disasters are listed in the works [3-6]. Generally, it stands that the disasters have certain characteristic features, which are the origin of impacts causing the damages, losses and harms to the important assets, links or flows and that from the human point of view, because this is de facto the only thing in which a human is interested (human aim is to make human to survive). Among the impacts it belongs e.g. vibration; directed fast air, water or soil flow; damage to a stability and cohesiveness of rocks and soil; liquefaction; displacements of materials; outburst of liquids; anomalies in the temperature etc.

The impacts effect directly or vicariously through links and flows of human system. Humans, thanks to their intellect, deliberately create the resilience of areas, buildings, infrastructures and technologies against disasters. They do with a help of both, the choice of elements, links and flows and their interconnection; and the specific preventive measures and activities until the specific disaster extent (which is given by human knowledge, abilities, financial and technical possibilities etc.) [3]. It makes why the impacts of interconnections in the system (interdependences) appear only with beyond

design disasters, which by their extent lays above the border size of disaster against which the humans systematically provide resilience [3]. Understandably, there is a big difference - rich technically developed and quality managed countries or organizations (generally entities) have the threshold of assets resilience set higher that the counties with a lower standard.

Disasters cause or from certain extend cause damage, loss and harm on assets, i.e. they are the reasons of situations falling on a human and that is why human has to handle with them. By the reason of big variety of disasters, the arising situations classified as “the emergency situations” have either the same or highly specified impacts. The relation between a disaster and an emergency situation is the relation *“cause-consequence”* [3]. This relation is not simple because the intensity (destructiveness, severity, criticality, cruelty) of emergency situation in a given place is predetermined not only by the size of disaster but also by the local vulnerability of assets, failure of implemented protective systems (e.g. the system of warning in the area, security mechanism etc.) which were created for increasing the assets resilience, the humans’ mistakes during the response etc. [3,4,7].

The internal risks in technical facilities originate at designing [5,7,8] at:

- selection of material for construction and equipment,
- selection of ways of manufacturing,
- embedding of passive barriers, which prevent the phenomena as an expansion of fragments or dispersion of dangerous substances when the loss of cohesion of a device or construction (e.g., envelopes of different types),
- inserting the backup devices and systems, i.e. several devices having the same role, and respectively, using the different physical principles to achieve a task,
- inserting the protections of safety critical elements (e.g. containment, shelters),
- selection of types of control systems that according to continual monitoring results adapt the operation,
- neglection of means for organisational measures to protect both, the employee, labour environ and also surroundings from the harmful impacts, and the construction and equipment from the great destruction because the complex technological facilities are not cheap and for preservation of the capability of development there are their products required.

According to [8], the risks at design are mainly connected with:

- neglecting the changes of conditions of internal technical parts during the time; they are not possibilities for maintenance and repair,
- neglecting the changes of internal technical processes during time; they are not possibilities for maintenance and repair,
- unexpected and wrongly managed organisational processes; void, interlaced and inexplicit arrangement of fittings, components and systems.

Figure 2 shows the logical idea of the occurrence of the organizational accident, which occurred on the basis of the formation of the process that occurred when the gaps in the protective barriers of the technical facility were interconnected due to shortcomings caused by errors in the design of the technical facility and in the acts of its management.

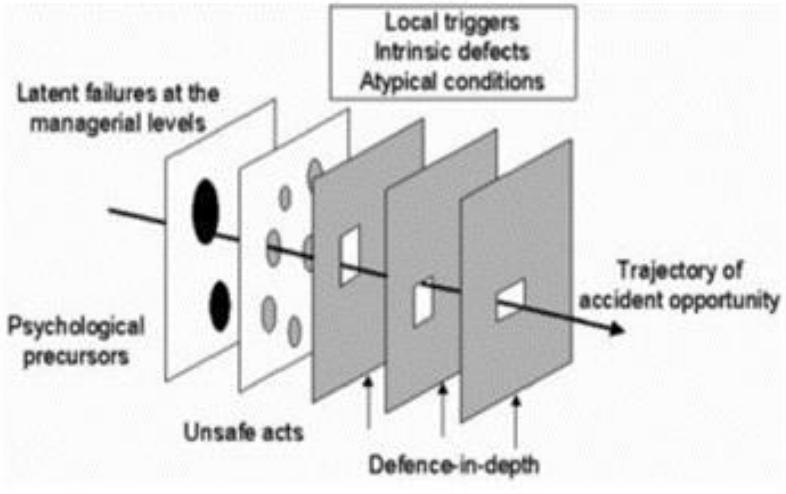

Figure 2. An organisational accident model indicating the basic barriers to prevent a crash and are created in the context of the management of the safety of a technical facility; processed according to [9].

References

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

[2] PROCHÁZKOVÁ, D. *Study of Disasters and Disaster Management*. ISBN: 978-80-01-05246-4. Praha: ČVUT 2013, 202p.

[3] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organisation* (In Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.

[4] PROCHÁZKOVÁ, D. Principles of Mitigating and Managing Human System Risks. *Information & Security*, 28 (2012), No 1, 21-36, ISSN: 0861-5160, e-ISSN 1314-2119, http://infosec.procon.bg

[5] CVUT. Czech Technical University archives.

[6] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Their Control* (in Czech). ISBN: 978-80-01-05479-6. Praha: ČVUT

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

[8] PROCHAZKOVA, D. *Analysis and Coping with Risks Connected with Technical Facilities* (in Czech). ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222p. http://hdl.handle. net/10467/78442

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

ANNEX 3 – Hazard determination

The quantity “hazard” is defined in work [1] as a set of maximum disaster impacts that are expected in a given place in specified time interval with a certain probability. According to technical norms and standards, the normative hazard is determined by identified size of disaster (so called design disaster). Hazard expresses the disaster potential to cause at origin losses, damages and harms on assets in a given site.

1. Introduction to problem

Procedures for determining the hazard posed by individual disasters for humans, a real territory and real complex technical facilities have been evolved over time [2,3]. From the estimates based on the selection of the maximum observed size of the disaster in the place since the historic to the present, through the application of:

- the methods of mathematical statistics,
- algorithms of theory of limit / marginal values,
- theory of large numbers,
- mathematical modelling,
- analysis based on the probability of boundary values,
- analysis based on the upper and lower estimates of the values of the occurrence probability,
- the theory of fuzzy sets,
- the theory of options until after the theory of Dempster-Shafer [4,5], which combines accurate calculations and heuristics, and in this way, it is considering the random uncertainty and epistemic uncertainty in the mode of occurrence of the disasters.

In work [6], it is given an example for the earthquake, which shows the variance between values obtained by different approaches.

It is to be noted that when determining the hazard, the incorrect data are often used (incomplete or short time series) or incorrect calculation procedure is, of course, it is endangered the safety of the followed facility, see the examples for the earthquakes, which are referred to in [7].

The impacts of disasters on the territory and on the complex technical facilities depend on the type of disaster [8,9], and on the vulnerability of given assets [2,8,9]. From safety reasons, we need in accordance with the practices of major reinsurance undertakings, such as Swiss Re, Munich Re and others, to know the size and properties of the maximum sizes of the disasters. By the methods used in the cases of long time series on the occurrence of disasters we are able to specify just the size of the maximum expected disasters (and it is still subject to certain restrictions), because of extreme disasters come irregularly and rarely; their return periods range from a few hundred to a few thousand years. It is true that each method has a discrimination capability [10].

After each major disaster, the engineers responsible for safety of complex technical facilities put questions [11]:

- may such a disaster occur in our country?
- how are our territory and our facilities protected in the case of the impacts of such large disasters?
- are ready support teams and the means for timely and adequate response?

Due to completeness, it is necessary to note, that we do not have a methodology for the evaluation of phenomena that are typical for the evaluation of hazards which represent real disasters for the interconnected systems with different sizes; for example, the reality is that a large disaster associated with processes in a hierarchically higher system will undermine the regimes of all systems at a lower hierarchy (see planetary earthquake, large solar flares). The consequence is both, the failure of modes of processes in the hierarchically lower systems and the occurrence of unusual disasters, i.e.. with unusual sizes or unusual characteristics. Many such examples it shows a detailed study of the seismic regime [12,13].

For obvious reasons, when determining the specifications for terms of references of the facilities from the well-known disasters, the list of which is in [2,3,14], there are considering only those that can have impacts in a given site. Because of the extreme disasters occur irregularly and sparse, so it cannot be used for determination of their size the common methods of mathematical statistics, and therefore, since the 1980s they have been used the methods based on the theory of extremes. A thorough analysis of the procedures applied to associate with applications on the existing knowledge of the physical medium [15] showed that the theory of extreme values is based on the following assumptions:

- the conditions that prevailed in the past, shall also hold in the future,
- the largest observed phenomena in a given time interval are independent,
- the behaviour of the greatest phenomena in a given interval will be the same in the future as in the past.

In practice, according to the theory of extreme values there are determined two quantities, namely: the return period; and the annual probability of excess.

2. Determination of size of maximum expected disaster

The theory of extreme values is a specific sector of mathematical statistics, which deals with the development of methods and techniques for describing, modelling and prediction of unusual and little frequent phenomena, which may occur in many areas of human activity. In these cases, it is always necessary to estimate or predict the level of values for some of the real process, usually outside the range of the observed data yet.

On the basis of theoretical studies [13,15,16], described in the works carried out for real time series of observed values, which have expressed the occurrence frequency given by relationship

$$\log N_{ci} = a - b\, M_{oi}$$

in which ***for i = 1,2, ..., n*** they indicate N_{ci} cumulative frequency M_{oi} the size of the disaster, ***a***, ***b*** the numerical parameters, provided that the above mathematical terms it is a hazard ***H = value of*** $M_{o\,i}$, for which the probability of not exceeding the level is $R_t(M_o \geq M_{oi}) = 0.05$ for the chosen time interval and they hold relationships

$$R_t(M_0 \geq M_{0i}) = 1 - \left[\frac{T}{T + t \cdot P(M_0 \geq M_{0i})}\right]^{n+1}$$

$$P(M_0 \geq M_{0i}) = \frac{e^{-\beta M_{0i}} - e^{-\beta M_{0max}}}{e^{-\beta M_{0min}} - e^{-\beta M_{0max}}}$$

The format of the results is shown in Figure 1 for time intervals ***t = 0.5 in, 1 year up to 1000 years***.

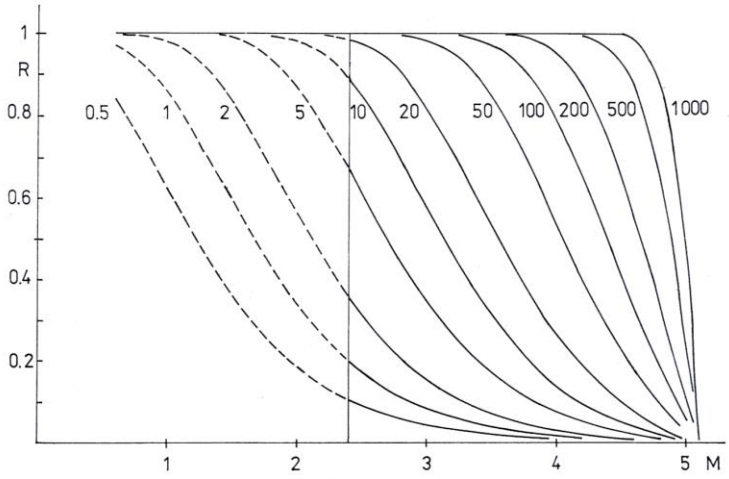

Figure 1. The course of the function describing the probability of not exceeding for the time intervals 0.5, 1,2, ..., the 1000 years.

The size of the largest expected disaster ***M*** is determined as the intersection of the curves on Figure 1 with the chosen level of significance. Significance level reflects the inaccuracy with which we determine the conclusion – the most commonly it is chosen ***v = 0.05*** or ***0.01.*** Value of 0.05 means the possibility of error 5%, ***p = 1 - v*** is the probability with which the result is correct.

The mean return period τ for disaster with the size ***M_o = time t,*** for which it holds the equality

$R_\tau = 0.633.$

In cases in which the time series is not available, they are made the estimates; for example: the size of the largest observed disaster for technical facilities — the participation of all hazardous substances in the stack, object, etc. The estimates are very imprecise, because it usually is in the accident involved only some part of the substances, or observations are from a very short time, and therefore, it cannot be determined nor mathematically variance of the values.

At determining the hazard, there are used the deterministic and probabilistic approaches with the fact that when the application it is usually added the safety reserve. This means that in practice they are only considered random uncertainty, i.e., no epistemic uncertainty.

For the place in which is located the complex technological facility from the specified maximum size of maximum expected disaster it needs to determine the disaster size for the place, in which is located the facility, i.e. it needs to consider the attenuation of size of impacts with distance and other physical factors that for real disaster affect the size of the impacts in a particular site.

3. Attenuation of disaster impacts´ size with distance and influence of anomalies in medium

On the basis of knowledge about individual disasters [8,9,11-13,15-17] the attenuation of the impacts´ sizes of the disaster with the distance depends on:

- the nature of the phenomenon (natural disaster, fire, explosion, technological accident, etc.),
- the mechanism of the origin of the phenomenon (usually it determines the distribution of impacts in the near zone),
- structure and properties of physical medium (that usually prevail in the far zone).

Examples of dependencies used in practice are:

- empirical – examples are in [6] – usual problem is large dispersion among regions,
- mathematical

$I_n = I_o \; e^{-\alpha D_n}$ - very rough estimate

$$I_0 - I_n = \nu \log \frac{D_n}{h} + 3\beta(D_n - h) \log e$$

in which I_0 is the size of the impact of disasters in the place of origin, I_n the size in place far away from the place of origin by D_n , h is the distance of place of origin from the Earth's surface locations, r_n, the distance measured along the Earth's surface ($D = \sqrt{(r^2 + h^2)}$, α, ν and β are numerical parameters. The first relation is just a very rough estimate, which applies only to the homogeneous and isotropic physical medium [9,15,16].

Since no real system (medium), i.e. territory, human society, technical facility, is not homogeneous and isotropic, there are not only regional and local dependencies, but also the anomalies (for example in detail for the earthquakes in [9,11-13]. The causes of the anomalies are:

- structural inhomogeneity,
- sources of domino effects,
- causes of synergies and accumulations.

Therefore, it needs to be carried out when are setting the terms of references the thorough investigation of vicinity of the complex technological facility and on its basis, then it is set the value of a site-specific hazard for a specific disaster.

4. Determination of size of design disaster for terms of references

Damages, losses and harms associated with disasters of all kinds, depend not only on hazards posed by the disaster, which are calculated on the basis of the characteristics for the occurrence of disasters, but also on the vulnerabilities of site and of its surroundings in which the facility is located, and on the vulnerabilities of the technological facility itself [2,9,12,15, 18,19].

Therefore, the credible specifications (terms of references) for the safe technological facilities are not only compiled on the basis of the results of the calculations which were characterized in the previous paragraphs, but they are corrected on the basis of a detailed study of the conditions in the surrounding territory, namely in several levels:

- regional,
- vicinity,
- near vicinity,
- and the site itself.

Their exact destination substantially depends on the disaster and on the real technological facility [18-21].

To the value of the local hazard obtained by calculating or by estimation according to relationship specifically derived for the given disaster and the territory, it is added the safety reserve, which shall be determined by a thorough investigation around the place, which is selected for the complex technological facility. According to the nature of a real disaster, there are pursued the specific features in the territories bounded by radii: 1 km; 5 km; 25-50 km; and greater than 150 km. In the case of significant structural anomalies, they are added the safety reserves on the basis of good engineering practice. The complexity of the analyses they show the analysis that have been made to the earthquakes [9,21]:

1. Regional research covers the territory within a radius of 150 - 400 km around the site of a technological facility and its aim is to assess the ability of the geodynamic structures because the greater impact of earthquake under certain real conditions. The research is carried out by expert assessment and in relevant cases to the calculated site hazard value is added the safety reserve; a number of examples is in [21].
2. Investigation of the near vicinity covers the territory within a radius of 25 - 50 km around the site of a technological facility and its aim is to assess the ability of geological structures to invoke the higher impacts of disaster on the technological facility from the perspective of stratigraphy, structural geology and tectonic history under certain real conditions. The research is carried out by expert assessment and in relevant cases, to the calculated site hazard value is added the safety reserve; a number of examples is in [21].
3. The investigation of the vicinity is carried out in the territory of about 5 - 10 km radius around the site of a technological facility and its aim is to assess the ability of the subsoil and its fabric composition cause higher impacts of disaster on the technological facility under certain real conditions. The research is carried out by expert assessment and in

relevant cases, to the calculated site hazard value is added the safety reserve; a number of examples is in [21].

4. The investigation of the site is carried out in the territory of about 0.5 - 1 km radius around the site of a technological facility and its aim is to assess the ability of the conditions of the hydrological, meteorological, hydrogeological and geotechnical characteristics, subsoil liquefaction and the composition of the slide material cause greater impact on technological facilities under certain real conditions. The research is carried out by expert assessment and in relevant cases, to the calculated site hazard value is added the safety reserve; a number of examples is in the [21].

Similarly, large territories as at the earthquakes are considered when evaluating the tornados, hurricanes, extreme rainfalls, etc. [11,21].

By that way, the resulting values of criticality for each disaster include in terms of references, which therefore summarize the parameters of design disasters. Using the terms of references the designers propose the parameters for design of technological facility (a way of foundation, specification of materials used, method of building, method of construction, types of equipment, fastening devices, etc.), so that it was ensured against the impacts of all the disasters with sizes less than or equal to the sizes of design disasters. Then, the criticality assessment is completed by calculation of the hazard from the downs of aircraft and from possible explosions in the immediate surroundings.

On the basis of the interface of design parameters with the parameters of technological processes it is then provides possible malicious processes for the actual technical facility and their risks [2,3,11,12,15,16,18-20], namely either, provided that the process is deterministic or random. ***Deterministic processes*** are described by analytical functions of time, and therefore, it can be at any point in time determined their values. ***Random processes*** are described by the probability function, that in each moment determines the probability of the possible values, which it can accidentally acquire process realization. ***Random process is stationary****,* when the probability density function is independent of the choice of the beginning of the timeline (i.e. the mean value does not depend on time). The statistical properties of no stationary processes are variable in time. ***Random process is ergodic,*** when all of its implementations have the same statistical properties (it allows to estimate the parameters of the process from one implementation or the long-term process of the use of data from several different starting conditions); this is often tacitly assumed at calculations - and it can be a source of errors.

5. Risks and instructions for their getting over in benefit of safety

Damages, losses and harms caused by the disaster to the asset or of the system, i.e. to the facility depend on the physical, chemical, biological and temporal characteristics of disaster and the characteristics of the followed facility, namely the technical and social ones. Direct damages are due to direct exposure to the disaster. Indirect damages are caused by the domino effects, i.e. by other disasters, which trigger the original disaster and by disorders of the infrastructures, which lead to a disruption of life sustaining services.

To ensure the safe territory and safe facility it is in practice for management needs (see the procedures for insurance companies and designers) computed the expected average annual damage

$$OPR = \Sigma_i OPR_i * N(i),$$

where the OPR_i is the expected damage when ***i***-the phenomenon and the ***N (i)*** is the annual occurrence frequency of the phenomenon.

At the critical complex facilities, it is in process management [22] counted the so-called ***RPN* value** – i.e. the order of priority of risk with regard to the potential failure by help of the relationship

$$RPN = S * O * D,$$

where ***S*** is the severity of the impact ***O*** the occurrence probability and ***D*** is detection. Criticality is determined by

$$C = S * O * B,$$

where ***S*** is the severity of the largest impact , ***O*** the occurrence probability of the, and ***B*** the conditional probability that it occurs the most serious impact.

At design and operation of each complex technical facility, it is necessary to consider the total risk ***R***, which includes both, the direct and the indirect losses on assets. Analysis of the emergency situation caused by disasters [9,11, 21] shows that indirect losses are increased by:

- delays or errors in the response,
- cascades of failures caused by synergic and cumulative effects, which are caused by links and couplings among assets
- domino effects.

According to [1,2] the total (integral) risk, which it is the need to cope can be mathematically expressed by a relationship

$$R(H) = \left[\sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int F(H, A_i, P_i, O, t) \mathrm{d}S \mathrm{d}t \right] \cdot \tau^{-1}$$

where: ***H*** - hazard; A_i – the value of assets, ***i = 1,2, ..., n,*** where ***n*** is the number of monitored assets; Z_i – the vulnerability of assets, ***i = 1,2, ..., n***; ***F*** --loss function; P_{ij} – the occurrence probability of asset damage – conditional probabilities; ***O*** – vulnerability of safeguard measures; ***S*** – followed territory / facility; ***t*** – time that is measured from the origin of the harmful phenomenon; ***T*** – time for which they arise losses; and τ - return period for the disaster.

Due to the loss function unknowing, for the management and trade-off with risks, it needs to use the procedure shown in Figure 2, which is the result of detailed research [2,3].

In practice, however, simpler procedures for hazard assessment are used, namely the PSA method based on the application of the trees, which copied the architecture of the facility production devices, and this cause that it does not see the interdependences, nor in the facility, nor among the facility and its surroundings [11,18-20].

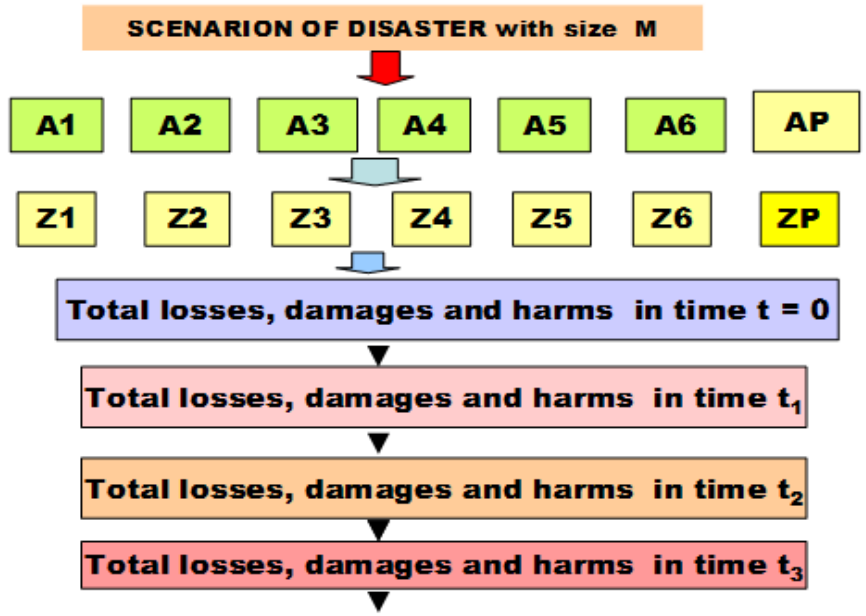

Figure. 2. Flowchart for determining the risks which is used in practice for the strategic management of safety; A – assets and Z losses, damages and harms to the assets; Description: 1-the human lives and health, 2- human security, 3 - property, 4 - the public welfare, 5 - the environment, 6 - infrastructures and technologies, P – private.

References

[1] PROCHAZKOVA, D., PROCHAZKA, J. *Analysis, Management and Trade-off with Risks of Technical Facilities.* ISBN 978-80-01-06714-7. Praha: ČVUT 2020, 172p. http://hdl.handle.net/10467/87451.

[2] PROCHÁZKOVÁ, D. *Risk Analysis and Management* (in Czech). ISBN 978-80-01-04841-2. Praha: ČVUT 2011, 405 p.

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

[4] SHAFER, G. A. *Mathematical Theory of Evidence*. Princeton: University Press 1976, 292p.

[5] DEMPSTER, A. P. Upper and Lower Probabilities Induced by a Multivalued Mapping. *The Annals of Mathematical Statistics*, 38 (1967), No 5, pp. 325-339.

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

[7] PROCHÁZKOVÁ, D. Analysis of Nuclear Power Plant Fukushima Accident and First Lessons Learned (in Czech). In: *Požární ochrana 2011*. ISBN: 978-80-7385-102-6. Ostrava: SPBI 2011, pp.288-291.

[8] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Trade-off with Them* (in Czech). ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234 p.

[9] PROCHÁZKOVÁ, D. *Methodology for Estimation of Costs for Property renovation in Territories Affected by Natural or Other Disaster* (in Czech). Ostrava: SPBI SPEKTRUM XI 2007, ISBN 978-80-86634-98-2, 251p.

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

[11] ASCE. *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters", Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards", Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters".* Washington: ASCE 2001.

[12] PROCHÁZKOVÁ, D. *Seismic Engineering on Threshold of Third Millennium* (in Czech). ISBN 978-80-7385-022-7. Ostrava SPBI SPEKTRUM XII 2007,CD-ROM.

[13] PROCHÁZKOVÁ, D., ŠIMŮNEK, P. *Fundamental Data for Determination of Seismic Hazard of Localities in Central Europe*. Praha: Institute of International Relations 1998, 132p.

[14] PROCHÁZKOVÁ, D. *Strategic Management of Safety and Organization* (in Czech). ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.

[15] PROCHÁZKOVÁ, D. *Analysis of Earthquakes in Central Europe* (in Czech). Doctor´ Thesis. Praha: GFÚ ČSAV 1984, 462p.

[16] PROCHAZKOVA, D., DEMJANCUKOVA, K. *Earthquakes, Hazards and Principles for Trade-off with Risks*. ISBN 978-80-261-0170-3. Pl zen: University of West Bohemia 2012, 212p.

[17] PROCHÁZKOVÁ, D. *Study of Disasters and Disaster Management. ČVUT Study in Frame of FOCUS Project.* ISBN 978-80-01-05246-4. Praha: ČVUT 2013, 207p.

[18] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2007. www.ns.iaea.org/standards

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

[20] 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.

[21] CVUT. *Database on World Disasters, Technical Entities Accidents and Failures – Causes, Impacts and Lessons Learned.* Praha: CVUT 2020.

[22] OECD. Guiding Principles on Chemical Accident Prevention, Preparedness and Response. Paris: OECD 2003, 192 p.

[23] KUHLMANN, A. Does Safety Science Fulfil the Requirements of Modern Technical Systems? In: *Safety of Modern Systems*. Congress Documentation Saarbruecken 2014.

[24] MEYN, S. P. *Control Techniques for Complex Networks.* ISBN 978-0-521-88441-9. Cambridge: Cambridge University Press 2007.

Titul:	Risk management at technical facilities designing, building and commissioning
Autorský kolektiv:	Doc. RNDr. Dana Procházková, DrSc., RNDr. Jan Procházka, Ph.D.
Recenzenti:	Prof. Ing. Tomáš Čechák, CSc. Doc. Ing. Jaromír Novák, CSc.
Vydavatel:	ČVUT v Praze
Forma vydání:	Open Access – dspace.cvut.cz
Počet stránek:	144
Rok vydání:	2020

ISBN 978-80-01-06716-1