RISK MANAGEMENT AND SETTLEMENT AT TECHNICAL FACILITIES OPERATION

Dana Prochazkova, Jan Prochazka

PRAHA 2020

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Reviewers:

Doc. Ing. Viktor Kreibich, CSc.

Doc. Ing. Branislav Lacko, CSc.

ISBN 978-80-01-06713-0

https://doi.org/10.14311/BK.9788001067130

CONTENT

LIST OF ABBREVIATIONS

Abbreviation	Title
ASME	American Society of Mechanical Engineers
BLEVE	Boiling Liquid Expanding Vapour Explosion
CBA	Cost Benefit Analysis
CVUT	Czech Technical University
DSS	Decision Support System
EPRI	Electric Power Research Institute
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
OSH	Occupation Safety and Health
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBI	Risk Based Inspection
SMS	Safety Management System
SoS	System of Systems
TQM	Total Quality Management
UN	United Nations
US	United States
VCE	Vapour Cloud Explosion

ABSTRACT

The monograph deals with a risk management at the technical facilities operation for the benefit of safety; the management aim is to ensure their co-existence with their vicinity throughout their life cycles. The problems´ solution way is based on the simultaneously preferred concept, in which the safety is preferred over the reliability.

For research, the original database of technical facilities accidents and failures for the world was compiled. Its analysis shows that in spite of a lot of knowledge on technical facilities´ structures, interdependences, risks and safety, the accidents and failures of technical facilities have been forever occurred. The causes of this reality are several: world dynamic variability; insufficient human knowledge and capabilities; slow application of knowledge and lessons learned from accidents and failures into practice; and unsatisfactory awareness on risks and their consequences for technical facility and public interest. The accidents´ and failures´ studies show that important factor is correct performance of responsibilities on different management levels. Assessment of legislations and organizations of present States shows that for technical facilities safety, they are also responsible politics and public administration. These subjects create conditions for behaviour of humans and technical facilities´ operation, and pursue supervision at technical facilities. Present humans´ cognition shows that the quality work with risks aimed to any entity safety needs knowledge, means, forces, finances and responsibilities´ performance, and therefore, the government and legislation need strictly to involve rules for its correct realization.

The present knowledge shows that for prevention of accidents and failures, it is necessary to avoid to: large mistakes in risk prevention; and origination of small mistakes, the realization of which in short time interval is dangerous. For this purpose, it is developed tool “Decision Support System” for determination of risk level of technical facility during the operation respecting the present knowledge on technical facilities´ risks and safety and the lessons learned from the past accidents and failures of technical facilities, the causes of which were connected with their operation. Due to dynamic world development, technical facilities parts ageing, wear and tear, and limited human knowledge, sources and capabilities, the technical facilities´ management and public administration need to be prepared for future risk realizations, which can be different from the present ones. For this purpose, it is developed tool “Risk Management Plan” respecting the present knowledge on technical facilities´ responses and the lessons learned from the past responses to accidents and failures of technical facilities, the causes of which were connected with their operation.

The publication “***Risk management and settlement at technical facilities operation***“ summarizes problems and shows methods and procedures for their solution based on system concept and present findings and experiences from practice obtained by special research. It 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_018/0002649***”. At the request of the CTU Rectorate and the Ministry of Education, Youth and Sports, the submitted version of the book was supplemented in 2022 with data related to the RIRIZIBE project and the format was modified to keep the original pagination.

Key words: technical facility; risk; safety; risk sources; risk management; risk-based operation; integral risk; risk acceptability.

1. INTRODUCTION

The attention of present publication is concentrated to the results of research directed partly to technical facilities accidents and failures sources at their operation, and partly to tools that enable the improvement of technical facilities´ risk management towards the safety [1]. It goes from the present knowledge in the field, through detection of causes of technical facilities´ accidents and failures up to finding out the effective tools for management of risks, so the technical facilities safety and their coexistence with their vicinities would be ensured throughout their life cycles.

The problems solution way is based on the simultaneously preferred concept, in which the safety is preferred over the reliability. Respecting the present knowledge on technical facilities´ safety and the lessons learned from the past technical facilities accidents and failures, the causes of which originated during their operation, two tools are developed, namely Decision Support System and Risk Management Plan [1]. They were reviewed by experts [2] and tested in practice [3], and therefore, this text contains some improvements in both tools in comparison with text [1], which comprises the complete research results of project "***Řízení rizik a bezpečnost složitých technologických objektů (RIRIZIBE). CZ.02.2.69/0.0/0.0/16_018/0002649***".

For recommendations and comments authors thank to reviewers Assoc. Prof. Dipl. Ing. Václav Kreibich, PhD. and Assoc. Prof. Dipl. Ing. Branislav Lacko, 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.

1.1. Problem description

On the basis of current knowledge, the human society needs to care for public assets (human life and health, property, welfare, environment, technologies and infrastructures), recognizing that:

- each asset constitutes an open system with its own objective,
- all systems overlap and develop with time and space to own targets,

and therefore, as a result of the interconnections of systems and different objectives, from time to time, they originate unexpected phenomena, which endanger humans and other public assets on which humans depend; there are originated dangerous situations, i.e. conflicts in human society life. For the security and development of human society, the humans need to behave in such a way that their behaviour and efforts ensure that conflicts´ resolutions are done for the benefit of humans.

Therefore, in line with current knowledge and experience summarized in [1-26], the humans need firstly to identify sources of risk (i.e. disasters designating the harmful phenomena of all kinds with regard to public interest), to appreciate their harmful potential (i.e. to identify their hazards, which they present and the distribution of their impacts) at each location and to determine the size of possible losses and damages depending on the distribution of public assets (i.e. to determine the risk). Depending on the real possibilities of the human society in question, the risks can be classified as acceptable, conditionally acceptable and unacceptable. For risks that are:

- unacceptable, it is fast necessary to ensure the application of effective preventive measures against their sources,
- conditionally acceptable, it is necessary to prepare for application the mitigation, reactive and restoration measures for the assets under review,
- and, for acceptable ones, to see if the harmful potential of their causes does not increase over time.

In this way we perform the activity, which we call "risk management".

As the world is changing dynamically, so there are occurred the processes that cause the phenomena (commonly called disasters) that are causing the risks. Because, the harmful potential of disasters changes over time, i.e. the size of the hazards and also the size of the risks are changing. To these changes, they also contribute the changes over time in the distribution of public assets in the area of interest or in the technical facility under review. From this reason, we need to carry out the activity "risk management of a technical facility"; its diagram is shown in Figure 1.

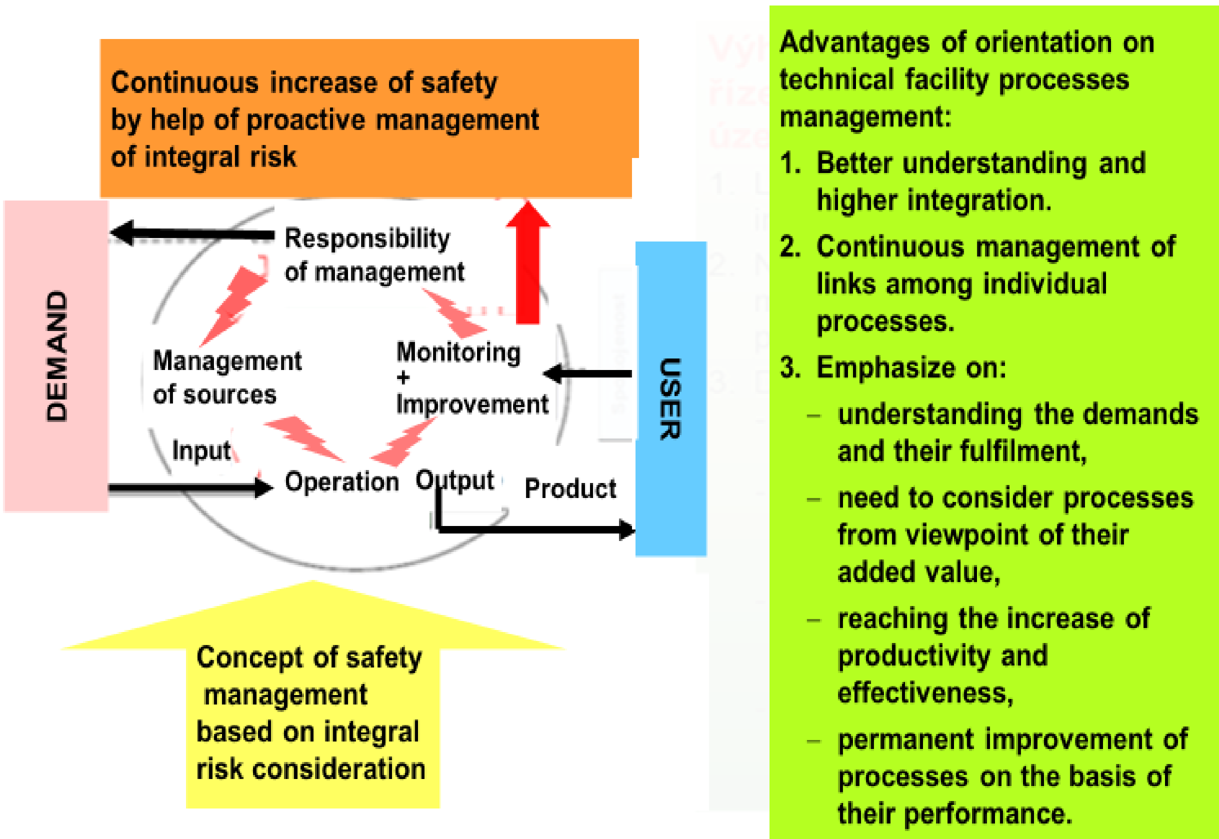

Figure 1. Risk management of a technical facility aimed at the integral (overall) safety of a technical facility and its surrounding.

The attention of the publication mainly focuses on complex technical facilities of an object or network nature, where due to their complexity and the limited humans´

capabilities, ensuring their safety is limited and thus their coexistence with the social and environmental systems is also limited. The technical facilities in question have different structures and arrangements depending on the purpose and local conditions. Based on the knowledge summarized in the works [1,15-19,23,24], their model is the system of the system (SoS), i.e. a set of open and mutually interconnected systems.

The technical facilities are designed and manufactured, so the interconnected systems may work together and may perform demanding tasks under certain conditions, which we call normal or design. Due to world development, the conditions are variable, and sometimes sudden changes occur. However, for safety reasons (the security of humans and other public assets), there is needed so technical facilities also ensure continuity of services or production under beyond design (critical) conditions, which at followed case manifested by accident or failure of technical facility. Therefore, it is necessary to carry out the technical facility management with regard to conditions monitoring and to solve all serious conflicts.

Figure 2 shows the basic idea of problem understanding, the target of which is the human security and development during the process of the technical facility operation. Conflicts between technical facility and its vicinity originate during the technical facility life cycle, and therefore, they need to be permanently solved.

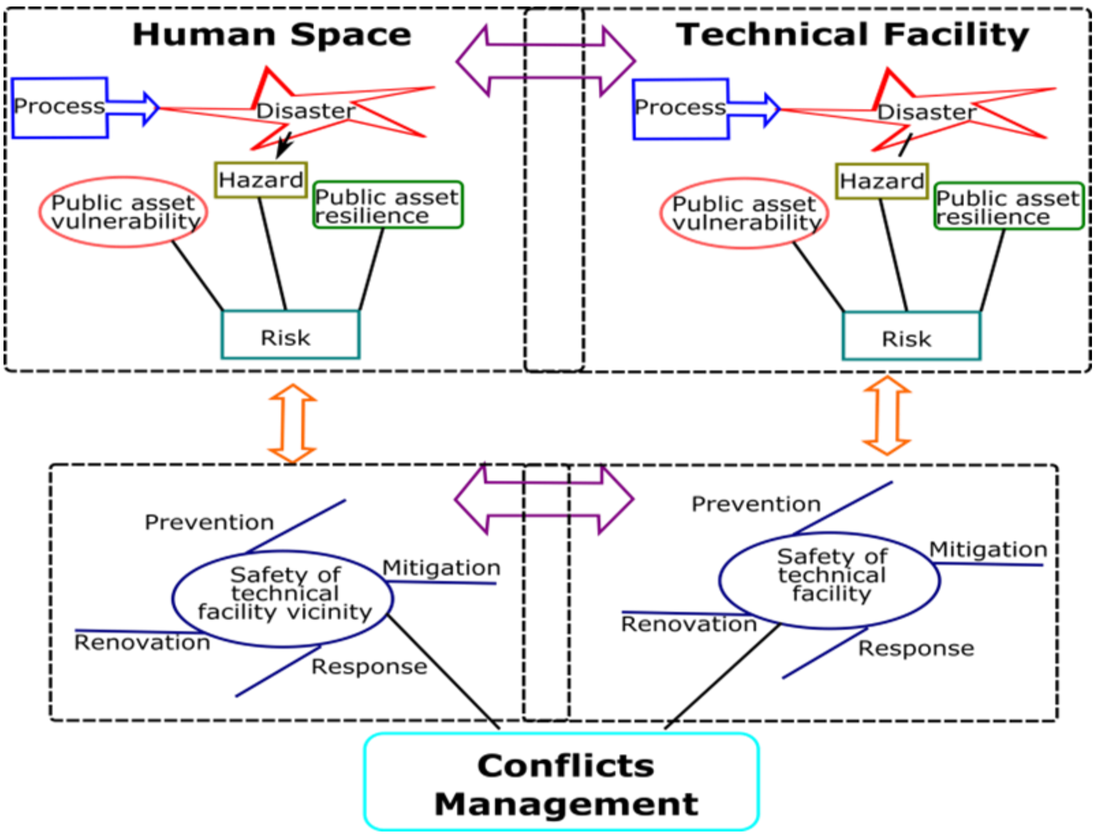

Figure 2. Idea of risk management that needs to be considered during the technical facility life cycle.

The publication summarizes problems and shows methods and procedures for problems´ solution based on system concept, present findings and experiences from practice obtained by special research. It summarizes results of specific research and shows:

- the causes of the risks that led to the failure or accident of technical facilities in operation in the past,
- appropriate tools from the set that is used by engineering disciplines, which work with risks to ensure the quality work with the risks associated with the operation of the technical facility.

It is about organizing the knowledge and experience about risk and safety in conjunction with technical facilities, technical fittings and technical products. The arrangement of knowledge is carried out in a way that follows the logic that helps to ensure the safe operation of technical facilities under various conditions (normal, abnormal and critical) that arise from the dynamic evolution of the world and its parts, the development of which is not synergistic. It carries out the task of technical disciplines, which is to educate professionals with such knowledge of processes and their risks that technical facilities (objects and infrastructures) perform their tasks well throughout their lifetime, thus creating a basis for quality life, safety and human development. The point is that, when operating technical facilities, the care needs to be taken to ensure that humanity is fundamentally cared for basic public assets, including the technical facilities, and humans´ behaviour that ensures the coexistence of basic systems, i.e. social, environmental and technological ones.

1.2. Manifestations of technical facilities´ complexity

Technical facilities are interconnected physical, cyber and organizational systems (including personnel); i.e. social-cyber-technical (physical) systems [17]. Examples of physical / technical systems are: buildings; technical installations for energy production or transmission; networks for water distribution; transport vehicles; material equipment. Examples of cyber systems are: computer systems for the management of production and other processes; information sources, etc. Examples of organizational systems are economic and organizational units.

The safety of technical facilities is currently understood in an integral sense. Great attention is, therefore, paid to the inter-linking and existing flows among the different sectors that manage the subsystems; this is currently being taken into care of in the so-called critical infrastructure [23,24]; Annex 1. In the event of a failure of one system, the interconnectedness can have irreconcilable consequences in the form of chain reactions and domino effects accompanied by failure or gradual failure of other important systems and services. E.g. power outages can cause outages in the supply of drinking water, food supply, heat supply, fuel, malfunction of transport infrastructure, failure of management and information technologies for the functioning of the banking sector, state administration and emergency services, etc. [16-18,23,24]; example is shown in Annex 1.

Large and complex technical facilities include: power plants, industrial plants, dams, airports, railway stations, warehouses, hospitals, large shopping centres, banks, information networks, large cultural or sports centres, etc. (including the complex systems as health protection system, banking system, legal system etc.). These technical facilities belong to the management of various sectors and their aim is to ensure the quality of life of humans. As already mentioned, they include physical, cyber, organizational and social systems, i.e. individual equipment, machines, components, systems or entire production or service units.

Based on the above facts, technical facilities are complex systems, which means that the behaviour of the whole cannot be inferred from the behaviour of individual parts, and under certain conditions there are unexpected phenomena that lead to the destruction or failure of the functionality of a given of a technical facility [17,18]. It is about:

- suddenly emerging feature of behaviour that cannot be derived from knowledge about the behaviour of components (it is so-called emergence),
- hierarchy,
- self-organization,
- a diversity of management structures that together resembles chaos.

Therefore, in order to ensure the safety of complex technical facilities, many branch and interdisciplinary approaches [17,18,24] are required to ensure their:

- existence (ability to ensure balance),
- efficiency (ability to cope with resource shortages),
- freedom (ability to handle challenges from around),
- security (ability to protect yourself from phenomena inside and outside),
- adaptation (ability to adapt to external changes),
- and safety which ensures the coexistence (the ability to change its behaviour so that the behaviour responds to the behaviour and orientation of other systems and that the system does not endanger them and they do not endanger it).

1.2.1. Vulnerability of technical facilities

A vulnerability is an integral dynamic property of the system. It changes over time and space by certain and territorially specific way because it depends not only on system conditions but also on conditions to which the system is inserted [1,3]. It means, that in the scale of time and space, certain aspects dominate at different point in time and at a different site. Verbally, it is the antonym for the two established concepts of robustness and resilience. Generally, it refers to the condition or predisposition [16,20,25,26].

As based on collected facts, the vulnerability is a property of place in the system. Due to the dynamic development of all systems, the vulnerability is also a function of time [16,25]. Because, each site has a certain structure, composition, its own network of links and flows, etc., which, moreover, change over time, and each disaster in the monitored system and its surroundings has its certain physical characteristics, so the vulnerability of the entity (site, system, building, infrastructure, human, etc.) also depends significantly on the physical characteristics of disasters, i.e., some entity is only vulnerable to beyond design (extreme) winds and intentional human activities, other to beyond design (extreme) earthquakes, floods and intentional human activities, and others fail to beyond design (extreme) failure of technological processes and deliberate human activities etc.

The applications of technical norms, standards and best practices procedures reduce the vulnerability of buildings and infrastructure, etc. The main problem of our times are complex technical facilities, e.g. the critical infrastructure, which represents a system of systems (i.e. the system of overlapping systems) for which we only look for measures to reduce its vulnerability with respect to all the above aspects, with necessity to find principles to reduce vulnerability across different systems and across systems of systems.

In literature it is possible to find variety of scales and curves for the classification of vulnerabilities [16,24,25]. Since each area is site specific, the following procedure needs to be applied for each area separately, with the vulnerability assessment made by a single, well-defined relative scale, such as grade 1 to 5 in order to achieve comparability. I.e., it needs to be told what damage corresponds to individual degrees, and what response / specific scenario is most suitable for it.

Procedure for determining vulnerable zones in the technical facility in question is as follows:

1. Setup of file of possible disasters D_1, D_2, ... D_n, which may occur in a given technical facility (e.g. fire, flooding, wind, impact of a moving object, explosion, earthquake, landslide, vibration, hazardous substances, poorly secured supply of electricity, gas, water, information, lack of physical protection; lack the possibility of evacuation, inadequate air conditioning, etc.), in which the vulnerability will be monitored, as they can reach size, to which tracked public assets and technical facility assets are not inherently resistant (i.e., unacceptable damages can be caused).
2. The technical facility shall be assessed in terms of vulnerability to disasters D_1, D_2,….D_n for protected public assets A_1, A_2, ..., A_m and technical facility assets T_1, T_2, ..., T_k, which are located in the territory, in which the technical facility is located, e.g. using the checklists adapted for the territory. It is advisable to use a scale from 1 to 5 for the evaluation, so that to ensure that degrees are at same level for all disasters (e.g. expected size of damage expressed in money for 1 year [24,25]).
3. For each followed asset O_1, O_2, ..., O_l we set the order of vulnerability V_1, V_2, ..., V_l to disasters D_1, D_2, ... D_n, see the example in Table 1.
4. Assets are grouped together for practical reasons (acceptable number of specific response scenarios) to the sub-units in order of vulnerability.
5. Determination of specific response scenarios / or specific inspection activities, which is allowed by existing legislation, for partial units.

Table 1. Example of assessment of overall vulnerability of the object [24,25].

Disaster	**Assessment of vulnerability**
Fire	5
Violation of safety	4.8
Storage	4.5

Flood	4.2
Other threats	4.0
Explosion	3.9
Service disruption	3.8
Communication disruption	3.7
Data protection violation	3.6
Lack of contingency plans for situations	3.5
Overall rating	**4.1**

It needs to be noted that when evaluating the multiple entities to more disasters, the problem does not usually occur in a process model according to which the evaluation is conducted, but in the scale of values, by which different aspects are assessed and according to which an overall assessment is carried out [24,25]. Therefore, it is appropriate to create a value scale for vulnerability according to the procedure described in [24,25], based on procedure below:

1. For disaster D_i (i = 1,2,..., n), with the size that occurs on average once a year (some simplification of precise calculations used in practice for monitoring needs) to evaluate the vulnerability of the monitored assets as follows:

   stage 1 - the expected damage to assets <5000 EUR

   stage 2 - the expected damage to assets between 5000 and 50 000 EUR

   stage 3 - the expected damage to assets between 50 000 and 500 000 EUR

   stage 4 - the expected damage to assets between 500 000 and 5 000 000 EUR

   stage 5 - the expected damage to assets above 5 000 000 EUR

2. At fifty-year disaster D_i (i = 1,2,...,n), i.e. at the size of the disaster that occurs on average once in fifty years (some simplification of precise calculations used in practice for the purpose of monitoring) to evaluate the vulnerability-controlled assets as follows:

   stage 1 - the expected damage to assets <0.5 million EUR

   stage 2 - the expected damage to assets between 0.5 and 5 million EUR

   stage 3 - the expected damage to assets between 5 and 50 million EUR

   stage 4 - the expected damage to assets between 50 and 500 million EUR

   stage 5 - the expected damage to assets above 500 million EUR

3. At one hundred-year disaster D_i (i = 1,2,...,n), i.e. at the size of the disaster that occurs on average once in one hundred years (some simplification of precise calculations used in practice for the purpose of monitoring) to evaluate the vulnerability-controlled assets as follows:

   stage 1 - the expected damage to assets <5 million EUR

   stage 2 - the expected damage to assets between 5 and 50 million EUR

   stage 3 - the expected damage to assets between 50 and 500 million EUR stage 4 - the expected damage to assets between 5 and 50 billion EUR

stage 5 - the expected damage to assets above 50 billion EUR

When vulnerabilities are determined, and according to the disaster hazard size and the vulnerability measure size the risks are assessed, it is necessary to make an action plan focused on defeat of each risk. Usually 4 to 5 most danger entities are selected and for them the plan of activities is set. An example is in Table 2.

Table 2. Example of action plan - it consists of response scenarios S1,... S5 [24,25].

Disaster	**Response scenario**
Disaster meaning the highest vulnerability for the object / infrastructure / organization.	S1
Disaster meaning the second highest vulnerability for the object / infrastructure / organization.	S2
Disaster meaning the third highest vulnerability for the object / infrastructure / organization.	S3
Disaster meaning the fourth highest vulnerability for the object / infrastructure / organization.	S4
Disaster meaning the fifth highest vulnerability for the object / infrastructure / organization.	S5

The problem of the system vulnerability in a certain area is so dependent on local conditions, that it is not possible to outline its general solution, because it is dealing with the solution of risk of system of systems [16]. For each area it should be solved by using a case study [27] of a suitable type. Based on the knowledge and practical experience in safety management it is primarily associated with search for:

- extreme (aberrant) cases (the reason is that usually in terms of security and development it is necessary to avoid these cases, i.e., to take appropriate measures to not allow their occurrence),
- critical cases (the reason is that usually in terms of security and development these cases are strategically important because they create an interface at which the risk of default and losses associated with the materialization of risk are high, and when it is exceeded the catastrophe occurrence is highly likely and irreversible, i.e. these risks are unacceptable),
- paradigmatic (current) cases (the reason is to design a suitable implementation of possible solutions for the usual case in practice).

Another example is an application of verbal scale for vulnerability assessment in Table 3 for industrial plants.

Table 3. Vulnerability of an industrial plants with regard to damage or failure of key equipment classified as verbal numerical scale, according to data compiled in the works [28,29].

Sign	Verbal description	Characteristics of vulnerability of protected asset
5	Extremely high	Loss of equipment or disposal of function causes an immediate cessation of operation, output, production or service. The user cannot continue without this facility in the activity.
4	High	Loss of equipment or disposal of function causes a cessation of operation within 1 day or decreases, output, production or service by 75%.
3	Medium	Loss of equipment or disposal of function causes a cessation of operation within 1 week or decreases, output, production or service by 50%.
2	Small	Loss of equipment or disposal of function causes a cessation of operation within 2 weeks or decreases, output, production or service by 25%.
1	Negligible	Loss of equipment or disposal of function causes a cessation of operation within 1 month or decreases, output, production or service by 10%.

Because the humans through their intellect and historical experience protect and consciously develop resistance of areas, buildings, infrastructures and technologies to disasters by selecting elements, links and flows, their connections and specific preventive measures and activities up to a certain size of disaster (which is determined by its knowledge, capabilities and financial, technical possibilities, etc.), the cascading failures caused by interconnections (the interdependences) might occur only at beyond design disasters, i.e. when the disaster size exceeds the disaster limit, against which the entity resistance is systematically provided [15,20,21], but due to epistemic uncertainties in disasters´ occurrences and due to possible combination of different phenomena they can occur also under another conditions; e.g. at failures of safeguards´ measures installed for reliability or safety improvement.

Therefore, the scenario of safety management of both, the territory and the technical facility shown in Figure 3 is necessary to consider. In this phase of technical facility life cycle, they are important parts III and IV that show how to ensure the safety for technical facility and territory in which technical facility is located.

In addition, each area or technical facility is different, has different structure, composition and arrangement, and therefore, it has a different vulnerability, which manifests itself during disasters [15,20,21,25,26], and therefore, the cascade effects are very different and they need to be monitored separately.

The aim of the third part (III), denoted in Figure 3 as ***"what to do"*** is to evaluate the real impacts in the disaster scenarios for the disaster sizes: current; design; and beyond design, which are in technical facility operation documentation [30,31]; they were compiled in second part for each real disaster, which belong to specific disasters in a given territory; and it is assessed whether there are adequate quality of safety management scenarios and whether there is a readiness on their implementation in practice. On the basis of critical evaluation, they are detected deficiencies and searched for better procedures for safety management with the fact that each process needs to include a number of specific measures and activities, the way of implementation, evidences of their material, technical, personnel and knowledge ensuring, and be accompanied by the relevant competencies and responsibilities. Whereas that management procedure consists of different, intersecting processes that have one objective, and some are mutually conditional, i.e. are mutually dependent, it is necessary to construct matrixes of responsibilities [27] for the management of activities that support the basic functions of the territory associated with safety.

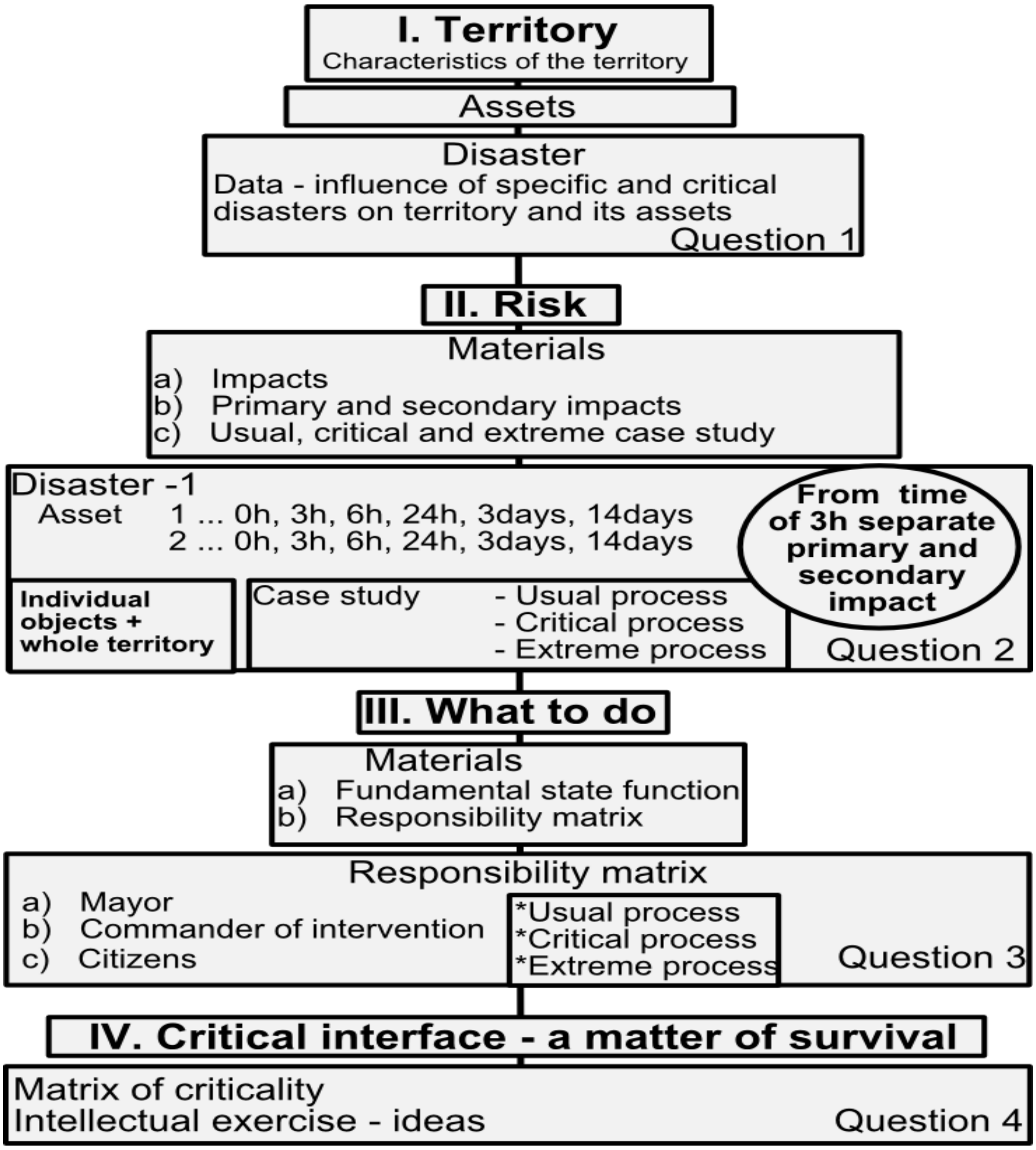

Figure 3. Scenario of management of territory and technical facilities located in it directed to integral safety (i.e. human survival).

Therefore, there are evaluated the measures and activities to individual disasters, and it is considering the fact that some of the measures and activities which are the best for a particular disaster are in real territory of conflicting with those for another disaster, and therefore, it performs their optimization [32] in consideration of all possible disasters in the sizes, which are the design disasters values. It is required so that the documents ensure the response, its material, technical, personnel and knowledge ensure, and also the pass of the respective competences and responsibilities.

From the viewpoint of removing the causes of organizational accidents, there are on the basis of existing documentation for the SoS safety management, which currently means that it will consider the measures and activities for the management of the risks used at individual systems and it will be performed evaluation of their effectiveness in the area of the SoS risk management, namely for individual items of management of risks (acts of management, technical area, knowledge area, the financial area, personnel area, responsibilities), i.e. it:

- performs the screening of the existing measures and activities for risk management of the SoS subsystems and it assess their appropriateness for increasing the SoS safety,
- performs the evaluation of level of trade-off with risk all disasters that were identified as dangerous for the SoS, particularly for highly critical and moderate critical items of the SoS, and for the needs of the SoS safety management this level is classified according to the appropriate level of the scale,
- builds matrixes of responsibilities and their level it shall be assessed from the perspective of the relevant competences at the level of the SoS individual systems and the whole SoS; logically, the responsibility for the SoS safety management need to be the primary,
- examines the practices and modes of the SoS control, that result from aggregation of procedures and modes of management subsystems, and the attention will focus on the detection of conflicts and gaps in implementation in practice, and how they are ensured by knowledge, materially, technically, financially and by personnel,
- assesses the adequacy and accessibility of resources, forces and means with regard to cope with failures of the moderate and highly critical of the SoS items with acceptable losses and damages,
- assesses the effectiveness of specific procedures such as a warning, the capability to respond, warning instructions, etc.

Finally, they are identified the areas in which the SoS risks are managed insufficiently or not managed.

The aim of the fourth part, denoted in Figure 3 as ***"critical interfaces"*** is to:

- create matrixes of criticalities as a basis for the administrative management of the territory, on the basis of the individual impacts´ scenarios for each real beyond design disaster, or also for such design disaster when it was revealed that it is not in the territory considered at all,
- gain the capability to determine the severity of potential situations in the territory and in the critical facilities and to identify the key interfaces for the origin of a social crisis in the territory, which are a necessary basis for choosing the right management methods,

- collect realistic ideas of experts to ensure the survival of the population and to find a way to implement it in practice that will be respected by the fact that the measures and activities cannot be chosen with regard to just one disaster, or just property, but it is necessary to strive for optimal measures for all the assets and all the potential real critical disasters in a given territory.

Therefore, there are considered beyond design disasters and criticalities of their impacts, and there are identified interfaces for origin of social crises and they are searched ideas for ensuring the inhabitants survival.

It means that main target is identifying the critical items of the SoS risk management and proposal of solution of gaps related to survival or continuity of assets at critical assets, there are determined interfaces, which lead to the collapse of any of the assets to the demise or the whole SoS. The procedure is the following:

- it is assessed the severity of the areas in which the SoS risks are managed insufficiently or not managed at all, and for very serious areas from the perspective of public interest, they are proposed real measures and activities against the breakup to the demise of any of the assets or the whole SoS, it is processed the plan of their implementation (usually long-term), and it is ensured its implementation in all respects,
- on the basis of a critical perspective on the extreme and critical scenarios of possible dangerous disasters with regard to essential public assets (the lives and health of people, the quality of living conditions and the possibility of developing), there are again examined possible measures and activities for human survival or continuity of public assets, in order to avoid the interference threshold of the criticality of their conditions of existence.

The same argument applies to the human community, as rich and developed countries have far higher level of safety than the poor countries or rich countries economically, but in which the public interest is ignored and governance respects the interests of only certain social strata.

1.2.2. Parameters important for safe operation of technical facilities

From the point of view of current knowledge [17,18,24,25], there are now at least two tasks:

- to solve the problem of the functionality of a set of interconnected (i.e. dependent) objects and infrastructures under normal, abnormal and critical conditions,
- to look for critical conditions of complex fittings or facilities that are unpredictable or are the result of a serious operator errors, and under certain conditions they may go to highly non-demanded, i.e. highly unacceptable situations, i.e. situations in which the very existence of the device, or even humans, is threatened, and which we usually refer to as crisis in normal communication.

Therefore, in practice they are followed specific characteristics [19,21] such as:

- interoperability (i.e. the ability of the technical fitting or facility as a whole to perform well-given tasks under normal, abnormal and critical conditions),
- safety integrity (SIL), which is mostly monitored in connection with human errors (specification, design, installation, maintenance, modification, etc.),

- criticality (i.e. the extent to which personal injury, destruction of material, damage or other losses on assets can occur – this is the threshold below which the condition of the monitored facility is demanded and vice versa),
- dependability (operational reliability), which ensures that the system meets the specified requirements and that its operation complies with the specified conditions (it extends to two basic characteristics, such as vulnerability and resilience).

In this context, we divide technical facilities into reliable, secure and safe systems [17]. A reliable system is a system that performs the required functions at a probability level of 95%. A secure system is a reliable system that is protected from all risks. A safe system is a secure system, which does not threaten itself or its surroundings, namely not at its critical conditions,. In the creation and operation of all these types of systems, it is worked with risks, relied on the Defence-In-Depth principle, and management is required through the safety management system of the technical facility as a whole (SMS) [17,18].

When it is not clarified in the design and operation of a technical facility what objective is pursued in practice, confusions arise in the setting of priorities, leading to the existence of conflicts and it is necessary to optimise measures [17,32,33]. Misplaced priorities bring damages, e.g. in the people were burned to death in a thoroughly secured object in Australia because they could not leave the building in the fire; five girls lost their lives in an escape game in Poland because they were in a secure room; pilot Andreas from Germanwings could have guided the plane to the mountain massif of the Alps because the cockpit was secured - the armoured doors could not be opened from the outside, etc. [34].

The starting point is the use of the concept of integral safety, which is based on the consideration of all phenomena that can damage the territory and the technical facility (the so-called All-Hazard-Approach), which inherently connects the two instruments [17,18], and to reduce costs for less important technical facilities it clearly specifies what was neglected by the fact that the facility or equipment is merely a system secure or just a reliable system [18]. It understandable that All-Hazard-Approach needs to be also respected during the technical facility operation.

1.2.3. Aspects relevant to safety management of technical facilities

The safety of technical facilities is the level of measures and activities by which risks are managed and settled [19,21]. Technical facility risk management is a structured, consistent, and continuous process across the whole technical facility for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the safety, which is strategic goal. On opportunities and priorities at decision-making on risks, the context and way of work with risks play main role. The aspects playing the main role at risk management are shown in Figure 4.

Safety needs to be an integral part of the business activities of the owners of technical facilities. All technical facilities shall be managed in such a way that the occurrence of accidents affecting the safety is minimal. It is about integral safety (Annex 2). All activities and efforts of managers and employees need to be directed towards this. The key elements for the objective in question are mutual cooperation, open communication and regular monitoring of the achievement of safety objectives [17,18,24,35,36]. On the basis of the current requirements enshrined in the legislation of developed countries, owners and operators of technical facilities need to:

- promote safety as a whole part of their business activities and promote safe activities,
- actively search for safety information,
- cooperate with administrations and other entrepreneurs in order to improve safety,
- create, together with other technical facilities, the conditions for joint response and mutual assistance,
- create professional organizations to provide a platform for the exchange of knowledge and experience.

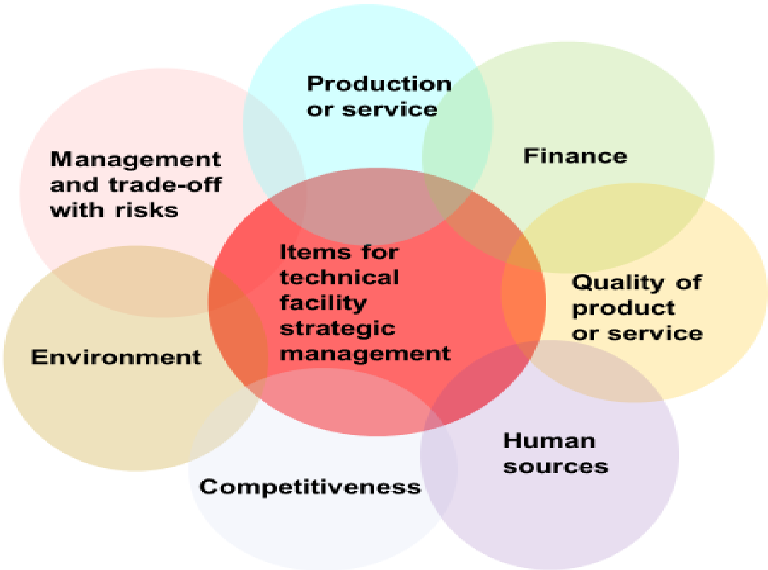

Figure 4. Items determining the technical facility safety and development (i.e. also competitiveness during the life cycle).

Public administration needs to set safety objectives, to establish a clear and holistic framework for safety management and, through appropriate inspections and enforcement measures, to ensure that all relevant safety requirements are met.

The safe operation of the technical facility depends on a number of diverse aspects [15,35,36], such as the training of the serving staff, the organization of technological components and their interconnections, the process of works, cooperation and how to understand the situation of the service personnel.

In view of the current knowledge, it is necessary to monitor in the technical facility internal dependencies, which mediate the secondary and other impacts of disasters on the protected assets of the technical facility and its surroundings. To achieve this, it is necessary [17,18,35,36], to:

- put into practice safety monitoring,
- develop and codify methodologies for data collection, professional processing of the quantities necessary for risk management in the system of systems,
- develop risk decision-making methodologies and linked control-list systems to support decision-making,

- develop for employees sets of measures on what to do before, when and after the implementation of the risks, which in the technical facilities belong among specific or even critical risks,
- develop plans for the strategic technical facility management aimed to security and development of the technical facility, emergency plans, continuity plans and crisis plans of the technical facility, which shall be interconnected and in which safety and development management tasks are underpinned at all times,
- ensure support systems for the safety management of the technical facility skilled solutions always save money, strength and resources. The knowledge so far shows that simplified solutions are only possible sometimes, but even in cases where they are possible, it is necessary to know what simplifications have been made, why they could be applied and whether there is no need to take further action after some time.

The security policy tools put into practice by safety management are:

- concepts that set out security policy objectives,
- strategies that identify the basic ways in which the objectives will be achieved,
- plans that describe in detail and include activities in a specific timetable,
- instruments and institutions, i.e. resources, forces and means to achieve security policy objectives.

In the case, in which there is no effective defence of a technical facility against a disaster, i.e. against realization of significant risk, it is necessary to be prepared to response. It means that the technical facility needs to have prepared procedures in place to ensure a response to the situation aimed at stabilising the affected part of the technical facility and restoring the critical processes and resources for their implementation.

Emergency planning does not reduce risks and needs to be tailored to those, who perform both, the response and the follow-up recovery. It is by no means a cheap thing. It is about ensuring that the knowledge set is organised and that each responsibly managed institution has a security concept. This shall be based on the classification of emergencies and a risk analysis aimed at determining expectations of what impacts are likely in the event of a disaster of expected (legally defined) size.

In practice, the term ***functional / operational safety*** is often used. This is the part of the overall (integral) safety that relates to equipment, systems, infrastructures and their control systems and which depends on the proper functioning the safety-related systems. Due to the critical role of safety-related systems, international risk management standards IEC 61508 and IEC 61511 have been established for them, which are based on reliability, i.e. they do not solve the integral (overall) safety of the technical facility.

The authors of the work [37] propose to revise 10 errors that are made in the operational safety domain. They are based on the strength of the safety integrity level (SIL) [18,19], safety-related systems (the probability of these systems to perform specific safety functions). Based on models based on Petri nets and Bayesian networks [27], they show the consequences of aging the important components. They focus on changes to the components of safety systems and show that safety margins of operation need to be maintained, Table 4.

According to the standards [38,39], the functional safety management of a technical facilities is the integral part of the engineering of reliability during the life of the technical facility. For new technical facilities, it is intended to ensure technical safety, engineering functions and all planning and management activities over the lifetime.

Table 4. Return periods (PT) for each SIL level; processed according to [37].

SIL	PT (years)
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

The problem is that functional safety is not part of the design process, and therefore, the principles of inherent safety are not introduced into it. During operation, a functional safety plan is then created, containing:

- the schedule of activities,
- the responsible persons,
- the description of the system of activities with regard to the identification of threat sources and risk assessment, verification of activities, evaluation of the level of functional safety,
- the description of the programme for internal and external audits,
- the description of the hierarchy of documents and responsibilities for each document,
- the evaluation of functional safety,
- the description of the roles of each member of staff included in the creation of safety during the life cycle of the technical facility,
- the plan for communication, especially on the interface of individual organizational units.

In order to determine individual items in terms of operations and roles, it is necessary to:

- have engineering knowledge, training and experience in the operation, technology, sensors and final outputs,
- have engineering knowledge of safety, including the risk analysis,
- identify supervisory requirements,
- have the ability to manage and guide employees in the performance of specific tasks,
- be aware of the consequences of failure of safety functions,
- have knowledge of the level of safety integrity, i.e. to know the complexity of the application and technology.

Since modern systems are flexible and dependable (operationally reliable), so to ensure operational safety, the switching mechanisms need to be used to change the structure or behaviour of the system according to conditions. The relevant reconfigurations can be motivated by functional requirements (change of the task phase), targeting to the error tolerance (replacement resource management), predictive maintenance policy, production needs, etc. The complexity and diversity of reconfiguration strategies are important to consider when the system is being repaired.

Again, it should be remembered that operational safety ensures the reliability of the operation of the technical facility, but does not in all cases ensure the overall (integral) safety of the technical facility.

The Safety Integrity Level (SIL) established in IEC 61508 [38] and related specific standards provide examples of risk information from the point of view of safety classification. However, the reasons for SIL are completely different from the principles of classification of nuclear safety, making it difficult to apply those standards in a nuclear context.

Reliability is a special feature that describes the dependability of components, which means that the component performs the required function consistently for a certain period of time in order to meet the objectives and needs of the operator (customer). In theory, reliability can be described as:

Reliability = 1 - probability of failure.

The lower the probability of failure, the higher the reliability of the element, component, production line, or system. However, there are many factors that are a source of epistemic uncertainty in the design of systems that are in the field of material changes, factory changes, transport, storage and use.

The reliability of the equipment is measured in terms of quality, performance and productivity. The equipment reliability programme aim is to effectively monitor equipment, procedures and data related to the lifetime of the equipment. The advantages of introducing a reliability program for a given device are:

- to eliminate unexpected device shutdowns,
- reduction of production losses that occur during the shutdown of the equipment,
- extend the life-time of the device.

In addition, repair and maintenance costs are reduced, delays are reduced and safety is increased.

The reliability of the equipment depends significantly on the maintenance of the equipment, the quality of inspections and also on the use of new technologies. New technologies, such as sensors, can provide real-time performance and condition data for the device, allowing for better decisions on preventive, predictive and corrective maintenance.

The availability of a technical device or system means that the device or system is available whenever it is needed. Maintainability means easy maintenance of the device or system in normal operation. Security is a set of measures that prevent accidents and protect against infringements.

According to data in professional papers, published by authors and summarised e.g. in [1,2,18-20,30], in order to ensure a safe technical facility, it is necessary to know:

- impacts of the largest (in terms of maximum expected) accident,
- critical tasks from a safety point of view,
- and to understand tasks in connection with risks,
- and to have critical task scenarios,
- possible human errors in the execution of critical tasks,
- measures to ensure the safety.

Critical safety tasks are physical activities or activities through which a person contributes positively or negatively to the realization of the largest accident by:

- initiation of adverse events,
- detection and prevention of phenomena,
- management and mitigation of the impacts of phenomena,
- response to emergencies.

For operational safety management, they are important data on:

- reliability (component failure distribution, component failure types, monotonous backups, traffic profile),
- maintenance data (repair and replacement policy, repair time, corrective maintenance, preventive maintenance, inspection),
- logistics data (replacement parts, delivery times, delivery time, delivery time),
- financial data (costs of spare parts, penalties for non-compliance, corrective maintenance, preventive maintenance, inspection).

The safety of technical equipment (so-called technical safety) depends on many items, i.e. on the material, method of manufacture, method of operation and operating conditions [15,17-19,24]. In order to ensure it, all risks associated with those items should be monitored and controlled in such a way that the monitored equipment works safely throughout its life-time, i.e. it reliably performed functions in the required quality, in the required quantity and at the required time, and under its critical conditions it did not endanger either itself or its surroundings [15,17-19,24].

On the basis of investigations related to the processing of works [17-19,24], in the technical sector it is often only considered the context of the technical equipment, technical components, technical facility or the context of the undertaking managing the technical facilities and, in many cases, only the context of the production equipment. With a view to the security and development of human society, i.e. from the point of view of the public interest, it is necessary to consider wider context, i.e. also the surroundings of the monitored technical entity. In doing so, it should be borne in mind that the benefit of a technical facility in the long term is not only due to performance, i.e. number of products, energy or services, but also by avoiding losses caused by accidents.

Therefore, in the case of technical equipment, components and whole technical facilities, it goes on ensuring their safety in an integral sense, which can only be achieved by targeted management of all priority risks, including those associated with their material [17-19,24].

The research described in [19] shows two important facts and their interconnections, namely:

- the seven important items for risk determination, management and settlement were given, Figure 5,

Figure 5. Items that decide on risk size.

- the proper risk management and settlement steps, Figure 6.

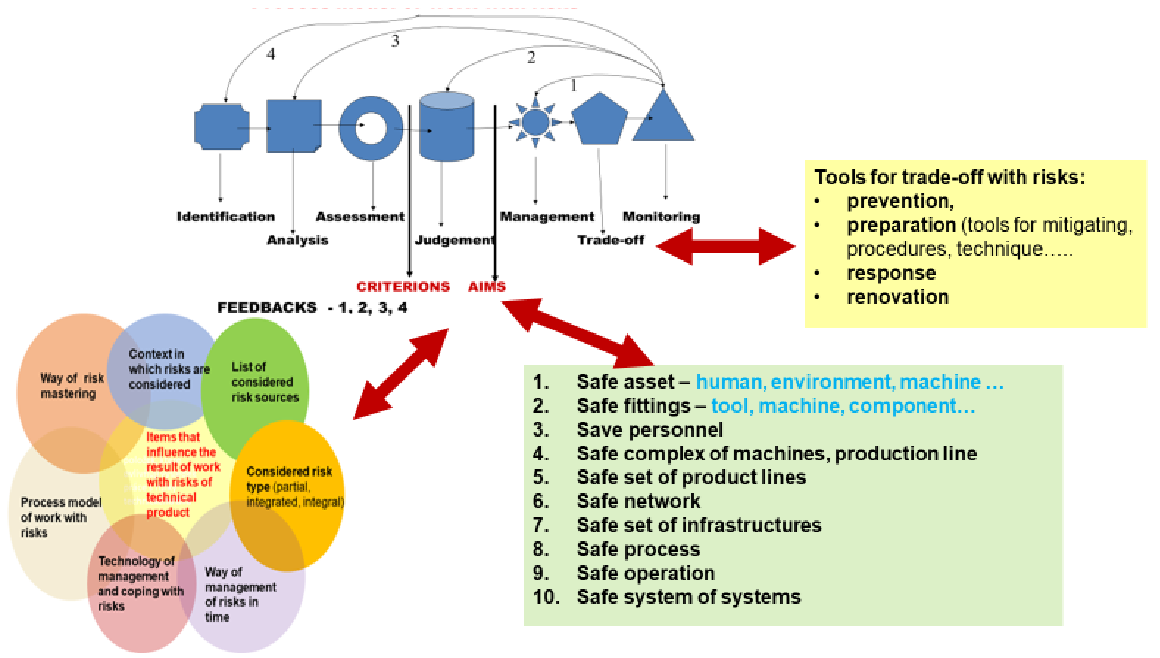

Figure 6. Risk management procedure directed to technical facility safety and important connections.

With regard to knowledge summarized in [1], the management procedure of technical facilities risks consists of:

1. Identification of strategic goals of technical facility.
2. Identification of critical activities, functions or services that rely on technical facility or which technical facility provides.
3. Identification of external context: legal / regulatory requirements, stakeholder perceptions and expectations, and any relevant social, political, economic, financial, technological or market factors.
4. Collection of data on risk sources and their impacts on technical facility – external, internal, organizational etc.
5. Investigation of technical facility opportunities and specially at occurrence of cascading or cumulative impacts.
6. Risk identification – process of finding, recognizing and describing the risk.
7. Risk management – sources, events (conditions for realization), causes, impacts / consequences.
8. Risk owner solutions – person with accountability and authority to manage a risk.

From the management viewpoint, the failure / malfunction is a result of the process compossing of:

- initiator (false operation, mistakes, violation of rules, ignorance),
- contributing effects (incorrect organisation, inaccurate deciding),
- spread of defects leading to accident (organizational non-functionality).

Because the influence of style of management and deciding is important, we speak on so called organisational accident in the form of Reason model [40]; Figure 7.

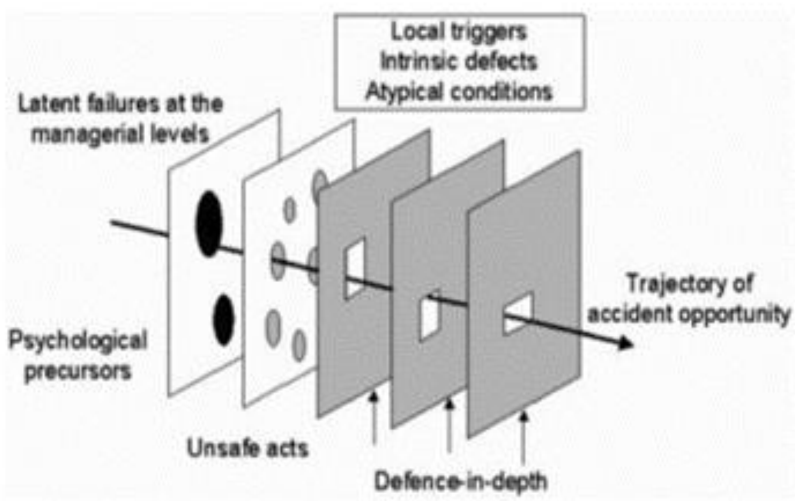

Figure 7. An organisational accident model indicating the basic barriers to prevent a crash and are created in the context of the management of the safety of a technical facility; processed according to [40].

Safe (including the dependable) system behaviour arises from a condition that technical workers (operation, maintenance) always proceed according to the requisite procedures (the procedure is formed from correct tasks / operations performed correctly). Therefore, in the risk determination it is necessary in the frame of process analysis to understand the motivation of intended acts of both, the terrorists and the insiders (actual employee). Among the insider´s motives it belongs e.g.:

- inconvenient safety procedures (for a safe human live they must be skiped),
- inconvenient plans (for a safe human life the modus operandi solutions must be used),
- poor perception of security risks,
- insufficient responsibility,
- stress and management attitude or finance profit.

The insider´s motivation is directily related to a safety culture.

We separate the human factor in the sense of human error (human failure) to intentional and unintentional [41]. The human errors origate at both:

- the performance of activities, where their sources are: routinist behaviour; not respecting the operation and security codes; default; omission; bad health state; bad conditions on the workplace etc.,
- the management process, where their sources are: ignorance; not respecting the rightfulnesses natural, technical, economic and social; arrogance and the like).

Organisational processes include four processes that are part of each technical or technological organisation at technical facility:

- designing and manufacturing,
- outfitting the equipment and commissioning,
- operation,
- and maintaince.

All these processes are built in three interconnected activities:

- assignment of targets in the framework of economic and social situation of the organisation,
- set-up of organisation for the realisation of determined long-term strategic goals,
- and management of operational activities.

Each of these processes and activities forms a separate general type of failure scenario:

- determination of targets – contradictory targets,
- organisation – disproportionate arrangement (set-up),
- management – bad communication, bad planning, inappropriate inspection and monitoring,
- projection and construction - faulty projection, incorresponding barriers,
- operation – bad operational procedures, bad training and education,

- maintenance – bad maintenance plan, bad maintenance proscedures.

The conditions that caused the origination of errors are:

- insufficient teach-in with task,
- lack of time,
- bad separation of signal from noise,
- misapprehension between designer and user,
- inreversibility of errors,
- congestion by information,
- negative convert among tasks (bad hand over / pass of tasks),
- bad perception (underestimation) of risk,
- bad backward link from system,
- lack of experiences,
- bad instructions and procedures,
- insufficient check-up,
- unsuitable education of person for a given task,
- unfriendly atmosphere,
- and dullness and boredom.

The conditions that caused the violation of provisions and rules are:

- lack of safety culture in organisation,
- coflicts among managemental workers and emploees,
- bad moral,
- bad supervision and check-up,
- norms and standards permiting the violation of rules,
- bad perception of the sources of risk,
- perceptible lack of the solicitude and interest of managemental workers,
- low pride to own work,
- dab hand approach to work that stimulates to undergoing risks,
- belief that nothing bad can happen,
- low self-respect; recognised weakness,
- perceptible permit for the violation of rules,
- double-dealing, ambiguous or obviously meaningless rules,
- age and gender – young man execute the violation of rules.

Dangerous pursuance can be split up to errors and violation of provisions / rules:

1. The errors that become as a consequence of problems in information processes and may be comprehended in relation to the cognitional functions of an individual.

They may be reduced by training, improvement of the workplaces, interfaces, better informing etc.

2. The violations of provisions / rules that are based on motivation. They are social phenomena and they can only be comprehended in connections being in a given organisation. The violation can be removed by a change of approaches, persuasion, norms, standards, moral and safety culture.

On the ground of present knowledge and experience in the organisation safety management system the task "*how to avert the human failures?*" is fundamentally important. In agreement with research results [15,41-46] it is possible to avert the human failures of activities and management if:

1. By management of professional problems only the professionals with the capability to lead the working team are authorized (they: become to be object lesson; know to explain; know to support; know to avert the bullying and the like).
2. By the qualified management of processes is ensured that projects, programs and these furthermore partial processes, the outputs of which are products, i.e. results of organisation.
3. The conditions for a qualified work are created.
4. They are provided both, the sufficient education of workers and the system of the offer of aid at the solution of complex tasks.
5. The motivation and stimulation of workes for the adherence of operationg and security provisions are ensured.
6. The in-depth supervision of processes and their interconnections to projects and furthermore also programs, that professionally and directly averts the intentional and unpremeditated errors is performed.

The biggest errors originate from human errors in management, especially if manager prefers risky decision [41]***.*** Among management workers two extremes occur:

- the gamblers who adjudicate in the benefit of matter, even though possible losses are great,
- the prudential humans who adjudicate in the benefit of matter even though possible losses are low.

The gamblers occasionally reach huge profit, and therefore, they are certain ideal in human society.

The moral principles of human society conforming to the UN principles [47] give that gambling with human lives and health is inadmissible, i.e. the risk here is not permitted (tolerated). This finding might be the main principle in a selection of a personnel for activities on which the human lives depend, namely directly (drivers, pilots and the like) and indirectly (managerial workers of land, enterprises and other organisations who adjudicate the activities and measures that are directly or immediately connected with unacceptable risk for persons, property and other basic protected assets.

1.2.4. Safety culture

Because the human aim is to live in a safe world with the potential of development, it is necessary to include the human factor into the safety management respecting that human system is the system of systems [16] and that it represents territory, organisation and the like. We need also to include the human factor into engineering in which we realise the targets of safety management in way by which we negotiate / trade-off with risks. Because each human is an active element of a human system, humans need systematically to build the safety culture, namely in workplaces and in territory / land [15]. All given ways are important and will be followed in next paragraphs.

The safety culture systematically needs to be built considering the actual piece of knowledge and experience. The appurtenant tool for its establishment is called “safety management“. In each system it represents the strategic, pro-active and process management based on the risk management and on results of science and advanced technologies. It includes:

- a prevention against the disasters of all kinds, i.e. natural, technological, environmental, social and caused by interdependencies; it includes terrorist attacks and existing interactions between the technical facility assets and its vicinity,
- a preparedness to put all emergency and critical situations under the control with the capability to renovate the affected part of technical facility,
- a response if emergency or critical situation affects the technical facility,
- a renewal after each emergency or critical situation.

The safety management establishing the safety culture has three basic phases:

- standard (current) management,
- emergency management
- and crisis management.

All these phases need to be reasonably interconnected and need to respect characteristic features and targets. The standard management is directed to build the safe community, safe territory, safe state etc. Its attention is mainly focused on the technical facility development, prevention and preparedness. Its main tool is a strategic planning based on knowledge, experiences and good engineering practice. The emergency management is focused on copying the emergency situations with the help of standard sources, forces and means. The crisis management is focused on copying the critical situations, human survival and stabilisation of situation so that the renewal and follow up development might be started, namely with the help of standard and beyond standard sources, forces and means, details are in [15,17,18].

Only at known and frequent disasters the risk level perceived by humans is near to real risk level. At infrequent and low known disasters, the humans perceive the risk level as shadowy and remote. Perception of risk is also influenced by further factors – e.g. at activities that we perform voluntarily (mountaineering, ski jumping etc.) we consider the insignificant level of risk. The risk acceptability is the result of comparison of several types of acceptability – technical acceptability (reliability and complexness of technologies, machines and devices), economic acceptability (costs) and socio-political acceptability (general risk perception).

The important role in technical facility safety management plays the safety culture [1,15,35,36]. It means that humans in all their roles (manager, employee, citizen or victim of a disaster) adheres to the principles of safety, i.e. they behave in such a way that they do not themselves trigger the realisation of potential risks and when they become participants in the implementation of risks, in order to contribute to an effective response, stabilisation of protected assets and their recovery and to kick-start their further development. According to some authors, this is a set of positions, assumptions, standards and values that exist in a given entity, which reflects how the entity is managed, i.e. these are general principles of division of powers and responsibilities, principles of management and a certain ratio between emphasis on work outcomes, authority, care for people, respect for the principles of safety and ensuring the entity functionality.

The safety culture is realized by adherence of safety rules; determined as golden rules for safety [1,15,35]. According to them for all participants, it e.g. holds:

- to prevent disasters, or at least their unacceptable impacts, as possible, ensure preparedness to cope with unacceptable impacts on the protected assets of a technical facility and to respond effectively to incidents, accidents and failures of the technical facility,
- to communicate and to cooperate with others involved in all aspects of the prevention, preparedness and response of the technical facility,
- to know the threat from disasters and possible risks in the technical facility and its surroundings,
- to implement and respect a 'safety culture' that is respected and promoted by all stakeholders at all times,
- to establish safety management systems, monitor and, if necessary to correct their activities,
- to apply inherent safety principles when planning, designing and operating the facilities and their equipment,
- carefully to manage changes in the technical facility,
- to be prepared to cope with all the disasters that may arise,
- to assist other stakeholders in carrying out their roles and responsibilities,
- continuously to improve the facility safety in accordance with a culture of safety, safe procedures and training,
- to strive to ensure all awareness and to provide information at all times and to provide feedback to managers,
- to develop, strengthen and continuously improve the concept of safety, regulations and directives,
- to lead and to motivate all others involved to fulfil their roles and responsibilities,
- to know the risks within the sphere of self-responsibility, appropriately plan measures for their proper management,
- to use appropriate and coherent policies at planning and follow-up activities,
- to be aware of the risks in the technical facility and to know what to do if they are implemented,
- to participate in emergency planning and response.

1.2.5. Automation of technical facilities and new risks

Currently, technical facilities are operated and constructed as socio - cyber - technical (physical) systems. Automation penetrates into the life of all technical facilities. On the one hand, it brings huge benefits and savings to humans´ work, and on the other hand, also brings other risks. The information safety and cyber safety become very important.

In the context of automation, the control of a technical facility is defined as the targeted operation of the control system on a controlled object in order to achieve the specified objective. In this context, the management of the technical facility is divided into automatic by help of information technology, semi-automatic (by intervention of technical mechanisms) and manual (carried out by man). In practice, they are distinguished control, regulation and higher forms of control (optimal and adaptive control, learning and artificial intelligence).

The work [18] summarises the findings of this area and shows that the current rules of automatic control are based on modelling based on reliability theory (i.e. only on the basis of data on random processes; knowledge uncertainties are not considered) Therefore, the safety of the equipment and facilities is not guaranteed under all conditions, i.e. at critical and extreme conditions caused by knowledge gaps or extreme influences. On the basis of the fact in question, a number of other sources of risk for technical facilities arise, especially those that use remote data transmissions. For example, the dropped cable at Fyodor robot made it impossible to make the first attempt at landing on the ISS (International Space Station); the connection was only successful after the intervention of the cosmonaut, who carried out the repair [34].

There are examples at work [18] where the root cause of the accident or failure of technical facility was neither a technical fault nor an error in anthropogenic control, but an automatic control failure consisting of an error in the flow of information – the correct information was not in the right time in the right place and with the right person. Therefore, attention should be paid to the risks associated with automation in technical facilities as well as in modern technologies.

1.2.6. Risk management

On the basis of recent knowledge summarised in the works [17-19], the correct risk management carried out by the process described above in Figure 5 needs to be applied. The methods of performing each sub-operation are discussed in detail at work [19]. Since in the case of technical facilities, software such as ROZEX, ALOHA, WHAZAN, EFFECT, TerEx, PSA according to TECDOC – 727 and others [27] based on tree models are still preferred in several operations, it should be noted that the results of the tree models do not respect a number of real facts, and they can only be used for simple tasks, where neglection of knowledge uncertainties cannot have catastrophic consequences. ***They cannot be used for example if the realisation of risk from one source is possible simultaneously in multiple places of the technical facility***.

The proposal of the tools for work with risks at individual risk management objective is one of the results of the research related to monographs resulting from the analysis of accidents and failures of complex technical facilities in Chapter 5.

In terms of the integrity of the information, the results of the European Union project FOCUS (Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles), listed in the work [22] are further given. The results show weaknesses in the management of the risks associated with technical facilities in the European Union and the areas in which actions and measures are needed; Table 5. Table 6 shows the causes of organizational accidents in technical facilities.

Table 5. Deficiencies identified in management of accidents and failures of technical facilities. Areas which are particularly important for addressing these deficiencies are indicated in bold. In the column "other" M indicates the need for monitoring and K the need to draw up a plan of continuity.

Disaster	**The list of shortcomings**	**The type of measures and actions for elimination the deficiencies**				
		legislation	**specific management**	**research**	**education**	**other**
The loss of serviceability of the territory (the failure of some of the infrastructure)	It is missing the concept for creating both, the robust critical infrastructure and the robust partial infrastructures; in particular the cyber infrastructure.	**Yes**	**Yes**	**Yes**	**Yes**	**K**
Beyond design accident with the presence of radioactive substances	Safety management is based on assumption, that multiple backed-up safety systems ensure the safety always. Lessons from Fukushima [24], however, show that the assumption is not true.	**Yes**	**Yes**	Yes	Yes	**K**
Beyond design accident with the presence of dangerous substances, mutagenic, carcinogenic	Safety management based on management of integral safety is required only in specified cases.	**Yes**	**Yes**	Yes	Yes	**K**
Misuse of substances CBRNE	It is missing an effective system of management with the CBRNE substances.	**Yes**	**Yes**	Yes	Yes	M
Misuse of nanotechnology	It does not solve.	**Yes**	**Yes**	**Yes**	**Yes**	M
Misuse of genetic engineering	It does not solve.	**Yes**	**Yes**	**Yes**	**Yes**	**M**

Misuse of IT technologies	It does not solve.	**Yes**	**Yes**	**Yes**	**Yes**	**M**

Table 6. Phenomena which cause the organizational accidents in technical facilities.

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

1.3. Requirements on technical facilities operation

Technical facilities belong to public assets because they ensure products and services on which the humans are dependent, e.g. [1-14,17-19,21-26]. Present knowledge shows that each public asset is open system with real time development and these developments are during the time sometimes conflicting [19,21]. The conflicts´ management is influenced by complex nature of all public assets which is described by system of systems models and time variability.

For humans´ security and development, the coexistence of technical facilities with their vicinity is necessary to be ensured throughout their life cycles [17,18]. Therefore, in line with current knowledge and experience, we need:

- to know the sources of risk at using the All-Hazard-Approach [48,49],
- to appreciate their harmful potential (i.e. identify the sizes and distribution of their impacts on public assets) in individual places, and the size of their potential losses and damages depending on the distribution of public assets, i.e. to determine the risk [19].

As it was said above, depending on the concerned human society possibilities, the risks are divided into acceptable, conditionally acceptable and unacceptable. In the case of risks which are:

- unacceptable, the application of effective preventive measures against their resources should be ensured,
- conditionally acceptable, the mitigating, reactive and renewing measures for the monitored assets should be prepared,
- acceptable, the risk monitoring over time should be installed with aim to reveal an increase of their harmful impacts over time.

In this way, we carry out activity which we call "risk management". The activity effectiveness depends on tools. The article deals with compilation of effective tools for technical facilities risk management directed to integral safety with aim to ensure their coexistences with their vicinity during their operations. The problems solution given hereafter respects that the safety is preferred over the reliability.

1.3.1. Checklists for identifying the technical facilities cross-cutting risks

On the basis of the above given facts, the integral safety of complex technological facilities is based on:

- the system concept of reality,
- considering the nonlinear phenomena,
- the building of the coexistence of systems,
- application of All-Hazard-Approach [48,49],
- application of Defence-In-Depth access [50] .

On the basis of the information referred to in the work [17] for the management of a complex facility of the type system of systems, i.e. the system in which conflicts are possible, it is necessary to:

1. To assess whether at the siting, construction and operation there are adequately considered all possible disasters at a given site and what type of measures in the area of disaster management are aimed at them, Table 7.
2. To assess for every possible specific disaster weakness from the perspective of the application of access the Defence-In-Depth, Table 9.
3. To assess for each critical disaster influence of possible couplings, Table 9.

Table 7. Identification of deficiencies (i.e. spots leading to the criticality of the complex facility) performed according to demands of the All-Hazard-Approach. How to fill the table – considering the only disasters that have direct impacts, i.e. boxes, requiring a response that do not make sense are blacken out, and they are not include to the total assessment.

Disaster-the name	Is disaster relevant?		If the disaster is into the category of specific disasters, is this reflected in the siting, design, construction and operation of facility by effective preventive technical measures?		If the disaster is into the category of specific disasters, is this reflected in the operation of facility by the effective preventive organisational measures?		If the disaster is into the category of critical disasters is this reflected in operation of facility by reactive measures for the protection of employees, technology and the environment inside the facility?		If the disaster is into the category of critical disasters, is this reflected in the operation object to reactive measures aimed at the protection of workers, technology, people and the environment inside and outside the facility?	
	NO	YES	NO	YES	NO	YES	NO	YES	NO	YES
....										
TOTAL										

Table 8.Identification of deficiencies for specific disasters in a given territory, i = 1,2, ..., n, i.e. assessment of the criticality of the viewpoint of the application of access the Defence-In-Depth.

i	Question	The answer		Note
		YES	NO	
1	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe design?			
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?			
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).			
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions measure for emergency response that mitigate impacts on technological facility system and ensure the capability to return to a normal state? Operation of a technological object is successful, if it is a good continuity plan, which ensures that the technological facility shall ensure all the necessary tasks.			
	5. Does management system (SMS) for the case of loss of control, i.e. supercritical (beyond design, extreme) conditions the measures for: - maintaining the operability of the technological system following its repair and maintenance, - and measures to ensure the protection of public assets (people, the environment and other assets) in the surroundings of technological facility?			
2	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe design?			

	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?			
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).			
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions measure for emergency response that mitigate impacts on technological facility system and ensure the capability to return to a normal state? Operation of a technological object is successful, if it is a good continuity plan, which ensures that the technological facility shall ensure all the necessary tasks.			
	5. Does management system (SMS) for the case of loss of control, i.e. supercritical (beyond design, extreme) conditions the measures for: - maintaining the operability of the technological system following its repair and maintenance, - and measures to ensure the protection of public assets (people, the environment and other assets) in the surroundings of technological facility?			
....				
(n)	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe design?			
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?			
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to			

	keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).	
	4. Management System (SMS) for the case of loss of control, i.e. critical conditions for emergency response measures to mitigate effects on technological system and ensure the ability to return to a normal state? Operation of a technological object is successful, if it is a good plan of continuity, which ensures that the technological system shall ensure that the necessary tasks.	
	5. Does management system (SMS) for the case of loss of control, i.e. supercritical (beyond design, extreme) conditions the measures for: - maintaining the operability of the technological system following its repair and maintenance, - and measures to ensure the protection of public assets (people, the environment and other assets) in the surroundings of technological facility?	

Table 9. Identification of weaknesses, i.e. the specific critical spots for critical disasters, i = 1,2,...n – expert investigation. YES = 3; rather YES = 2; rather NO = 1; NO = 0.

Critical disaster	**Are assured of protective measures and activities for**					**Are ensured protective procedures for the poor response?**		**Are ensured protective procedures for poor management of operation?**		**Are ensured protective procedures for the application of bad rules?**	
	employees and people in the facility surroundings	operation of technology	the environment in surroundings	people in facility surroundings	reconstruction of operation within 14 days	**YES**	**NO**	**YES**	**NO**	**YES**	**NO**
1											
2											
....											
n											

The tables are used in practice, the scales of values in the first phase are set the same as they were originally set up for standards [1,13-15], Table 10, which is close to the scale used by the FEMA.

Table 10. Scale of values.

Criticality rate	**Values in%**
Extremely high-5	More than 95%
Very high – 4	70-95%
High-3	45-70%
Middle – 2	25-45%
Low-1	5 – 25%
Negligible-0	Less than 5%

1.3.2. Risk management and settlement at technical facilities

According to [51] the management of technical facilities in Europe has been project management since World War II, namely the TQM (total quality management) type [52], and relies on risk management. According to the data in the current professional literature summarised in the work [18], the various types of management used for technical facilities, which according to the objectives of the management of technical facilities are in practice:

1. Reliability management.
2. Security management.
3. Safety management.
4. Continuity management.
5. Resiliency management.
6. Asset management.

Each of these types has certain specifics. The first type of management is regulated by technical standards and norms. The second type in addition to reliability management focuses on protecting technical facilities from internal and external harmful phenomena (disasters), including the behaviour of the humans, who create and operate them [19]. Security in conjunction with a certain object generally means a set of measures and activities to ensure that the object does not suffer losses, damage and damage in the event of internal and external harmful phenomena. To its realisation, it is used physical and cyber protection of the object [41], not only against attacks from the outside, but also from the inside.

The rules on ensuring the technical facilities security are elaborated in the work [53], in which it is also the delimitation from the technical facilities safety [54]; the distinction is also in IAEA documents [55]. Although logically the safe object is also a secure object [17,18], there are still conjectures as to what is more important. The consensus is that a secure technical facility, as well as a safe technical facility, performs the tasks set for a specified period of time under certain conditions, while being protected against all internal and external disasters, including the human factor. The difference is that a secure technical facility does not have the protection of the surroundings built in. Other types of control are described below.

The components of all types of management are specific types, such as emergency management and crisis management. A comparison of types shows that:

- all types use the same methods and tools for working with risks which, because of the different objectives of the procedures in question, do not give the same results in specific cases [18],
- all types have generally the same objective, namely taming the risks and assets protection; however, they differ by risks´ concepts and by set of assets that followed,
- starting with the second type, they are the superstructure of reliability management, which has been a royal discipline in the management of technical facilities for many years; analysis of significant contexts is summarised in [18].

Despite the different names their methodology is the same, namely to get:

- awareness of risk,
- understanding the risk and its relation to assets and their security,
- and to apply relevant knowledge of what to do to achieve the goal.

In the next text, we focus primarily on risk management in favour of safety (i.e. safety management), but because of the existence of scientific and commercial schools that promote risk management under the above names, we will briefly mention the relevant places instruments of other disciplines.

1.3.3. Difference between asset management and risk management oriented to safety

Management is a comprehensive set of activities, the implementation of which in practice helps the quality process of managed organization and the achievement of its objectives. In general, they form a set of procedures and procedures for finding and solving problems. It consists of planning, conducting and organising people's work, allocating resources, evaluating the effectiveness of procedures, checking the status and, if necessary, applying corrective measures [15].

For reasons of tasks and objectives, there are differences between the private sector and the public sector. In the public sector, which is represented by municipalities and regions, the objective is not profit or other benefit for a particular legal or natural person, but the objective is the public interest and its performance. Another important difference between these sectors is legal regulation. The public sector has a greater link to the law, which results in a significant restriction in the field of decision-making. This is due to the need to respect and fulfil the obligations and principles of public administration, respect the elected authorities, the adjustment of the status of the organizational units of the State, the rights and obligations of their employees, the requirements for financial and property management, etc. Another difference between sectors is due to the absence of profit in the public sector, resulting in some benchmarks and indicators being used in the private sector to promote better management.

Technical facilities are both, the public and the private, but all in the rule of law have an obligation to respect the public interest. This means that any organisation (legal or natural person) operating a technical facility needs to respect, in addition to the objectives to which it was set up, the objectives of the State, the protection of public assets (the health, lives and security of humans, property, the public good, the environment, other technology and infrastructure) and the moral and ethical rules of human society in the place in which they operate. In terms of the basic functions of the State, protected public assets are pre-assigned to the organisation's own protected assets. The good management of matters for the benefit of the public interest and the interest of the organisation takes the form of the project management and process management of organisation, which is governed by a linked set of measures and activities, and in which risk negotiation plays a major role [15,56].

In order to achieve the demanded objective, which it is a safe organisation at present (i.e. a safe technical facility in the case under review), which has the potential to develop sustainably, it is necessary to:

- know and consider all possible internal and external risks to the organisation in question, both individually and in context,

- properly negotiate with all the risks,
- have the risk management set up correctly.

From a professional point of view, on the basis of current knowledge, it is necessary to understand each organization as an open system, the behaviour and conditions of which are influenced by processes and phenomena that take place inside and outside the organization. Their impacts are modified by a convoluted network of links and flows that are within subsystems, across subsystems, some of which are interdependent, across the system and around the organization. Risk management needs, therefore, to be comprehensive and its priorities need to be focused on the security and sustainable development of the organisation in a safe territory and in a safe human society.

An asset of a technical facility is a tangible or intangible item that can be owned. The resource of a technical facility is the tools and competences that use assets and without which the assets would not have its value. They also include cognitive and social capital, i.e. specific skills and competences that enable people to acquire additional resources. The preventive capacity of the system is the measure of system capability by which the system is prepared for failure. The absorption capacity of the system is the limit rate of failure that the system is able to handle. The adaptive capacity of the system is a measure of the system's ability to be reorganized to cope with unexpected operation conditions. The restorative capacity of the system is the rate of repairability of the system after failure. Capacities shall be measured in the following areas: technical; organisational; social; and economic.

Another important feature is the integrity of the safety of the technical facility, which according to [57] is intended to include the ability of the system to provide early warning to the user that the system is not in order. The system for safety ensuring /support is designed to avoid obstacles that may occur during the operation of the device / facility, with the help of the detection system in SMS.

The basis of the type of management "asset management" is the development of the assets of the technical facility; i.e. focus on the highest performance. It is about linking the separate disciplines, namely process safety and integrity management of the entity, which means profit and competitiveness for technical facilities. According to the above facts and works [17,58], in the case of complex technical facilities, account should be taken of a number of criteria, some of which are conflicting, Figure 8.

In order to avoid the initiation of large risks, which at realisation cause great losses and damage to people and other public and private assets, the fundamental objective of the management of technological units is not to achieve a large number of products, but also to prevent losses on their assets and public assets, and therefore, a consensus is sought between risk management and asset management of the object. This means having an operating regime such as to ensure the prevention of large losses that could be liquidated for a technical facility. It is about finding a way to avoid risk-taking that will cause losses and damage to public and private assets that are de facto higher than the profit of increased production.

Because when focusing on loss prevention, it is not only about reducing the likelihood of failure of a technical facility, but also about improving the conditions of operating assets, so SMS (safety management system) of technological objects must be flexible and be targeted at interoperability of public and private assets. The work [15] elaborates on the issue in more detail. Based on [59-61], the loss prevention procedure focuses on assets that affect the security of the technical facility, humans and the environment in the accident. The aim is to ensure safety and long service life of the technical facility. The factors that determine it in this type of management are:

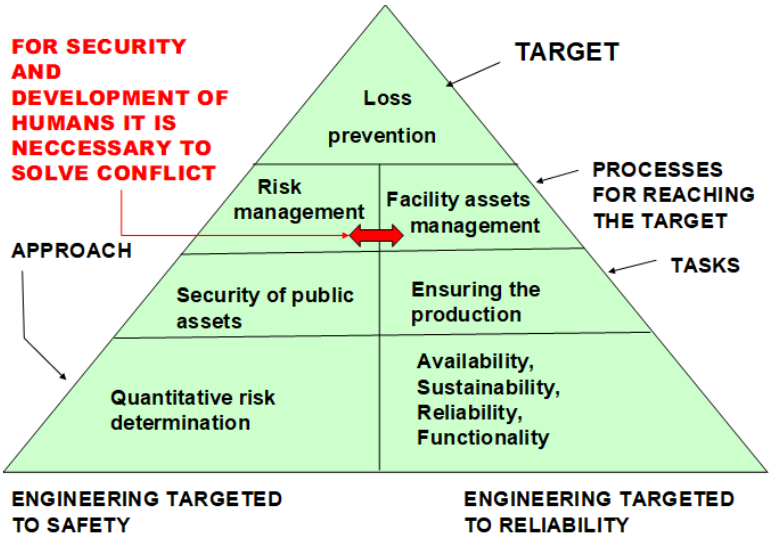

Figure 8. An example of a basic conflict in the management of critical facilities — it is compiled with consideration of ideas in [58].

- risk management, i.e. identification of hazards, incidents, accidents, risk assessment and methods of risk settlement – PHA, FMEA, HAZID, HAZOP, FTA, ETA, SIL, LOPA, AQR [25] and Bow Tie [30,31] are used; their weaknesses have already been mentioned above,
- the size of the reliability and maintainability index, i.e. they are performed RAM, analyses of maintenance and inspections,
- human factor. The human factor analysis is required to answer the questions: what can happen; what are the consequences of a bad human reaction; which human features affect the reliability of man; and what is necessary to increase human reliability and prevent human errors.

On the basis of the knowledge set out in [19], this means that external disasters and human factors are not considered in the asset management type, which reduces the effectiveness of the type of management in question.

1.3.4. Safety margins

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 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 [62]. Figure 9 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 [27] with compliance with safety requirements.

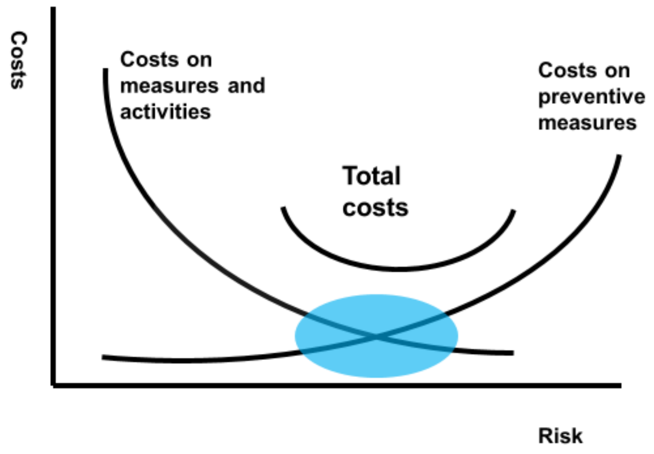

Figure 9. The total cost interval in which safety is ensured; processed in [62]; the area of optimal costs for safety margins is marked in blue.

The outputs from the risk management process to ensure safety according to [52] 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 [1,17,18] applied. These risks should be given in the project documentation [30,31] and need to be systematically managed during 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 [1,7,17,18]).

According to knowledge summarized in [1,6,17,18,30,31], the risk management strategy in project uses: 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. At operation it is necessary to respect the project safety strategy and all changes perform with regard to it. For overcome sudden risks ‘occurrence it is necessary to have tools such as continuity plan and response plans [15,17,18].

1.3.5. Responsibilities for technical facilities´ risk management

To derive the technical facilities risk management responsibilities, there are used the knowledge and experience listed in the previous chapters and the base viewpoints:

1. The technical facilities need to be safe throughout the lifetime, and therefore, risk management needs to be: focused on the integral safety; and in all aspects comprehensive, systemic and proactive.

2. The technical facilities need to fulfil during the lifetime the tasks in demanded quality, and at its critical conditions it must not endanger itself or its surroundings, i.e. they are applied the All-Hazard-Approach developed for Europe at work [49], the Defence-In-Depth developed for the technical facilities, including the critical infrastructure [17,18,50]; it, has a program for the continuous improvement of safety and safety culture.
3. The technical facilities are important for ensuring the basic functions of the State (power plants and electricity distribution, water works and water supply, sewer, highways, big airports, transportation communications, large production units, etc.), and some its parts also for the EU, and therefore, the obligations for putting the risks under control are divided among all stakeholders.

According to results in work [18] and principle which is common in Europe [63,64], which means that responsibility for the safety of a technical facility, i.e. the level of work with risks associated with a technical facility, lies with the owner / operator and also public administration. 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.

The States belonging to category "Parliament Democracy" have the public administration formed as organizational structure constitutes from hierarchical structure of executive offices. The structure is: Parliament; government; regional office; municipality office (in some countries district office is between regional one and municipality one). According to this structure the responsibilities are: Parliament chairman; government chairman; region chairman; municipality chairman. For execution of real tasks, the government has ministers and mentioned offices have special departments; e.g. for development, environment, civil protection, health etc., which have real officers for solution of administrative matters.

The important role in ensuring the responsibilities in technical facilities plays the organizational structure, which is mechanism used to coordinate and control technical facilities operation. According to [3], the technical facility organization structure constitutes a hierarchical arrangement of relationships of superiority and subordination and addresses mutual competences, links and responsibilities. Of course, large financial and other means releases on risk management is only at the highest hierarchical level. According to experience from practice [3], complex technical facilities have several hierarchical levels arranged in the following organizational structure and responsibilities:

- top management – group of managers responsible for technical facility performance – the responsibility has the technical facility top manager,
- higher management – projects´ (set of production lines) leaders – the responsibility in appurtenant matter has the appurtenant technical facility project manager in a given matter,
- medium management – processes´ (e.g. one production line) leaders – the responsibility in appurtenant matter has the appurtenant technical facility process manager in a given matter,
- technical management – persons for individual technical equipment operation – the responsibility in appurtenant matter has the appurtenant person for technical fittings operation in a given matter,

- operation personnel – persons responsible for technical and supporting activities - the responsibility has the appurtenant technical fittings operator and each participant.

It is understandable that the higher position in the management structure, the higher responsibility due to higher power, which means the higher competences [41].

Therefore, from the perspective of human security and development, it is important the responsibilities for risk management in two areas [18]:

A. The territory administration and the technical facilities management.

B. The technical facilities real safety management.

Based on critical analysis of the accidents and failures of the technical facilities, thereinafter, there are given risk management principles for the territory administration and the technical facilities management in the number 40 for the levels:

A1. Political (Parliament, Government, public administration) - a total of 4 requests.

A2. Strategic (public administration, owner, investor, operator) - a total of 8 requests.

A3. Tactical (public administration, owner, investor, operator) - a total of 4 requests.

A4. Operational / functional (local administration, operator) – a total of 5 requests.

A5. Technical (operator) – a total of 19 requests.

A1. Principles for technical facilities risk management – political level: for Parliament, Government and public administration:

- to create conditions for the long-term stability of public space, which the technical facilities need for quality operation, (it goes about all on ensuring the stable government, mitigating the corruption, prevention of formation of intolerant groups, mitigation of impacts of terrorism and national and transnational conflicts on the technical facilities),
- to promote the public interest and to respect the fact that the technical facilities risks enter into the public area, i.e. it goes on the externalities that cannot be solved by market mechanisms (harmful impacts; by operation failure it is threatened a considerable part of the public; the political decision has the potential to trigger an event, in which the risk is realised; and adverse events, which are caused by unacceptable risks are distributed by the way that they do not take respect to the political fairness),
- to respect that the frequent changes in legislation, taxes and the requirements to the technical facilities operators may lead to technical facilities lower quality of service,
- to consider the views of specialists when deciding on the technical facilities and not to prefer momentary political interests and actions of pressure groups.

A2. Principles for technical facilities risk management – strategic level: for public administration, investor, owner and operator of the technical facilities:

- to respect the value and cultural context (comfort strategy of insurance and compensation is not fully reliable, because at the great risk realization, it can happen hitting the social system, and therefore, it needs to be promoted the precautionary principle and responsibility from all participating),

- to prevent the use of incorrect technologies, the technical facilities technological inadequacy and insufficient preparedness of the site for the technical facilities operation (surveillance, supervision of the State),
- to ensure that the liabilities associated with the technical facilities may be fulfilled in good quality (surveillance, supervision of the State),
- to ensure the technical facilities staff training, mainly at the level of technical and technical-organizational; the relevant research, planning and legislation to support the technical facilities operation,
- to promote a proactive, systematic and strategic approach at working with the technical facilities risks,
- to pay attention to the technical facilities goodwill at work with the risks,
- to ensure that significant risk sources for the technical facilities might not been underestimated, which are: uncertainty in the labour force (unsuitable qualifications, lack of staff, the unreliability of the workers - fluctuation, strike, etc.); the uncertainty of the financial resources (insolvency of business partners, credit uncertainty, problems with insurance, etc.); accidents and large faults on operating equipment; industrial accidents in other bodies; natural disasters; and political or economic instability in the region,
- to ensure the capability of public administration and the technical facilities management to handle the impacts of extreme disaster and to perform recovery of the technical facilities and its vicinity.

A3. Principles for technical facilities risk management – tactical level: for public administration, investor, owner and operator of the technical facilities:

- to ensure that at designing, building, construction and operation of the technical facilities, all serious disasters that are possible in the technical facilities site are considered and properly dealt with,
- to ensure so that the technical facilities design documentation is correct and errors-free; the technical facilities building and construction done according to professional requirements, i.e. without errors, exceedance of construction costs and unnecessary environmental pollution at the site,
- to ensure that the technical facilities is safe under the conditions normal, abnormal and critical (monitoring and supervision of the State),
- to ensure the cooperation with the local population and local security forces for case of accident or failure of the technical facilities (to build organizational resilience [37].

A4. Principles for technical facilities risk management – operation / function level: for public administration and the technical facilities operator:

- to ensure a proper settlement of all risks, in particular market risks, such as the reduction of demand for the product, changes in the exchange rate; inflation, deflation and changing the interest rates,
- to ensure the technical facilities high-quality operation from the perspective of ensuring the material inputs and qualified personnel,
- to create inside the technical facilities, the safety culture based on mutual cooperation, i.e. to have the tools to control conflicts among employees,

- to provide resources and protective equipment for employees and the local population, including the information fittings and documents (for case of accident occurrence),
- to ensure the appropriate training and education of employees, and the local contractors and local population.

A5. Principles for technical facilities risk management – proper technical facilities management level: for the technical facilities operator:

- to improve permanently the risk understanding, risk management and trade-off with risks,
- to implement the risk sources continuous monitoring,
- to consider the risks of organizational accidents,
- to consider the risks associated with the technical facilities complexity (because the complexity not only creates new dangers, but makes them even worse identified; new hazards are e.g.: increasing the automation, the growth of production capacity, the large pace of technological change),
- to count with the appearance of atypical accidents, the causes of which are unexpected combination of events, and for this case to have a high-quality response plans for multiple scenarios of accidents and also for special accident caused by a combination of a series of unacceptable phenomena,
- to admit that the safety systems and safety related systems may fail,
- to process a response plan to extreme phenomena,
- to train responses to situations created by extreme phenomena,
- to have prepared place for response management in the case of great accident and technical equipment for clearing debris,
- to ensure that the professional top management is constantly interested in the development of knowledge and evaluated the experiences from the technical facilities operation, because there is no previous experience, which could be used to overcome new dangers and the relevant laws and standards for many of the new engineering and technology sector are not yet developed,
- to ensure performance of all tasks associated with the real technical facilities operation,
- to ensure the implementation of all tasks of the State (the products in the required quality, services, accessibility),
- in the technical facilities managing to be based on the qualified professional criteria for risk assessment (established according to: the nature and kind of consequences that may occur during the realization of risks including their measurement; the way of risks occurrences setting; the time frame of the consequences and the risk probability occurrence; the way of determination of risk level, i.e. the level below which the risk is acceptable or tolerable, and the level of risk, from which it is necessary to ensure a targeted response; and the possibility of combining multiple risks),
- to ensure the professional performance of actions, qualified maintenance, skilled repairs, timely modernizations; and timely adaptation to changing conditions (to have a qualified professional management and a highly effective professional

inspection, including motivational resources to target employees on the safe implementation of the activities and cooperation),

- to ensure the protection and the necessary training the critical employees, i.e. also the protective equipment and utilities and other necessary formalities, including the appropriate resources and protected space for hide of employees,
- to ensure the technical facilities high-quality operating rules for normal, abnormal and critical conditions,
- to ensure high-quality monitoring and timely response to operational deviations, failures, near accidents and accidents (to ensure that in due time there are accepted necessary measures, especially in sites where it is accumulation of a large amount of failures and near accidents),
- to provide the making up the basic plans: technical facilities safety management plan, which will provide safety during the life cycle; the risk management plan, in which the clear responsibility for the individual measures and individual activities are given; in-site emergency plan (in which the clear responsibilities for the individual measures and individual activities are given); business continuity plan (to overcome the highly critical to the extreme conditions in which they will be clear responsibilities for each of the measures and activities for the conservation and survival of the technical facilities; the external emergency plan and crisis plan (in which the clearly defined cooperation and accountability of the technical facilities components and their security forces, the public security forces, and public administration),
- to ensure permanent consideration of new knowledge and lessons learned from the near accidents and their implementation into practice in a form suitable for the technical facilities.

It goes on a real subject area that deals with data, methods, material and technical issues, organisational, legal, financial and personnel matters directly in the technical facilities. Risk management needs to respect that fundamental role has: knowledge; respect for the physical and other patterns (properties of material, structures, buildings and environments and their changes in time), i.e. the existence of limits and conditions; the human factor and with it connected the performance of high-quality work and the proper execution of responsibilities at all stages of the life cycle; the availability and the modalities of application of processes and technologies, etc. General principles for working with risks are:

- to be proactive,
- to imagine the possible consequences,
- to properly prioritize public interest,
- to think of mastering problems,
- to consider synergies,
- and to be vigilant.

At all stages of the technical facilities life cycle it is required so risk management may be complied with the main principles:

- it is targeting to an integral safety, using the All-Hazard Approach [18,49], the Defence-In-Depth developed in [18,50], and relying on the program for safety improvement targeted on the safety integrity (i.e. to have a safety management system, process safety management and safety culture),

- it is containing in each decision-making the followed technical facilities – TQM [52] and ISO standards (International Organization for Standardization),
- it is complying with the key concepts in risk engineering targeted at safety, i.e. it considered a critical quality attributes and critical process parameters (quality of implementation of measures and actions of prevention, preparedness, response, recovery and lessons learned),
- it is using: high-quality data, methods, and engineering approaches, progressive types of safety approaches - the inherent, passive and active safety,
- it is optimally governing the factors of different nature: knowledge; experience; the budget; competences; the way of management and decision making; team work; etc.
- it is optimally dealing with the conflicts.

Based on critical analysis of the accidents and failures of the technical facilities, thereinafter, there are given risk management principles for real technical facilities management in the number 66 for the domains:

B1. The concept and way of real technical facilities management - 21 requests,

B2. Requirements for data, methods, and techniques that ensure the quality of decision-making and management of the technical facilities - 9 requests,

B3. Procedures for the correct sitting, the quality of: the technical facilities design, building, construction and operation - 13 requests.

B4. Provisions for the technical facilities business continuity and for support the basic functions of the State, i.e. public interest – 23 requests.

It goes on the requirements for data, methods, and ways of solving problems in the areas of technical, methodological, organizational, staffing and financial; the results are at work [65].

2. FINDINGS ON TECHNICAL FACILITIES TYPE OPERATION

Each technical facility is created by human activities and it provides products or services important to human´s lives; technical facilities aimed at promoting policy objectives only were not been subject to research. Technical facility architecture is object or network. Each technical facility type has its specifics; e.g. there is a significant difference between the control of stable ones and moving ones.

The human lives in modern society are made easier through technical and cyber systems. However, all these positive consequences of technical progress on the human system functioning are redeemed by existence of a much larger number of risks that lead to:

- the failure of the State basic functions,
- safety level reduction,
- and disruption of technical facilities coexistence with their surroundings.

The reason for increased number of risk sources [17,35,36,66] is existence of a large number of different types of complex systems, their elements and interconnections on which the human system depends.

Each technical facility and its surroundings change over time, these changes are not synergic, and therefore, they also change their mutual interactions. From the human security and development viewpoint, it is important so these interactions throughout the technical facility life cycle should be adequate. They may not cause the sources of risks that would significantly undermine the conditions necessary for the human lives and cause the situations that human society would not have the capacity to deal with the risks to its advantage.

As the world dynamically evolves, the progressive anthropogenic management already notes that due to the technical facilities´ and the world´ complexities and time changes in conditions that humans do not have the ability to influence, the accidents and failures of technical facilities are a reality with which the anthropogenic management needs to deal [67].

Therefore, it needs to go on such technical facilities managing that performs well-established tasks during their lifetimes for their safety. Due to the existence of dynamic transformations, the management is foreseen that situations may arise where technical facility becomes dangerous to itself and its surroundings [67]. In order to ensure security for human society and other public assets, it is, therefore, necessary to have the tools to reveal risk sources and to manage emergencies so that their impacts on public assets and on technical facility itself may be minimal.

It should be remembered that in critical situations, the solution is not a " to sacrifice the technical facility", i.e. to carry out measures and activities that completely destroy it, since the technical facility supplies products or provides services, employs humans and is a source of economic capital for given territory. Therefore, serious risks should be managed with targeting the technical facilities safety in all possible conditions [16,20]. However, our research shows lacks in awareness on risks, especially among managers and politicians.

2.1. Technical facilities attributes

Technical facilities are physical, cyber and organizational (including personnel) interconnected systems – social-cyber-technical systems. Examples of physical / technical systems are buildings, technical equipment for the production or transmission of energy, networks, means of transport, material equipment. Examples of cyber systems are computer systems for the management of production and other processes, information sources, etc. Examples of organizational systems are economic and organizational units.

Because technical facilities are complex systems (system of systems - SoS), their behaviours cannot be inferred from the behaviour of individual parts and, under certain conditions, there are occurred unexpected phenomena that lead to the destruction or failure of the technical facility functionality. It goes on:

- a sudden emerging the behaviour feature that cannot be derived from knowledge of components´ behaviour,
- hierarchy,
- self-organization,
- diversity of management structures, which together resemble chaos [17,18].

Therefore, to ensure complex technical facilities safety, it needs to be used multi-disciplinary and interdisciplinary approach [19], which ensure their:

- existence (ability to ensure balance),
- efficiency (ability to cope with resource shortages),
- freedom (ability to handle challenges from the surroundings well),
- security (ability to protect itself from phenomena inside and outside),
- adaptation (ability to adapt to external changes),
- coexistence (the ability to change its behaviour so that it may responds to the behaviour and orientation of other systems and so that the systems do not endanger each other).

Due to technical facility complexity, their safety is necessary to understand in integral sense. Great attention needs to pay to interconnections and existing flows among different parts and sectors that manage partial subsystems. At one system failure, interconnections can have unforeseen the consequences in form of chain reactions (cascades) and domino effects accompanied by failure, or by gradually failing other important systems and services; e.g. power outages can cause outages in drinking water supplies, food supplies, heat supply, fuel, failure of transport infrastructure, failure of management and information technologies for the functioning of the banking sector, state administration and emergency services, etc. [17,18]; examples of failures impacts are also in [1,67]; Annex 1 shows model of such failure impacts.

In terms of current knowledge, at least two tasks are ahead today:

- to solve the functionality of set of interconnected (i.e. dependent) objects and infrastructures under normal, abnormal and critical conditions,

- to search critical conditions of complex fitting, equipment or facility that are unpredictable or are result of serious operator´ error, and that may, under certain conditions, go to highly non-demanded, i.e. highly unacceptable conditions, i.e. situations in which the very existence of facility or even humans is threatened, and which we usually refer to as crisis.

Therefore, they are followed specific characteristics such as:

- interoperability (i.e. ability of technical facility as a whole to perform quality tasks under normal, abnormal and critical conditions),
- safety integrity (SIL), which is mostly tracked in conjunction with human errors (at specification, design, installation, maintenance, modification, etc.),
- criticality (i.e. extent to which personal injury, material destruction, damage or other asset losses may occur – threshold below which monitored equipment condition is demanded and vice versa),
- dependability (operational reliability), which ensures that system meets specified requirements and its operation complies with specified conditions (it extends to two basic characteristics, which are vulnerability and durability,
- the other characteristics are in [21]).

In this context, we divide technical facilities into reliable, secure and safe systems [17]. Reliable system is system that performs required functions at 95% probability level. Secure system is reliable system that is protected from all risks. Safe system is secure system that, even in its critical conditions, does not endanger itself and its surroundings. In creation and operation of all these system types [17,18,33], it needs to:

- work with risks,
- apply Defence-In-Depth principle,
- and require management using the technical facility safety management system – SMS.

When at the technical facility designing, creation and operation, it is not clarified what objective is pursued in practice, the confusions arise in prioritization, and they lead to conflicts, and therefore, the optimization of measures need to be carried out. Misplaced priorities bring harm, e.g. five girls lost their lives in an escape game in Poland because they were in a secure room; pilot Andreas, from Germanwings, could have led the plane to the Alpine mountain massif because the cockpit was secured - the armoured door could not open from the outside, etc. [19].

The suitable solution offers the use of the integral safety concept, which root is that it:

- considers the priorities in public assets,
- is based on consideration of all phenomena that can damage the territory and technical facility, i.e. the All-Hazard-Approach [48,49],
- and which at reducing the costs clearly determines what risks can been neglected by fact that facility, fittings or equipment is only considered as a secure system or only a reliable system [18].

Its application at operation according to knowledge in Chapter 1 and in [1]. requires to:

- monitor priority risks and conditions of critical fittings, components and personnel,

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

2.2. Present findings on technical facilities

The architecture of each technical facility is determined by the level of knowledge and experience of the promoters, manufacturers, and supervisors. It is true that over time the principles and procedures used in design, construction and operation are obsolete. The fact in question in the operation of the technical facility leads to the detection of shortcomings in the project. Although, only some shortcomings in the project can be eliminated by technical measures that are more effective than the organisational measures [17], the operator needs to square with them to support the safety.

Hollnagel [68] by analysing the critical infrastructure showed that failure of complex systems only needs to be a consequence of malfunctions or bad project, but also the consequence of interdependences (internal interconnections) that occur between elements, components and systems of the technical facility. As previously mentioned, the architecture of complex technical facilities is described from a theoretical point of view by the model of an open system of systems. Therefore, the problems in the management of technical facilities in terms of current knowledge [1,17,18] are:

1. Description and characteristics of a technical facility which has multiple immeasurable protected assets understood systemically, i.e. among assets they are different internal links and flows.
2. Durability, vulnerability and adaptability of individual fittings, components, systems and system systems. When (in what combination of characteristics of individual elements or systems) is an individual system or system of systems sustainable?
3. Identification of integral risk (there are multiple protected assets in the system that are linked by internal links) by considering risk sources inside and outside the system.
4. Relationships between partial, integrated and integral risk in system of systems.

5. Relationships between the integral risk of the system of systems and the integral risks of subsystems.
6. Criteria for the integral safety of a technical facility as a system of systems (a set of safe systems may not be safe, because there are interdependences that are non-demanded and will only manifest themselves under certain conditions).
7. Principles for safety management of system of systems (e.g. required for critical infrastructure).
8. Legislation to support the safety management of system of systems.
9. Control mechanisms for monitoring the level of safety of system of systems.

Each technical facility is a complex dynamic system with a certain level of adaptability. It consists of physical elements and processes that use these elements to perform tasks that are linked. According to the work [69], the connectivity means dependency between at least two elements or two sub-components or components of a technical facility. Through this connection, the condition of one subcomponent affects or correlates with the condition of another subcomponent. The definition in question should be extended to include the condition for the mutual sharing of certain physical elements or processes, and those elements or processes may be located in a particular territorial area. Therefore, interdependences can be physical, cyber, logical and territorial. In doing so:

1. Subcomponents are physically mutually interdependent if the condition of one of them is dependent on the material output of the other.
2. Cyber mutual dependence means that the condition of one subcomponent depends on information from another subcomponent. Cyber interdependence assumes the existence of an informational component.
3. Subcomponents are territorially interdependent when events in the territory can change the conditions of subcomponents.
4. Logical interdependence means that the condition of one subcomponent depends on the condition of another subcomponent, and the interconnection mechanism is not physical, cyber, or territorial. It goes on dependencies transmitted through flows, which are regulations, finances, legislation, etc., e.g. financial markets.

At work [69] the characteristics of subcomponents are supplemented with other items, such as:

- types of disorders and failures (cascading and escalating disorders, disorders from the same causes – for example, natural disaster),
- operating conditions (normal, abnormal and critical operation),
- the level of tightness of relations and interconnections (loose, tight, complex),
- characteristics of critical objects or infrastructures (temporal, territorial spatial, organizational, ownership and institutional).

Due to interdependence, a disorder or failure of one subcomponent (system) causes a disorder or failure of the subcomponent of the other. The fact in question contributes to the criticality of the whole technical facility. Therefore, it is not enough to ensure the safety of the sub-components separately, but it is necessary to ensure the safety of the entire technical facility.

At present, nonlinear interactions and dependencies should also be considered from the point of view of complexity, and therefore, the works [68-72] propose a hierarchical structure of complex systems that represent every important technical facility; it was created FRAM (Functional Resonance Accident Model) [68], in which the planes are distinguished:

- tasks,
- functions,
- and resources

and by help of matrixes they are followed their interconnections, with they are searched the couplings, which may lead to a cascade of non-demanded phenomena, i.e. to the failure of the technical facility.

Other important aspects, which need to be correctly applied at the technical facility operation, are:

- All-Hazard-Approach principle,
- Defence-In-Depth principle,
- inherent safety,
- active and passive elements to promote safety, and barriers;

they are described in detail in the work [30,31].

The Defence-In-Depth principle is a deterministic principle by which multiple barriers are inserted into the system when creating the technical facility project. The aim of which is to ensure the prevention of accidents or failures and, in the event of their occurrence, mitigating the impacts. Ideally, barriers should not be interdependent, so that the failure of one does not cause the disorder of the other. In practice, however, this is not possible. Therefore, the task of probability risk analysis (PRA) is to show that the risk is acceptable through this dependency, and to identify important dependencies with regard to the risk, which need then to be treated by preparing an appropriate response.

In practice [3], various I&C systems are used to ensure the execution of functions at different levels of the Defence-In-Depth principle; for many there are overlaps. In many I&C systems there are backups, e.g. they have multiple sensors, processors and distributors. Backup requirements depend on what level of Defence-In-Depth is performed and depends on the analysis of initiation events. Diversity between Defence-In-Depth levels is required to avoid failures from one cause.

Common I&C targeting at the safety are implemented differently. Those that are targeted at safety need to include various technologies (preventive, protective, various protective functions). Requirements on diversity lead to the need to introduce several options that can be incorporated by

- hard-built backups in the system software,
- the use of a variety of measuring processes,
- introducing the manual backups for automatic functions.

Since full independence between Defence-In-Depth levels cannot be achieved, the sufficiency of the degree of diversity of backups needs to be assessed. Physical backup separation helps to make that at hazard only one backup stop working, and therefore, it is carried out at arrangement of cables, equipment, separation of normal and emergency surveillance departments, as well as at different levels of Defence-In-Depth levels.

Barriers are made up of technical, operational and organisational elements that are inserted into the system to individually or collectively reduce the possibility of specific errors, threats or accidents, or to limit their impacts. According to the work [72], the quality of safety barriers needs to be evaluated in the operation of the technical facility according to:

- effectiveness – how well the safety barrier meets the thoughtful function,
- resource needs - project costs, creation and maintenance of the safety barrier in operation,
- robustness – it refers to reliability and measures of how well the barrier can withstand changes in surroundings,
- implementation time duration – a measure of the time that elapses from the concept of a safety barrier to its implementation,
- availability – whether the barrier can perform its task at any time,
- evaluation - how easy it is possible to determine whether the barrier is working as expected,
- independence – the barrier's response does not depend on the human response to achieve its goal.

Barrier safety management is an important activity to maintain or reduce risks that interfere with the safety of the operation of the technical facility. Barriers form the equipment of a technical facility, they need to be functional throughout the operation and human needs to be able to control their combinations.

The degradation of barriers leads to an increase in risk for technical facility. In order to avoid the degradation of barriers, it is necessary to combine their inspections, preventive maintenance, audits, sensors, process management, analysis of faulty and near-misses, and concepts for working with large amounts of data, i.e. barrier safety control needs to be dynamic. Degradation of barriers is not a simple or constant factor. The rate of degradation of barriers is:

- short-term – procedural barriers, some active barriers (gas detection, emergency lighting), batteries, hydraulic reserves,
- medium-term - safety documentation, protective envelope and mechanisms of its corrosion, active (flares, safety belt), process control systems and loads,
- long-term – passive (firewalls); semi active – inspections, audits, sensors, conditional monitoring, analysis of incidents, accidents and near-misses, maintenance and test records, personnel training and records of its competence

Safety barriers are installed in many critical systems and infrastructures to prevent dangerous phenomena or to mitigate their consequences, such as fire prevention and rail signalling systems.

Many changes need to be made during the life of the technical facility, e.g. in the replacement of fittings, components, equipment due to repair or modernisation. In doing so, it should be remembered that managing changes in the technical facility is a critical skill that is part of safety management.

Although safety and risk are not additional quantities, the level of safety of the technical facility is determined by the work of the technical facility with risks. It is in some way relative because it depends on the acceptability of the risk. In addition, it depends on available resources, forces and means which are spent on risk management and settlement; i.e. a wealthy company can afford to ensure a higher level of safety by having the sources, forces and means to manage and settle risks and vice versa.

From the point of view of the objectives of human society, the process of ensuring the safety of a technical facility needs to respect all phenomena that may have unacceptable impacts on the human system, i.e. disasters, existing or man-made interactions, links and flows in the human system. The process of ensuring the safety of a technical facility and technology shall be based on the principles, methods and procedures of engineering that works with risks and, as the main unknown, it needs to follows the internal dependencies across the different parts of the technical facility that occur at several levels, namely physical, cyber, organisational and site-specific. In other words, they arise as a result of financial flows, energy flows, information flows and flows caused by the regulated management activity.

The knowledge and experiences of practice show that methods of selection of priorities usually very costly. In practice, it has proven a multi-criteria assessment method based on assessing the vulnerability of individual elements of the system to disasters, including the internal links, including the transversal ones at different hierarchical levels. The value ranking is a top priority for human's lives, the environment, public welfare and functionality of the technical facility, followed by the protection of monuments, recreation, entertainment, etc. When choosing in practice, it is preferred to make options that mean great vulnerability in individuals and little vulnerability in society.

In the evaluation, it is necessary to classify a rather complex system of links, in which the action of individual factors on the resulting effect cannot be quantified. The overall assessment is, therefore, relative and may be influenced by the subjective approach of individual evaluators. It is, therefore, advantageous if the evaluation is carried out by several independent experts. The results of the evaluation apply only to the evaluation system and cannot be compared with the results of the evaluation of the different systems assessed separately. Therefore, in the US and some other countries, expert methods for these complex evaluations are codified, e.g. multi-stage Delphi method [27].

2.3. Critical items of technical facilities

In the observed technical facility safety concept, safety also includes the quality of the parts for which the technical facility is established. From this point of view, critical elements or systems of technical facilities are those elements or systems that are simultaneously highly important for safety (i.e. for reliability and functionality) and highly vulnerable.

Each technical facility consists of a controlled object and a control system [25]. Both of these items need to be followed for the safe operation of the technical facility. A controlled object is mostly a complex nonlinear system that:

- consists of the final number of elements (equipment, components, lines, sub-units),
- each element is clearly described by the final number of measurable quantities,

- interconnected relationships among elements are clearly formulated.

Dynamic properties of a controlled object can be described using the differential equations, the solution of which is a state vector. The state vector allows by help of use of the minimum number of variables to determine the state of the system at any time. The control system shall maintain the specified physical quantities at predetermined values. In the control process, the control system changes the state of the technology system by acting on action quantities in order to achieve the demanded state (condition).

Since the first item (controlled object) is highly dependent on the technical design and the technology used, it is not a fundamental subject of attention for the above reasons. Attention is focused on the control system, which includes:

- technical procedures,
- human,
- knowledge and skills to create new products in a targeted way.

Its ties are of different natures:

- technical "machine-machine",
- mixed "human-machine",
- mixed "human-PC”
- mixed "machine-PC",
- and purely cyber “PC-PC”.

The flows in the system are:

- energy,
- material,
- information,
- financial
- and instructional.

It goes on the socio-cyber-technical (physical) systems of systems [18].

Control systems are governed by organizational procedures and rules that affect the technical performance and quality of human's work. The main principles that determine their quality and performance are according to work [73] the following factors:

- responsible autonomy,
- adaptability,
- integrity
- meaningfulness of tasks.

Today, the operation control of the most of technical facilities is performed by software. Due to deficiency of standards and norms for software construction with regard to the safety of both, the technical facility and the technical facility´ parts operation under normal, abnormal and critical conditions, the software levels in this domain are different. Because, the software is not clearly tested in this direction, they present the risk for technical facility [74].

Because the human behaviour is not deterministic, the main characteristics of the systems in question are the emerging characteristics, nondeterministic behaviour, and complex relationships among organizational objectives.

In the control system, according to recent concepts, which place the highest emphasis on safety, which includes reliability [30,31], they are monitored in the priority order of properties such as:

- safety (level of compliance with established operating conditions and non-creating harmful (unacceptable) impacts on and around the system itself),
- functionality (level of performance of required tasks),
- operability (level of performance of required operations in dependence on normal, abnormal and critical conditions),
- operational stability (level of compliance with specified operating conditions over time),
- inherently built-in resistance to potential disasters.

The technical facility and its safety are always decided by a human (maintenance, renovation, changes). The engineering system is characterized by structure, hardware, procedures, working conditions, information flows, organizations (problem of organizational accidents – [19]) and the interface between these components. Technical facilities are stable and mobile. Of great importance to human society are critical infrastructures that are under specific attention (Annex 1).

2.4. Overview on internal risk sources of technical facilities

Information on all sources of risks for technical facilities is in Annex 3. Table 11 summarises clearly the essential areas in which the key causes of accidents or failures of technical facilities lie. It is clear from Table 11 that the causes of accidents and failures of technical facilities are not only technical or natural disasters, but fall within many other areas, and therefore, safety-focused risk management needs to be very sophisticated and coordinated [16,18].

Table 11. Areas of sources of risk of technical facilities.

Category of disasters	**Examples of sources of risks of technical facilities**
Technical	Aging. Corrosion – internal and external. Quality of welds. Wear and tear of fittings. Specific phenomena connected with critical fittings – e.g. turbines: mechanical vibration, aging, load, etc.

Procedural	They relate to the production process – leaks, explosive or flammable material, dust, emissions, etc.
Working activity	Danger activities – work at heights, driving vehicles or excavators, underwater work, work in solitary confinement, etc.
Working environment	Floor adjustment – slipping, tripping and falling; rough surface, hot / frosty surface, cramped space, etc.
External	Natural disasters, external crashes, plane crashes, terrorist attacks
Employees´ behaviour	Non-compliance with rules.
Organizational	Poor organisation of work, heavy workload, inadequate training, poor change management.
Working environment contamination	Noise, hazardous emissions, pools, puddles, spills, etc.
Finance	Pay outs, contract payments, taxes, material availability, inventory management, etc.
Project management	Availability of human resources, project implementation, lifetime management, contract management, etc.

Failures and accidents of technical equipment with the presence of dangerous substances are usually accompanied by one or all of the following phenomena:

- fire,
- blast,
- leakage of a dangerous substance into the surroundings.

A fire is any unwanted fire in which persons or animals have been killed or injured, occurred damages to material values or the environment, and unwanted combustion in which persons, animals, material values or the environment have been imminently endangered.

An explosion is a physical phenomenon in which there is a sudden, very sharp release of energy and a sharp local increase in temperature and pressure; for persons, animals, material values and the environment, they are dangerous pressure waves, sound waves and uplift of debris (missiles).

The dispersion of hazardous substances into the surrounding area causes air contamination, which is dangerous for living beings and, under certain conditions, causes fires and explosions in reactions with the surrounding area.

For technical facilities, the specific types of fires and explosions are very dangerous [63]. It goes on:

1. Flash Fire, which is a burning cloud formed by flammable vapours or gas mixed with air – Figure 10 - 1.

2. Pool Fire, which is a vapor fire that evaporates from the liquid level – Figure 10 - 2.
3. Jet Fire, which is a fire of leaking gas or a two-phase mixture of liquid and gas from the hole – Figure 10 - 3.
4. Fireball, which is a burning cloud that rises, expands and acquires a spherical shape – Figure 10 - 4.
5. The explosion of the vapour cloud of boiling liquid that manifested by pressure wave and uplift of debris (Boiling liquid expanding vapour explosion - BLEVE) – Figure 11 - 1.
6. The explosion of the vapour cloud, which is formed by flammable vapours and aerosol and in mix with air, it produces overpressure (Vapour cloud explosion – VCE) – Figure 11 - 2.

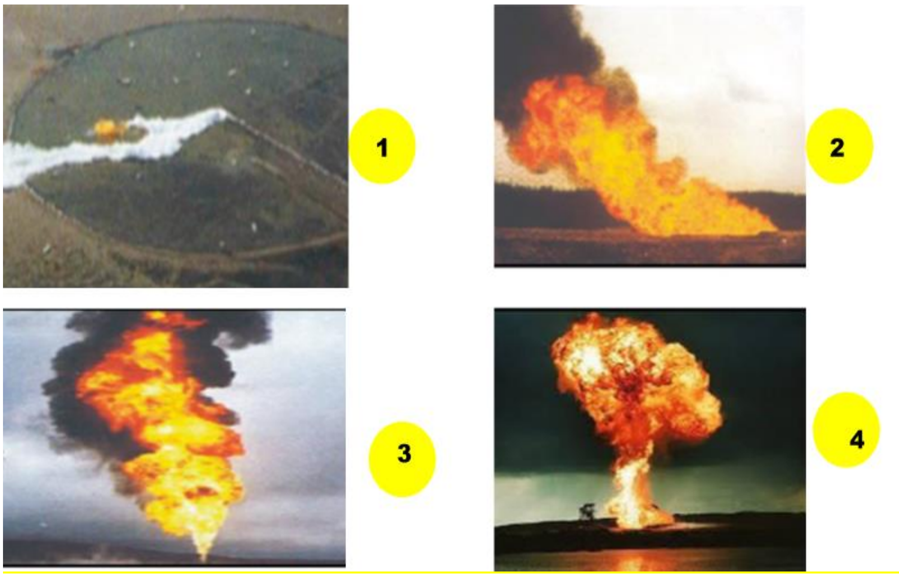

Fig. 10. Specific types of fire.

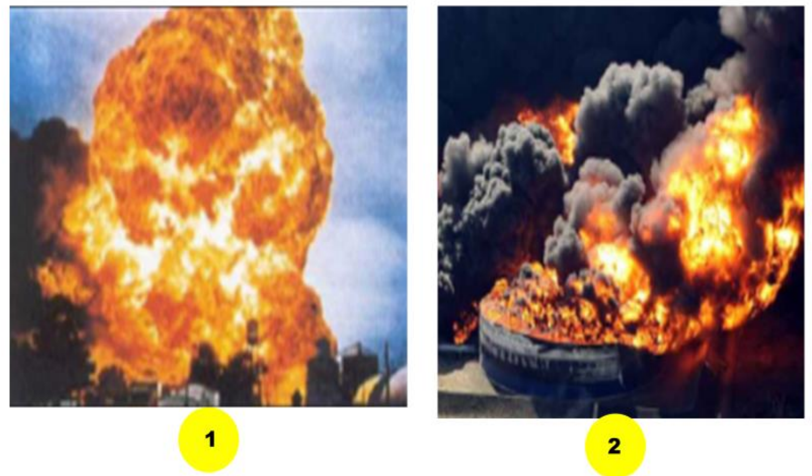

Fig. 11. Specific types of fire with explosion.

To prevent such dangerous phenomena, specific measures should be taken in the design and operation of the technical facilities against specific types of fires and explosions may arise.

2.5. Operating rules

In order to ensure the safe operation of a technical facility, certain rules need to be followed, i.e. operating regulations (operating rules) processed in accordance with valid legislation and recommendations in the project documentation [3,30,31]; the operator is responsible for them and their adherence. In a number of areas, operational regulations need to regulate safety-related requirements laid down by law (industry, transport, protection of humans and property, environmental protection, construction, public interest, financial sector, trade, etc.).

For example, in order to ensure the safety of each machinery fittings and the operator security, it is very important to identify all possible dangers arising from the design or method of presumed use of the equipment [1,75]. Therefore, we need to have a tool and procedure for identifying the hazards and identifying the risks in a timely manner to identify that something is wrong and to identify where action needs to be taken to achieve the right result. The tool in question should be used correctly so that in the case under review the test is of good quality and give the correct results.

In practice, the safety audit according to the checklist tool has proven itself, e.g. [76,77]. It is a tool specific to each installation and place of use. At its compilation, they need to use both, the theoretical knowledge and technical documentation and the working procedures specified in the project documentation [19,76,77]. The second cited example is referred to welding. Welding is one of critical process that is used to create a permanent, inseparable connection of two or more components. The general requirement for the welding process is the creation of thermodynamic conditions under which the formation of new interatomic bonds [78] is possible.

Welds change during time and working regime and conditions, and therefore, ASME has a comprehensive set of standards that regulate the welding process for different weld types and that monitor their conditions [79]. For risk management of more complex technical parts, the other methods are necessary to use [1,21].

The operating regulations are part of the operational documentation of the technical facility [3]. They respect the designer´s and manufacturer's recommendations and the relevant legislative requirements, i.e. they consider the public interest, the protection of public assets, and the protection of the assets of a technical facility which are important for the safety of the technical facility, i.e. for the reliable performance of the tasks for which the technical facility is created. They adjust:

1. Rules for ensuring: the safe operation of technical equipment from the point of view of technology, i.e. technological procedures for the use of a particular device, namely under normal, abnormal and critical conditions; and safe products.
2. Rules for ensuring: the safe workplace, namely under normal, abnormal and critical conditions; and good performance.
3. Rules for the security of humans in the workplace, under normal, abnormal and critical conditions.

In the first case, the operating rules determine:

- the method of handling the equipment,
- the working regime,

in order to ensure the safety of the production process and the general safety of the final product (i.e. how to treat the equipment and how to use it properly). This is based on the design, materials, layout, purpose of technical equipment and the situations that occur. They also determine the conditions and field of use, operating conditions, maintenance and inspection of the relevant equipment, which the operator needs to observe. For some devices, there are standards containing device-specific instructions. Special regulations are for:

- plants processing the dangerous substances [3,35,36,80],
- pressure equipment and their fittings, especially those which are classified as critical (especially important) technical equipment according to special law,
- lifting equipment,
- electrical equipment,
- air-conditioning,
- etc.

In the second case, the regulations lay down requirements for ensuring:

- safe working environment (i.e. fire safety, methods of protection for torque machines, proper handling with hazardous substances, methods of working in a contaminated environment, distribution of materials, production tools, products, waste management),
- economy (saving the material, energy savings, refrigerant savings, etc.) competitiveness of production.

For a number of specific plants, there are laws and standards containing the requirements and guidelines for specific cases.

In the third case, the regulations lay down safety requirements for:

- equipment operators,
- other workers when forced to move around the equipment,
- visits,
- contractor's staff.

It is an adjustment of the requirements of the Labour Code and related legal and statutory regulations.

Requirements for operating regulations need:

- to be based on an assessment of the serious risks in the area,
- to contain exhaustively the conditions to which they apply and, where applicable, instructions on what to do if the limit conditions are exceeded,
- to address, in particular, issues related to potential hazards or expected conflicts,

- to be regularly reviewed (due to the dynamic development of the world) and screened after any serious near-miss or incident, or in the law change, which contains the requirements for the operation of the equipment.

All levels of management of the technical facility are responsible for the existence and regularity of the operating regulations. The technical correctness shall be the responsibility of the operation manager, who is responsible for the technical correctness.

For complex technical facilities, it is about creating the operational regulations at the different levels of management that are interconnected, both at the level of responsibilities and the level of activities, considering the competences set.

2.6. Tests aimed at assessing the risk of technical equipment during operation

Knowledge of physics and technology shows that the condition of materials of technical equipment, components and whole technical facilities is influenced by the conditions in which they are operated and also by the time resulting from their construction. The issue of ageing management of materials, from which technical equipment, technical components and entire technical facilities are made, therefore, belongs to the basic technological fields [81,82]; and therefore, we focus on it at work and monitor the sources of risks that predetermine the behaviour of the materials of the technical equipment.

Therefore, in order to ensure the safety of technical equipment, components and entire technical facilities, it is necessary to monitor the risks associated with degradation processes and to maintain an acceptable level of safety, i.e. the item safety needs to be managed by means of optimal maintenance, optimum operation mode or timely replacement of worn parts [17,18,23,24].

It means that the items should be monitored and controlled in such a way that the monitored equipment works safely throughout its useful life, i.e. so it reliably performed functions in the required quality, in the required quantity and at the required time, and under its critical conditions it did not endanger either itself or its surroundings [17,18,23,24].

The material of each technical equipment changes over time, in structure, physical characteristics and appearance; it goes to material ageing. E.g. the work [83] states that material degradation due to ageing is faster when the technical equipment is made of non-homogeneous material, is located in an aggressive chemical environment, is under mechanical pressure and often changes in operating conditions. Material fatigue, corrosion, liquefaction and creep are originated. As a result of these phenomena, there are:

- a reduction in the safety and integrity of the technical equipment and, in the case of critical technical equipment, also the entire technical facility,
- reducing the reliability and availability of technical equipment,
- forced downtime of technical equipment,
- increased demands on costs on maintenance,

- and pertinently also to fear and reduction of the acceptability of the technical facility in the public.

The management of the aging of critical technical equipment consists in the fact that the condition of the material of critical technical equipment is monitored, carefully maintained and in case of limit degradation, it is carried out timely replacement. This is the only way to ensure the long-term safe operation of the technical facility. They are used the non-destructive tests methods [30,31,35,84,85].

Diagnostic methods [82,85-91] allow to know the current state (condition) of the technical fittings and, on this basis, to determine their possible behaviour in the next time. In operation, non-destructive methods are the main price. They are used in the framework of permanent monitoring, in interval measurements and fitfully in the event of problems. The aim of non-destructive methods according to the data in the works [82,85-91] is to:

- determine the integrity of the technical equipment, which guarantees its reliability,
- prevent the failure of technical equipment due to failures, thereby preventing the injuries and accidents, ensuring the protection of investments and their return,
- ensure the user satisfaction of the facilities and services provided by those devices,
- promote the goodwill of the operator,
- improve the design of technical equipment,
- improve the operation processes management,
- reduce operational costs.

Six main categories of non-destructive methods are distinguished: visual; radiation; magnetic-electric; mechanical vibrations; thermal; and chemical/electrochemical. According to the data in the works [82,87-91] and the experience of the authors, each method is characterized by the following five factors:

Subject of monitoring during the test (pressure, temperature, flow, performance, behaviour of X-rays, behaviour of ultrasonic waves, behaviour of thermal radiation, behaviour of magnetic field intensity, etc.).

1. Monitored physical parameter (deformation, stress, hardness, attenuation of X-rays, attenuation of ultrasonic waves, reflection of ultrasound, magnetic field intensity, concentration of disturbances, etc.).
2. Equipment used to detect or scan the resulting signals (photo emulsion, piezoelectric crystal, induction coil, etc.).
3. Quantity used to indication or recording the signals (deviation, oscillograph track, magnetogram, thermogram, radiogram, configuration in area or space, etc.).
4. Basis for interpreting the results (direct or indirect indication of qualitative or quantitative change).

The aim of each method is to find out data on one material parameter or several material parameters:

1. Existence of discontinuities in the material and their division (cracks, cavities, varicosity, cleavage, layer division, etc.).

2. The nature of the material structure (crystalline, amorphous, grain size, internal defects, segregation, disorders, etc.).
3. Size and characteristics of material failures (surface, penetrating inside, width, thickness, diameter, joints, cracking, etc.).
4. Physical and mechanical properties of discontinuities (reflectivity, conductivity, modulus of elasticity, speed of sound, etc.).
5. Composition and chemical analysis of the material (identification of alloys, impurities, admixture, distribution of impurities, etc.).
6. Tension and dynamic material response (residual tension, crack build-up, wear, vibration, etc.).
7. Occurrence of thermal, magnetic, electrical and other anomalies in the material.

From the followed sources knowledge and experience of the authors it follows that no method reveals all the defects in the material. In order to assess the risk associated with the in-service register of technical equipment, one correctly selected method is sometimes sufficient and at other times several methods need to be used.

As a rule, by non-destructive test methods, we monitor one asset, namely technical equipment, and measure the size of the risk by its impact on selected material parameters (accumulation and number of cracks, magnetic intensity), the condition of the material of the technical equipment and its contribution to the failure of the equipment.

Each used technical equipment has a certain task, which it should perform safely, i.e. reliably and simultaneously not to threaten itself and its surroundings [15-18,23,24]. It is a fact that every problem in the material from which it is composed affects the performance of this task. Experience shows that this happens only from a certain size of problems. If we use a scale of 0 to 5 to classify the risk size, which is consistent with world practice [17], the description of the development of defects can be described as follows:

0 – there are no indications of defects,

1 – insignificant technological defects (pitting, inhomogeneity),

2 – signs of material infringement (small fissures, decrepitating),

3 – clear material violations (cracks),

4 – serious material breaches (many cracks – proximity to the safety limit),

5 – critical violations indicating failure of the technical equipment.

If size and number of defects exceed safety limits, the risk is realized. The result is a failure of the technical equipment, which for critical devices such as the pressure vessels, pipelines with compressed hazardous substances, etc. means serious accident.

At works [1,92], they are shown the impacts of realized risk associated with the wear of the technical equipment, identified by non-destructive methods, namely by measuring the acoustic emission and measuring the magnetic memory of the material. Examples clearly show the places on the technical equipment in which the material defects occur and allow to determine their extent. This allows for a correct decision on the risk associated with the condition of the technical equipment material, which makes it possible to correctly select follow-up measures to increase or at least maintain the existing level of safety.

Although diagnostic activity does not bring immediate profit to the owners of production facilities in the economic concept, it is important because it enables early interventions to prevent the failure of important technical equipment that can cause major accidents, and thus loss of human lives, damage to property and the environment, loss of competitiveness and reputation of the operator, and in many cases to damage the whole region by missing products, increase of unemployment, which lead to other unfavourable phenomena (criminality, civil disorders etc.).

2.7. Inspections related to technical facilities

The inspection shall refer to human activities consisting of official supervision, expert supervision, substantive control, detailed inspection and the like. In technical facilities according the legislation and nature, it carries out supervision: Environmental Inspection; School Inspection; Traffic Inspectorate; Railway inspection; Institute of Technical Inspection; Fire Inspection; Energy Inspection; State Labour Inspection Office; State Agricultural and Food Inspection; Technical inspection; State Nuclear Safety Authority; Inspection of the Ministry of Health; State Drug Control Authority; etc.

In general, inspection is a specific check carried out by a state / public administration / enterprise or other organisation that supervises and oversees products, technical facility operation or technical facility safety. Its aim is to know the true state and to determine the level of compliance with the established regulations and rules. It is based on an overall investigation of the situation, its comparison with legislation, norms and standards, and, when unauthorised deviations are detected, it imposes corrective measures and controls their implementation [1].

As mentioned above, each technical device is made of a specific material and operates under specific conditions, which determines the limits in which the device is safe. The more aggressive the external conditions, the shorter the life of the device; they occur phenomena such as material fatigue, corrosion, liquefaction and creep. Therefore, it is necessary to monitor the condition of the device, mainly critical ones. The aspect in question is monitored by technical inspections. E.g.: pressure vessels belong to critical equipment of technical facilities, and their critical attributes are the conditions and limits for mechanical integrity, and therefore, the EPRI has a plan for inspection of pressure vessels for different external conditions [78].

The technical inspection shall base the results of the non-destructive tests, which were described in the preceding paragraph. Inspections shall be carried out regularly, irregularly as necessary (e.g. after an accident, in the accumulation of near-misses, before an important task), or according to the results of condition monitoring [1,93] . Their preformation will determine the criticality of the device. In the event that the criticality exceeds the allowable rate, either targeted better maintenance shall be introduced or an early repair or replacement will be carried out to prevent one of the common causes of the accident [17,18].

Since the monitoring and, in particular, the tests themselves mean a break in production, i.e. the economic losses of technical facility, it is necessary to use optimal approaches that mean to pay the most attention to items that are highly important and at the same time highly vulnerable [1,17,18].

Risk Based Inspection (RBI) is of great importance in terms of safety of technical facilities [1]. The inspection in question shall focus on specific technical equipment, such as pressure vessels, heat exchangers and pipes in industrial installations, and shall assess the risk level of the technical equipment being monitored by methods qualitatively or quantitatively. This enables economic maintenance optimisation, which is achieved by assessing the level of default risk and, if its level is close to an unacceptable risk limit, repairs and maintenance are carried out. It is based on the results of the non-destructive tests.

International technical standards and recommended procedures introduce requirements, methodologies and implementation of the RBI. In practice, they are used for example the following standards:

- API 571: Damage Mechanisms Affecting Fixed Equipment in the Refining Industry,
- API 580: Risk-Based Inspection - Recommended Practice (Third edition, February 2016),
- API 581: Risk Based Inspection Methodology - Recommended Practice (Third edition, April 2016),
- ASME PCC-3: Inspection Planning Using Risk-Based Methods,
- DNV-RP G101: Risk Based Inspection of Offshore Topsides Static Mechanical Equipment,
- EEMUA 159: Chapter 17 - RBI Methodology for Aboveground Storage Tanks,
- EPRI TR-112657: Revised Risk-Informed Inservice Inspection Evaluation,
- NCHRP Report 782: Proposed Guideline for Reliability-Based Bridge Inspection Practices.

2.8. Maintenance of technical facility and its equipment

The findings gathered in the professional literature and experience in practice summarized in [1,3] show that neglected or improperly performed maintenance leads to the growth of the vulnerability of the monitored item, and in practice there is a more frequent failure of the item. On each item, human decides, and therefore, the knowledge in question needs to be considered. It is understandable that, in view of the resources available, maintenance needs to be financially optimal. Therefore, according to [1,7,17,18], it is necessary to create a representative set of possible maintenance scenarios, to identify and evaluate the impacts of their risks with regard to the quality of operation, and then to select that with the highest quality, i.e. to determine transparent, repeatable and correct method of optimal maintenance scenario from the point of view of technical and financial.

Cost-effective maintenance of a company or company's assets is absolutely essential for the maximum profitability and long-term survival of the company, business, infrastructure or technical facility. Documentation and inspections, including regular audits, in particular external ones, are necessary to assess the level of maintenance [1]. According to US models, the safety of business or device features ensures availability (accessibility) and requires the application of an integral safety concept that includes reliability and sustainability. According to the work [1] in cases where there is little operator's ability to reduce or mitigate the risk, more frequent sophisticated maintenance activities and more frequent sophisticated inspections should be ensured.

Maintenance should be thoroughly planned and prepared according to [1,3]:

- instructions for operation and maintenance from the manufacturer,
- design and construction documents,
- workflow, the means used for work, data on the hazardous substances present,
- operational experience,
- experience of operators and maintenance personnel,
- operating conditions and local conditions,
- operational alarm plans,
- knowledge of the site control in a given place,
- the deployment of protective equipment (e.g. fire alarm sensors),
- potential sources of threat to the site and its surroundings, including the surrounding equipment.

Maintenance depends on the operation of the system. We usually divide it into a reactive or unplanned and proactive or planned one. In the first case, it is a correction of the device, component or system carried out after their failure. In the latter case, we distinguish preventive and prognostic (smart) maintenance. Preventive maintenance includes replacement of parts or maintenance based on aging. For critical items, prognostic maintenance should be used, which is based on the results of continuous monitoring [1].

According to the work [94], the optimal total cost involving maintenance is characterised by the situation shown in Figure 12.

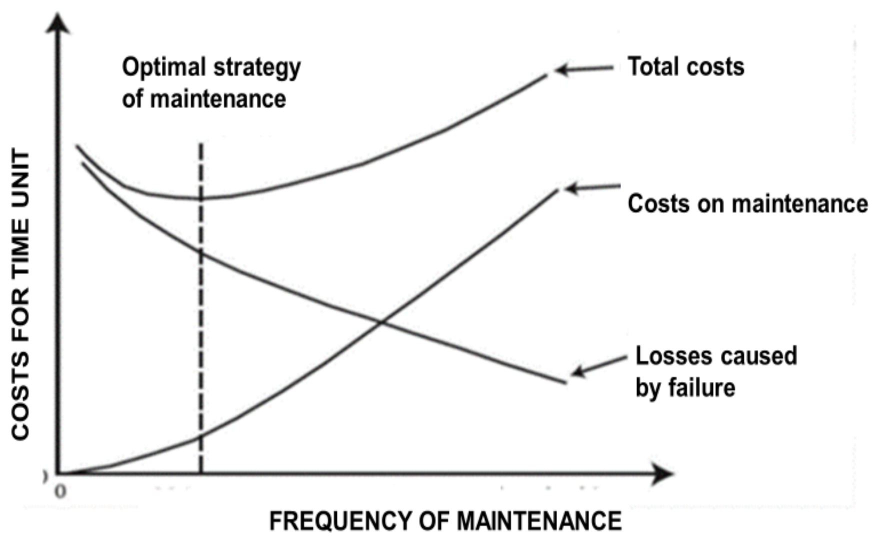

Figure 12. Total costs on maintenance costs and on time delays; processed in [94].

2.9. Measures for promoting the technical facilities safety

To promote the technical facility safety, it is necessary on present knowledge and experiences summarized above and in [1] to:

- consider manifestation of human factor and to build safety culture,
- take care on workers' health and safety,
- have tools for safety improvement.

2.9.1. Management of human factor

Human reliability is a critical parameter for the security and safety in the industry, because the 70-90% of the failures is related to the human factor [17,45,46]. Although automation would eliminate the human factor, because it eliminates the presence of human in process, so this is not so, because on the other side the automation increases the complexity and this is also the source of the errors.

The human responses to the external (and internal) inputs are very diverse. They may take the form of unconditioned responses, such as "automatic", the innate (inherent) ways of responding to inputs (flinch when unpleasant initiative), conditional responses (e.g. in the form of habits), or purposeful, by the will directed negotiations. In the psychological literature, with the issue of decision making we encounter most frequently in connection with the wills and volitional processes, thinking, purposeful behaviour, often in connection with the fight of rational motives (in the solution of internal conflicts). In the process of purposeful management of human action, it is applied decision making not only in the choice between the different motives and objectives, but also in the choice between alternatives to act - not to act. The individual also decides when selecting the resources and processes to achieve the goal, in a situation requiring the suspension or cessation of activities. The capability to make decisions properly, judiciously and in a timely manner is one of the basic assumptions of the practical activities and creative thinking, and it is also an important component of the human personality.

The human factor is positive, when the decision of human leads to profit and to strengthen the assets, which ensures greater security, profit and development. It is negative, when human will weaken or damaged. In the present case we are talking about human failures, which occur, either due to errors in the implementation of certain activities, or as a result of errors in management. The source of the error in the first case, it is routines, non-compliance with operating and safety regulations, omission, poor health or stress. The source of the errors in the second case it is ignorance, disregard for the laws of natural, technical, economic and social, and dab handing (the most common error of managers in the evaluation of technical, natural and economic grounds) [1,30,31].

According to the data in the work [41,46] the failures of human in the organization can be prevented, when:

- by management of technical issues, they are only authorized the experts with the capability to lead the work teams who go for example, can explain, support, prevent bullying, etc.),
- it is provided the application by qualified management processes that create projects and programs that result in products,

- they are systematically created conditions for skilled jobs,
- it is ensured adequate training the workers and the system of providing the assistance in the solution of complex tasks,
- it is implemented the motivation and stimulation of employees for compliance with operating and safety regulations,
- it is carried out in-depth inspection of processes and their interconnections to projects and programmes.

In today's technology practice, it is used the term of "organizational accident". It was defined at the implementation of the Seveso I directive into practice [80], when it was based on an analysis of the major accidents which have been reported since the introduction of the directive, identified areas for new provisions in the new directive. One of the areas of causes of accidents they have been proven the approaches to management (management concept) and management systems in the facilities understand as system. From the analysis of the collected data it followed that the ***failure of the management system has contributed to the causes of more than 85% of the reported accidents*** [36].

Risk reduction in the context of safety management covers several topics:

- safety of processes,
- the protection of workers' health and safety (safety of work),
- and reducing the impacts on the environment.

Therefore, in practice, it was introduced that the analysis of the impacts of management on the safety of the facility shall be carried out according to the Reason model of organizational accident [40]. The causes of organizational accidents are in three basic aspects:

- organizational processes,
- the conditions which cause the origin of errors or infringements of rules,
- neglection of solution of problems, which permit errors at adherence of requirements of regulations.

Organizational processes include four processes [41] that are part of any technical or technological organization:

- design and construction, building, operation and maintenance. The given processes are built in three interconnected activities:
- establishment of objectives within the framework of the economic and social situation of the facility,
- organization of the facility for reaching the long-term strategic goals,
- and management of operational activities.

As it was mentioned in paragraph 1.2.3., the conditions, which lead to the origin of errors [41] are:

- no familiarisation with the task,
- a lack of time,
- a bad signal to noise ratio,
- misunderstanding between the designer and the user,

- irreversibility of errors,
- information overload,
- negative transfer between tasks (bad transfer of tasks),
- bad perception (underestimation) of risks,
- poor feedback from the system,
- inexperience,
- bad instructions and procedures,
- lack of control,
- inappropriate education of the person with the given task,
- hostile environment,
- and the monotony and boredom.

As it was mentioned in paragraph 1.2.3., the conditions, which make violations of regulations and rules [41] are:

- the lack of a safety culture in organization,
- discrepancies between top managers and employees,
- the bad morale,
- bad oversight and control,
- norms permitting the infringement of standards,¨
- the bad perception of risk sources,
- notably lack of care and interest of managers,
- a little pride in own work,
- dab handing access to work that encourages the risk-taking,
- the belief that nothing can happen,
- low self-esteem,
- recognised impotence,
- noticeable permits for breaches of the rules,
- ambiguous or apparently meaningless rules,
- and the age and sex: young men are committing violations of the rules.

As it was mentioned in paragraph 1.2.3., no solved problems that allow errors and violations of the laws / rules [41] are:

1. Errors are happening as a result of problems in the information processes and they are understood in relation to the cognitive functions of the individual. They can by reduced by training, improving the workplaces, determination of interface, better information process, etc.
2. Violations of laws / rules are based on motivation. They are a social phenomenon, and they can understand only in the context of the given organization. Violation can be only removed by changing the attitudes, beliefs, norms, morals and safety culture.

More details can be found in [36,41] and in the works that are cited in them.

On the basis of investigations of major accidents [1,3,17,18], it can be stated that many of primary (causal) and secondary causes of accidents are repeated though there is quite a lot of the knowledge needed to prevent not only near misses, but also major accidents or to mitigating their impacts, and by this reducing the losses and damages associated with them. The cause of the given situation, in addition to the human factor, there are the shortcomings in both, the implementation of the effective safety management system and the ignorance of the conclusions from the already investigated incidents and accidents.

The reality is that, even in organizations in which the accidents occurred, there are with the passage of time and changes in the staff, the original measures taken after the disaster forgotten or are not transferred to all workers in a given organization. Therefore, it is necessary to introduce the following measures to improve the common memory of the organisation:

1. Attaching the note to each order, regulation or standard, why it is just such.
2. Description of the old and the recent accident in the facility printing with the lessons resulting from them, and discussion lessons on the training of safety for all components of the business.
3. Regular checking of the compliance of the measures.
4. Removal of existing equipment only after the knowledge of why it was being installed. The deletion of the original procedure after finding out why it was accepted. It is necessary, in order to eliminate something, what is to prevent an accident or to mitigate its impacts has.
5. The introduction of a better information system to find details about the accidents and issued recommendations after the accident.

Based on the concept that safety is a matter for all stakeholders in the framework of research under the auspices of the OECD [35] there were compiled ***the so-called golden rules of all concerned***, which was supplemented by knowledge from safety management that promotes the IAEA and according to the knowledge and experience of the author. As it was shown in paragraph 1.2.3., the basic rules are:

- according to their possibilities to aver by preventive measures to disasters or at least their unacceptable impacts, to ensure preparedness to deal with unacceptable impacts on the protected assets and the effective response,
- to communicate and collaborate with others interested in all aspects of prevention, preparedness and response,
- to know the hazards associated with possible disasters and possible risks in the territory as well as in complex technological facility,
- to establish a "safety culture", which is respected and enforced by all stakeholders in all circumstances,
- to establish safety management systems, to monitor and, if necessary, to correct their activities,
- to use the principles of inherent safety in the design, planning and operation of the complex critical facilities and their equipment,
- carefully to manage changes,

- to be prepared for all possible disasters that may occur in a territory or complex facility,
- to help others interested in carrying out their roles and responsibilities,
- to search constantly the improvement of safety,
- to work in conformity with the safety culture, safe practices, and training,
- to strive constantly for all awareness, provide information, and the management staff featuring the feedback,
- to strive for the development, strengthening and constant improvement of the concept of safety, regulations and directives,
- to lead and motivate all other stakeholders in order to fulfil their roles and responsibilities,
- to know the risks within own sphere of responsibility, respectively, to plan measures for its proper management,
- to use the appropriate and coherent policy of security planning and follow-up activities,
- to be aware of the risks in the surrounding area and to know what to do in case of their realization,
- to participate in emergency planning and response.

Golden rules are commonly used in procedural control [35,41]. In many cases, the roles of individuals who are involved are specified as follows:

1. Top (senior) management and management teams operating the technology and infrastructure need to be familiar with:
   - knowledge of the hazards from disasters and possible risks in the territory as well as in facility,
   - introducing and promoting the targeted safety culture, which is respected and enforced by all stakeholders in all circumstances,
   - establishing the safety management systems, their monitoring and if necessary. corrections of their activities,
   - use of the principles of inherent safety at design, building, construction and operation of the facilities and their equipment,
   - careful managing the hangs,
   - preparing for any disaster that may occur,
   - helping others interested in carrying out their roles and responsibilities,
   - carrying out the continuous improvement of safety.
2. The workers in the complex technological facility needs to:
   - work in conformity with the safety culture, safe practices, and training,
   - strive constantly for all awareness and provide information and to provide feedback to managers.
3. Public administration needs to:
   - strive for the development, strengthening and constant improvement of the concept of safety, regulations and directives,

- lead and motivate all other stakeholders in order to fulfil their roles and responsibilities,
- know the risks within their own sphere of responsibility, respectively, to plan measures for their good management,
- motivate facilities to negotiate with the risks responsibly,
- help with the effective communication and cooperation among all stakeholders,
- to promote cooperation between the administrative authorities,
- use of appropriate and coherent policy of planning and follow-up activities,
- mitigate risks through appropriate measures of the response that falls within its scope.

4. The public (other participants) needs to:
   - be aware of the risks in the community and know what to do in case of their realization,
   - cooperate in deciding on the location, construction and operation of the technological facilities,
   - participate in emergency planning and response.

The safety culture means that the humans in all their roles (executive, employee, citizen or victim of the disaster) observes the principles of safety, i.e. it behaves so that he / she alone prevented the realization of the potential risks and when it becomes a participant in the realization of the risks, to contribute to an effective response, stabilization of the protected assets and their recovery and to kick off their further development. According to some authors it is a set of attitudes, beliefs, norms and values that exist in the facility, which reflect how the facility is managed, i.e. they are general principles of the distribution of powers and responsibilities, policies, procedures and a certain ratio among the emphasis on work results, authority, care about the people, respect for the principles of safety and to ensure the functionality of the facility.

An effective safety culture is an essential element for safety management. It reflects the concept of safety and it is based on the values, opinions and discussions of key management personnel and their communication with all stakeholders. It is a clear commitment to actively participate in addressing issues of safety and advocates that all participants did so safely and to comply with the relevant legislation, standards and norms. Rules of safety culture needs to be incorporated into all activities in the territory, or another facility. Their basis is not the concentration on the punishment of the guilty party / agent of the bugs, but the lessons learned from the mistakes and the introduction of such remedial measures, in order to not repeat mistakes or at least it significantly reduced the frequency of their occurrence.

In the context with the safety culture there are often in the current literature related to technologies used the terms as loss prevention and process safety. Their definitions are also given, because they are the tools that are used in correlation with the technological facilities to protect people and assets.

Loss Prevention is a systematic approach to prevention of accidents or to minimizing their impacts. It includes resources for the elimination of sources of risks or the reduction of their occurrence probability and for mitigating the impacts associated with this realization (preventive and follow-up measures). It also includes the identification of the appropriate control measures, the identification and application of appropriate remedial measures, by which it is ensured a safe facility having an appropriate level of security and sustainable development and to present an unacceptable danger to their surroundings [16].

Process safety or better safety of processes is the part of the safety focused on safety in the industry (complex technical facility), in which there are series of production and additional processes that are necessary for creation of the final product of the facility. It is about prevention of accidents, which have special and distinctive features for the specific industry (complex technical facility). It deals with e.g. the prevention of immediate releases of chemical substances, or energy in the harmful quantities and, in the event that these leaks occur, thus limiting their size, impacts and consequences. It does not include questions of classical safety and health protection at work, i.e. it deals with purely technical problems, which differ from the previously-defined system safety.

Analysis of the current situation shows that we can systematically handle with a number of adverse processes, i.e. disorders and failures that we can detect in advance. Sometimes, however, there is a mutual interlocking a series of seemingly unrelated factors, and as a result of non-linearity in the system there are originated very atypical accidents. Now, we recognize that complex technical facilities are for different reasons from time to time in an unstable state and formed organizational disasters cascade failures without apparent cause, i.e. we recognize the uncertainty and random epistemic (knowledge) in their behaviour; we denote them as critical facilities. In order to ensure the safety of critical facilities and privacy of people we are looking for a solution of the response for possible cases that you cannot reveal by the probabilistic approaches and we build for them, alternative sources of water and energy, specific response systems and specific training of first responders.

To achieve the required level of safety it means well to manage and properly to decide. Good management and good decision making are possible only when we have good data, and we can take advantage of the instruments that we have available. The data need to be correct [65], i.e.:

- their size and accuracy are known,
- they have explanatory power for the problem, i.e. they are validated.

The data files need to be representative [65], i.e.:

- be complete,
- contain the correct data,
- have a sufficient number of particulars,
- the particulars need to be spread homogeneously throughout the reference interval and they need to be validated.

In the application of models, they need to be properly considered random uncertainty and epistemic uncertainty in the data. It should be noted that in the real world, in ensuring the safety of complex technical facilities we work with non-trivial problems, i.e.:

- it is more protected assets, the objectives of which are conflicting,
- assets vary in time and space,
- and the space in which the assets are, i.e. the facility and its surroundings are in dynamic development, the manifestation of which is often different in mentioned entities.

In conclusion, it is therefore possible to conclude that for ensuring the safe technical facility it needs:

- to aware the technical facility aspects, which are essential for its safety,
- to understand the causes of failures of safety of technical facility and the context of their actions,
- to focus on the similarities and differences among disasters (i.e. phenomena that undermine the safety of technical system) themselves,
- to understand the role of the territory in connection with the safety of technical facilities, i.e. particular characteristics of the territory, which escalate or suppress the impacts of the disasters always or only under certain circumstances,
- to use conscious methodologies for assessment of disasters, their impacts and for identification of corrective measures,
- to set goals, timetables, monitoring, organizational structures, norms, standards and legislation for the conscious management of safety of facility,
- to delete the multiplicities in the preparation of measures to cope with the impacts of disasters,
- to prepare the response to the disaster in and at restoring do not apply measures, which increase the risks associated with other potential disasters.

2.9.2. Occupation safety and health

On the basis of systematic and long-term studies [42,43], there are three priority guidelines, the factors of which need to be monitored in the protection of technical facilities´ staff:

1. In order for the workplace to be a safe place for employees, it is necessary to monitor:
    - emergency preparedness of all persons,
    - the quality of the equipment that are present on workplace,
    - presence of dangerous substances,
    - noise level,
    - quality of electrical equipment,
    - reality, whether a basic risk assessment is carried out,
    - reality, whether inspections and monitoring of the site are carried out with regard to the risks,
    - reality, whether people's safety and security are monitored,
    - the quality of waste management,
    - quality of machines,
    - cleaning quality,
    - the quality of the change management,
    - quality of preventive maintenance and repairs,
    - quality and location of entrances and exits,
    - quality of ergonomic evaluations,

- radiation level,
- presence and level of biological threats,
- quality of taking and removing material, goods, etc.
- quality of things for the human´ life comfort and for the environment.

2. In order for humans to be safe at the workplace, it is necessary to monitor:
   - the level of their training,
   - the quality of the job description and the structure of tasks,
   - the ability to provide first aid,
   - the existence and quality of personal protective equipment,
   - conflict resolution and decision-making methods,
   - the quality and level of estimation of a person's performance,
   - the existence and quality of the worker's recovery in and after strenuous work,
   - the quality of assistance programmes for employees (or in the territory for citizens by public administration),
   - quality of work organisation and ways of dealing with physical and mental fatigue,
   - quality and level of equal opportunities – whether or not there are anti-discrimination measures,
   - level and quality of accommodation,
   - the level and quality of health surveillance,
   - the level and quality of health procedures,
   - the level and quality of supervision under visitors and contractors (in the territory above non-demanded elements),
   - the level and quality of the selection criteria for the management and the specific operation,
   - the level and quality of monitoring the stress susceptibility,
   - the level and quality of the revision of the fluctuation of persons,
   - the level and quality of response programmes and their feedbacks,
   - the level and quality of building a social network,
   - level and quality of behaviour modification.

3. In order for the workplace to be a safe system, it is necessary to monitor:
   - the level and quality of accident management (generally emergency situations of all kinds) by managers,
   - the level and quality of the cooperation of managers with occupational safety authorities in considering health aspects,
   - the level and quality of the work safety authorities' policies and procedures,

- the level of possibilities of consultations and procedures for safe work,
- the level and quality of the competence of the management,
- the level and quality of the task setting,
- the level and quality of customer service, the level and quality of management to contractors,
- the level and quality of resource allocation,
- the level and quality of responsibility,
- the level and quality of care for records and archiving,
- the level and quality of legislative modernisation,
- the level and quality of communication,
- the level and quality of compliance with the criteria of the occupational safety authorities,
- the level and quality of the revision of the workflows, including the analysis of gaps, deficiencies and revision of the system,
- the level and quality of audits,
- the level and quality of self-assessment,
- the level and quality of modernisation of procedures.

On the basis of the same sources, high risk-related items have been identified:

1. High risk to a safe place is connected with:
   - presence of dangerous substances,
   - non-existent or poor-quality emergency preparedness,
   - presence of electrical equipment,
   - presence of means of production,
   - presence of taking or removing material, goods, etc.,
   - the presence of entrances and exits,
   - failure to carry out or miscarry out ergonomic evaluations,
   - failure to carry out or miscarry a basic risk assessment (often infringing).
2. A high risk for a safe person is posed by:
   - non-existent or poor health surveillance,
   - non-monitoring of susceptibility to stress,
   - non-existent or poor supervision of visitors and contractors,
   - unused or poorly used personal protective equipment,
   - poor organisation of work and disregard for fatigue (often violated).
3. A high risk to a safe system is posed by:
   - poor accident management,

- the impossibility of consultations,
- mismanagement of contractors,
- poor allocation of resources,
- failure to carry out or miscarry the revision of workflows, analysis of gaps and gaps,
- wrong quality of responsibility ensuring.

The employer is responsible for the safety of the employee according to the Labour Code and other legislation in force in real country. The employer is obliged to:

- equip machines with protective and other equipment that protects the life and health of employees,
- operate the machines according to the instructions for use or local operating safety regulations,
- for older machines, evaluate the risks and take the necessary measures to eliminate or minimise them (identify all dangers, evaluate risks, take measures to minimise identified risks, carry out ongoing technical checks and periodic revisions, eliminate identified deficiencies - repeat and adequately document).

The protection of persons in technical facilities (employees, contractors, visitors) is regulated by Labour Code and related regulations. The OSH is part of integral safety. The OSH main objective is to reduce the risks to the lives and health of workers at work. The employer's obligations and responsibilities to ensure safety and health at work are enshrined in the Labour Code and in the laws governing other occupational safety and health requirements in industrial relations and on ensuring OSH in the activity or provision of services outside of employment law relationships. The provisions of the Labour Code are followed by implementing and other related regulations.

2.9.3. Tools for safety improvements

For technical facility safety ensuring, they are used many plans for promotion of technical facility safety [15,17,24]. On the top is the strategic development plan aimed at ensuring long-term safety means the plan for continuous ensuring the technical facility safety and development. It leans on land-use plan, space-use plan [30,31,35] and plan for permanent building the safety (safety plan) [17,35]. For important activities connected with response to dangerous phenomena of different nature, they are used special plans which are interconnected and respect the long-term strategy. It goes on:

- emergency plans, i.e. response plans to a set of disasters that belong to categories 3-4 that are foreseeable. It is in-site (for accidents inside the technical facility) and off-site (for accident in technical facility or its failure, the impacts of which exceed the technical facility territory) [15,24,25]. The off-site plans are compiled by regional offices and the technical facility has duty to give all necessary data to the office,
- contingency plan, i.e. response plan to unforeseeable situation [15,24,25],
- continuity plan, i.e. a plan of such a form of response which ensures the limited operation of the technical facility and its survival in such a condition (state) that it can be gradually restored [15,24,25],

- and crisis, i.e. response plans to handle critical situations, i.e. response plans to a set of disasters that belong to category 5. In this case it goes mostly on protection of public assets in territory in technical facility surroundings [15,24,25]. Especially, critical facilities connected with critical infrastructure have duty to help the State to cope with critical situation by ensuring the special tasks and services [15,24,25].

Recent knowledge and experience in practice show the importance of risk management plan, which will be created for technical facilities operation in Chapter 6.

2.9.3.1. Safety plan

The coexistence of technical facility with its surrounding during operation is ensured by the continuous management of integral safety of technical facility. The scheme for such procedure is shown in Annex 2. In practice, this concept is realized by I & C systems of technical facility [18].

The I & C system is main part of the technical facility safety management system (SMS). The SMS ensures data for safety management in time by the way shown in Figures 13 [17,18]. 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.

Due to reality that dynamic development of technical facility and its surrounding is not necessarily synergic, the safety and co-existence of both need to be systematically monitored and corrected by effective measures from the long-term viewpoint. The tool used for it, is the entity safety management system (SMS) [15,17,24,25,35]. We concentrate to the technical facility SMS.

The SMS is defined as a systematic application of processes to which the technical facility is exposed. This systematic approach to safety management is preferred as the most effective way of allocation of sources for safety, because it not only improves the working conditions, but also positively influence attitudes and behaviour of employees with regard to safety and subsequently improves climate of safety. The approach monitors the physical or operational conditions of the workplace, humans and systems used in workplace. It requires pro-actively to respect a dynamic behaviour of world [15,17,35], for practical purposes in works [15,35] the golden rules for workplaces and territory / land are given; they facilitate daily safety management in each entity. Due to dynamic world development, the safety management with time is necessary [1,17-21]; the management scheme is shown in Figure 13.

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 [17-19,35,36]. 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.

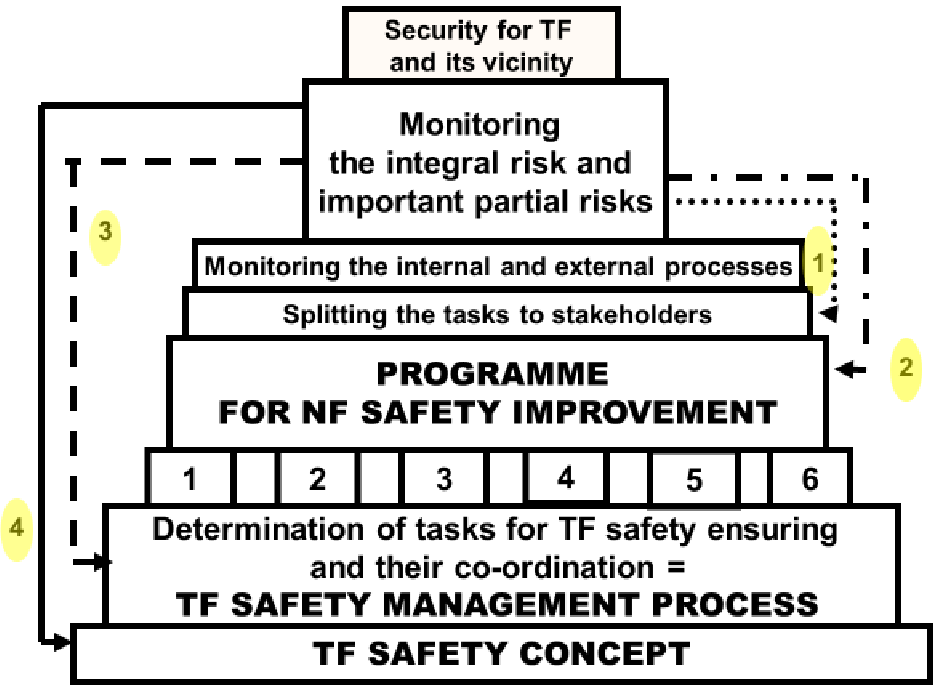

Figure 13. Model of the technical facility (TF) safety management in time. Processes: 1 - concept and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. Feedbacks that are used to control when the risk is unacceptable - the numbers in the yellow circle.

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 Figure 14 [17,18].

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.

Based on the concept that safety is a matter for all stakeholders in the framework of research under the auspices of the OECD [35] there were compiled ***the so-called golden rules of all concerned.*** The basic rules are:

- according to their possibilities to aver by preventive measures to disasters or at least their unacceptable impacts, to ensure preparedness to deal with unacceptable impacts on the protected assets and the effective response,
- to communicate and collaborate with others interested in all aspects of prevention, preparedness and response,

- to know the hazards associated with possible disasters and possible risks in the territory as well as in complex technological facility,
- to establish a "safety culture", which is respected and enforced by all stakeholders in all circumstances,
- to establish safety management systems, to monitor and, if necessary, to correct their activities,

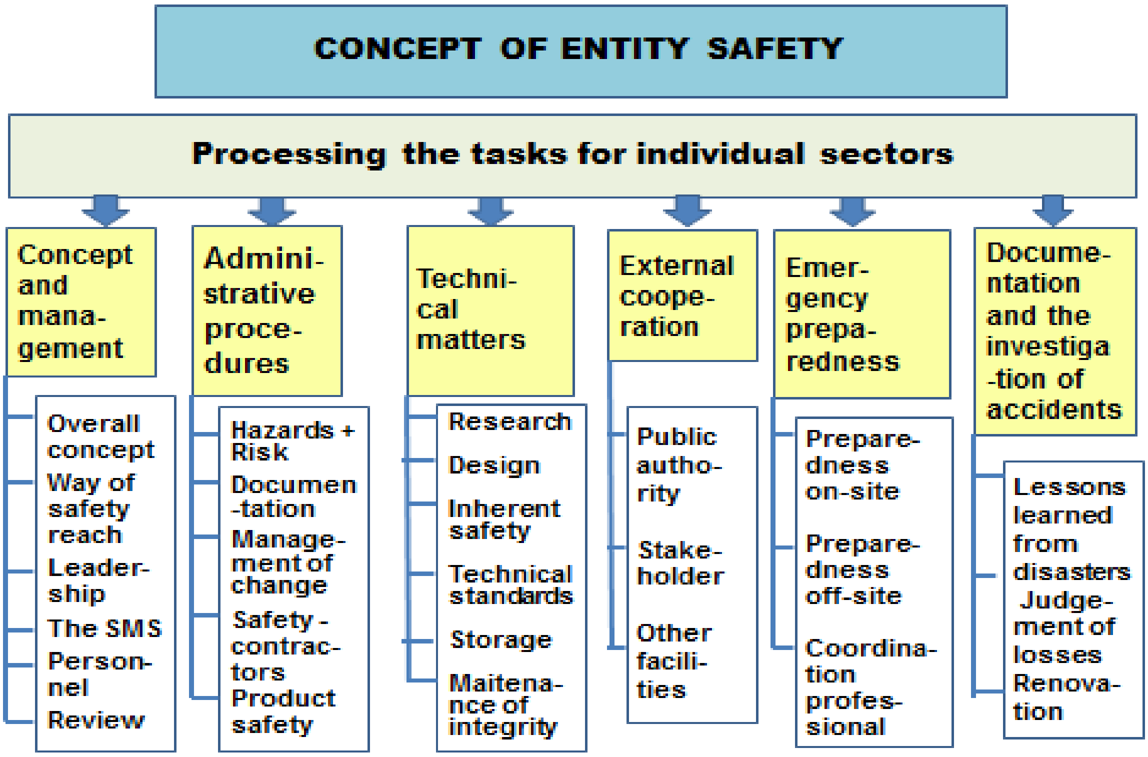

Figure 14. Concept of entity safety and its main parts.

- to use the principles of inherent safety in the design, planning and operation of the complex critical facilities and their equipment,
- carefully to manage changes,
- to be prepared for all possible disasters that may occur in a territory or complex facility,
- to help others interested in carrying out their roles and responsibilities,
- to search constantly the improvement of safety,
- to work in conformity with the safety culture, safe practices, and training,
- to strive constantly for all awareness, provide information, and the management staff featuring the feedback,
- to strive for the development, strengthening and constant improvement of the concept of safety, regulations and directives,
- to lead and motivate all other stakeholders in order to fulfil their roles and responsibilities,

- to know the risks within own sphere of responsibility, respectively, to plan measures for its proper management,
- to use the appropriate and coherent policy of security planning and follow-up activities,
- to be aware of the risks in the surrounding area and to know what to do in case of their realization,
- to participate in emergency planning and response.

Golden rules are commonly used in procedural control [15,17,35]. In many cases, the roles of individuals who are involved are specified as follows:

1. Top (senior) management and management teams operating the technology and infrastructure need to be familiar with:
   - knowledge of the hazards from disasters and possible risks in the territory as well as in facility,
   - introducing and promoting the targeted safety culture, which is respected and enforced by all stakeholders in all circumstances,
   - establishing the safety management systems, their monitoring and if necessary. corrections of their activities,
   - use of the principles of inherent safety at design, building, construction and operation of the facilities and their equipment,
   - careful managing the hangs,
   - preparing for any disaster that may occur,
   - helping others interested in carrying out their roles and responsibilities,
   - carrying out the continuous improvement of safety,
2. The workers in the complex technological facility needs to:
   - work in conformity with the safety culture, safe practices, and training,
   - strive constantly for all awareness and provide information and to provide feedback to managers.
3. Public administration needs to:
   - strive for the development, strengthening and constant improvement of the concept of safety, regulations and directives,
   - lead and motivate all other stakeholders in order to fulfil their roles and responsibilities,
   - know the risks within their own sphere of responsibility, respectively, to plan measures for their good management,
   - motivate facilities to negotiate with the risks responsibly,
   - help with the effective communication and cooperation among all stakeholders,
   - to promote cooperation between the administrative authorities,
   - use of appropriate and coherent policy of planning and follow-up activities,
   - mitigate risks through appropriate measures of the response that falls within its scope.

4. The public (other participants) needs to :
   - be aware of the risks in the community and know what to do in case of their realization,
   - cooperate in deciding on the location, construction and operation of the technological facilities,
   - participate in emergency planning and response.

To safety culture means that the humans in all their roles (executive, employee, citizen or victim of the disaster) observe the principles of safety, i.e. they behave so that they alone prevented the realization of the potential risks and when it becomes participants in the realization of the risks, to contribute to an effective response, stabilization of the protected assets and their recovery and to kick off their further development. According to some authors it is a set of attitudes, beliefs, norms and values that exist in the facility, which are reflection of how the facility is managed, i.e. they are general principles of the distribution of powers and responsibilities, policies, procedures and a certain ratio among the emphasis on work results, authority, care about the people, respect for the principles of safety and to ensure the functionality of the facility. An effective safety culture is an essential element for safety management. It reflects the concept of safety and it is based on the values, opinions and discussions of key management personnel and their communication with all stakeholders. It is a clear commitment to actively participate in addressing issues of safety and advocates that all participants did so safely and to comply with the relevant legislation, standards and norms. Rules of safety culture needs to be incorporated into all activities in the territory, or another facility. Their basis is not the concentration on the punishment of the guilty party / agent of the bugs, but the lessons learned from the mistakes and the introduction of such remedial measures, in order to not repeat mistakes or at least it significantly reduced the frequency of their occurrence.

In the context with the safety culture there are often in the current literature related to technologies used the terms as loss prevention and process safety. Their definitions are also given, because they are the tools that are used in correlation with the technological facilities to protect people and assets.

Loss Prevention is a systematic approach to prevention of accidents or to minimizing their impacts. It includes resources for the elimination of sources of risks or the reduction of their occurrence probability and for mitigating the impacts associated with this realization (preventive and follow-up measures). It also includes the identification of the appropriate control measures, the identification and application of appropriate remedial measures, by which it is ensured a safe facility having an appropriate level of security and sustainable development and to present an unacceptable danger to their surroundings [3,15,17,18,25].

Process safety or better safety of processes is the part of the safety focused on safety in the industry (complex technological facility), in which there are series of production and additional processes that are necessary for creation of the final product of the facility. It is about prevention of accidents, which have special and distinctive features for the specific industry (complex technological facility). It deals with e.g. the prevention of immediate releases of chemical substances, or energy in the harmful quantities and, in the event that these leaks occur, thus limiting their size, impacts and consequences. It does not include questions of classical safety and health protection at work, i.e. it deals with purely technical problems, which differ from the previously-defined system safety.

Analysis of the current situation shows that we can systematically handle with a number of adverse processes, i.e. disorders and failures that we can detect in advance. Sometimes, however, there is a mutual interlocking a series of seemingly unrelated factors, and as a result of non-linearity in the system there are originated very atypical accidents. Now, we recognize that complex technological facilities are for different reasons from time to time in an unstable state and formed organizational disasters cascade failures without apparent cause, i.e. we recognize the uncertainty and random epistemic (knowledge) in their behaviour; we denote them as critical facilities. In order to ensure the safety of critical facilities and privacy of people we are looking for a solution of the response for possible cases that you cannot reveal by the probabilistic approaches and we build for them, alternative sources of water and energy, specific response systems and specific training of first responders.

To achieve the demanded level of safety it means well manage and properly decide. Good management and good decision making are possible only when we have good data, and we can take advantage of the instruments that we have available. The data need to :

- be correct, i.e. it is known their size and accuracy,
- have explanatory power for the problem, i.e. they need to be validated.

The used data files need to be representative, i.e.:

- complete,
- contain the correct particulars,
- sufficient number of particulars,
- the particulars need to be spread homogeneously throughout the reference interval and they need to be validated.

In the application of models, they need to be properly considered random uncertainty and epistemic uncertainty in the data. It should be noted that in the real world, in ensuring the safety of complex technical facilities we work with non-trivial problems, i.e.:

- it is more protected assets, the objectives of which are conflicting,
- assets vary in time and space in which the assets are, i.e. the human system is in dynamic development.

In conclusion, it is therefore possible to conclude that for ensuring the safe technical facility it needs:

- to aware the technical facility aspects, which are essential for its safety,
- to understand the causes of failures of safety of technical facility and the context of their actions,
- to focus on the similarities and differences among disasters (i.e. phenomena that undermine the safety of technological system) themselves,
- to understand the role of the territory in connection with the safety of technical facilities, i.e. particular characteristics of the territory, which escalate or suppress the impacts of the disasters always or only under certain circumstances,
- to use conscious methodologies for assessment of disasters, their impacts and for identification of corrective measures;
- to set goals, timetables, monitoring, organizational structures, norms, standards and legislation for the conscious management of safety of facility,

- to delete the multiplicities in the preparation of measures to cope with the impacts of disasters;
- and at land-use planning, design, construction, operation, the response to the disaster in the territory and at restoring the territory do not apply measures, which increase the risks associated with other potential disasters in a given territory.

To ensure the safety of large technical facilities the EU issued on the basis of the recommendations of the OECD for Seveso companies following the instructions [35,36]:

1. Measures to support the safety need to be based on a clear understanding of the primary production processes and from all their associated ones and from all the important scenarios of phenomena leading to damages and losses.
2. Safety management needs to be carried out throughout the life cycle of technological unit, i.e. in the design, construction, installation, operation, maintenance, modification, putting out of operation. The risk analysis needs to cover all phases by which the facility acts by impacts on its surroundings.
3. Way of ensuring the safety needs to include the identification, control and monitoring the management scenarios on 3 levels:
   - direct risk control by humans under normal, abnormal, and critical state,
   - plans, procedures, and regulations for the optimal direct risk control,
   - the structure of the inspection activities of the safety management system and the implementation of the improvements.
4. Loops feedback and monitoring, which are among the activities on the above 3 levels trigger revisions and improvements of the control system.
5. Hierarchically higher systems level controls the critical safety tasks at a lower level. The request provides:
   - always available human reserves,
   - competence to operate safely in all situations,
   - be focused and motivated to ensure safety,
   - communicate inside and outside the of intertwined tasks,
   - the existence of the procedures, rules and plans for achieving the safety,
   - the selection of appropriate technical project to ensure optimal safety,
   - the use of user-friendly and ergonomic interfaces man-machine,
   - the existence of a system to control conflicts among safety and the other objectives of the company in the production and maintenance, design, etc.

In order to achieve certain optimal safety of technical facilities, it is necessary to control the safety by the way, that is the nature of the multidisciplinary and interdisciplinary, which understands the internal dependencies, the so-called interdependences, and knows how to deal with them.

The procedure for creating a program to increase safety in the facility consists from:

1. Define the tasks (targets), and the strategic objectives with respect to safety.

2. On the basis of data for facility / public administration or administrative office / community of other participating to select areas that are important for the safety and for them appropriate target and run trend indicators.
3. Compile a list of terms used for the management of safety and the other is to reconcile with all the other parties of management.
4. Collect local procedures, standards and norms.
5. Create a list of target indicators according to the requirements and conditions in facility / public administration / other participating groups of the community.
6. Create a list of interim (run trend) indicators according to the requirements and conditions in facility / public administration / other participating groups of the community.
7. Establish the method of evaluation of the target indicators (i.e., the value system) according to the requirements and conditions in facility / public administration / other participating groups of the community.
8. Establish the method of evaluation of each intermediate (run trend) indicators (i.e., the value system) according to the requirements and conditions in facility / public administration /other participating groups of the community.
9. Specify the scale for the measurement of file of target / file of interim (run trend) indicators (i.e., the system of values) and the boundary limits according to the requirements and conditions in facility / public administration / other participating groups of the community.

2.9.3.2. In-site emergency plan

Emergency management is understood as the process of preparing and implementing mitigation, response and recovery measures in the event of a disaster that triggers a major emergency. It includes:

- the control and management of the response so that the situation is handled with adequate forces, resources and resources, i.e. it regulates the management structure,
- the list of commands, the instructions for the operation of the Operational Centre,
- the principles of cooperation and ensuring the safety of humans (safe food and drink, protecting lives and health, evacuations, shelters, protection of property),
- own response and recovery (technical, financial, legal, personnel, security – e.g. protection of undestroyed property).

Based on the experience gained from the response to the Fukushima nuclear power plant disaster [17,18,95], it is necessary so technical facility management has for case of technical facility accident or failure:

- established response centre and related rescue operations,
- the authority providing contact with the relevant public administration and operators of the same technical facility at home and abroad,
- the authority for the coordination of assistance and rescue measures in the affected areas and for cooperation with the security forces,
- the response support authority,
- ensured cooperation with public administration, media and citizens,

- ability: to implement recovery programmes; to evaluate the effectiveness of rescue operations; to collect and keep records of response activities; and draw up lessons for the next similar actions.

In the event of the accident or failure, it is necessary to ensure cooperation with public administrations, security forces and citizens. Therefore, the correct information should be provided. The content of the information that needs to be communicated is as follows:

1. What happened?
2. What is the development of the relevant situation?
3. What area is potentially threatened?
4. What could be the size of the impact swelled compared to the upper limit?
5. What can be the impact of the situation on the safety of the population, the environment and society?
6. What needs to be done to avoid unacceptable impacts?
7. What is not appropriate to do? I.e. submit a list of ''inappropriate' activities, if possible.
8. What is likely to include response and recovery?
9. What recovery programs will be implemented at the site?
10. What services and resources are available for company renewal?

In order to be successful in the public, all authorities concerned with the management of the situation need to pay particular attention to the planning and ensuring the communication readiness, as well as testing and training the communication among the institutions and the media and, where possible, with the population.

Due to insufficient human knowledge and dynamic development of territory and technical facility even with the best preventive measures, unexpected situations should be expected. According to the analysis carried out at particulars in [3,15,17,22], there may either be a disaster with altered physical characteristics, or some preventive measures may fail, or unforeseen phenomena may accumulate and even very well-secured infrastructure may fail. To ensure the preparedness of technical facilities owners, these are mainly:

- the processing of specific disaster scenarios and response scenarios considering the specific characteristics of disasters on the infrastructures monitored,
- allocation of specific funds, aids and funds to carry out a response to accident or failure,
- the preparation of the management scenario, i.e. the manner of negotiation and decision-making the management staff of the owner or operator of a particular technical facility at failure; and the appointment of the head and members of the relevant staff and the specification of the documentation for response,
- preparing an optimal response scenario to manage the failure of a particular technical facility caused by this or that disaster according to the variant scenarios of one or another disaster at the site and depending on the possible conditions that, for objective reasons, may sometimes occur in a given territory/object,

- ensuring the specific executive components, resources and aids that will or may be needed to cope with the impact of one or another disaster in the event of a specific technical facility failure.

Tools are emergency plans and continuity plans. In the strategic decision-making process, they need also to consider secondary impacts and to have prepared competent response plans and recovery plans.

Response of technical facility is a disaster management process that requires to bring off impacts of all disasters (including the technical facility accidents) with reasonable losses and adequate resources. Response from the point of view of management optimisation means to implement an optimal scenario of response to the occurrence of one or another disaster, thereby ensuring that disaster management takes place at acceptable costs and reasonable losses [15,17]; for economic reasons, only personnel, means and aids that are adequate need to be used for response.

The formal procedure for the process of managing the response is the main features of the following:

- analysis of the situation in the affected technical facility,
- identifying the current impacts of technical facility accident or failure and identifying the risks that could be further realised by technical facility vulnerabilities and the evaluation of other impacts,
- determination of critical processes in the technical facility and the identification of the resources needed for their operation,
- determining the time at which critical processes need to be renewed in order not to further escalate the emergency caused by technical facility failure. The point is that for too long the affinity resulting from the internal links that are the source of the cascades of other impacts does not cause for too long.

Establishing a team that connects response and recovery activities in the field of technical, legal, organizational, financial, education, health and safety and creates several level management structures. The creation of an emergency management programme, i.e. the creation of an emergency management programme, is to be an analysis of potential disasters and the magnitude of their impact on protected assets and an assessment of the capacity of available forces, resources and resources designed to manage the identified impacts on the protected assets (i.e. consider what they can do about fire-fighting plans, evacuation plans, health plans, safety plans, insurance, etc.) with consideration first of all of internal forces, resources and resources (personnel, specific aids, equipment and resources, backup , organisational procedures) and when these are inadequate, using external resources (public administration, firefighters, health ambulances, technical services, cooperating organisations, citizens, etc.).

It is an evaluation of the reliability of emergency management with regard to possible problems arising from historical factors, geographical factors, technological factors, human errors, failures in food, drink, fuel, electricity, etc. Preparation of the response and recovery coordination plan, i.e.:

- specification of response and recovery activities,
- establishing their interconnection and processing of relevant procedures and documents,
- a list of the resources on which the response, recovery and their links depend,

- objectives and priorities in the activities,
- setting training requirements and timetables,
- consultation with external authorities,
- approval and distribution of the plan.

When drawing up a response plan, it should be remembered that the process of managing an emergency situation in a technical facility takes place in a certain, repetitive life cycle:

1. Normal conditions / operation of the technical facility, i.e. no disaster.
2. Response to the occurrence of an emergency caused by a disaster.
3. Restoration of the basic functions of the technical facility.
4. Provisional operation of the technical facility.
5. Restoration of the full operation of the technical facility.
6. Normal operation of the technical facility after the restoration of full functionality.

The restoration of full operation means the transition from emergency operation of the technical facility to full operation. It is usually neglected most when planning.

Another example is the formal procedure for the process of managing a specific emergency situation, which is always in the main features of the following:

- risk analysis,
- identifying impacts, vulnerabilities and their valuations,
- identification of critical processes and resources needed for their implementation,
- determining the time during which critical processes must be renewed in order to avoid further escalation of the disaster-induced emergency. The point is that for too long the couplings created in the organization do not act as a result of internal ties.

2.9.3.3. Continuity plan

From human safety viewpoint, the continuity of vitality important technical facilities is important [96-98]. Technical facility continuity is understood as the technical facility capability to ensure that the required functions are used without unplanned interruptions. Continuity of the technical elements can be ensured [24,25] by means of:

- backup device that works parallelly,
- fast early recovery measures,
- operation in alternative location.

Experts also show that to address operational continuity by ensuring the operations in an alternative location is not always a solution to the situation from the point of view of the territory, as products and services are needed in the affected area and it is not always easy to arrange their transport to the affected area.

The continuity planning is a process designed and implemented by measures and procedures to enable the facility management to respond to a disaster so that technical facility activities are maintained with the planned level of interruption. It is the business continuity planning, i.e. a process of proactive planning of mitigation and reactive disaster mitigation measures in order to minimise losses to the level that the facility management can afford [15].

The continuity plan used for a technical facility is a strategic plan for management of safety and development plan embedded in an SMS. The plan is based on the way of integral safety management (Annex 2) and the fundamental requirement of management that management acts need to be linked at all levels of management. The plan provides not only data relevant to the operation of the technical facility, but also a way of solving problems that can seriously impair the operation and competitiveness of the technical facility. In accordance with works [17,18,35,36], the continuity plan of the technical facility includes:

- the way of getting over the with risks, the sources of which are outside the technical facility and seriously affecting the technical facility work and appropriate responsibilities and procedures for resolving conflicts between the public interest and the interest of the technical facility,
- procedures for ensuring a safe technical facility over the planned lifetime so that the technical facility might deliver quality products or services, might be competitive and might not endanger itself and its surroundings,
- responses to changes of conditions that due to reality that dynamic development of technical facility and its surrounding are not always synergic; it goes on measures of emergency and crisis management that are in detail processed in all aspects in valid documents on all technical facility management level,
- for critical technical facilities that are vital to safeguard the essential functions of the State, there is also a contingency preparedness plan which includes measures and their ensuring aimed to support the State (and in case of selected technical facilities also the EU) in coping with critical situations.

3. RISK ENGINEERING METHODS

Both, the logical methods, i.e. analysis, synthesis, deduction, evaluation and assessment, as well as the specific engineering methods described in [27] are used to obtain the results in the next chapters. At this point we will give only the methods on which the following results are based. These are: what, if; check list; 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 12 [17-19,27] using the data from experts obtained by brainstorming or panel discussion.

Table 12. 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 [17-19,27]. 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 [17-19,27]. 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 needs to be described in detail by data, while the random and knowledge uncertainties [17-19,27] 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, i.e.: complete; containing the correct data; have sufficient data number; the data need to be spread homogeneously throughout the observed interval and was validated [17-19,27].

The tool under review supports the analysis of the causes and consequences of a particular process, phenomenon or state 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 departmental concepts, in identifying the starting state 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.

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.

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.

The case study methodology is, according to the knowledge gathered in [17-19,27], 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.

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 practice, they are used two forms, evaluation case study and 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 work and its surroundings?
3. What is the root cause of the safety damage 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 Figure15.

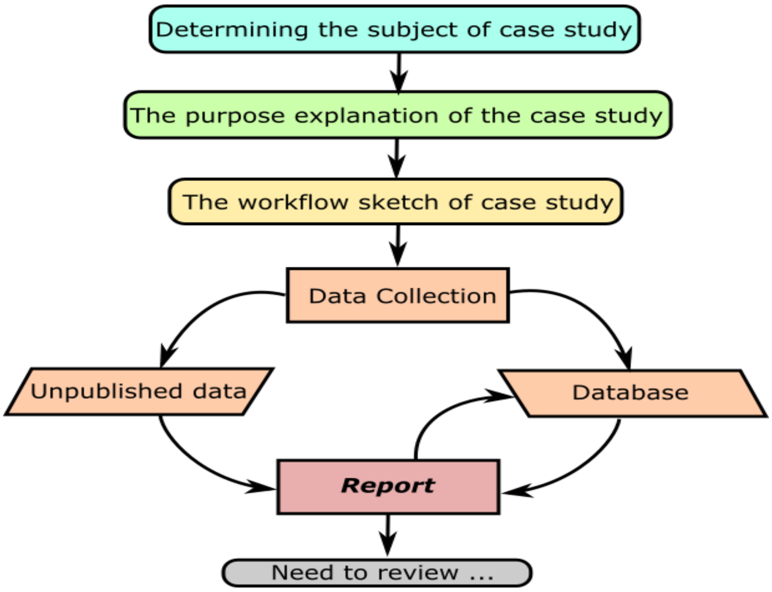

Figure 15. Process of case study compilation.

3.5. Decision support system

The Decision Support System (DSS) [17-19,27] 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 [99], 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 [100]. Otherwise, the method must 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 work 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 [24,25] supplemented by a rule for evaluating questions in terms of [99] and assigning a logical value scale.

DSS application aims are:

- identifying, managing, eliminating or minimizing unforeseen events that have an adverse impact 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 which disasters (harmful phenomena) the technical facility is exposed to, 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 [24,25] 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 [16-25] or to categorize objects according to their criticality [17,18,24,25]. 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 [52], 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 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 magnitude 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 [101].

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 possibilities of response in critical situations.

As is has been shown, that the risks are associated with itself work with the risks, a checklist (Table 13) 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 13. 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 CSN 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 14.

Table 14. 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, the original database of technical facilities accidents and failures [3] from the world data was compiled and several case studies were analysed in great details [1]. The database contains 7829 events from the whole world sources that were accessible in last 35 years to authors; more than 90% events originated during the technical facilities operation. 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. [27] in dependence of data quality and amount [3]. They were also considered get-at-able results of other authors [3,102-107].

Their results were critically assessed and separated into classes according similarity of causes and created the basis for Decision Support System enabling to multicriterial assessment of possible technical facility risks. The obtained results on lessons learned from risk impacts suppressions were also critically assessed and separated into classes according similarity of response tools and created the basis for Risk management Plan.

Analyses of tools for working with risks summarized at [1] and the experience gathered [3] show that risk management tools depend on many factors. At technical facilities strategic management, it is necessary to consider both, the safety and the long-term functionality. This means that two facts need to be considered:

- technical facilities are complex multi-level systems
- and the specific sources of some risk are not the same at all technical facility levels.

In practice, it is necessary to work with risks at:

- the lowest level (simple technical equipment – machines),
- higher levels (e.g. pressure vessels; production lines, sets of production lines, whole technical facility),
- the highest level (technical facility and its surroundings).

Safety at the highest level ensures the coexistence of technical facility with the surroundings throughout its life cycle.

In terms of needs and economic use of resources, it is true that in a number of practical tasks it is sufficient to consider only certain sources of risk, because the aim is a safe machine and not the whole technical facility and its surroundings safety. Therefore, for each risk-related work task, it is important to determine the risk management objective. At the same time, it is important to follow that certain technical equipment (insurance valves, drain valves, etc.) or certain components of a technical facility (pressure vessels, reactors, control systems, etc.) are essential for integral technical facility safety, and therefore, it is not sufficient for them to work with risks only from the point of view of entity itself, but it is necessary to work with risks that are also important in terms of whole technical facility safety. It goes on critical elements, critical equipment, critical components and critical technical facilities systems [1,17,18,24,25] that require special work with risks in siting, designing, construction and operation.

Depending on entity complexity, three risk-related objectives are distinguished:

- operation safety,
- process safety (component operation, production line)
- and entity integral safety.

Because the higher the objective is used, the higher the demands (knowledge, data, finance, time) are connected with its use, so in practice they are preferred tools with the lowest demands, which, based on current knowledge and experience, have the capability to solve a task if they are respected the safety culture basic rules and the operating regulations corresponding to operation conditions; i.e. it is not considered intent to damage the entity.

Based on experience in practice from technical facilities operational practice [1], it is an applicable tool that is fast and not very demanding for knowledge and time. The evaluation of usefulness of risk management tools in the technical facilities operation performed in cited book is that at:

- simple entities, a proven tool is checklist that is locally specific and has a properly calibrated scale for risk assessment,
- not very interconnected entities, a proven tool is a set of checklists that are locally specific and have properly calibrated risk assessment scales, with the results of those checklists are aggregated in a designated and locally specific manner
- and at complex entities, a proven tool is decision support system (DSS) that consider both, the asset connectivity and the time changes and external risk sources.

Detail database accident and failure study [1,3] shows that causes of technical facilities accidents and failures belong to categories:

- natural disasters,
- outages of external infrastructures that are important for technical facility operation,
- internal disasters as outages of internal critical infrastructures, critical fittings malfunctions, bad maintenance etc.,
- top management errors,
- project management errors,
- process management errors,
- low level of operation provisions,
- errors in technical fittings operation regime and maintenance,
- insufficient control of fittings and component conditions,
- bad safety culture,
- insufficient training, motivation and workmanship of workers,
- bad working conditions or regime,
- errors in cyber concept, fittings and nets in automatic and semiautomatic systems supporting the management decision,
- bad public administration supervision,
- insufficient legislation with regard to technical facilities safety,
- attacks of hackers, terrorists, insiders etc.

The scheme is in Figure 16. Detail division of individual categories is in [1].

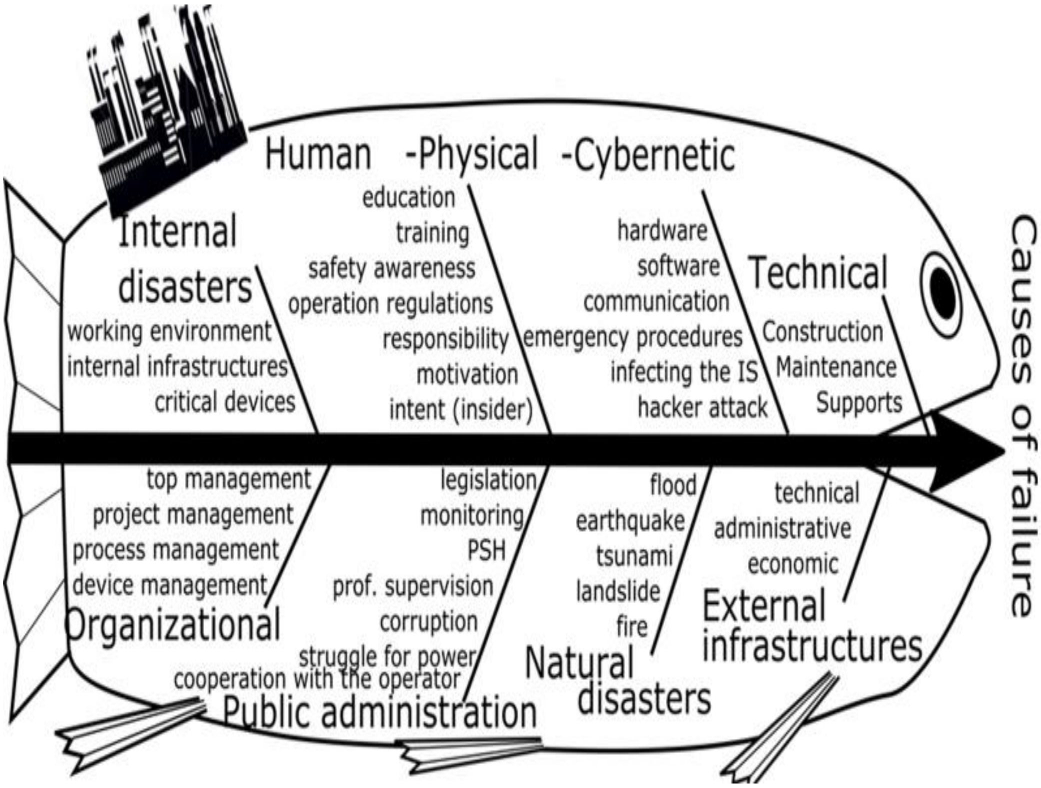

Figure 16. Basic categories of risk sources associated with the technical facilities operation which lead to the failures of the coexistence of technical facilities with surrounding areas during their operation; IS = information system; PSH = personnel safety and health.

The database analysis shows that in spite of a lot of knowledge on technical facilities´ structures, interdependences, risks and safety, the technical facilities accidents and failures have been forever occurred. Very significant source of accidents and failures is the human factor, especially in areas associated with:

- management on all hierarchical levels; the highest on the top level,
- maintenance of critical technical fittings and components,
- risk based inspections, the frequency of which needs to correspond to fittings and components criticality,
- critical fittings, components and personnel working modes,
- critical personnel education and training.

The causes of this reality are several: world dynamic variability; insufficient human knowledge and capabilities; slow application of knowledge and lessons learned into practice; and unsatisfactory awareness on risks and their consequences for technical facility and public interest.

The technical facilities accidents and failures research [1,3,108] shows that originators of technical facilities accidents and failures except of great natural disasters are:

- large mistakes in risk prevention made in technical facility terms of references, designing and operation,
- origination of small mistakes, the realization of which in short time interval is dangerous.

The second cause is much more common and is confirmed by a number of recent accidents, e.g. the accident of a Boeing 737 MAX 8 by Lion Air, which failed down on 29 September 2014 in Indonesia – according to the investigation, the cause was problems in the construction of the machine (mainly automatic flight levelling system), maintenance errors and errors of crew and ground personnel [109].

It means that both these factors need to be managed. For management improvement, two tools were developed, namely decision support system and risk management plan.

It is apparent from Figure 16 that the main causes of the risks in the operation of the technical facility, which lead to the disruption of coexistence, are primarily linked to the way and objective of the management of the technical facility and its processes, which take place in the fields of technical, organisational, financial, through their interfaces, as well as with the way in which responsibilities are fulfilled on the part of the public administration.

Based on a detailed analysis of documentation on accidents and failures of technical facilities [3], it can be concluded that very often an accident or failure occurs because:

- to date, outdated methods of risk assessment are used for complex technical facilities, e.g. tree models that do not consider confluences of phenomena,
- the operators or owners are mainly oriented towards performance (i.e. profit) and the public administration allows them to do so,
- personnel in contact with the causes and impacts of the risks do not have sufficient competence to implement proactive measures and operating regulations adapted to current conditions (normal, abnormal, critical),
- technical decisions are due to products of various particular, political or economic pressures and do not consider the specific risks that arise during operation.

The basic reasons why operators of technical facilities are not willing to influence the risks are usually:

- lack of awareness of the risks and their impact on and around the technical facility,
- subjective feelings of the responsible person, who does not consider the risk to be important,
- the idea that the risks relate to the distant future,
- the steps leading to the identification of the risk and its reduction are mostly contrary to the immediate (mostly economic or political) interests of the operator or owner,
- a particular competent worker is usually not the one, who can make direct decisions about the steps to reduce the risk.

Incorrect settlement of risks in technical facilities is due to:

- decision-making processes directly in technical facilities tend to be multi-level. At a level, on which increasing risk symptoms can be realistically identified and the risk involved is appreciated, it is not possible to decide on the additional costs of eliminating that risk,
- it is insufficient awareness on risks, their management and settlement. Working with risks is understood to be an activity consisting in compliance with standards and regulations, which is not true, as the rules in place cover only 68.4 % of the possible conditions [18]. Programmes of the vast majority of training courses taking place often exacerbate this inadequacy,
- engineers in operation and its management has narrow understanding the safety; the orientation on the technical safety of the equipment is prevalent in such a way that the technical equipment does not pose a hazard during the service life,
- there is a lack of cooperation among professions – builders, engineers, economists, chemists, computer scientists, recruiters, etc. – each profession works separately, which does not allow to solve interdisciplinary and multidisciplinary problems,
- many top managers are convinced that everything is eternal, i.e. they do not consider changes in technical equipment over time and with changes in conditions, thereby underestimating the maintenance, repair, skill and compliance with work regimes that respect physical, chemical and biological regulations.

5. TOOL - DECISSION SUPPORT SYSTEM FOR ENSURING THE COEXISTENCE AT TECHNICAL FACILITY OPERATION

Tool “Decision Support System” respects present knowledge on technical facilities´ safety and lessons learned from past technical facilities accidents and failures, the causes of which were connected with their operations. Its base goes out from critical assessments of all findings collected and the results of engineering tools as compiled What, If tables, Case studies, fault trees etc. [3]; examples of case studies are in [1].

In system entity understanding, each technical facility is socio-cyber-technical (physical) system of systems, i.e. it has a lot of interfaces of different nature and relevance under certain conditions that in each place changing with time. From this reason, at DSS compilation, attention is concentrated to aspects that assess:

- way of consideration of risks and their sources,
- achieved level of safety in technical facility design,
- measures on technical levels – maintenance regime,
- risk based inspection performance etc.,
- material and energy demandingness,
- measures implementation speeds,
- demands on staff education and training,
- information security demands,
- financial demands,
- claims of liability,
- and as well as claims on management of all interested parties (i.e. in technical facility and territory).

On the basis of the requirements for technical facilities risks summarized in detail in [1,17,18]; data on accidents and failures descripted above and summarized with related lessons learned in [1,3,17], the DSS in the form of checklist for the operated technical facilities risks assessment was compiled – it has 302 criteria; Table 15.

The check list is in the form so it may be possible to use classification scale 1 to 5 with the philosophy “the higher number, the higher risk” which means lower safety and lower coexistence of technical facility with its surrounding. For DSS application, the auxiliary scale Table 16 derived in [24,25], and the second scale for the evaluation of the entire checklist based on the principle that was introduced into standards in the 1980s, Table 17.

The assessment of Table 15, hereafter given, assumes that all criteria have the same weight. Practical examples [3] 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 17 by appurtenant way.

Table 15. Checklist for the assessment of operated technical facilities risk; number of criteria n = 302. The aim is technical facility and its surrounding safety; i.e. their co-existence; A – assessment; N - note.

Criterion	A	N
The rate in which the top management of the technical facility understands and realizes responsibility for the integral safety of the technical facility*).		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of disasters according to All-Hazard-Approach, which are possible in a given territory, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of possible beyond design natural disasters, which are possible in a given territory, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of aircraft fall down, fire and explosion in technical facility surrounding, which are possible in a given territory, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of external electric network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of external water network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of external communication network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of external traffic network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of troubles with material supply, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of troubles with		

take-off products, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of changes in support from public administration (loss of support) troubles with take-off products, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of lack of labour forces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility impacts of lack of qualified labour forces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of high increase of taxes, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of high change in interest change, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of rejection of state grant, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of recession, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of sharp and fast changes in monetary politics on market; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of insolvency of customers, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of failure of contracts with suppliers; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of failure of		

contracts with customers; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation impacts of crisis conditions / war, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of competition on power among political rivals, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of intent damage of good will, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of terrorist physical attack from surrounding, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of hacker attack from surrounding, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of pressure gangs from surrounding, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of unauthorized use of technical facility intellectual property, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of bad co-operation with local public administration, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of internal fire, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of internal explosion, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of air contamination		

in workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of contamination of drinking and utility water on workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of contamination of buildings and fittings in workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of internal electricity network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of internal lighting, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of internal drinking and utility water network, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of cooling system in workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of ventilation system, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of internal communication system, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of defects in in distribution of materials or semi-finished products among the workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of defects in transport of products from workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of emergency lightening, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of emergency communication system, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of outage of emergency smother fittings, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of non-acceptance of corrective measures if errors in project or construction of technical fittings were found, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of neglection of monitoring of near-missed and low incidents and acceptation of appurtenant lessons learned, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of neglection of corrective measures (technical and organizational) targeted to reduction of near-misses and low incidents; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of neglection of quality monitoring the conditions of critical fittings, critical components and critical systems with aim in time to reveal, e.g.: - damage of pressure pipelines with cooling substance or utility water necessary for operation, - damages or leaks of valves at pressure vessels, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of wrong maintenance, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of wrongly performed repairs of technical fittings and their interconnections, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of bad reaction of technical fittings and their interconnections to change of operating conditions with aim to ensure in time replacement or modification of machines, fittings, components or systems, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of non-existence of protective barriers for: - work of operators, e.g. covering the machines with rotate fittings or cutting tools, - measures for work in great heights or under water etc., - critical activities, e.g. digester for performing the critical chemical reactions, - waste management, e.g. containers for collection of rests of oils, solid waste) and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors in support of operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of lack of place for location of production material, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of lack of place for location of final products, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of missing the standby energy sources for fittings, which need to work in permanent regime, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of missing the standby source of cooling substances for fittings, which need to work in permanent regime, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of strategy, conception and operating conditions,		

and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of integral safety management, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of long-term development strategy, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of resolving the conflicts, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management effectiveness, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of vertical and horizontal communication, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of management style, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of functionality of co-ordinating the functions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of managemental capability, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of understanding to customers, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of anticipation of development of external conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of objectivity of judgement of organizational competences, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of use of development potential, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of involvement of top management in technical facility prosperity, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of time needs of operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of communication strategy with appurtenant public administration, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of communication strategy with subordinate persons, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of adequacy of monitoring the production and working conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of adequate use of human sources, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of contracts for in time ensuring the supply of materials and resources or services, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of contracts for in time ensuring the sale of products or services, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of adaptation to changes of universally obligatory rules, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of adaptation to changes of taxes system, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of adaptation to changes in rate charges, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of adaptation to changes in market situations, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of adaptation to changes in support from the state, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability at ensuring the sufficient amount of qualified personnel, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of capability of ensuring the finance reserve for operation at external changes, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of interest on safe technical facility, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of level of necessary technical findings, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of documentation for safe operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of quality of standards, norms and procedures for change management, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of supervision and check-up of operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of determination of responsibilities and their hierarchy, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the knowledgeableness, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the sufficient system of response to emergency situations, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of determination of requirements on qualification and skill of personnel, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		

The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the quality education system of personnel, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the working discipline at works in dangerous workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the quality of technical control of machines, fittings, components and systems, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the quality of automatic control of machines, fittings, components and systems, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the operation monitoring aimed to operation safety, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of performance of technical inspections, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of financing aimed to operation safety, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of finance reserves on renovation of machines, fittings, components and systems after incidents in operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of finance reserves for renovation of machines, fittings, components and systems after beyond design accident, and carry		

out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of processing the ensuring the readiness plan, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of processing the necessary emergency (on-site) plans, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of processing the continuity plans for extreme situations, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of distribution of fire signalling and extinguish equipment, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of protection against organizational accidents (i.e. it is missing: - strategic conception of technical facility management with time, - quality risk monitoring, - and programme for safety improvement, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of quality of operational rules for normal conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of quality of operational rules for abnormal conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of quality of operational rules for critical		

conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of quality preparation of production processes before their starts, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of check-up of machines and fittings before start of critical production operation, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of verification of qualification and skill of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of make-up and verification of procedures for critical processes, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of in-depth check-up of outputs from critical processes, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of procedures for effective response to critical conditions and material, technical a personal reserve for its realization, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of rules / instructions for personnel at occurrence of: - external disasters (natural disasters, aircraft crash, unfavourable climatic conditions, disruption of supply of electricity, water etc. from outside networks), - internal disasters (fire, explosion, outage of internal electricity network, outage of supply of water or other cooling, outage of emergency lightening, flooding the object, outage of internal communication network, outage of information network), - technical defects (wrongly adjust machines; wrongly adjust components; wrongly adjust systems; using the wrong data at adjustment of fittings; disorder or failure of safety fuse, fittings or systems; damage of		

critical fittings, components or pipelines – e.g. pressure vessels, pipe with cooling; dripping valves; failure of fittings for blocking; defects of welds, cables, pumps, compressors, diesel generators; short circuit; loss of function of equipment for emergency warning; demotion of automatic extinguish equipment at emergency situation; seized up safety valve; insufficient cooling; insufficient protection against dangerous substances or ionizing radiation; insufficient layout of work with dangerous substances or ionizing radiation; bad contacts in relay of control system; insufficient containers for storing or transport of dangerous substances; wrongly realize transport of materials, semi-finished products or products etc.), - non-determination of responsibilities for production operations and principles for mutual help (safety culture), and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of adequacy of protection of priority machines, fittings, components and systems at beyond design accident, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring: - the quality of working conditions for personnel, - the quality regime measures for operation of machines, fittings, components and systems considering the personnel potential, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the adequate protection of lives, health and security of personnel (OSH) at possible conditions, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the adequate protection of lives, health and security of personnel (OSH) at extreme conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the sufficient protection of lives, health and security of visitors at possible conditions, and carry out		

improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the sufficient protection of machines, fittings, components and systems against dishonest or danger action of personnel, contractors´ persons or visitors, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the favourable atmosphere in workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the promotion of principles of safety culture, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the motivation of personnel to quality work and safe behaviour by help of special care on workers, training and finance rewards, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the open communication on all hierarchical levels of technical facility management and among them on problems dealing with production, operation, safety etc., and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the physical protection of priority machines, fittings, components at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the cyber protection of priority automatic machines, fittings, components and systems at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top		

management in section of ensuring the reserves on decontamination of machines, fittings, components and systems after decommissioning, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the quality co-operation with public administration in matters connecting with grounds for off-side emergency plans and mutual support aimed to pulling off the critical (crisis) situations, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of verifying the effectiveness of organizational measures, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the quality co-operation with other technical facilities that are mutually interconnected in: - territory, - production, - similar technology etc., and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the correct risk assessment, and carry out improvement of defects; i.e. rate of level of ensuring the adequate. safe operation of technical facility.		
The rate in which the top management of the technical facility and managemental documents for operation consider impacts of errors of top management in section of ensuring the tried-and-true rules for management of: - transport, - manipulation and storage with material, products and waste, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider and realize responsibility for safety of technical facility, i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization		

consider the impacts of errors of higher management in section of implementation of effective project safety management, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of sufficient awareness on risks and safety, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of implementation of communication vertical and horizontal, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of implementation of management style, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of implementation of weak involvement of higher management in benefit of projects, and carry out improvement defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of monitoring the project´ results, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of use of human sources, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of supervision and check-up under project, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of		

determination of responsibilities in project, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of ensuring the knowledgeability, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of response to emergency situations, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of management in domains: - technical, - IT, - personnel, - control of machines, fittings, components and systems, - waste handling, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of response to high critical (crisis) situations, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of monitoring the operation aimed to safety including the quality production or quality service, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of performance of technical inspections, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of		

operational rules (instructions) for normal operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of operation rules (instructions) for abnormal operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of operation rules (instructions) for critical operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of maintenance and check-up of its quality, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of quality preparation of critical processes before their starts, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of requirements on check-up machines and fittings before start of critical production operation, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of verification of qualification and skill of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of ensuring: - the quality working conditions for personnel, - the quality regime measures for operation of machines, fittings, components and systems, considering real personnel possibilities,		

and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of protection of lives, health and security (OSH) at under all conditions (protective aids, tools, shelters, evacuation), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of operating rules for critical operation (activity), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of creating the favourable atmosphere in workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of enforce of principles of safety culture, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of motivation of personnel to quality work by help of special care on workers, training, finance, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of open communication on all management levels of technical facility on problems dealing with production, safety etc., and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of physical protection of machines, fittings, components and systems at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization		

consider the impacts of errors of higher management in section of cyber protection of priority machines, fittings, components and systems at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of work with risks, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of manipulation and transport of materials, semi-finished products and final products, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of storage, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of management of working operations (activities) of interconnected systems of technical fittings, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of management of key processes (process safety management), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of working regimes of critical fittings, components and systems (integrity management strategy), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of determination of barriers, limits and conditions for critical processes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of determination of reactions to changes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of making impossible the work / activity apart from allowed limits (representing the disruption of working instructions), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of strategy of maintenance of critical technical fittings, their interconnections and infrastructures that support their operations (activities), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of response plans, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of accuracy of information on operation (activity), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of supply by materials, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of tidiness and order on workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of education of personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of motivation of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of warning system, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of marking the evacuation ways, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of shelters for workers for case of need, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of test of way of execution of convert of activities from common fittings, components or systems to standby ones, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider and realize the responsibility for technical facility processes; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of management of safety of processes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of setting the working regimes (personnel stress, ensuring the demanded output quality), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of		

awareness on risks and safety, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of communication vertical and horizontal, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of managemental style, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of involvement of process managers in the process benefits, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of monitoring the results, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of use of human sources, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of supervision and check-up under process and its results, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of determination responsibilities, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of knowledgeableness, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization		

consider the impacts of errors of middle management in section of response to emergency situations, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of management in domains: - technical, - IT, - Personnel, - control of machines, fittings, components and system, - waste handling, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of monitoring the operation (activities) aimed to safety including the quality production or service, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of maintenance and check-up of its quality, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of performance of technical inspections, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of operating rules (instructions) for norm operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of operating rules (instructions) for abnormal operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of operation rules (instructions) for critical operation conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of preparation of critical production processes before their start, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of demand of check-up of machines and fittings before start of critical production operation (activity), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of verification of qualification and skill of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of: - quality of personnel working conditions, - quality of regime measures for operation (activity) of machines, fittings, components and systems that considering the personnel possibilities, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of protection of lives, health's and security of personnel (OSH) under all possible conditions in workplaces (protective aids, means, shelters, evacuation), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of care for creating favourable atmosphere on workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of enforcement of principles of safety culture, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of motivation of personnel for quality work and safe behaviour by help of special care on workers, training, finance, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of open communication on all technical facility heretical levels and among them on problems dealing with the production, safety etc., and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of physical protection of priority machines, fittings, components and systems at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of cyber protection of priority machines, fittings, components and systems at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of work with risks, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of procedures for manipulation and transport of materials, semi-finished products and final products, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of procedures for storage, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of management of operation of interconnected systems of technical fittings, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of management of key processes (process safety management), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of working regimes of critical fittings, components and systems (integrity management strategy), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of determination of barriers, limits and conditions for key processes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of determination of reactions to changes in processes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of forestall to work / operation out of allowable limits (safety culture promotion, rules of correct behaviour, execution of responsibility, adherence of principles of mutual helps, execution of calibration, check-up of sources before operation (activity) start), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of		

processing the response plans to expected emergencies, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of correctness of data on operation (activity), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of supply of material, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of order on workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of education of personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of motivation of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of warning system, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of marking the evacuation ways, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of shelters for employee for case of need, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of testing		

the transfer of activities from usual fittings, components and systems to standby ones, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of ensuring the preventive maintenance of critical fittings, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of correctness of procedures (regimes) of work, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider and realize responsibility for safety of real technical fittings of technical facility; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of maintenance and check-up of its quality, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of safety management, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of correctness of: - working regime, - waste management, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of communication vertical and horizontal, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of care aimed to creation of favourable atmosphere on workplace, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of enforcement of safety culture principles, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of strengthen the motivation of personnel to quality work and safe behaviour by help special care on workers, training, finance, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of ensuring the open communication on problems dealing with the production, safety etc., and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of ensuring the physical protection of priority machines and fittings at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of ensuring the cyber protection of priority machines and fittings at normal, abnormal and critical conditions, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of work with risks, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of		

manipulation and transport of material, semi-finished products and final products, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of storage of materials, semi-finished products final products and waste, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of management of safety at performance of key operations (activities), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of working regimes at critical operations (activities), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of barriers, limits and conditions at critical operations (activities), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of mandatory reactions to changes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of forestall of work / operation (activity) out of allowable limits, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of response to emergency situations, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of OSH requirements, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of correctness of data on operation, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of supply of material, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of order on workplaces, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of personnel education and training, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of motivation of critical personnel, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of warning system, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of marking the evacuation ways, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of shelters for employee for case of need, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		

The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of testing the way of transfer of activities from usual fittings, components or systems to standby ones, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of rules of preventive maintenance, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of proposed working procedure (regime), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of training the personnel from technical fittings, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of ensuring the functionality of barriers and adherence of limits and conditions at critical operations (activities), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of adherence of determined reactions to changes, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate in which the critical technical personnel responsible for real operation task in the technical facility operation consider and realize responsibility for safety of operations (activities); i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The rate of education level of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
The rate of training and skill level of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		

The rate of awareness on risks of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
The rate of adherence of safety culture of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
The rate of capability and motivation of the critical technical personnel responsible for real operation task in the technical facility operation to adhere operation rules and waste management rules; i.e. rate of level of ensuring the safe operation.		
The rate of dishonest intent of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
The rate in which auxiliary personnel in the technical facility operation consider and realize the responsibility for safety of activities; i.e. rate of level of ensuring the safe operation.		
The rate in which auxiliary personnel in the technical facility operation respect rules of safety culture; i.e. rate of level of ensuring the safe operation.		
The rate in which auxiliary personnel, performing the support activities, is motivated to perform activities safely and correctly handle with waste; i.e. rate of level of ensuring the safe operation.		
The rate in which auxiliary personnel performing the support activities, has responsibility to perform activities safely and correctly handle with waste; i.e. rate of level of ensuring the safe operation.		
The rate in which auxiliary personnel performing the support activities can have dishonest intent; i.e. rate of level of ensuring the safe operation.		
The rate in which technical facility information system hardware supporting the facility and its operation, is secured against impacts of disasters according to principle All-Hazard-Approach, which are possible inside and outside of technical facility, so technical facility operation might be safe.		
The rate in which technical facility information system software supporting the facility and its operation, respects the impacts of disasters according to principle All-Hazard-Approach, which are possible inside and outside of technical facility, so technical facility operation might be safe.		
The rate in which transmissions of technical and organizational information is ensured against impacts of disasters according to principle All-Hazard-Approach, which are possible inside and outside of technical facility, so technical facility operation might be ensured.		
The rate in which transmissions of technical and organizational information is ensured at failure of information infrastructure.		

The rate in which it is forestalled to infection of technical facility critical information systems by worms, hackers´ attacks etc. ; i.e. rate of level of ensuring the safe operation.		
The rate in which legislation in force require from owner and operator to ensure the technical facility integral safety.		
The rate in which public administration ensures the education on risks and safety.		
The rate in which public administration performs supervision under technical facility integral safety.		
The rate in which public administration enforces the operator to implement measures supporting the technical facility integral safety.		
The rate in which public administration monitors the technical facility integral safety.		
The rate in which public administration checks-up the adherence of OSH requirements.		
The rate in which public administration checks-up the adherence of environment protection requirements.		
The rate in which public administration checks-up the adherence of user protection requirements.		
The rate in which public administration co-operates with technical facility operator at ensuring the safety at critical situations.		

*) Note: the technical facility integral safety is the rate in which the technical facility, even under its critical conditions, does not endanger itself and its surroundings; the technical facility project safety is the rate in which the project, even under its critical conditions, does not endanger itself and its surroundings; the process safety is the rate in which the process, even in its critical conditions, does not endanger itself and its surroundings; the particular technical equipment / fittings safety is the rate in which the technical equipment / fittings, even in its critical conditions, does not endanger itself and its surroundings; the operation / activity safety is the rate in which the operation / activity, even in its critical conditions, does not endanger itself and its surroundings.

Table 16. Scale for determination of rate of risk that planned technical facility means for its surroundings (rate of coexistence disruption); by analogy to scales in [24,25]; 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 17. 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 15; N = 1510.

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 Table 15 needs to be performed by a team of specialists from different fields independently; in practice [23-25], it comes in useful team consisting of:

- worker of public administration responsible for territory safety,
- worker of public administration responsible for the development of the territory,
- representative of technical facility,
- representative of the professional institution for the technical facility safety assessment, for example from the technical inspection,
- representative of the Integrated rescue system.

The resulting value is the median for each criterion, and in cases of great variance of the values in one criterion it is necessary, so that the worker of public administration responsible for territory safety 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 risk rate 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 [1], Table 18 For application in practice, two scales are assigned to the checklist: one in Table 19 for assessing selected criteria when applying the classification scale (0-5) and the concept 'the higher the value, the higher the contribution of the technical facility to the territory"; and the scale for the evaluation of the whole principle-based checklist introduced into technical standards, Table 20.

Table 17. Checklist for assessment of the technical facility return for territory. A- result of assessment (YES or NOT).

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 19		

	It improves situation in technical and economic spheres in territory - Table 19		
	It improves the situation in environment protection and welfares in territory - Table 19		

Table 19. 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 [24,25], 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 20. Value scale for determining the rate of return of the technical facility for its surroundings; N is quintuple of criteria in Table 18 (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 15 we consider the responsibility principle that is general in Europe [63]. It means that in the followed technical facility phase (operation) both, the operator (owner) and the public administration are responsible for the technical facility safety.

Considering:

- the ALARP principle as in works [63,110-112],
- the integrated approach as in works [113,114],
- 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***

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

where ***HTD*** is the technical facility utility value, $\boldsymbol{k_i}$ are result evaluations of risk sources in Table 4, *n* is the number of risk sources (in our case 302) 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 18-20 and the principles for expected return [115] 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

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

where ***CPTD*** is the total utility technical facility return during the lifetime ***T**, k_i* are result evaluations of return sources in Table18 (assessed by experts with help of data in Tables 19 and 20) and ***n*** is the number of benefit sources (in our case 10). The expected pure annual technical facility return ***RPTD*** is given by

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

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)

$$R = RZTD - RPTD \quad (4)$$

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 [15], 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. The technical facility operates surficial safely and it is profitable.

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. The technical facility operation needs to be permanently under public administration surveillance.

In the latter case, unacceptable risk, it should be thorough reflection on conclusion – either to reject the proposed technical facility operation variant, or to ask for further measures associated with an increase of technical facility operation 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.

6. TOOL - RISK MANAGEMENT PLAN FOR ENSURING THE COEXISTENCE AT TECHNICAL FACILITY OPERATION

Due to dynamic world development, technical facilities parts ageing, wear and tear, and limited human knowledge, sources and capabilities, technical facilities´ managements and public administration need to be prepared for important risk realizations in next time. For this purpose, it was developed tool "Risk Management Plan" that respects present knowledge on technical facilities´ response and the lessons learned from past responses to accidents and failures, the causes of which were connected with their operation. 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 operation – conditions of machines, fittings, components and systems, their interfaces and supporting internal infrastructures,
- internal incidents and accidents,
- personnel,
- external sources of risks linked to natural disasters,
- external sources of risks linked to supporting external infrastructures,
- external sources of risks related to the supervision of public administration, competition, market, etc.,
- terrorist attacks,
- cyber sources of network-related risks,
- war.

Since technical facility and its surroundings are interconnected, two important players are considered – technical facility management and public administration. Risk management plan in question needs to be concerned with preparation of technical facility for management of risks directly related to it and risks associated with interconnection of technical facility – the territory; and for public administration pays the same. Therefore, the compiled plan is linked to continuity plan (paragraph 2.9.3.3).

In order the risk management plan would fulfil its role, it needs to be based on quality data processed by experts using quality methods and it shall have a foothold in legislation that ensures properly distributed competences and forces accountability, thereby contributing to the building of safety culture in society. The risk management plan helps to resolve conflicts, because in the event of an expected conflict of interest, it can be in advance:

- agreed the objectives of solving the problems caused by risk realization,
- established the relevant responsibilities,
- and codified the resolution procedures.

The risk management plan contains four basic items:

- area of risk causes from all areas (technical, organizational, internal causes, external causes, cyber, etc.),
- description of risks causes,
- risk assessment results: occurrence probability and size of risk impacts,
- risk mitigation measures and responsibilities for their implementation.

The management type TQM [51,52] and its principles are considered when drawing up a risk management plan.

From the viewpoint of responsibilities [18,63], two cases need to be distinguished, namely risk management in following areas:

- connection between public administration and management of technical facility,
- and technical facility management.

Good governance is based on the openness, accountability and efficiency of institutions and public participation in decision-making and other processes. Good governance means transparency, accountability, integrity, the appropriate type of governance, efficient and affordable services, a commitment to partnership and the continuous development of public administration institutions [15]. 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 five basic features of good governance cannot achieve sustainable development. In every case in management it holds that the manager (officer) on higher position has 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 complex world, both, the technical facility management and the public administration management represent the hierarchical interconnected systems; their structure is descripted above in Chapter 1.

On the basis of the data collected (data on the causes of accidents and failures of technical facilities during operation, and relevant lessons learned [1,3], the knowledge described above, a priority risk management plan for the field of operation of the technical facility.

In plan (Table 21), two areas are considered:

- sources of risk in territory which have potential to cause technical facility accident or failure,
- and sources of risks within technical facility which have potential to cause technical facility accident or failure with impacts that they may cause loses and damages in surroundings.

From these facts it follows that plan is site specific. At its compilation, it comes useful [1,17] the team:

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

Table 21. Risk management plan to ensure the coexistence of operated technical facility with its surrounding.

Risk source	**Description of risk**	**Occurrence probability** **Size of impacts**	**Measures for risk mitigation**
INTERFACE OF PUBLIC ADMINISTRATION AND TECHNICAL FACILITY MANAGEMENT			
Sources of risks in territory			
Beyond design natural disasters	Losses, damages and harms connected with public assets and technical facility assets – big accident in technical facility that worsen losses, damages and harm in surrounding.	Probability: low Impacts: Great	***Measures:*** Crisis plan of State, region and municipality. ***Execute:*** *Government chairman /* Region chairman / Municipality mayor. ***Responsibility:*** Region chairman
Broad fire outside the technical facility	Fire can affect the technical facility and cause big accident.	Probability: medium Impacts: great	***Measures:*** Crisis plans of municipality. ***Execute:*** Municipality mayor. ***Responsibility:*** Region chairman .
Aircraft crash outside technical facility	Possible fire or explosion can affect the technical	Probability: medium	***Measures:*** Crisis plans of municipality.

	facility and cause big accident.	Impacts: great	***Execute:*** Municipality mayor. ***Responsibility:*** Region chairman .
Failure of critical infrastructures in technical facility vicinity	In case that sufficient internal sources are missing, the technical facility accident or failure can occur or emergency regime would be necessary.	Probability: medium Impacts: great	***Measures:*** Crisis plan of region and municipality. ***Execute:*** Region chairman / Municipality mayor . ***Responsibility:*** *Government chairman.*
Insufficient technical education in region	Due to insufficient quality of technical facility directed to technical facility quality operation that consider not only norms but also possible risks, it goes to problems in operation or to accidents accompanied by enormous costs also from public budget, disruption of humans´ security, State stability, which consequently lead to decrease of life standard, economy instability etc.	Probability: medium Impacts: great	***Measures:*** Change of education system and heighten budget for education. ***Execute:*** *Government chairman /* Minister for education. ***Responsibility:*** *Parliament chairman*.
Lack of qualified labour force in region	Due to lack of qualified labour forces, the technical facility cannot fulfil tasks and services, which leads to discontent and losses, also in state budget.	Probability: great Impacts: great	***Measures:*** Change of education system and heighten budget for education. ***Execute:*** *Government chairman /* Minister for education. ***Responsibility:*** *Parliament chairman*.
Lack of labour force for technical facility	Due to lack of qualified labour forces, the technical facility cannot fulfil tasks and services, which	Probability: medium	***Measures:*** Recruitment of workers abroad.

	leads to discontent and losses, also in state budget.	Impacts: medium	***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
Insufficient political culture (manifestation of fight on power among political rivals)	Conditions for technical facility are unfavourable, because support for its activities misses.	Probability: great Impacts: great	***Measures:*** Introducing the clear rules for safety culture in public sphere. ***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
Pressure groups	Conditions for technical facility are unfavourable, because its good will is continuously impaired and permanently it is necessary realise counteractions with aim to disprove untruths.	Probability: great Impacts: great	***Measures:*** Introducing the clear rules and safety culture in public sphere. ***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
Terrorist attacks	Huge losses for technical facility and its surrounding (human, material, finance).	Probability: great Impacts: great	***Measures:*** Implementation of effective safety concept and protection in the State. ***Execute:*** *Government chairman* / Region chairman / Municipality mayor. ***Responsibility:*** Parliament chairman.
Hacker attacks	Huge losses for technical facility and its surrounding (human, material, finance).	Probability: great Impacts: great	***Measures:*** Implementation of effective safety concept and protection in the State. ***Execute:*** *Government chairman* / Region chairman / Municipality mayor.

			Responsibility: Parliament chairman.
Corruption	Huge losses for technical facility and its surrounding (social, material, finance). It goes to loss of authority of State.	Probability: great Impacts: great	***Measures:*** Implementation of effective safety concept and protection in the State. ***Execute:*** *Government chairman* / Region chairman / Municipality mayor. ***Responsibility:*** Parliament chairman.
Conditions for technical facility safe operation (taxes, interests etc.)	Huge losses for technical facility and its surrounding (material, finance).	Probability: great Impacts: great	***Measures:*** Stable strategy of development and public budget. ***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
Wrong or insufficient technical legislative	Due to wrong and insufficient legislative (e.g. incorrectly determined requirements on technical facility operation with regards to ensure the co-existence of technical facility with surrounding at operation; at accidents the State has enormous costs from public budget, it comes to disruption of humans ´security and State stability.	Probability: great Impacts: great	***Measures:*** Adjustment of legislation connected with technical facilities and education. ***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
Supervising the technical facility safety	Due to insufficient or wrongly use of competitions of public administration at surveillance on technical facility safe operation, it comes to accidents accompanied by enormous costs from public budget and to	Probability: great Impacts: great	***Measures:*** Adjustment of legislation for technical facilities operation, on public administration and on public surveillance. ***Execute:*** *Government chairman*.

	disruption of humans´ security.		***Responsibility:*** Parliament chairman.
Wrong co-operation between public administration and technical facility management	Huge losses and damages originate at crisis situations – under normal conditions they will be lower but they do not good for both.	Probability: medium Impacts: medium to great	***Measures:*** Use of all legal tools for correction. ***Execute:*** *Government chairman,* Region chairman, Municipality mayor. ***Responsibility:*** *Government chairman in co-operation with* Parliament chairman.
War	It goes to lack of finances, personnel, change of support from the State etc., which will lead to disruption of technical facility operation, which will cause high expenses, social problems (unemployment, disruption of security) or even harms in environment and by that problems for public administration (expenses for social allowances, fight against criminality etc.).	Probability: low Impacts: great	***Measures:*** To implement protective measures and to ensure acceptable technical facilities ´operation. ***Execute:*** *Government chairman in co-operation with* responsible technical facility top manager. ***Responsibility:*** Parliament chairman.
Sources of risks in technical facility			
Discrepancy with OSH requirements	Frequent injuries at work. High valetudinarianism. Discontent of workers.	Probability: medium Impacts: great	***Measures:*** Ensuring the adherence of requirements of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:***

			responsible technical facility top manager.
Contamination of environment (under allowable limits)	Penalties from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to demands of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Non-cover finance obligations to public administration	Penalties from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to demands of legislation in force. ***Execute:*** Technical facility finance manager. ***Responsibility:*** responsible technical facility top manager.
Technical facility indebtedness	Damaged good will. Unfulfillment of commitments. Bankruptcy.	Probability: medium Impacts: great	***Measures:*** Change of conception and application of effective corrections according to legislation in force. ***Execute:*** Technical facility finance manager. ***Responsibility:*** responsible technical facility top manager.
Wrong waste management	Penalties from public administration.	Probability: medium	***Measures:***

	Damaged good will.	Impacts: great	Corrections according to demands of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Discrepancy with legislative requirements	Penalties from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to demands of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager ***Supervise:*** Responsible worker of public administration
Discrepancy in data (necessary for off-site plan) transfer to public administration for potential beyond design accidents	Right of recovery from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to legislation in force. ***Execute:*** Responsible worker of technical facility. ***Responsibility:***

			responsible technical facility top manager. ***Supervise:*** Responsible worker of public administration.
Discrepancy in data (necessary for crisis plan) transfer to public administration for extreme accidents	Right of recovery from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to legislation in force. ***Execute:*** Responsible worker of technical facility. ***Responsibility:*** responsible technical facility top manager. ***Supervise:*** Responsible worker of public administration.
Omission of finance reserve for decommission and territory treatment	It is possible from public administration to expect finance penalties with fast requirement on technical facility decommissioning.	Probability: great Impacts: great	***Measures:*** Corrections according to legislation in force – to respect moral responsibility to territory and its citizens. ***Execute:*** Finance manager of technical facility. ***Responsibility:*** responsible technical facility top manager. ***Supervise:*** Responsible worker of public administration.
TECHNICAL FACILITY MANAGEMENT			
Sources of risks in territory			
Occurrence of natural disaster higher than design one	Disruption of operation or technical facility accident.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:***

			responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Aircraft crash on technical facility or in its close vicinity	Disruption of operation or technical facility accident.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Fire or explo-sion in close surrounding higher than design one	Disruption of operation or technical facility accident.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Failure of external critical infrastructures	Disruption of operation or technical facility accident or failure.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Loss of public administration support	Disruption of operation or technical facility accident or failure.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Lack of qualified labour forces	Insufficient of technical facility operation up to accident or failure.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager for labour forces. ***Responsibility:*** responsible technical facility top manager.
Disruption in supply of	Insufficient technical facility performance up to	Probability: medium	***Measures:***

material for production	production failure, i.e. lack of expected products or services.	Impacts: great	According to continuity plan. ***Execute:*** responsible technical facility manager for material supplies. ***Responsibility:*** responsible technical facility top manager.
Consumption crisis	Unmarketability of products or services, i.e. economic losses.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager for sale. ***Responsibility:*** responsible technical facility top manager.
Changes in market	Economic losses for technical facility. Reduction of number of workers. Social problems in region.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Finance technical facility manager. ***Responsibility:*** responsible technical facility top manager.
Insolvency of customer	Economic losses up to indebtedness for technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Finance technical facility manager. ***Responsibility:*** responsible technical facility top manager.
Hacker attack	Insufficient production up to accident or failure of technical facility.	Probability: medium	***Measures:***

		Impacts: great	According to continuity plan; especially appurtenant response plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Intent abuse of good will	Economic losses for technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager. ***Responsibility:*** responsible technical facility top manager. ***Co-operate:*** Responsible worker of public administration.
Terrorist physical attack	Disruption of operation, failure or accident of technical facility. Economic losses for technical facility. Impacts on region – lack of products, services and unemployment.	Probability: low Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:***

			responsible technical facility top manager. ***Co-operate:*** Responsible worker of public administration.
Attack of pressure interest groups	Loss of competitiveness and economic losses for technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager. ***Responsibility:*** responsible technical facility top manager. ***Co-operate:*** Responsible worker of public administration.
Unauthorized use of intellectual property of technical facility	Loss of competitiveness and economic losses for technical facility.	Probability: great Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager. ***Responsibility:*** responsible technical facility top manager. ***Co-operate:*** Responsible worker of public administration.
Sources of risks in technical facility			
Obsolete technical outfit	Low performance, danger of failure or accident of technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant development plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for

			technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Critical technical fittings or components are wearied down	Low or disrupted performance, danger of failure or accident of technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant development plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Missing funds on maintenance, repairs and modernization of equipment	Low or disrupted performance, danger of failure or accident of technical facility.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant development plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Internal fire	Losses and damages, disrupted performance of technical facility. Unfulfillment of commitments to third party.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:***

	Sanctions.		Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Internal explosion	Losses and damages, disrupted performance of technical facility. Unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Air contamination	Human health problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Drinking and utility water contamination	Human health problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Contamination of equipment and building parts	Human health problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of internal electricity network	Human and equipment problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical

			fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of lightening	Human health problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of ventilation or climatization	Human and equipment health problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of internal network of drinking or utility water	Human and equipment problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:***

	Sanctions.		Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of cooling systems	Human and equipment problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of communication network	Human and equipment problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Outage of emergency lightening	Human problems lead to disruption of performance of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in hardware of information system supporting the technical facility control and management	Accident or failure of technical facility, which means in fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in software of information system supporting the technical facility control and management	Accident or failure of technical facility, which means in fulfilment of commitments to third party. Sanctions	Probability: great Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Information system manager and appurtenant responsible technical facility project managers, responsible technical facility process managers,

			responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in transmissive channels	Accident or failure of technical facility, which means unfulfillment of commitments to third party. Sanctions	Probability: great Impacts: great	***Measures:*** According to continuity plan; especially appurte-nant response plan. ***Execute:*** Manager for communication and appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of emergency communica-tion system	Accident or failure of technical facility and their impacts on assets, which means disruption of oper-ation, which leads to in fulfilment of commitments to third party. Sanctions	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurte-nant response plan. ***Execute:*** Communication system manager and appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Outage of extinguish equipment	Accident or failure of technical facility and their impacts on assets, which means disruption of operation, which leads to unfulfillment of commitments to third party. Sanctions	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Outage of critical fittings / components / processes / projects (production lines)	Disruption of performance, accident or failure of technical facility and their impacts on assets, which means disruption of operation, which leads to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Occurrence of accident with size of design accident	At certain conditions it comes to failure of protective measures, which can lead to accident or failure, which leads to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: medium	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical

			fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Beyond design accident	It comes to failure of protective measures which lead to severe accident or failure, and to damages around the technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: low Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Extreme accident	It comes to failure of protective measures which lead to severe accident or failure, and to severe damages and losses around the technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Extinction. Loss of competitiveness.	Probability: low Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insufficient maintenance	Frequent disruption of performance, accident or failure of technical facility and their impacts on assets.	Probability: great Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:***

	Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.		Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong reaction of technical equipment to change of conditions	Frequent disruption of performance. Danger of origination of accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in OSH	Injury or death of personnel. Disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** Corrections according to legislation in force. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Errors in conditions for contactors work	Injury or death of contractors 'personnel. Disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** Corrections according to legislation in force. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Ineffective safety management system	Frequent disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially plan for safety ensuring. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insider	Frequent disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings.

			Responsibility: responsible technical facility top manager.
Errors of top management in section of strategy, conception, supervision and check-up	Frequent disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management in section of operation, maintenance and repair of technical equipment	Frequent disruption of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management in section of responses to emergency situations and their	Significant disruption of performance after accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Manager for emergency protection and appurtenant

prepared-ness's	unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.		responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management in section of performance of technical inspections	Frequent or long disruptions of performance, accident or failure of technical facility and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management in section of ensuring the financial reserves for renovation of technical equipment	Long disruption of performance of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Finance manager and appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Wrong operating rules for normal operation	Frequent disruption of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong operating rules for abnormal operation	Frequent disruption of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong operating rules for critical operation	Frequent significant disruption of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical

			fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Defects in critical personnel education	Frequent disruption of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Manager for personnel and appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong verification of critical personnel qualification	Frequent disruptions of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Manager for personnel and appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in working regime	Overload of personnel which lead to frequent disruptions of performance up to accident or failure of technical facility	Probability: medium Impacts: great	***Measures:*** According to continuity plan and legislation in force. ***Execute:***

	and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.		Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insufficient safety culture	Overload of personnel. Missing the co-operation. Frequent disruptions of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan and legislation in force. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insufficient motivation of key personnel	Neglecting the co-operation, frequent disruptions of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management	Frequent disruptions of performance, frequent	Probability: medium	***Measures:***

in section of work with risks connected with technical equipment, production, transport of material and products	near-misses, danger of origination of accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Impacts: great	According to continuity plan and legislation in force. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of project management (strategy, conception, supervision and check-up)	Frequent disruptions of performance, frequent near-misses, danger of origination of accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of operation, maintenance and repair of technical equipment	Frequent disruptions of performance, frequent near-misses, danger of origination of accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Errors of higher management in section of response to emergency situations and their preparedness's	Long disruptions of performance due to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of performance of technical inspections	Frequent disruptions of performance due to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of safety culture	Frequent disruptions of performance due to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Errors of higher management in section of OSH	Frequent injuries up to death of personnel which lead to disruptions of performance of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Damage on good will.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of education of critical personnel	Frequent disruptions of performance due to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of motivation of critical personnel	Insufficient or frequently disrupted of performance, many near-misses up to incidents of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.

Errors of higher management in section of working regime of critical personnel	Insufficient and frequently disrupted of performance, many near-misses up to incidents of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of higher management in section of work with risks connected with technical equipment, production, transport of material and products	Insufficient and frequently disrupted of performance, many near-misses up to incidents of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of middle management in section of operation, maintenance and repairs of technical equipment	Insufficient and frequently disrupted of performance, many near-misses up to incidents of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.

Errors of middle management in section of response to emergency situations and their preparedness's	Long disruption of performance due to accident of failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of performance of technical inspections	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of safety culture	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in	Frequent injuries up to deaths, which led to	Probability: medium	***Measures:*** Continuity plan.

section of OSH	frequently disruptions of performance. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Damage on good will.	Impacts: great	***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of critical personnel education	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of motivation of critical personnel	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of working	Overload of personnel, discontent personnel. Frequent disruptions of performance due to incidents up to accidents or	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:***

regime or critical personnel	failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.		Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of middle management in section of work with risks connected with technical equipment, production, transport of material and products	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility project manager.
Errors of technical management in section of maintenance, repair and function ability of technical equipment	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of responses to emergency situations	Long disruption of performance due to accident or failure of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for

and their preparedness's	Sanctions. Loss of competitiveness.		technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of performance of technical inspections	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of safety culture	Frequently disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of OSH	Injuries up to death of personnel. Disruption of performance. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings.

			Responsibility: Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of education of critical personnel	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of motivation of critical personnel	Negligible co-operation lead to frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of working regime of critical personnel	Overload of personnel and frequently disrupted performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:***

			Appurtenant responsible technical facility proccess manager.
Errors of technical management in section of work with risks connected with technical equipment, production, transport of material and products	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility proccess manager.
Errors of critical personnel at performance of operation, maintenance and repair of technical equipment (non-respecting rules)	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.
Errors of critical personnel at response to emergency situations and their preparedness's	Long disruption of performance due to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.
Errors of critical personnel	Neglecting co-cooperation and frequently	Probability: medium	***Measures:***

in section of safety culture	disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Impacts: great	Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.
Errors of critical personnel at adherence OSH requirements	Injury up to death of person. Disruption of performance. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.
Errors of critical personnel at work with risks connected with technical equipment, production, transport of material and products	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.

It is apparent from the table 19 that a lot of the sources of risk for the technical facility operation, which need to be treated with a risk management plan, are related to the management of the technical facility. From real data [3] , it follows that errors f top levels of management, namely at both cases, the public administration and the technical facility, mean far greater losses, damage and harms to the public assets and assets of the technical facility than errors at the lower levels of management. This is due to the fact that top management has greater possibilities (power, resources, finance) to influence safety-targeted risk management than lower ones. What has already been stated at the end of Chapter 4 – when the plane crash of a Boeing 737 MAX 8 by Lion Air, which failed down on 29 September 2019 in Indonesia, the high educated and experiences pilot evaluated situation as follows - The aircraft was produced by clowns driving the monkeys – it means in this case top management did not consider the comments and requirements of pilots, who aircraft tested [109].

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

Technical fittings and technical facilities are the result of the skill of human generations. Each of these entities consists of a series of parts that are interconnected to form object or network structures. Particular attention is currently being given to large-scale technical facilities that provide quality basic services to humans [17,18,23-25]. They take the form of socio-cyber-technical [17,18,23-25]. Many of them ensure the fulfilment of the basic functions of the State, and therefore, the word critical is associated with them. Engineering systems, from the simplest to the most complex, meet the daily needs and demands of citizens, and therefore, require targeted anthropogenic care.

Technical equipment and technical facilities belong to the different sectors management and are very diverse by the design and nature. Therefore, the criteria and measures for managing and settling their risks are sector-dependent, even if they have the same objective, namely safe technical equipment or safe technical facility. For reasons of great diversity, the different procedures are ***site and sector-specific***. Aspects important for operation of technical equipment and whole technical facilities are very diverse, especially those of:

- knowledge and technical, which predetermine the capacity possibilities of technical facilities and technical equipment,
- organizational and legal matters enabling the technical facilities operation and technical equipment operation at a certain level of safety in the territory and over time,
- financial,
- personnel,
- social
- and political at national and international level.

Based on the findings summarized in the works [17,18], each engineering system is characterized by the structure, hardware, procedures, environment, information flows, organization, and interfaces among these components. The basic element of safe operation of technical facility and technical fittings in the field of technical solutions is the application of safe (i.e. reliable, functional and non-threatening themselves and their surroundings) technical elements, their qualified interconnection and operating mode allowing safe (i.e. reliable and trouble-free) operation, and proper maintenance, back-up of priority parts of technical fittings, components or systems, use of various back-up principles and thoughtful deployment of back-ups in the territory.

However, the aspects important for the operation of technical installations and whole technical facilities are very diverse, in particular:

- knowledge and technology which determine the capacity of technical facilities and technical equipment,
- organizational and legal matters which allow the operation of technical facilities and technical equipment at a certain level of safety in the territory and over time,
- financial,
- personnel,

- social,
- political at national and international level.

The findings obtained by research of technical facilities accidents and failures show that in the prevention of accidents and failures, the following should be avoided: major risk prevention errors (e.g. underestimating the size of external risk sources or sources of organizational accidents); and occurrence of minor errors, realization of which in short time period is dangerous, although the impacts of separate individual errors are manageable by prepared response measures. To this aim the 'Decision Support System' tool is developed and recommended for practice

Due to world dynamic development, ageing and wear of parts of technical facilities and limited human knowledge, resources and possibilities, the technical facility management and the public administration needs to be prepared for future occurrence of risks. To this aim 'Risk Management Plan' tool is developed and recommended for practice.

Both tools respect current knowledge of technical facilities safety and lessons learned from their past accidents and failures, the causes of which have been linked to their operation. They need to be compiled as sector and site specific in order to be effective and effective.

Examples from practice gathered in the works [1-18,23-25] show that in many cases the safety does not require high reliability (e.g. a train under unfavourable conditions must not with regard to possible human loss of lives and material damages in the event of an accident to prioritize reliability over safety, i.e. endeavour to reach the station in time and endangering the public assets). As autonomous systems for the management of technical facilities are currently being built, it seems to be very important to establish a ranking of criteria according to which the autonomous system will decide with regard to the safety and health of humans.

Finally, it should be noted that the above knowledge and experience imply that when dealing with risks in the operation of technical facilities it is necessary to distinguish tasks according to:

1. Objective which depend on:
   - the nature and characteristics of the technical facility,
   - the nature and characteristics of the environment in which the technical facility is operated,
   - the mode of operation of the technical facility,
   - requirements for the results of risk management of the technical facility (integral safety, integrated safety, project safety, process safety, safety of individual installations, human safety and health at work, etc.),
   - and whether a short, medium or strategic solution is required.
1. Task and credibility requirement:
   - risk identification,
   - risk analysis,
   - risk assessment,
   - risk judgement for management needs,

- management and settlement of risks,
- risk monitoring.

3. Nature of followed entity:
   - technical device (equipment, tool, machine, fittings),
   - technical component,
   - production line,
   - technical process,
   - set of processes in the technical facility,
   - the whole technical facility,
   - the whole technical facility and its surroundings.

In order to get the right results in risk management economically, it is necessary to choose the right concept (linear model, tree model, network model, unstructured model) for each task, have the right data and be able to process the data correctly. The right choice of concept is very important because existing solution concepts and associated tools, methods and techniques of engineering disciplines working with risks:

- have different demands on data and their accuracy,
- have different demands on the time needed to obtain a result,
- have different knowledge requirements for their application,
- have different financial requirements,
- moreover, they do not give the same results.

Emphasis on good work with risks is in the standard ČSN ISO 31000 Risk management - principles and guidelines [101]. Since resources, forces and means for safety building, i.e. risk management towards safety, are never sufficient, for reasons of economy it is necessary to proceed as follows:

- to determine risks only by using data and methods that provide a quality basis for decisions of form of risk management at the appropriate level of management,
- at the strategic level of management and engineering settlement of risks, it is necessary to solve the risks of technical facilities by understanding them as SoS - it goes on ensuring the long-term existence and development of the technical facility and its surroundings,
- at the tactical and functional level of risk management and engineering settlement, the risks of engineering facilities need to be addressed in a safe system-oriented way,
- at the technical and functional level of risk management and engineering settlement, the risks of technical facilities can be addressed in a secure system-oriented manner only if potential damage around the system is unlikely or acceptable (e.g. handling with a tank with a highly hazardous substance does not belong to the category in question).

Analysis of the current situation shows that we can systematically handle many non-demanded processes, i.e. incidents, accidents and failures, which we can detect in advance. Sometimes, however, a number of seemingly unrelated factors intertwine, and non-linearities in the system create very atypical huge unexpected accidents. Therefore, we now accept that complex technical facilities are, for various reasons, from time to time in an unstable state (conditions), and there are occurred organizational accidents, cascades of failure without obvious cause, unusual phenomena, etc.- i.e. we count in uncertainties of both types, the random ones and the epistemic ones in their behaviours. In order to ensure the coexistence of a technical facility with its surrounding throughout its lifetime, we need to prepare the responses to possible expected (and in case of very dangerous entities also extreme) cases where risks are realized for reasons that cannot be detected by probabilistic approaches, and for these interventions we need to build alternative water and energy sources, specific response systems and specific training of engineers and responders.

The amendment of the international standard ISO 9000, issued in 2016, requires a risk analysis in connection with quality assurance of processes and products in companies seeking the certification or re-certification of the quality management system. The standard in question refers to EN 31010 Risk Management - Risk Assessment Techniques, etc. Therefore, it is necessary to introduce into practice the knowledge, tools and recommendations mentioned in the previous chapters.

Accident and failure studies show that an important factor is the proper allocation of responsibilities and their correct implementation at the various levels of management. For the safety of technical facilities are also responsible politicians and public administrations, who create the conditions for human lives and the operation of technical facilities and supervise technical facilities, their products or services. Quality risk management aimed at the safety of any entity requires knowledge, resources, finance and also correct performance of responsibilities, and therefore, the Parliament and the government must create both, the conditions and the rules for their proper implementation (legislation, quality technical education) as well as tool for their enforcement.

REFERENCES

[1] 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

[2] PROCHAZKOVA, D., PROCHAZKA, J. Tools for Risk Management of Technical Facilities Operation. *European Journal of Engineering research & Science (EJERS).* ISSN 2506-8016. 5 (2020), 4, pp. 494-500. doi10.24018/ejers.2020. 5.4.1854

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

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

[5] 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.

[6] 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

[7] 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.

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

[9] 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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

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

[18] 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

[19] 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

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

[21] 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

[22] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Their Control.* ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234p.

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

[26] PROCHAZKOVA, D. *Challenges to Future Disasters Management*. ISBN: 978-3-659-53926-8. Saarbruecken: Lambert Academic Publishing 2014, 170p.

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

[28] US DoD. *Security Engineering Facilities Planning Manual*. Washington: US Department of Defense US. UFC 4-020-01, 3 March 2006. http://www.wbdg.org/ndbm/DesignGuid/pdf/FINAL%20DRAFT_UFC_4-020-01. pdf

[29] US DoD. *Unified Facilities Criteria (UFC). Minimum Antiterrorism Standards for Buildings*. Washington: Department of Defense US. UFC 4-010-01, 22 January 2007.

[30] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Management of Risks Connected with Technical Facility Manufacturing and Commissioning* (in Czech). ISBN 978-80-01-06609. Praha: ČVUT 2019, 207p. http://hdl.handle.net/10467/8446634

[31] PROCHAZKOVA, D., PROCHAZKA, J*. Risk Management at Technical Facilities Designing, Building and Commissioning.* ISBN 978-80-01-06716-1. Praha: ČVUT 2020. dspace.cvut.cz. http://hdl.handle.net/10467/87491

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

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

[34] www.idnes.cz

[35] 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.

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

[37] BRISSAUD, F., TURCINOVIC, D. Functional Safety for Safety-Related Systems: 10 Common Mistakes. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1. London: Taylor &Francis Group 2015, pp. 1159-1166.

[38] ISO. *IEC 61508. Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems.* Geneva: International electrotechnical commission 2010. Geneva: ISO 2011.

[39] ISO. IEC 61511. *Functional safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements.* Geneve: ISO 2011.

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

[41] PROCHÁZKOVÁ, D. *Protection of Persons and Property* (in Czech). ISBN 978-80-01-04843-6. Praha: CVUT 2011, 301p.

[42] PAPAZOGLOU, I. A. ET AL. Occupational Risk Management for Contact with Moving Parts of Machines. In: *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-2285509-8. Leiden: CRC Press/Balkema 2009, pp 713-720.

[43] MALKIN, A. M., WINDER, C. Applying the Safe Place, Safe Person, Safe Systems Framework: Case Study Findings across Multiple Industry Sectors. In: *Reliability, Risk and Safety, Theory and Applications*. ISBN 978-0-415-55509-8. Leiden: CRC Press / Balkema 2009, pp 697-704.

[44] BRAGATTO, P. A. ET AL. The Impact of the Occupational Safety Control Programs on the Overall Safety Level in an Industrial Cluster. In: *Reliability, Risk and Safety. Theory and* Applications. ISBN 978-0-415-55509-8. Leiden: CRC Press / Balkema 2009, pp. 745-752.

[45] XENIDIS, Y., GIANNARIS, K. Modeling and assessment of performance shaping factors in construction. In: *Safety and Reliability: Methodology and Applications.* ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2015, pp 1019-1026.

[46] PROCHÁZKOVÁ, D. The Human Factor and Its Handling. Chapter 7. In: *Advances in Intelligent Vehicles.* ISBN 978-0-12-397199-9. Oxford: Elsevier 2014,

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

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

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

[50] IAEA. Assessment of Defence in Depth for Nuclear Power Plants. ISBN 92–0–114004–5. Vienna: IAEA 2005, 119p.

[51] NENADÁL, J. *TQM. Role of Quality Economy in TQM Conception* (in Czech). 1999, www: http://fmmi10.vsb.cz/639/qmag/mj03-cz.htm.

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

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

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

[55] IAEA. *Safety Guides and Technical Documents*. Vienna : IAEA 1954 – 2019.

[56] US PMI. *A Guide to the Project Management Body of Knowledge*. Washington: US Project Management Institute 2004.

[57] BARALDI SESSO, D., VISMARI, L. F., CAMARGO, J. B. jr. An Approach to Assess the Safety of Automatic Dependent Surveillance Systems Considering Aspects of Integrity in Positional Data Based on Computational Simulation. In: *Safety and Reliability of Complex Systems.* ISBN 978-1-138-02879-1. London: Taylor & Francis Group 2015, pp. 305-313.

[58] BORGES, HICKEY, C. Balancing Safety and Performance through QRA and RAM Analyses. In: *Safety and Reliability: Methodology and Applications.* ISBN: 978-1-138-02681-0. London: Taylor & Francis Group 2015, pp. 445-452.

[59] ISO. *ISO 55000:2014, Asset management - Overview, Principles and Terminology.* Geneve: ISO 2014.

[60] GALASSI, T. *A Starting Point for Workplace Safety.* U.S. Department of Labor Blog. OSHA 2016, https://blog.dol.gov/2016/10/18/top-10-osha-citations-of-2016-a-starting-point-for-workplace-safety/.

[61] CORDARO, T. *Top Ten Violations*. OSHA 2016. http://www.oshalawblog.com /2016/10/articles/oshas-2016-top-ten-violations/.

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

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

[64] DĚDINA, J. *Management and Organizational Behaviour* (in Czech). Praha: Grada 2005.

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

[66] OECD. Machine-to-Machine Communications: Connecting Billions of Devices. *OECD Digital Economy Papers, No. 192.* OECD, Paris, 2004, http://dx.doi.org/10.1787/5k9gsh2gp043-en.

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

[68] HOLLNAGEL, E. *FRAM: the Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems.* Ashgate Publishing, Ltd. 2012.

[69] STEIN, W., HAMMERLI, B., POHL, H., POSCH, R. (eds). Critical Infrastructure Protection – Status and Perspectives. *Workshop on CIP*, Frankfurt am Main 2003, www.informatik2003.de

[70] LEVESON, N. A New Accident Model for Engineering Safer Systems. *Safety science* 42 (2004), 4, pp. 237–270.

[71] LUNDBLAD, K., ET AL. FRAM as a Risk Assessment Method for Nuclear Fuel Transportation. *International Conference Working on Safety*, 2008.

[72] HOLLNAGEL, E. Risk + Barriers = Safety? *Safety Science* 46 (2008), pp. 221–229.

[73] ROPOHL, G. *Philosophy of Socio-Technical Systems.* In: *Society for Philosophy and Technology*, 4 (1999), No 3.

[74] LACKO, B. The Risk Analysis of Soft Computing Projects. In: *Proceedings International Conference on Soft Computing – ICSC 2004*. Kunovice: European Polytechnical Institute 2004, pp. 163-169.

[75] MAREK, J. et al. *Management of Risks at Production Machines Construction* (in Czech). ISSN 1212-2572. *Průmyslové spektrum* 2009, speciální vydání.

[76] KRÁL, J., PROCHÁZKOVÁ, D. Example of Management of Risks in Machinery (in Czech). In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 91-100.

[77] PROCHAZKOVA, D., PROCHAZKA, J. Tool for risk reduction at specific component aircraft engine welding. In: *Proceedings of International European Safety and Reliability Conference, ESREL2018*. ISBN 978-1-351-17466-4. London: Taylor & Francis Group 2018; https://www.ntnu.edu/esrel2018; pp. 3135-3142.

[78] EPRI. *Characterizing and Controlling Weld Residual Stress.* http://www2.epri.com

[79] ASME. *ASME Codes and Standards for welding*. http:www.asme.org

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

[81] RAMUHALLI, P., HENAGER C. H., GRIFFIN, J. W., MEYER, R. M., COBLE, J. B., PITMAN, S.G., BOND, L. J. *Material Aging and Degradation Detection and Remaining Life Assessment for Plant Life Management*. IAEA-CN-194-1P28. www.inis.iaea.org

[82] BOND, L. J., ET AL. Damage Assessment Technologies for Prognostics and Proactive Management of Materials Degradation (PMMD). *Nuclear Technology*, 173 (2011) 46, pp. 99-152.

[83] BALLINGER, R. G. *Materials Issue.* Massachusetts: MIT 2017.

[84] 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.

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

[86] ZOUHI, R. *Microwave Non-destructive Testing and Evaluation*. ISBN 0412-625008. London: Kluwer 2000,215p.

[87] BLITZ, J., SIMPSON, G. *Ultrasonic Methods of Non-destructive Testing.* ISBN 0412 604 70 1. Cambridge: University Press 1996, 269p.

[88] GAJDOŠ, L. ET AL. *Reliability of Gas Duct* (in Czech). ISBN 80-01-02143-2. Praha: ČVUT 2000, 217p.

[89] CHEVILEND, R. *Inzhenernaya nadezhnost i rasthet na dolgovecznost* (in Russian). Moskva: Energia 1966, 232p.

[90] MBA, D. U., RAO, R. B. K. N. *Condition Monitoring and Diagnostic Engineering Management*. ISBN 1-871315-91-3. Granfield: University Press 2006, 649p.

[91] KOPEC, B. ET AL. *Non-destructive Testing of Materials and Constructions* (in Czech). ISBN 978-80-7204-591-4. Brno: CERM, s.r.o. 2008, 571p.

[92] PROCHÁZKOVÁ, D., SVOBODA, V. Results of Non-destructive Methods Supporting Risk Decision-making (in Czech). ISSN 1211-443X. *Soudní inženýrství*, 2019, 30 (2), 32–39. DOI: http://dx.doi.org./10.13164/SI.2019.1.17.

[93] MBA, D. U., RAO, R. B. K. N. *Condition Monitoring and Diagnostic Engineering Management*. ISBN 1-871315-91-3. Granfield: University Press 2006, 649p.

[94] JARDINE, A. K. S., TSANG, A. H. C. *Maintenance, Replacement, and Reliability: Theory and Applications.* London: CRC Press 2013.

[95] IAEA. *The Fukushima Daiichi Accident.* Technical Volume 5/5. ISBN 978-92-0-107015-9. Vienna: IAEA 2015, 218p.

[96] SMITH, M., SHERWOOD, J. Business Continuity Planning. *Computers & Security*, 14 (1995), 1, pp. 14-23.

[97] GOLDBERG E. M. Sustainable Utility Business Continuity Planning: A Primer, an Overview and a Proven Culture-Based Approach. *The Electricity Journal*. ISSN: 1040-6190, 21 (2008), 10, pp. 67-74.

[98] DAI. *Business Continuity Planning*. Disaster Advisors Inc. 2003. http://www. disasteradvi sors.com/disasterplanning.htm

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

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

[101] IRM. *A Risk Practitioners Guide to ISO 31000*: 2018. London: IRM 2018. www.theirm.org.

[102] HEINRICH, H .W. *Industrial Accident Prevention: A Scientific Approach*. New York, NY, US: McGraw-Hill 1931.

[103] LEES, F. P. *Loss Prevention in the Process Industry*, *Volumes 1-3.* Oxford: Butterworth-Heinemann 2001.

[104] PAUL SCHERRER INSTITUTE. *Database ENSAD.* Zuerich: Paul Scherrer Institute 2019.

[105] BURGHERR, P., HIRSCHBERG, S. A Comparative Analysis of Accident Risks in Fossil, Hydro, and Nuclear Energy Chains. *Human and Ecological Risk Assessment.* 14 (2008), 5, pp. 947-973.

[106] BURGHERR, P., ECKLE, P., HIRSCHBERG, S. Comparative Risk Assessment of Severe Accidents in the Energy Sector Based on the ENSAD database: 20 years of Experience. In: *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013.

[107] BIRD, F. E. , GERMAIN, G. L. *Damage Control.* New York: American Management Associations, Inc. 1966.

[108] GEYSEN, W. The Acceptance of Systemic Thinking in Various Fields of Technology and Consequences on Respective Safety Phylosophies. In: *Safety of Modern Systems. Congress Documentaion Saarbruecken 2001*. ISBN 3-8249-0659-7. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.

[109] https://www.novinky.cz/zahranicni/svet/clanek/zpráva-o-spadlem-indoneskem-boeingu-chyby-byly-v-konstrukci-v-udrzbe-i-u-posadky-40301291

[110] 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.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

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

ANNEX 1 - Critical Infrastructure Safety

The basic function of the State from its establishment has been provided the protection of the human society and public assets, which humans need for life and development. Today, that function is fulfilled by the public administration which according to the European Union should realize so-called good governance. The important role plays the critical infrastructures (Figure 1) protection. The critical infrastructure is a set of mutually interconnected networks, i.e. the systems of various sectors of human system (model of present world). Interconnections of systems mean the mutual dependence. Therefore, their behaviours are dependent on many factors internal or external, which have permanent or random occurrences and under their special combinations they cause emergent phenomena leading to the cascade failures of interconnected infrastructures (Figure 2) [2].

Figure 1. Selected objects of critical infrastructure; compiled by help of [1].

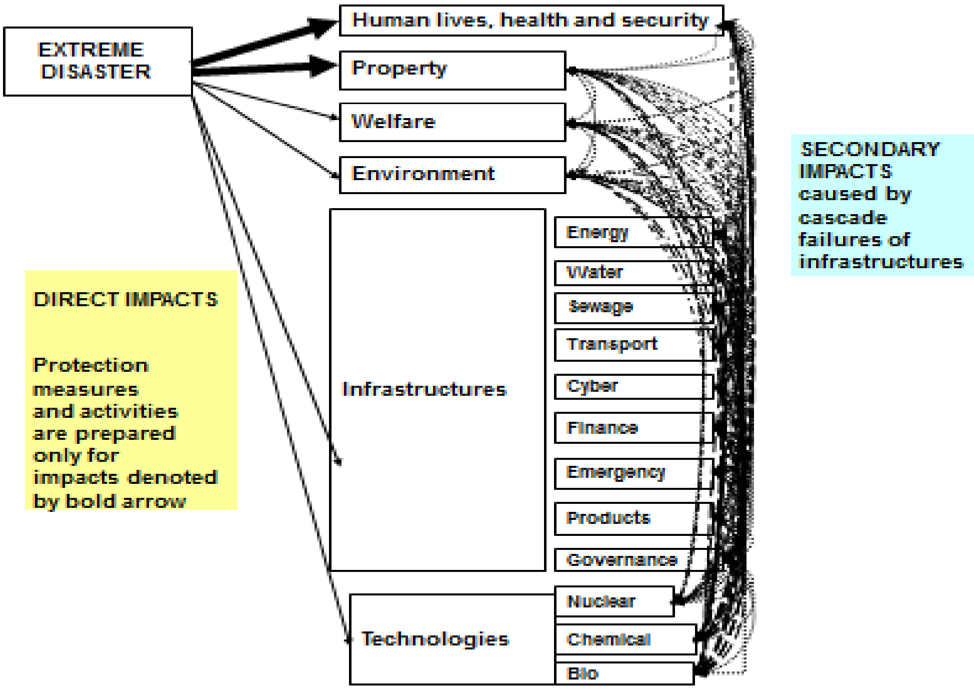

Figure 2. Impacts of beyond design (extreme, severe) disaster on human system. There are shown direct impacts on protected public assets and relevant secondary impacts caused by linkages and flows in human system and also cases for which protected measures exist in the Czech Republic (bold arrows)

Due to critical infrastructure complexity, its problems cannot be only solved theoretically by analytical methods, because they are very influenced by characteristics of regions in which they are located, which are multifarious. It is also caused by reality that each region has different possibilities for problems solution and these have been changing in time because the world and its parts have been dynamically varied [3,4].

From the viewpoint of system theory, the critical infrastructure as each other critical element is determined by help of criticality matrixes or by help of special methods of operational analysis [2]. The criticality matrix compares incommensurable items of infrastructure that are the vulnerability following from disasters and from properties of real territory, and the importance (relevance) for territory derived from quality of service of territory, Figure 3.

The vulnerability of infrastructure is the rate of the failure of infrastructure (i.e. the infrastructure stops working of will work incorrectly) in the time and space. This rate is possible to measure with e.g. normed overall (integral) risk by all the expected nature and other disasters in a given area or by the probability of the failures of infrastructure, which occur as a consequence of these disasters, to which also the inner problems of the infrastructure itself are included. Figure 2 shows that vulnerabilities of partial infrastructures induce cascades of phenomena that cause the failure of other infrastructures, i.e. it will be happen loss of services in affected territory, and secondary impacts on humans and property.

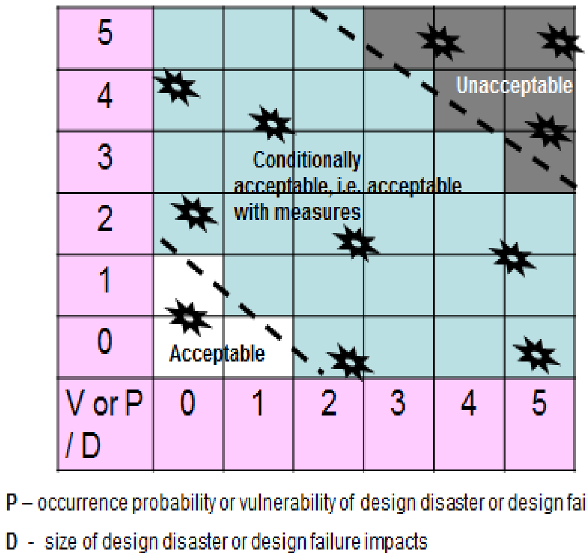

Figure 3. Criticality matrix of infrastructure, i.e. scaling the infrastructure vulnerability vs. infrastructure necessity at disasters.

The importance (relevance) of infrastructure in area is possible to measure by necessity of its products for human society in a given territory and the State.

The criticality rate is the result of the overall assessment of the impacts of infrastructure failure, i.e. of losses, damages and harms on the protected assets with reference to the duration of occurred emergency situation, which includes both, the time necessary for renovation of the infrastructure functionality when the direct damages arise and the time when the indirect damages, caused by the causal chain of impacts awakened by the infrastructure failure in area, are settled [4,5].

Human society needs the safe critical infrastructure; the safety includes its protection, function and reliability under conditions normal, abnormal and critical. Process model for critical infrastructure safety management is based on principles, methods and procedures of risk engineering in advance form (i.e. safety engineering) [2-4]. Its main unknowns are interdependences across critical infrastructure subsystems that are on several levels, namely physical, cyber, organisational and territorial. The interdependences also originate as consequence of disruption of finances, energies, information, material and flows induced by directed management activities [2-4].

The basic strategic approach for the critical infrastructure safety [2,3] is:

- nothing is absolutely safe,
- and elements and networks of critical infrastructure can fail sooner or later,

and therefore, it is necessary to establish the sophisticated regional safety management. The effective and efficient safety management needs to lean on the present knowledge and on their right assessment in a context that is valid for a given region [4]. It is necessary to distinguish the impacts according to their severity (Figure 3). Therefore, the basic role also belongs to the special research that at present solves:

- impacts of interdependences among the critical infrastructure subsystems and the human system subsystems on the basis of model “system of systems”,

- procedures and targets for ensuring the critical infrastructure safety from managerial view on the State level,
- possible distribution of tasks in the critical infrastructure safety management between the public and private sectors (it goes out of risks in a region with the aim to reach an optimal position for public and private sector),
- requirements on the personnel of critical infrastructure and technology owners,
- tasks of security components at defeating the emergency situations, induced by the extensive outage of critical infrastructure,
- general frame for critical infrastructure safety.

The interpretation of results for the given infrastructure (or for a set of infrastructures) is derived from the site position, the coordinates of which form obtained value of service measure (indeed measures of importance for region) and measures of vulnerability. If it belongs to the sector:

- „high vulnerability and high importance of service" the condition of infrastructure is precarious, i.e. critical for a given region and from the viewpoint of security and sustainable development the situation needs to be solved by back up and enhance of the given infrastructure,
- „lower vulnerability and lower importance of service" the condition of infrastructure is satisfactory and it is necessary from time to time to perform check-up of conditions in a given region,
- „high vulnerability and lower importance of service" the condition of infrastructure is conditionally satisfactory and it is necessary to ensure preparedness for sophisticated response in the case of infrastructure failure and the prevention to concentrate on preventive and mitigation measures leading to the reduction of infrastructure vulnerability against to possible disasters that can cause the failure,
- „lower vulnerability and high importance of service" the condition of infrastructure is conditionally satisfactory and it is necessary to ensure the preparedness for the sophisticated response in the case of infrastructure failure and the prevention to concentrate to reduction of criticality of infrastructure in a region or to build redundancies of being objects of infrastructure / technology / set of infrastructures.

For ensuring the critical infrastructure safety, there are on the basis of professional works, technical norms, technical standards and appropriate legal rules summarized in [2-4] used:

- special solutions in the land-use planning, sitting, designing, building, operating, maintenance, repair, upgrade, renovation, procedure changes and at putting out of operation – here it is used the concept of safety strategists, namely the emergency situations are always considered; they are not extraordinary, and therefore for the critical infrastructure safety support there are implemented the measures and activities, protection and security systems specially distributed in a site and backed up (today redundancy up to 4 x 100% is used),
- continuity plans for ensuring the critical infrastructure survive during the possible emergency situations – here it is used the concept of safety strategists, namely emergency situations are considered; they are not extraordinary, and therefore, for the critical infrastructure safety support they are implemented certain measures and activities, that ensure the conservation of minimal functionality of critical

infrastructure and the perspective for future, that after emergency situation stabilisation it would be possible to start and to renovate the critical infrastructure operation in a whole extent,

- crisis plan for a case in which all or the most of safety countermeasures fail owing to an extreme disaster size or owing to unforeseen combination of random phenomena that intensify disaster impacts. It contains protective and mitigating measures and activities for humans´ survival and for conservation of infrastructure state stabilisation which is necessary for interoperability needs in a given region.

For protection and development of humans, it is necessary above all to solve the problems of survival of humans at critical conditions. It is evident and logic that for human survival it is not necessary the function of all elements and nets of infrastructures that ensured comfort live and social welfare. According to estimations being in appropriate professional literature [2] about 27-30% of functional infrastructure elements conveniently distributed in the territory can ensure under critical conditions to ensure the human survival up to term of 180 days that is usually considered as time interval during which the qualified public administration is capable to find an alternative solution [2,5-7]. It of course puts demands of territory safety management that needs to know to regulate the humans´ behaviours and activities by way, so it may be possible to reach the conditions favourable for human survival. What restrictions, what rationing system is suitable, effective, having the promise of success; it is necessary to propose and to test in the practice.

As continuation to work [2], on the experiences from territory safety management [3-15] the method for critical infrastructure safety management for public administration needs as follows:

1. To identify elements and nets of infrastructures, which would be followed from the viewpoint of human system safety and development, to determine their location and to characterize them from the viewpoint importance for territory.
2. To determine elements and nets that are followed from the viewpoint of human system safety, which are under the public administration governance and those being out; i.e. they have private owners.
3. In the case of infrastructures that have insufficient capacity or are out of the public administration governance, the situation is more complicated, because public administration chances for influence of such infrastructures is not so simple. With regard to lessons from electricity blackouts (Table 1), this source of failure caused by increasing globalisation is not trivial. Therefore, it is necessary to find out, how reliable (from technical, finance, legal and managerial viewpoints) to ensure supply of services mediated by infrastructures from other territories, and for case of failure to prepare alternative solution for human survival from the higher regional unit management viewpoint. In the other case, it is necessary to solve problem of human survival at failure of followed infrastructures from own sources, i.e. as emergency up to critical situation.
4. To perform analysis and assessment of elements and networks of infrastructures, which are followed with regard to safety and development of human system, from the viewpoint of their function under normal, abnormal and critical conditions using the „All-Hazard-Approach“, i.e. to consider impacts of all possible disasters.
5. To perform analysis and evaluation of criticality of elements and nets of followed infrastructures in territory and to determine critical elements and nets of followed

infrastructures by help of decision matrix (Figure 3) rating their vulnerabilities (considered aspects – small number, function is violate at each higher disaster that have impacts on a given territory, no redundancies, no alternative solutions, repair and renovation take weeks till months etc.) and capability of service of territory (number of human affected by failure, damages caused by failure of technology or infrastructure exceeding the acceptable level (according to the UN the high critical condition is if damages exceed 10% of annual territory budget), number of victims that cannot be averted by measures of crisis plans).

Table 1. Expected impacts of long-term blackout of electricity (author summarizes results of 121 case studies collected for blackout) [2].

Asset	Expected impacts
Human lives and health	- loss of light, heating and air-conditioning, possibility to prepare meal, access to drinking water, liaison, connection and information sources, access to money (cash dispensers) and by those to purchase of foodstuffs etc., - loss of transport connection based on electric energy (fuel and petroleum pumping are based on electricity).
Property	- debased of meal in storage of foodstuffs and in refrigerators, - damages caused by fires that are induced by loss of function of regulative mechanisms on furnishings with open fire or on furnishings that burn down from other reason at regulation failure, - damages induced by transport and technological accident, - damages on technologies and another property caused by sudden loss of energy accompanied by dangerous fluids and gases, - damages on domestic animals caused by failure of service processes based on electric energy, - losses caused by consequences of production failure.
Environment	- increase of gaseous, liquid and teat emissions into environment as a consequence of loss of function of waste separators, disconnects, water cleaning plants, cooling devices etc., - impacts of technology accidents that occur as a consequence of electric supply disruption.

Security		- loss of furnishing the basic human needs (meal, hygiene, heat, connection with other people, isolation, lack of information etc.), - loss of medical care based on electricity supply (operation of advanced examinational instruments and installations), - loss of social care on children, old peoples, ill and handicapped people, - mental detriment at staying in closed space (lift, metro tube etc.), - origination of panic and chaos, - increase of frequency of occurrence of criminal actions and attacks etc.
Critical infrastructure		- loss of function of supplies, operations and services that are depending on electric energy and by those massive limitation of capability to put the situation under the control and to ensure the return into stable conditions and renovation, - cascading effects and domino impact in systems and networks, - origination of unexpected very unfavourable situations as a consequence of unforeseen phenomena.
	Energy supply system	- failure of heat supply from central sources (pumps and overpowering mechanisms), - failure of central gas supply as a consequence of loss of function of pumps and overpowering mechanisms based on electric energy, - failure of activities of storages (refrigerators, air-conditioning etc.), - outage of production, stores, physical and cyber networks and different services conditioned by electric energy supply.
	Water supply system	- failure of water supply into households, public facilities and operations (pumps, regulative mechanisms, control systems) and by that start of selected emergency conditions, - problems with regulation and maintenance of drinking and utilitarian water in tanks.
	Sewerage system	- loss of control of sewerage system, - putting out of operation of cleaning water plant, i.e. failure of waste water cleaning, - damage of pipes as a consequence of overfilling the pipes by waste waters and subsequent pollution of environment, subsoil liquefaction etc.

	Transport network	- failure of transport service based on electric energy (metro, trains, trams etc.), - outage of pumping fuel stations and mass stores of tractive material, - traffic jumps, traffic accidents and with time progress the lack of foodstuffs as a consequence of getting the traffic means into traffic jams etc. - failure of regulative mechanisms (lights on crossings, tunnels etc.), - lack of transport means that are not based on electric energy, e.g. busses substituting the metro).
	Communication and cyber systems	- loss of networks management during the time (after getting discharged redundant batteries), - loss of mutual connection (after getting discharged redundant batteries), - failure of cash dispenser safety protection, - failure of working performances controlled by cyber control systems, - loss of data put into information systems and databases, - loss of access to information put into media conditioned by operation of facilities droved by electric energy (after getting discharged redundant batteries).
	Bank and finance sectors	- loss of sector operation (banks, cash dispensers, insurance offices etc.) as a consequence of loss of access to data in information systems and in network and loss of function of controlled mechanisms, - loss on finance market as a consequence of sanctions provided for unrealised transactions and for wasted chances, - failure of cash dispensers and e-bank, - failure of service on clients, - loss of view on finance market as a consequence of loss of function of information means.

	Emergency services (Police, Fire Rescue Service, Medical Ser-	- loss of foreknowledge from information sources dependent on operation of equipment droved by electric current from central sources, - loss of connection based on systems dependent on operation of equipment droved by electric current from central sources, i.e. problems with population warning, - in health service loss of capability to perform surgeries and provide the care based on performance of equipment droved by electric current from central sources, - stopping the maintenance and repair works based on operation of equipment droved by electric current from central sources.
	Primary services (foodstuff supply, waste liquidation, social services, funereal services), industry	- stopping the production and sale of foodstuffs (dairies, bakeries, meat processing equipment, restaurant and workrooms preparing the food), - stopping the working plants for waste processing and liquidation, - in social service the loss of capability to provide the care dependent on operation of equipment droved by electric current from central sources, - stopping the store operation and the care on foodstuffs stored, - stopping the operation of schools, nursery schools and the other social facilities, - stopping the production of industrial plants, - stopping the agriculture plants dependent on operation of equipment droved by electric current from central sources, i.e. operation lines for feed production, equipment for drawing milk from cows etc.
	State and Regional Government	- loss of foreknowledge from information sources dependent on operation of equipment droved by electric current from central sources, - disruption of connection and loss of mutual communication and communication with citizens, - decrease of capability to manage the response to emergency and to sustain the situation in land under the control, - no chance to satisfy all tasks from responsibilities determined by legislation for state and regional governments dealing with good governance of public affairs, emergency management and crisis management.

	Public welfare	- stopping the marketing and services for citizens, - stopping the societal and cultural actions, - stopping the rehab and care personal services, - decrease of medical care service, - debase of medicaments and materials necessary for surgeries, - debase of foodstuffs and eatables, - decrease of level of hygiene.

6. To process territory continuity plan for case of failure of one or more followed technologies or infrastructures that are on the criticality analysis critical for a given territory. From it to derive the demands for territory management under critical conditions in critical technologies and infrastructures. By application What, If method to derive situation scenarios in a real territory and to process procedures for coping the possible situations in a given territory with aim to prevent victims and human injuries and to reduce expenses on response by the way that at response the loss prevention will be sophistically performed [8].
7. By legal and finance support of critical infrastructure owners to ensure the alternative technical solution. I.e. to assign commitment to process continuity plans and to verify their effectiveness from viewpoint of territory of both, the territory needs and the adjusted technical conditions of operation that ensure feasibility of measures of continuity plans under all possible conditions, i.e. it will be performed back-up of technical elements and nets, safety system installation, installation of passive and active security elements etc.
8. For high critical situations to propose special measures for crisis plans in which there are implanted e.g. rationing systems for inhabitants, obligations to performed determined activities in a designated extent, time and quality by all participated etc. To codify these special measures and to propose the way of their financing.

The effective and efficient safety management needs to lean on the present knowledge and on their right assessment in a context that is valid for a given region. Therefore, the basic role belongs to the determination:

- impacts of interdependences among the critical infrastructure subsystems and the human system subsystems on the systems system safety,
- procedures and targets for ensuring the critical infrastructure safety from managerial view on the level of the State,
- possible distribution of tasks in the critical infrastructure safety management between the public and private sectors (it goes out of risks in a region with the aim to reach an optimal position for public and private sector),
- requirements on the personnel of critical infrastructure and technology owners,
- tasks of safety components at defeating the emergency situations, induced by the extensive
- outage of critical infrastructure,

- general frame for critical infrastructure safety.

Regarding the core of critical infrastructure safety, the methodology for the critical infrastructure safety management (inherently containing the critical infrastructure protection) needs to lean on keeping the further given procedure [2-4], i.e. the management:

- is always directed to essential aspects,
- considers that the development needs to be sustainable and far-sighted (i.e. there must be balance among economy, technology, environment and social domain) and the primary target is the vulnerability reduction,
- pays attention to aspects that are the most vulnerable,
- defeats the emergency situations and during this it is directed to needs and priorities respecting that the basic priorities are the human protection and the protection of critical sources and systems on which the community existence depends,
- supports the prevention culture, programmes for the prevention and the preparedness to defeating the emergency situations and it insures that these items are included in the territory development programme,
- ensures that the citizens have right on rightful aid (remedial service) and that the aid is dispensed fairly and consistently without regard to economic or social circumstances and territorial location,
- ensures that citizens are included into the response management system not only as potential victims,
- ensures that citizens know emergency plans, content of plan of response to disasters, way of reaction and it's justifying at emergency situation origination etc.
- ensures that emergency management system is transparent also for citizens and it is adjusted to the local conditions,
- ensures that the emergency management system is legitimate and acceptable and it is based on systemic approach,
- ensures that the critical infrastructure safety (inherently including the critical infrastructure protection) is the matter of both, the private sector and the public sector.

For decision support system profiting the continuity of critical infrastructure at response and renovation of property in a territory affected by disaster is quite basic concept for determination of critical elements, critical processes, critical functions, critical infrastructures and critical technologies in a region. This concept leans on the risk analysis methodology and on actual terms of safety management in a region. It is possible to summarise that this process is determined by:

- way of assessment (acceptation) of risk, judgement and governance of risk,
- methodology of risk analysis and operation research,
- tools of safety management including tools of crisis management,
- specific particularities of cyber infrastructure,
- threat of conventional and unconventional terrorism,
- way of determination of priorities of system vulnerability,
- population awareness and by properties of post-modern society.

Reasons, why the critical elements, critical processes, critical functions critical infrastructures and critical technologies in the region are determined, are given by demand on reduction of risks in the human system from the view of its safety and development in the broadest sense. It is a matter of reduction of vulnerability (resilience increase) of key elements of human system that are basic for the society being on all levels of organisation and state administration, ensuring the functionality of life-giving systems and rational protection of critical infrastructure [2].

Regarding to the above given facts we can conclude that it is necessary to consider that the safe critical infrastructure we can ensure by two ways. The first one is more or less ideal and it consists in the construction of critical infrastructure on the “green field”, i.e. from the beginning we create safe systems system (each partial infrastructure is also resistant against to failure of the others). For this case we need criteria, limits, standards and norms for removing the interdependences and spots with inconvenient risk potential. The other way, more realistic, consists in an application of site-specific measures ensuring the inherent mitigation of impacts of each individual infrastructure failure on the other parts of critical infrastructure; e.g. the others start independently to work in an insular regime.

At critical infrastructure protection during the whole life cycle we need to consider external and internal hazards including the social hazards covering the human factor and especially those humans that cause the organising accidents.

Up to now we have been mostly concentrated to technical domain, the research of which shows that in practice it often comes up to failure of critical infrastructure from so called internal causes. Therefore, it is necessary to consider technical level, conditions and durability of a given infrastructure (35 – 40 years; max. 50 years), and the reality that through this time interval there need to be ensured the return ability of investments and that the human security needs not to be threaten. The longer time interval for which it is planned the infrastructure performance, the more modern (timeless) solution needs to be used. Each variant needs to be financially acceptable and needs to be also acceptable from the viewpoint of accessible technologies and of qualify human sources. At decision making on infrastructure renovation it is necessary to consider expenses and their return ability. Usually it is used a criterion that says “when expenses for infrastructure renovation do not return, e.g. after natural disaster to 10 years, so it is better to build new one”. From the public interest view it is necessary to remove or to limit interventions of politics into decision making on the infrastructure in the territory because their targets are usually another than long-term safety including the functionality and reliability of infrastructure in the region without regard to a politic party in a power.

In the frame of ensuring the human system security and sustainable development, it is necessary permanently to perform the measures that reduce an infrastructure criticality in a region. By building the new infrastructure it is necessary to ensure suitable number and regional distribution of objects of important infrastructure that are sufficiently resistant to expected disasters in a given region, and by that systematically to reduce infrastructure criticality.

Expenses for critical infrastructure are not only costs for its design and building but they also include costs for its operation, maintenance, repair and modernisation. Therefore, the risks connected with each infrastructure need also to include the risks from just given domains and the region management needs to know how to deal with them. It is necessary to assess the risks from disasters that can be denoted as financial market failure because with them it is connected failure of finances for maintenance, operation, repair and modernisation of objects of critical infrastructure. It is caused by the fact that critical infrastructure criticality increases if not good maintenance and good repair are performed (which cause the vulnerability increases).

Because nothing is out of defects, it needs to be prepared the plan for renovation of each infrastructure, namely critical one. This plan needs to be proactive, properly assessed; it needs to contain transparently managed risks and answers to questions as:

1. What to do?
2. How to do?
3. In which time interval?
4. Do not risks for other protected assets increase?

etc.

Because the critical infrastructure is a set of mutually connected (i.e. dependent) infrastructures, it is necessary to pay high attention to internal dependences study because analogy based on study of simple technological systems indicates that for critical infrastructure failure there are much more important links and flows that interconnect subsystems mutually. From the author's inspection experience it follows that couplings triggering the individual infrastructure failures and critical infrastructure failures often seem to be a random nature started by combination of several momentary weaknesses. For correct results we need in-depth analysis of sufficient number of critical infrastructure failures in connection with circumstances that were in their origin time.

The critical infrastructure protection means the ensuring of the continuity preservation of economic and social life of state and providing the response in case of danger or disruption of the basic conditions of life, services and systems, the continuity of which is fundamental for the State functioning. The main tasks in the field of critical infrastructure from a manager' point of view on the level of state are:

- to conduct the analyses of the vulnerability of critical infrastructure towards the possible disasters and attacks,
- to involve the legal, employee and citizens in the system of critical infrastructure protection,
- to elaborate a plan about removing of the biggest vulnerabilities of critical infrastructure,
- to elaborate a continuity plan for the individual critical infrastructures,
- to ensure the system of the detection of disasters and attacks (their possible scenarios) on critical infrastructure,
- to ensure the plan and realization of a response (its possible scenarios, means for its execution) to the functionality loss of critical infrastructure,
- to prepare the renovation plan for critical infrastructures,
- to provide education, awareness and collaboration of the public administration, private owners, employee and citizens in the issues of the critical infrastructure protection,

- to provide research and development for the needs of the functionality and protection of critical infrastructure,
- to provide intelligence analyses for the need of the critical infrastructure protection,
- to ensure the international cooperation at the protection of critical infrastructure,
- to ensure the legislative and financial demands for the need of the protection of critical infrastructure.
- the fact of the matter is that the major owners of critical infrastructure are the private subjects. Therefore, it is necessary that the critical infrastructure protection was an issue of both of the state and private sector. Until the effective mechanisms of management are not found, it will be necessary to use the tool of cooperation. We still have to look for a platform, on which the common way of funding the research will be sought and the way of funding the realization of relevant measures. If the State does not ensure the know-how, i.e. for example the monitoring of critical infrastructure, practice database for its operation and protection, units for its protection and relevant research, assessment and development of the approaches in protection and the relevant international cooperation, the private sector will cooperate with it because they don't have an easy access and possibilities of the creation of these tools [2].

For the ensuring of the reliable function of critical infrastructure, the relevant management [3,4] needs to respect the following principles:

- to always concentrate the activity on the fundamental aspects,
- to consider the early warning of citizens, employees, visitors before the up-coming disaster as a basis of success, as a basis of the reduction (or better the prevention) of the casualties,
- to set the target of management in a way that the sustainable development is ensured and that it would be far-sighted, i.e. so it would prefer the protection of lives, health and security of humans by paying the primary attention to the reduction of the system vulnerability,
- to always pay attention to the subsystem, which is the most vulnerable,
- to focus on the needs and priorities at dealing with emergency situations, while the basic priority is the protection of humans and the protection of critical sources and systems, on which the existence of society depends,
- to support the safety culture and to pay the maximal attention to prevention,
- to include the ensuring of preparedness on the emergency situations handling to the programme of the area development,
- citizens have the right to help (assistance service) and the help must be rendered consistently without regard to the economic and social circumstances and the area setting,
- citizens belong to the system of response to emergency situations not only as potential victims but also as the active elements of the response,
- to arrange, so as the citizens knew, what the crisis plans and response plans on emergency situation are and what do they bring about, what is their responsibility, how can they help in the prevention of the disaster or emergency situation emergence, how should they react and why, etc.,

- both, the system of safety management and crisis management need to be transparent even for citizens and must be adjusted to the local conditions,
- both, the system of safety management and crisis management need to have legitimacy, need to be sustainable and acceptable and need to be based on the systematic approach.

It is rational that it is not possible to include in the critical infrastructure all the facilities and all the networks of the observed sector, but only the priority ones. This priority facilities and networks are ensured specially. Each element of critical infrastructure consists of several different elements that are fundamental for its functionality. These are:

- the critical linear constructions,
- critical structures,
- critical machines and means of production,
- critical materials, critical parts of I& C,
- and critical personnel.

It is necessary to determine those elements and links that are important for the ensuring of the survival of humans and for the protection of their lives and health. This special protection requires finances, material sources and educated personnel. The analysis of real situations [5,16] often shows that the most important is usually the qualification of the top management, which controls the area and the personnel, which executes the measures in the area. Because the sources are limited everywhere, only the priority elements are being protected. It is also the truth that the easily attackable structures, based on the complicated technical accesses, are often replaced by the flexible and simple technical solutions that are able to work in the difficult conditions of critical situations [2].

Methods of the choice of priorities are usually very expensive. In practice, the method of multicriterial assessment, based on the evaluation of the vulnerability of the individual elements in system proved useful. At the selecting, the variants meaning the big vulnerability at individuals and little vulnerability at society are preferred [2]. At the assessment, it is necessary to classify rather complicated system of links, in which it is not possible to quantify the effect of the individual factors. Therefore, the total evaluation is relative and can be influenced by the subjective approach of single evaluators. On that account, it is worthwhile, if the evaluation is conducted by several mutually independent experts. The results of the evaluation count only for the evaluated system and it is not possible to compare them with results of the evaluation of different systems assessed separately. Therefore, in the USA and several other countries the expert methods are codified for these complicated evaluations, e.g. the multistage Delphi method [2].

At the determination of critical infrastructure and technologies in area, many factors need to be considered and between the most important; there are:

- operating and maintenance expenses for the lifetime period,
- preventive service and repair measures expenses during the response and renovation.

For each of the elements, the criteria need to be defined for the assessment of the physical conditions (respecting both the character of critical infrastructure and demands for the physical infrastructure), capacities and demands for services and for functionality assessment. On the basis of these criteria, the state of element is quantitatively assessed by a verbal scale containing levels from "very good" to "bad" and "critical (i.e. very bad)". The five-level scale is appropriate:

- very good state: the element is in a perfect physical state and it fulfils the intended functions. The expenses for maintenance are in accord with standards and norms. The element is new or recently renovated. Requirements for operation correspond to the project, there are no operational problems. The whole programme is being fulfilled efficiently and effectively,
- good state: the element is physically in a good state and it fulfils the intended functions. The expenses for maintenance are in accord with standards and norms but they are growing. The element is approximately in a half of its lifetime period. Requirements for operation correspond to the project, occasionally there are operational problems. The whole programme is being fulfilled acceptably,
- acceptable state: the element shows the signs of wastage and lower efficiency than it was intended. Some parts are already insufficient. The expenses for maintenance overcome the sums set by standards and norms and they are growing. It was used for a long time and it is in the last phase of its lifetime period. Requirements for operation correspond to the project, the operational problems are frequent. The whole programme is largely being fulfilled but the ineffective and inefficient ways of fulfilment occur,
- bad state: the element shows the significant signs of wastage and it fulfils the intended functions on a low standard. Many parts are insufficient. The expenses for maintenance overcome significantly the sums from standards and norms. The element comes near the end of its lifetime period. Requirements for operation overcame the data in project, the operational problems are apparent. The whole programme is being fulfilled only in a very limited range,
- critical state: the element is in a bad state and it does not work as it should be. There is a high probability of its failure. The expenses for maintenance are absolutely unacceptable in comparison with standards and norms; renovation is not cost-efficient. The replacement is necessary. Requirements for operation overcame significantly those in the project; operational problems are serious and continual. The set program is not being fulfilled.

For ensuring the continuity of critical infrastructure is considered [2-4] it is necessary the answer on the following questions is being sought:

1. What is the concept, on the basis of which the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area are determined?
2. Why the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area are determined in that way?
3. How is the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area executed in practice and to whom it serves?
4. Where is the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area used?

5. What are the requirements (data/equipment/intellectual potential etc.) necessary for the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area?
6. Who conducts the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area?
7. What are the advantages and disadvantages, weak points in the determination of critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area?

The existing concepts [2-14,16] show that the word “critical” is used either for the indication of the condition (state) of element / property / process etc. or with regard to the importance of element / property / process etc. for the area functioning. In the area of management, the word “critical”, e.g. in a phrase “critical disaster” means a disaster that is fundamental for the process of management functionality. In this concept, also the term “emergency management critical function” is used, which is applied in the response plans on emergency situations that are compiled in the USA [9].

On the basis of the critical analysis of information in professional literature, stated in [2-4], and experience from practice, the scale is proposed this way:

- level 0: the losses on infrastructure or technology do not have any impact on the safety and development of the area,
- level 1: the losses on infrastructure or technology have low impact on the safety and development of the area,
- level 2: the losses on infrastructure or technology have a medium impact on the safety and development of the area,
- level 3: the losses on infrastructure or technology have a significant impact on the safety and development of the area,
- level 4: the losses on infrastructure or technology have a serious impact on the safety and development of the area,
- level 5: the losses on infrastructure or technology have a fundamental impact on the safety and development of the area; they bring about its collapse.

In view of the area functionality, it is also necessary to assess the time period, in which it is possible to repair or replace the damaged infrastructure or technology. For the verification in practice, in [2-4], it is proposed to assess according to the following value scale:

- level 0: the damaged infrastructure or technology can be repaired or replaced in a time interval of 0-5 days,
- level 1: the damaged infrastructure or technology can be replaced in a time interval of 6-30 days,
- level 2: the damaged infrastructure or technology can be replaced in a time interval of 31-90 days,
- level 3: the damaged infrastructure or technology can be replaced in a time interval of 91-180 days,
- level 4: the damaged infrastructure or technology can be replaced in a time interval longer than 180 days,

- level 5: the damaged infrastructure or technology cannot be replaced.

It is necessary to get into practice the consciousness that the failure of critical infrastructures need to be evaluated at the risk assessment of enterprises / area / state, because the losses brought about by their failure deeply affect both the activity of every enterprise and its further existence. The systematic tool is the continuity plan that should be elaborated for the priority structures and networks of critical infrastructure [2-4]. I.e. it is necessary to introduce, both to the practice of public administration/ organizations and enterprises, the system:

- analysis of the impacts of the relevant natural and other disasters on enterprise / area / organization / structure / network etc.,
- assessment of risks and the ensuring of the sophisticated risk management,
- defining the management strategy of the continuity of both business and life in area, in case of unacceptable risks that remained, for some reasons, after the application of the measures of risk management,
- defining the emergency response and emergency activities for the case of natural or other disasters occurrence, i.e. if the realization of risks,
- processing and the implementation of the continuity plans of business and of crisis plans (for the case when the continuity plans fail),
- ensuring the consciousness and training of participants,
- actualisation and practising the existing plans,
- preparation and practising the crisis communication
- connection to offices and bodies outside of business/ structure/ network/ area etc.

The total investigation that is necessary to conduct for the ensuring of safety and development of critical infrastructure and technologies of organization / enterprise / structure / area / region / state/ community under the tools of safety management has also a general framework [2-4], which consists of the answers to the 14 following questions:

1. ***What natural or other disasters*** can appear in infrastructure location and what impacts do they have?
2. ***Where*** can natural and other disasters in infrastructure location appear and ***in what way*** are their impacts placed in infrastructure?
3. ***In which conditions*** can natural and other disasters in infrastructure location appear and what conditions can cause the escalation of their impacts?
4. ***How often*** can natural and other disasters in infrastructure location occur?
5. ***From what size*** do natural and other disasters in infrastructure location have undesirable and unacceptable impacts that cause damage on protected assets?
6. ***What is the maximal possible (expected) size of natural or another disaster*** in a given infrastructure location?
7. ***What damage*** on protected assets can cause the maximal possible or maximal expected natural or another disaster determined on the specified level of credibility in infrastructure location and what are its greatest possible impacts on infrastructure location and especially on the human society?

8. ***What we can do to avoid the undesirable and unacceptable impacts of natural or other disasters*** in infrastructure location in the section of land-use planning, designing, construction and operation of both public and private infrastructures or possibly in other fields, such as monitoring, inspection, education etc. so that we could avoid the disasters, which can be avoided or so that we avoided undesirable and unacceptable impacts, or at least, so that the undesirable and unacceptable impacts were reduced by preventive measures, preparedness, suitable response on a disaster and renovation, at which the prevention of losses and targets of suitable development will be respected?
9. ***What measures towards the real natural or other disasters*** in infrastructure location in the technical, organizational, financial, social, legal, educational and training section are desirable?
10. ***What unacceptable and remaining risks*** (i.e. the unacceptable impacts with the probability of occurrence higher that the set limit) with regard to possible natural or other disasters in infrastructure location remains, if the rational measures are executed that can the state/ public administration/ organization ensure in the technical, organizational, financial, social, legal, educational and training section?
11. ***In what way to execute the response on natural or another disaster***, what are its priorities, critical points etc.?
12. ***How to execute the renovation*** of infrastructure after natural or another disaster, so that the sources, forces and means were used rationally and so that other losses were prevented, the resistance increased to possible other disasters and the further development was started in infrastructure with all the elements of the human system (humans, environment, property, infrastructure, technologies etc.) that form it.
13. ***What form of the management*** and executing of the renovation of infrastructure and protected affaires after natural or another disaster in infrastructure is suitable and how it can be executed?
14. ***How to create the potential and financial reserve*** of infrastructure organization for the rational renovation of the infrastructure after natural or another disaster?

The up-stated results show that the domain of critical infrastructure is vivid and that there exist many unresolved problems. Therefore, it is necessary to continue the research and to prepare the application of its results into practice.

The gathered knowledge shows that the problem of critical infrastructure protection is a complex problem. The basic concept of protection needs to be based on the area planning and on the following activities. Because it is not possible to put out the entire existing critical infrastructure by a single act and replace it by the modern one, which fulfils all the ideal requirements and demands, many tasks exist also in the section of response. Therefore, these have an important place:

- special plans of response for critical infrastructure that are processed by the proprietor/ keeper/ holder of the licence of critical infrastructure,
- continuity plans from the side of the proprietor / keeper/ holder of the licence of critical infrastructure that ensure survival / minimal functionality of critical infrastructure for the fulfilment of the demands of area, the services of which depend on this infrastructure,

- continuity plans from the side of the guardian of area and the protector of the public welfare and public assets, that is the public administration ensuring the safety and development of area,
- crisis plans from the side of the proprietor / keeper / holder of the licence of critical infrastructure that ensures the survival of his business and will not cause unacceptable impacts on the protected assets, especially the human health and lives.

This means, that the basic concept of the critical infrastructure protection needs to be processed on the basis of the philosophy of safety management (integral / complex, i.e. not integrated / aggregated) and from it, we need to deduce the requirements for the response and renovation management for the case, where critical infrastructure is affected by unacceptable impacts caused by natural or another disaster. Only from this concept, it is possible to deduce the way of participation of executive units and their tasks.

Without enforcing the logical procedure and connection of activities, all the processional models created with the best intentions will represent the solution of the problem by a method ad hoc or differently defined as the method of the immediate idea/ impulse/ inspiration etc. All the publications cited in the lists of sources and that describes methods and principles suitable for the processional analysis conduction and for the seeking of critical links among the individual elements of critical infrastructure are based on causes, i.e. on disasters or inner links, that go across the individual infrastructures or across several infrastructures (electricity, informational technologies, anthropogenic management, financial flows) and not on the states, i.e. emergency situations.

The processional analysis is done in this way:

1. Concept of safety management is applied with the assessment of the whole process connected with the existence of critical infrastructure, i.e. the placement, designing, projecting, construction, operation and changes.
2. The processional model is compiled for the entire process connected with the critical infrastructure existence and only then, there are selected the models for the partial tasks or the very detailed models for the parts being a subject of a special interest are created.
3. The All Hazard Approach is used. This means that the protection against all the relevant disasters is ensured according to the laws, norms, standards and approaches of established practice for the area planning, choice of places, designing, projecting, construction, operation, repairs, maintenance, changes and renovations
4. The suitable methods of safety engineering are being used and that both for the determination of the risks' size and for the determination of the priority risks that contributes the most to the vulnerability of a given infrastructure.
5. Risks are understood as losses, damage and harms on the protected assets in a concrete area, i.e. not as numbers of no clear expression of the negative potential. At existing infrastructures, the existing risks are found out, the risks that contribute the most to the vulnerability of a given infrastructure are determined and to them the inner emergency plans, plans of continuity and possibly also the crisis plans are prepared.
6. For the critical links searching between the individual elements of critical infrastructure the decision matrixes are used the most often. Because the practice, time to

time, also requires the resolving of the special tasks, for which the application of the criticality matrix (i.e. the decision matrix for the critical infrastructure) is a too broad tool, the more precise methods are used, based on the theory of graphs; and that e.g. the method of critical path (so-called CPM), method of the optimization of resolving the problem in time and space (so-called PERT) and method of the modelling of processes in a network (so-called Petri net).

7. For the ensuring of the critical infrastructure functionality in time and space, the specific control lists are used. This method is common mostly in the public administration and the inspectorate bodies.

So that the state could fulfil its function i.e. to ensure the protection of protected affaires, for which he was created in antiquity, it has to have the functioning critical infrastructure and technologies. This means that in the normal, abnormal and critical conditions the basic elements, links and flows in the state system must be in function that are the basis of the state ability to reach stability at any situation and to start the further development [2-15]. This means that the protection of critical infrastructure needs to belong among the objects, which are the subjects both of the safety management of area and crisis management [2-4].

The Conference "Critical Infrastructure Protection and Resilience Europe" [17], which held in Milan on October 14 -16, 2019 included serious information, such as:

1. Today, in time of using the advanced automation and remote-control systems of technical devices, the critical infrastructure elements are attacking from space. A number of attacks were presented – e.g.:
   - an attack from a satellite on an equipment that checks employees when they arrive at work at a nuclear facility – the attack caused the employees could not enter in the facility, and therefore, shifts could not be replaced,
   - an attack from a satellite on the company's management centre caused the centre to be overwhelmed by a large number of queries and the subsequent interruption of the production process,
   - an attack from the satellite knocked out the equipment measuring water in the boiler and caused the boiler to overheat; etc.

   The term "new risks from space" began to be used. Additional risks are expected when quantum computers are introduced into widespread use – the number of cyberattacks will increase.

2. In the vast majority of reports, there was a recommendation on the need to use a systemic approach using multi-criteria methods based on DSS (decision support system) and finding that only a proactive approach can provide critical infrastructure protection. E.g.:
   - very popular are smart grids, and yet when put into practice, the risks associated with them are not addressed (there are no plans for response in case of their failure),
   - analyses of criticality of energy infrastructure revealed 28 critical elements for that need to be upgraded,
   - many risks are associated with the "Internet of thinks" network – interconnected chains are created where it is not easy to identify the originator of a malicious message (e.g. damage to the good will of the critical infrastructure manager),

and therefore, the principles for response plans for the implementation of cyber risks need to be drawn up.

3. In several reports there was a complaint about the poor-quality work of software processors – they do not give a deliberately thorough description of the software + instructions with corrective measures in case of failure – it was suspected that in this way software companies procure themselves work for the future. Even several specialists have stated that the same practice occurs in the design and construction of technical elements of critical infrastructure.
4. Based on an analysis of security events in critical infrastructure, the UK specialists have shown the following breakdown of causes:
   - cyber-attack 42%,
   - insider attack 28%,
   - terrorist attack 15%,
   - failure of human factor 14%,
   - natural disaster 1%,
   - and attack CBRNE 1%.
5. For increasing the safety and reliability of critical infrastructure, it is necessary in terms of references of critical infrastructure elements and whole to use the disaster sizes with a return period of more than 100 years. Another mistake is that during the design, it is only carried out the protection of elements and objects only for individual listed disasters, i.e. other some possible and unnamed disasters are not considered – it is necessary to use the application called "All Hazards". As critical infrastructure provides vital functions for humanity, care needs to be taken to ensure the continuity of operations, for which resilience is important. The idea of resilience is portrayed as the intersection of three circles, Figure 5. Resilience means continuously increasing both, the safety and the security while addressing potential conflicts that arise in practice; E.g. in present automobile industry [18].

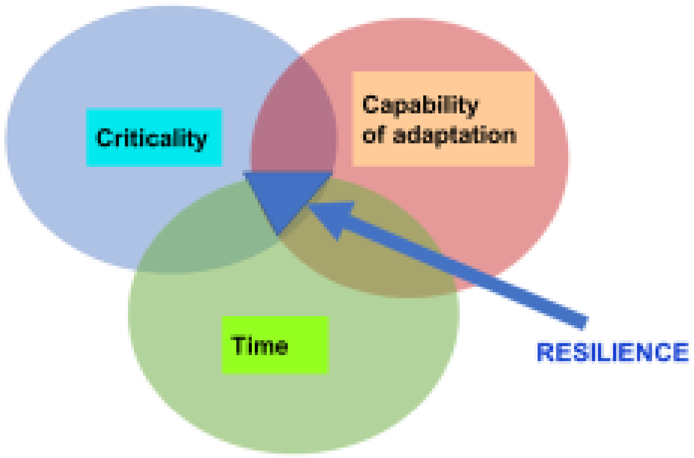

Fig. 4. Critical infrastructure parameters that are important for resilience.

References

[1] www.google.com

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

[3] 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

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

[5] HAYS, W. (ed.) *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.

[6] EMA. *Critical Infrastructure Emergency Risk Management and Assurance*. Handbook Emergency Management Australia, 2003, www.ema.gov.au

[7] FEMA. *Promoting Critical Infrastructure Protection by Emergency Managers and First Responders Nationwide*. Washington: FEMA 2005. www.usfa.fema.gov

[8] EU. *Green Paper on European Programme for Critical Intrastructure Protection*. Brussels: EU 17.11.2005, COM(2005) 576.

[9] US. *Critical Infrastructure Conception*. Washington: Government 2001.

[10] ESRIF: *ESRIF Final Report*. Brussels: EU 2009, 311p.

[11] US. *Federal Response Plan*. Washington: FEMA 1999, 304 p.

[12] US. *Emergency Management Plan*. State of Texas 2000.

[13] US. *The Tennessee Emergency Management Plan*. State of Tennessee 1995.

[14] FEMA: *Interim Assessment Guide for Hazardous Facilities*. Washington: FEMA 1999.

[15] GUSTIN, J. F. *Disaster: Recovery Planning: a Guide for Facility Managers*. ISBN: 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn: The Fairmont Press, Inc. 2002, 304p.

[16] CLOAKE, T., SIU, L. K. *Standardized Classification System to Assess the State and Condition of Infrastructure in Edmonton*. In: *Conference INFRA*, Montreal 2002.

[17] IACIPP. *Critical Infrastructure Protection Proceedings.* Milan: CIP Association 2019, www.cip-association.org

[18] KERTIS, T., PROCHÁZKOVÁ, D. Problems of Safety of Automation of Car Control (in Czech). In: *Řízení rizik procesů spojených s technickými díly*. ISBN 978-80-01-06656-0. Praha: ČVUT 2019, pp. 65-75. http://hdl.handle.net/10467/85587

ANNEX 2 – 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 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 the relation between safety and security; their often-discussed conflict is removed.

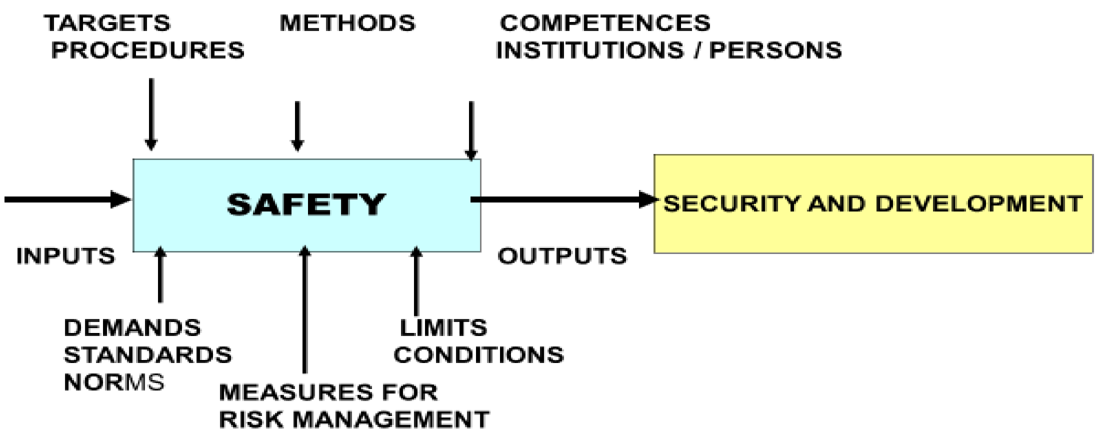

Figure 1. Process model for ensuring the security and development of entity.

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. 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 resource 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 3 – Risk sources of 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 it. 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.

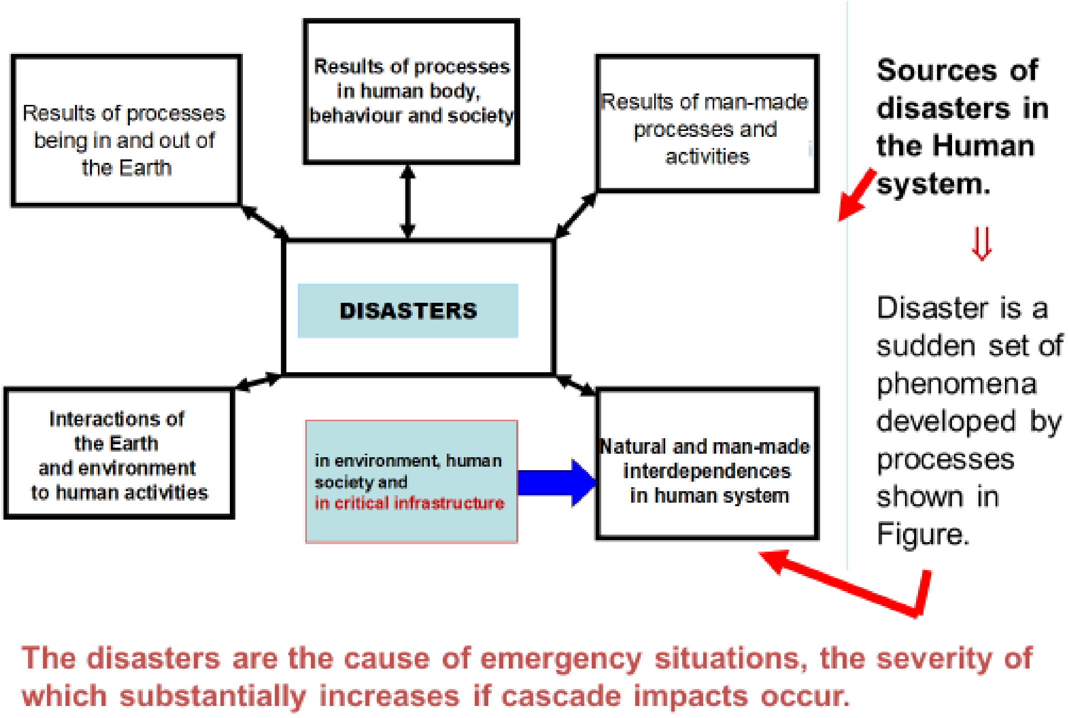

Figure 1. Sources of disasters.

The disaster list shows 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; 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 desirable.

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.

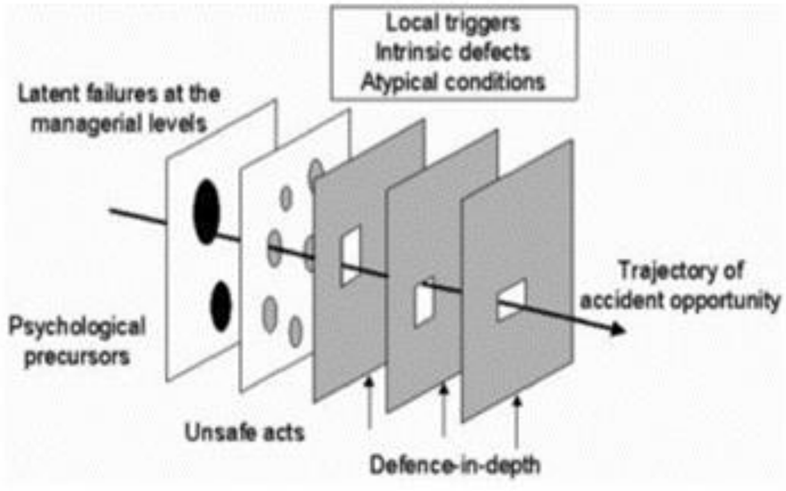

Figure 2. An organisational accident model indicating the basic barriers to prevent a crash and are created in the context of the management of the safety of a technical facility; processed according to [9].

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.

Titul:	Risk management at technical facilities operation
Autorský kolektiv:	Doc. RNDr. Dana Procházková, DrSc., RNDr. Jan Procházka, Ph.D.
Recenzenti:	Doc. Ing. Viktor Kreibich, CSc. Doc. Ing. Branislav Lacko, CSc.
Vydavatel:	DSPACE ČVUT v Praze
Forma vydání:	Open Access - dspace.cvut.cz
Počet stránek:	238
Rok vydání:	2020

ISBN 978-80-01-06713-0