ANALYSIS, MANAGEMENT AND TRADE-OFF WITH RISKS OF TECHNICAL FACILITIES

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:
Prof. RNDr. Šárka Mayerová, Ph.D.
Doc. Ing. Alena Oulehlová, Ph.D.

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

ISBN 978-80-01-06714-7

https://doi.org/10.14311/BK.9788001067147

CONTENT

LIST OF ABBREVIATIONS

Abbreviation	Title
ALARA	As Low as Reasonably Achievable
ALARP	As Low as Reasonably Practicable
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
CBA	Cost Benefit Analysis
CR	Czech Republic
ČVUT	Czech Technical University
DSS	Decision Support System
ESRA	European Safety and Reliability Association
ESREL	European Safety and Reliability Conference
EU	European Union
FEMA	Federal Emergency Management Agency
FMEA	Failure Mode and Effects Analysis
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information technologies
NEA	Nuclear Energy Agency
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
OECD	Organisation for Economic Co-operation and Development
OSH	Occupational Safety and Health
PC	Personal Computer
SIL	Safety Integrity Level
SMS	Safety Management System
SoS	System of Systems
TQM	Total Quality Management
UN	United Nations

ABSTRACT

Submitted work “Analysis, management and trade-off with risk of technical facilities“ deals with the all type of risks associated with the technical facilities, particularly with the complex ones, with aim to ensure their safety. It demonstrates the ways of work with risks at phase of identification, analysis, assessment, management and putting under control aimed to the safety of both, the technical facilities and their surroundings (i.e. their mutual coincidence), and simultaneously respecting the current knowledge that the risks are locally and time-specific.

The safety is understood as a property on the level of the whole technical facility, which is determined by the quality of the file of anthropogenic measures and activities aimed at the safe technical facility, and even at its critical conditions. Therefore, at safety make up, the publication proposes to monitor both, the public assets and the technical facility´ assets, and together to consider the diversity of their physical natures, vulnerabilities, and the constituent changes over time; which means continuously to solve emerging conflicts.

Since the risks are the causes of the technical facilities accidents and failures in the processes of the sitting, construction, operation and decommissioning with regard to public assets, so the considered goal is ensuring the coexistence of technical facility with the surroundings, i.e. with public assets, which include the human lives, health and security, property, public welfare, the environment, other technical facilities and technologies, and infrastructures.

With regard to the dynamic development of the world, it is necessary to monitor all priority risks and to implement their management and bringing under the control with regard to improving or at least maintaining each technical facility safety at an acceptable level. This means to make up the safety management system (SMS) of each technical facility that respect at work with risks the variability of the world in time and space, i.e. normal, abnormal, critical, and in some cases of technical facilities (e.g., highly dangerous chemical or nuclear facilities) also extreme conditions. The SMS needs to contain the procedures for the control and management of critical situations.
The publication “Analysis, management and trade-off with risks of technical facilities“ summarizes problems and shows methods and procedures for their solution based on system concept and present findings and experiences from practice obtained by detail research. It summarizes the 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”; detail data and results are in the Czech publication and in the CVUT archives. 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 engineering methodology; risk; safety; risk sources; risk management; integral risk; risk acceptability.

1. INTRODUCTION

The technical facilities belong to human system that is a model of our world. The security and development of whole human system and its components, i.e. also the technical facilities, are disturbed by disasters, i.e. internal and external phenomena that lead or can lead to damages, harms and losses of given entities assets. Each technical facility safety is affected by both:

- the processes, actions and phenomena that are under way in human system, technical facilities, human society, environment, planet system, galaxy and other higher systems,
- the humans´ behaviour and human management acts.

Therefore, we need to negotiate with risks of different origin and kinds.

The aim of human effort is to ensure the humans lives, health and security. Therefore, on the basis of current knowledge summarized in books from ESREL conferences [1-11] and in books [12-16], the humans need to take care on basic public assets (i.e. the human lives, health and security; the property and public welfare; the environment; infrastructures and technologies). The basic assets of human system (public assets) have system nature [12] and are shown in Figure 1.

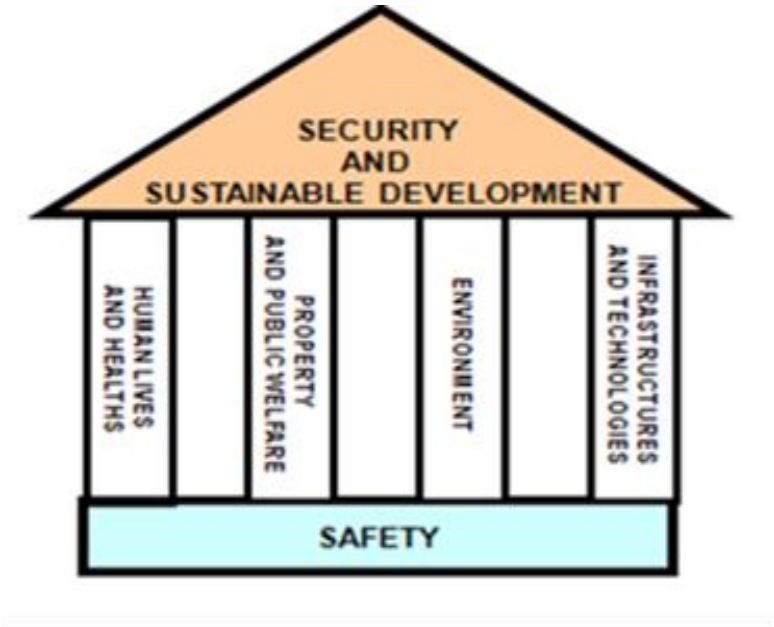

Figure 1. Human system public assets.

Due to world and its entities characters, we use the system (holistic) thinking, the typical feature of which is the focusing on the whole and its accessors. The accessors are elements, linkages and couplings among the elements. The characteristics of a system thinking [14] are to:

- see both, the whole and the details at the same time,

- focus on the dynamics of processes,
- pay attention to relations, associations and interactions,
- consider the roles of feedbacks,
- consider the relativity of possible situations,
- think in a long-term way.

According to system concept [16], each whole (entity) includes the elements, links and couplings among the elements which have different character, and therefore, accent needs to be put on:

- study of the interactions and associations,
- non-linear thinking, interactions,
- inductions,
- feedbacks,
- experiments or realistic simulations.

Findings and experiments show that feedbacks cause non-linearity's in the system behaviour that are not predictable, and therefore, it is not possible to use the common prognostic methods for the identification of the possible conditions of a system [13,15].

Since, in the world it is not only a human society, but also other systems (and all systems are open), which are not subordinated to the human society. Therefore, the conflicts originate, e.g.: human vs. environment; technique vs. environment; human vs. technique; human vs. human; human vs. IT; technique vs. IT; and IT vs. IT. Therefore, the co-existence of basic systems that represent environment, human society and technology is the main target of anthropogenic management [1-15].

Because the human kind grounds on its education, thus in the present case, it needs to realize the actions and management based on knowledge, which accumulated the science and historical experience of life. This shows that there is a limit for the human activities, which cannot be exceeded, in order to prevent the destruction of mankind. The starting point is to accept the need for the co-existence of several systems and search conditions and ways of controlling it [12-15].

The coexistence and sustainable development strategy are comparable with other systems of values, which do not have the final form (e.g. the system of human rights and freedoms). It leads to ensure the highest attainable quality of life for the present generation and to create conditions for quality of life of future generations, even knowing that the ideas of the quality of life of future generations need not to be compared with our visions [12].

The humans knew during their development that they need for live the nature and a number of other assets. They understood that:

- the great values for them are their existence, security and development potential,
- and that the safe world has been disturbed by harmful phenomena (disasters).

From the evaluation of credible data, knowledge and experience, e.g. [1-17], it follows that the human knowledge and capabilities are:

- small to avert disasters, which are the manifestation of the evolution of the planetary system of the Earth,
- adequate to mitigate the impact of disasters, which are the manifestation of the evolution of the planetary system of the Earth,
- sufficient to prevent disasters that are associated with the activities of humans and with the development of human society.

To use the knowledge and skills the humans consciously create a comprehensive system tool, which is called the ***safety management*** and also specific targeted tools to deal with emergency and critical situations, which are emergency management and crisis management; in the professional literature they can be found, as well as other tools such as disaster management [17]. This tool is based on the targeted work with risks, which would be integral part of entity management [15].

For qualified management of entities, according to the present knowledge and experience, it is considered a strategic safety management of entities in the dynamically varying world, which means the skilled management of disasters [17], which is based on the approach of "All Hazard Approach" that was introduced by FEMA in 1996 [18] and it is used by EU and OCHA [12,17]. For the Europe it was delimited by research in the FOCUS project, the result of which are in books [13,19-21].

For human life quality, it is necessary both, the co-existence of mentioned essential systems and the provision of humans needs that are in hierarchical Maslow pyramid [22] (needs are: physiological; security; social; sociable assertiveness, self-realization).

Having regard to the complexity (Figure 2), multidisciplinary and the interdisciplinary nature of the solved problems, understanding the situation and finding the solutions for the humans´ security and development, the technical facilities safety is based on the systems approach, a comprehensive concept of safety and proactive way of safety management, because the human space (our Planet and its surrounding) is dynamic, i.e. it is variable in the space and time in particulars and as well as in a whole [12,13].

From the critical analysis of emergency up to critical situations in human system, in detail described in [12,17], it follows that the cause of critical situations are natural, technological and other disasters. To other disasters, they belong the organisational accidents that are connected with a human factor [12-14]; especially with the phenomena as:

- low respect to knowledge and engineering experiences,
- low professional level of management,
- corruption,
- abuse of power,
- suppress of the public interest.

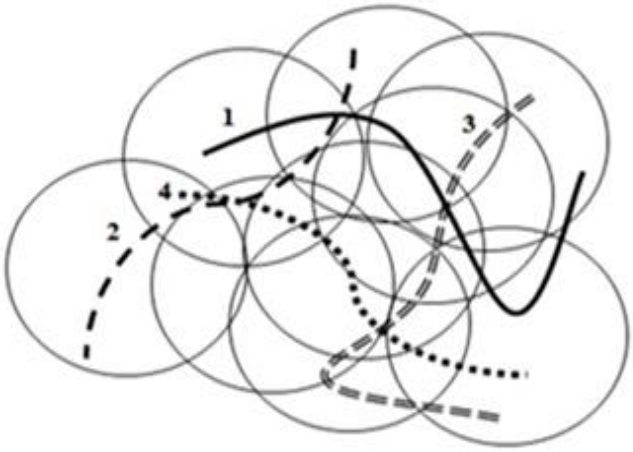

Figure 2. Scheme of complex systems - 1, 2,… are the processes being under way in mentioned entity.

On the basis of current knowledge, the reasonable humans negotiate with the risks so that systematically carry out the preventive, mitigating, reactive, and recovery measures and activities in order to they might avert unacceptable impacts that cause the losses to both, the humans and the public assets that are inevitable for human society existence and development [12-14,19-21]; scheme is in Figure 3. Because of their knowledge, capabilities and possibilities are limited in the subject area, so on the basis of the experience they constantly prepare to cope with the situations, which are caused by an occurrence of a variety of phenomena, with harmful impacts on them and on the vital assets.

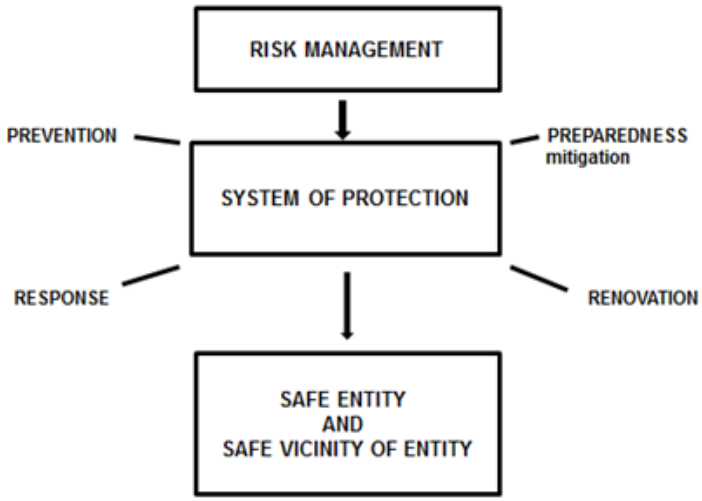

Figure 3. Time sequence of phases in which the measures and activities for defending the risks are performed.

From reason of human development, it is necessary to apply the strategic management to each important entity (State, territory, object, organisation) directed to the long-term sustainability, which on our knowledge means the targeted work with risks of all

kinds. Therefore, ***the risk is now the dominate concept of our society.*** According to findings summarized in [1-16,19-21], the risk is connected with complex phenomena, conditions or factors:

- uncertain natural hazards, technological accidents and other disasters [12],
- uncertainties that are in science and technology findings and their action on health and quality of human life, human vulnerability and lack of consistent explanation of living sorrows and their sense
- and the human play with fear, chances and opportunities.

Due to complexity of human system and all public assets including the technical facilities, the humans need to consider at management:

- system interconnections of living assets,
- mutual interconnections among many open systems,
- and development dynamics vs. human ways of problem solutions.

The human hierarchy of problem solution has the levels shown in Figure 4 [13].

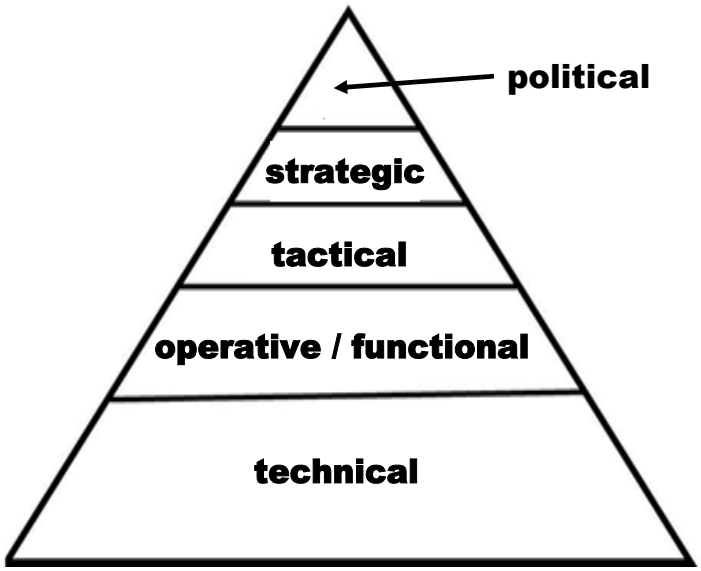

Figure 4. Levels of problem solving used in theory and practice.

For general aims reaching, the goals on all levels need to be targeted in same direction and to be co-ordinated [12-15]. With regard to different development of structural open systems in the world, there is necessary to expect the conflicts, and therefore, the human needs to monitor the changes in the world and to be prepared the originated conflicts to solve in time [13,14].

Basic tools of human society for provision of needs [12,14] are correct control of human society, which is divided in to:

- management of safety and development,
- emergency management,
- crisis management,

(Figure 5) and good asserting the knowledge and exercises at negotiation with risks directed to public interest [12,13]. In this respect, the big roles prove to managerial and engineering disciplines that have capability to ensure the human existence, human security and the potential for human development.

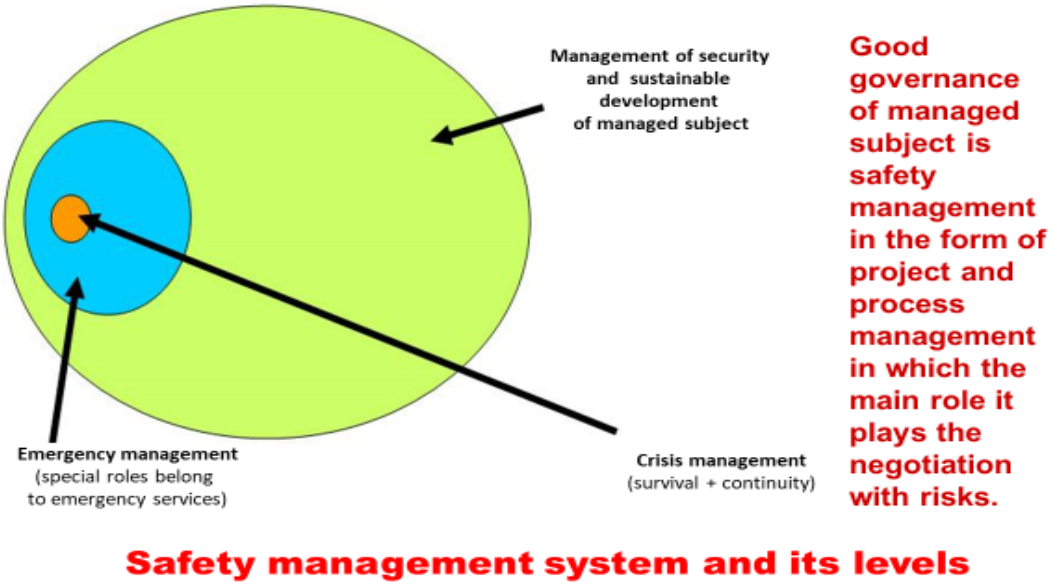

Figure 5. Three levels of the State (i.e. human system) management.

To ensure the human lives, health and security, therefore, on the basis of current knowledge [12], the humans need to:

- take care on basic public assets (Figure 1). Technical facilities belong to essential public assets because they: provide products and services that improve the human lives; contribute to employment, technical education, energy self-sufficiency and competitiveness; and create a background in response to critical situations (each response needs energy, technical resources, finance, transportation, material, etc.),
- adapt their behaviour so it might be preserved the coexistence of essential systems (environmental, social, and technological) that are inevitable for the existence and life of humans, i.e. for safe human system that has the nature of the SoS (Figure 2); i.e. an open system of systems, which is a collection of series of mutually penetrating open systems. Interfaces are the source of internal dependencies, called the interdependences, namely by those that are required and as well as by those that are troublesome; and some of which take effect only under specific conditions.

Therefore, in engineering sciences, the important role is connected with factor called “limits and conditions” [13-15].

For reaching the given target, the humans use the tool "management". Management is a very broad term and it means "to have something under direction, to control, to manage, to regulate, to govern". From the time of Mr. Taylor, the scientific management founder [23], and his successor Mr. Fayol [24], the basic management functions have not changed. The executors of the management are the humans, who lead the given entity to the prosperity and efficiency. The fact in question also applies to the semi-automatic and automatic control, because their algorithms are created by humans. In the real world, the humans may well drive their behaviour and the behaviour of the technical products and facilities that they created, when they perceive the limitations of their capabilities and skills, and with regard to it, they propose and implement their measures and activities.

This means that humans at all levels of management need to adhere to certain safety culture [13,14]. The effective safety culture is the fundamental element of safety management. It reflects the safety concept and it goes out from values, attitudes and manners of top management workers and from their communication with all involved persons. It is obvious obligation to participate in solving the problems of safety and it promotes so all involved persons perform safely and so they observe the appropriate legal rules, standards and norms. The safety culture rules need to be incorporated into all activities in each entity and in each territory. Their ground is not the concentration to punishment of malefactors / originators of faults, but the lessons learned from the mistakes and the introduction of such corrective measures so mistakes might not repeat, or rather their occurrence frequency might be distinctly reduced.

The safety culture level is the quantity that cannot be directly and exactly measured, but for all that it has fundamental influence on workers´ behaviours, the management style and the technology level. The definition of weak and strong features in individual parts of safety is important for safety culture level. The comparison of time series of investigations permits to evaluate the effectiveness of corrective measures.

This book is the result of project „Řízení rizik a bezpečnost složitých technologických objektů (Management of risks and safety of complex technical facilities - RIRIZIBE)“ CZ.02.2.69/0.0/0.0/16 _018/0002649. It summarizes the most important present facts on: risk theory; risk sources in human system; risk sources in technical systems, i.e. facilities, technologies, processes and technical fittings; causes of diagonal (cross-sectional) risks; work with risks in engineering disciplines – methods, procedures and tools; hazard determination; methods of risk engineering used in simple and complex technical systems; risk management for support reliability, security and safety; principles for risk management; responsibilities for risk management; risk management in time; risk engineering; risk settlement – measures; decision support system for risk management of technical facilities; and risk management plan. Detail data and lists of all used references are in book [15] and in given cited sources.

For recommendations and comments authors thank to reviewers Prof. RNDr. Šárka Mayerová, Ph.D. and Assoc. Prof. Alena Oulehlova, Ph.D. For working condition creating the authors thank to the Czech Technical University in Prague, the Faculty of Mechanical Engineering, namely to Department of Energy.

2. TERMS FOR MANAGEMENT AND TRADE-OFF WITH RISKS AND OTHER IMPORTANT MATTERS CONNECTED WITH TECHNICAL FACILITIES

Present terms go out from the UN concept [25] and are systematically used in the most world publications; e.g. [1-16,19-21]. Primary terms connected with technical facilities risks and safety are the following:

1. ***Technical facility*** is the result of engineering process, which ensures products and services supporting the human lives and development.
2. ***Fundamental State function*** is the State mission in ensuring the protection of public interests (assets) and their permanent sustainable development.
3. ***Human system*** is the smallest space for life of humans and human society. It is represented by a territory including the human society, the assets of which are in security and they have a certain potential for sustainable development.
4. ***Basic human system assets*** (protected interests or fundamental interests of the State) are items that are protected with priority (in the CR and in the most of the other countries there are human lives and health, property, welfare, environment, existence of the State and recently critical infrastructures and technologies) and there is pursued the care to their development.
5. ***Critical infrastructure*** is the set of interconnected physical, cybernetic and organizational (service) systems, that are necessary for ensuring the support and protection of human lives and health, property, minimum function of economy and administration of the State.
6. ***System of systems*** (systems system – abbreviation SoS) is a system that consists of several open systems of different nature and various locations, which are interconnected to ensure certain operations and activities. It should be aware that, when monitoring the SoS behaviour for the needs of some tasks, we need to address very detailed division of systems in several levels, and in other it will sufficient just division at the top level (the regional, municipal, local, etc.). Interfaces of systems, of course cause the interdependences. From this fact, it does not generally hold, that the SoS safety is the aggregation of safeties of partial systems (subsystems); it needs to respect as well as the cross-sectional risks caused by links and flows across the SoS and with the surroundings. This fact means that today used the integrated safety, which is based on integrated risk management, is not fully in place for those facilities [14,15]. Therefore, it needs to be gradually replaced by the integral safety, which also relies on the management of cross-sectional risks.
7. ***Safe space*** is a space in which on one hand the assets are protected against all kinds of internal and external devastative phenomena (disasters) including those connecting with the human factor, and which on the other hand does not

simultaneously threaten its vicinity. It is represented by safe open dynamically variable system of systems (SoS), i.e. several overlapping systems.

8. ***Security*** is a condition of system at which the occurrence of harm or loss on system assets (protected interests) has an acceptable probability (it is almost sure that harm and loss do not origin). To this there is also belonged a certain sure stability of system in time and space, i.e. a sustainable development in time and space which means that the system is protected against to internal and external disasters. It is a forming the sense of safety, safe feeling, certainty, ensuring the public welfare, permanent development of sound environment and reliable operation of technical (physical and cyber) facilities. In this view, it is necessary to understand that human is also system.

9. ***Safety*** is a set of human measures and activities for ensuring the security and sustainable development of certain system and its assets. Its measure is effectiveness size of appropriate measures and activities at ensuring the system assets security and sustainable development. By other words it is the capability of system to precede critical conditions of the system (active safety uses the elements of management; passive safety utilizes protective physical elements) and at their occurrence not to threaten the existence of neither itself nor its surroundings. From the engineering viewpoint [13,15], the system safety means the system integrity, reliability and functionality.

10. ***Secured system*** is a system, in which the system and its assets with an acceptable probability are not threatened by disasters, the origins of which are inside and outside of system, including the human factor.

11. ***Safe system*** is a system, in which with an acceptable probability the system and its assets are not threatened by disasters, the origin of which are inside and outside of system, including the human factor, and the system at its critical conditions does not threaten itself and its vicinity.

12. ***Danger*** is a condition / situation at which it originates or can originate detriment and damage on assets.

13. ***Harm / damage*** is a detriment on human life and health, property, environment and human society expressed in money.

14. ***Impact*** is an adverse effect / influence of phenomenon in a given place and time on assets.

15. ***Inadmissible (unacceptable) impact*** is an impact that causes or can cause unacceptable damage / harm on one or more assets.

16. ***Disaster*** is a phenomenon that leads or can lead to damages and harms on assets of the State or other followed entity (i.e. phenomenon which leads or can lead to impacts on protected assets of the State or other followed entity). From the view of cybernetics, the disaster is one of the possible conditions of system including the human society and environment, which leads or can lead to damages / harms on one or more assets of the State. Prominent World and European finance houses (World Bank, European Bank, UN authorities etc.) use the term „disaster “for phenomena with small number of victims; if number of victims is greater (usually more than 25), they use term „catastrophe “. Present knowledge

shows that due to human targeted effort, some phenomena have disastrous potential only from some size [15-17,20].

17. ***Domino effect*** is a cumulative effect produced when one accident or failure sets off a chain of similar phenomena which lead either to further accident or failure origination or to original impacts escalation.

18. ***Hazard*** is a set of maximum disaster impacts that are expected in a given place in specified time interval with a certain probability. According to technical norms and standards, the normative hazard is determined by identified size of disaster (so called design disaster). Hazard expresses the disaster potential to cause at origin losses, damages and harms on assets in a given site; details on its determination are in Annex 1.

19. ***Risk*** is a probable size of non-demanded and unacceptable impacts (losses, harms and detriment) of disasters with size of normative hazard on system assets or subsystems in a given time interval (e.g. 1 year) in a given site, i.e. it is always site specific.

    Simply, risk ***R*** depends partly on disaster size (in risk engineering on hazard ***H***) and partly on assets vulnerabilities ***V***. Simply it holds relation:

    $$R = H \times V.$$

    Further relations valid for risk management and engineering are in next chapters.

20. ***Threat*** is a measure of occurrence of attack (terrorist or military) in a given place. It is a probability that it originates or it can originate an event or set of events, quite different from those demanded (originally supposed) condition or development of protected assets of the State or other followed entity from the viewpoint of their integrity and function. It is determined by capability of attacker, vulnerability of protected assets of the State or other followed entity and by attacker intent.

21. ***Vulnerability*** is a sensitivity of asset (system) to impacts of disaster / threat. It is a predisposition of asset to harm / damage origination. It is a measure of system inability to react to a disaster occurrence. It is inherent attribute of the system and it is dynamically variable. Our knowledge and experience show that in the scale of time and space, certain aspects dominate at different points in time and at different locations.

    In behaviour of technical facility in the dynamic world in which there are phenomena of different kind and different sizes, which can damage facility, there are asserted both, the certain system properties and the certain protected assets properties. The vulnerability is understood as susceptibility to damage or loss, and it is variable in time and space. Its manifestation depends on both, the size of the disaster and the condition of the system [16]. Vulnerability of system responds to the question "why the system reacts to the way?". There are three different vulnerabilities: typological, specific and general. Typological vulnerability relates to the local socio-technological conditions in the entity before the disaster occurrence. For its mastery, it is assessed the

level of preparedness, i.e. the capability to withstand the impacts of the disaster, etc. Specific vulnerability refers to sources of social units (families, groups, companies, institutions), i.e. to a social adaptability. It is a rate of the organizational, economic, technological and cultural resources that determine the capability of followed social units to optimize their behaviour under stress (critical) situations. Specific vulnerability also affects the typological vulnerability in the phase prior to the disaster occurrence. General vulnerability expresses the level of socio-economic, organisational and technological development of human (social) system.

22. ***Scenario*** (model) of disaster is a set of isolated and interconnected disaster impacts in space and time that causes or can cause the given disaster in definite site, i.e. time sequence of events presented disaster impacts in entity.

23. ***Emergency situation*** is a situation caused by disaster origination. Usually, it is classified into 5 categories (0 - 5) that for simplicity are denoted by colours (uppermost by sequence of colours – green, yellow, orange, red) [16].

24. ***Disaster assessment, hazard assessment and risk assessment in a given territory, site, time interval*** are the risk engineering methods.

25. ***Human factor*** is the set of human properties, which determine the human behaviour that marks at decision-making in different situation. The human reactions have the form of unconditioned reactions, as "automatic", inherent ways of reaction to inputs (e.g. the wince at an unpleasant input), facultative reactions (e.g. in the form of habits), or purposeful action controlled by will. In engineering disciplines, the human factor is the aggregation of human properties, capabilities, experiences that have in a given situation influence on the safety, productivity, effectivity and reliability of system. At ensuring the complex entity safety with an accent to the protection of persons and properties, it is necessary to achive the right decision or at least such decision that will not lead sooner or later to destruction, namely in case of a decision under the stress. The decision in this concept becomes the social process. In this process, there are the human intellect and certain inherent (natural, tacit) human knowledge and skills put forward. In the forefront, they manifest the human properties as:

    - responsible approach to a problem and the results of its solution regarding the public or other assets,
    - moral properties as a discernment, sense for commitment and consistency,
    - the ability: to analyse the problem or situation; to take an attitude for creative approach to the problem solution; to know the art of the foreseen of the further development, to use analogy etc.,
    - and also the capability to use experiences and social skills that enable to regulate the activity and his / her behaviour or the behaviour of the subordinate humans.

26. ***Safety culture*** is the set of rules in entity directed to entity safety that all entity persons meet and respect.

27. ***Safety management system*** is a management of system directed to safety, the product of which is security and sustainable development of system and public assets. It is the basic part of the Information & Control system of each entity.

28. ***Human system safety management*** is a management of human system directed to human system safety the product of which is security and sustainable development of all public assets.

The causal relationship „disaster – emergency“ is shown in Figure 6. Management phases, as prevention and renovation are directed to causes, and management phases preparedness and response are directed to consequences.

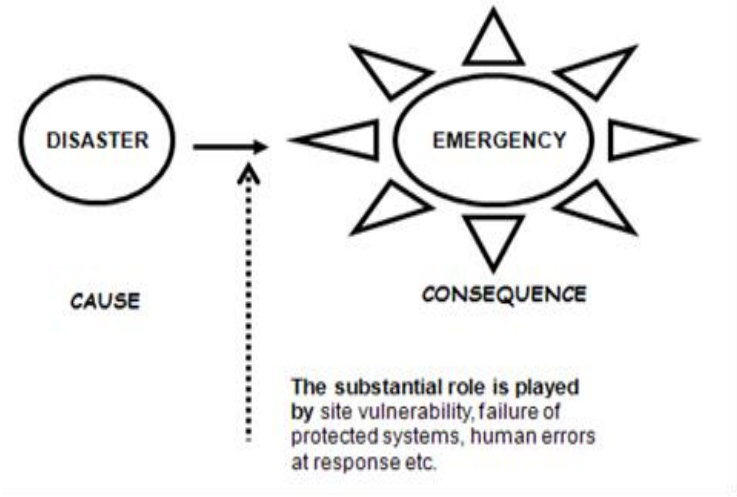

Figure 6. Relationship disaster vs. consequence.

The system behaviour at disaster is shown in Figure 7. Quantities that decide on disasters´ impacts on system are resilience, vulnerability and adaptability.

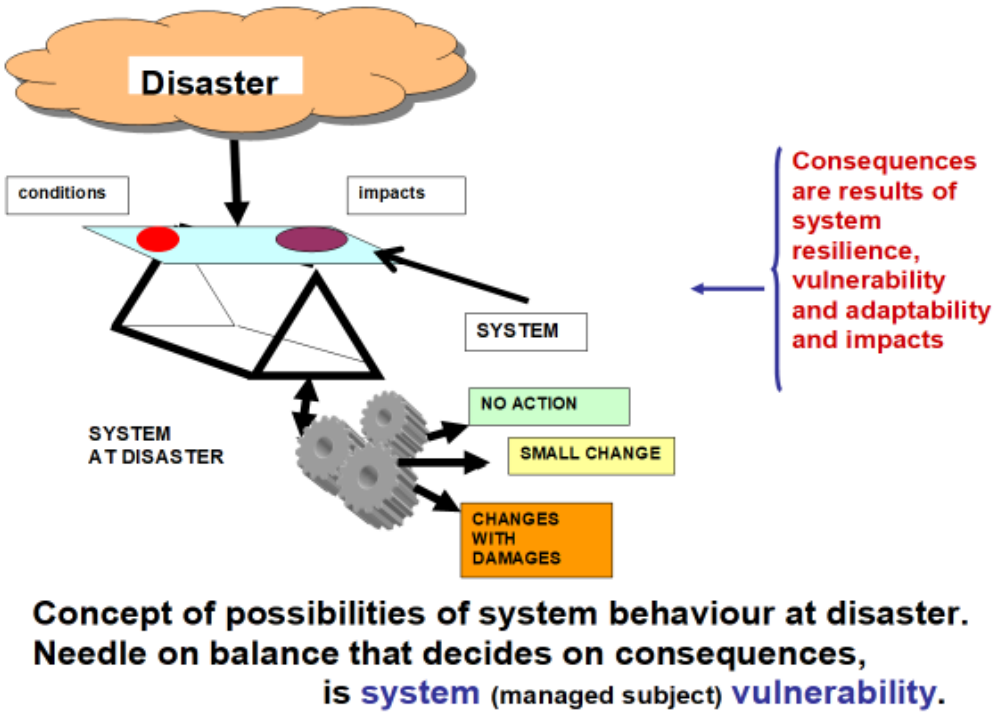

Figure 7. The system behaviour at disaster.

29. Risk management is management of followed entity aimed to the risk reduction. It is a planning, organization, allocation of work tasks and check-up of sources of entity so, that there might be reduced losses, damages, harms, injuries or deaths caused by various disasters. Work with risk is based on the process model shown in Figure 8. It starts with definition of concept of work with risk (system characteristics, determination of assets, specification of aims), on the basis of which the risks are identified, analysed, assessed, judged, managed, traded-off and monitored. The criterions determine the conditions at which the risk is acceptable, conditionally acceptable or unacceptable. The aims in real case are selected from further given possibilities: to reduce risk to certain level; to secure the system, i.e. to ensure system security; to ensure safe system, i.e. to ensure security for both, the system and its vicinity. The feedbacks denoted in Figure 8 are used in case if the monitoring shows that the risk level is not on required level; firstly, it is used the cheapest feedback 1; in case of its failure the feedback 2 etc.; at huge harms it is immediately used the feedback 4 that means the change of concept of work with risks.

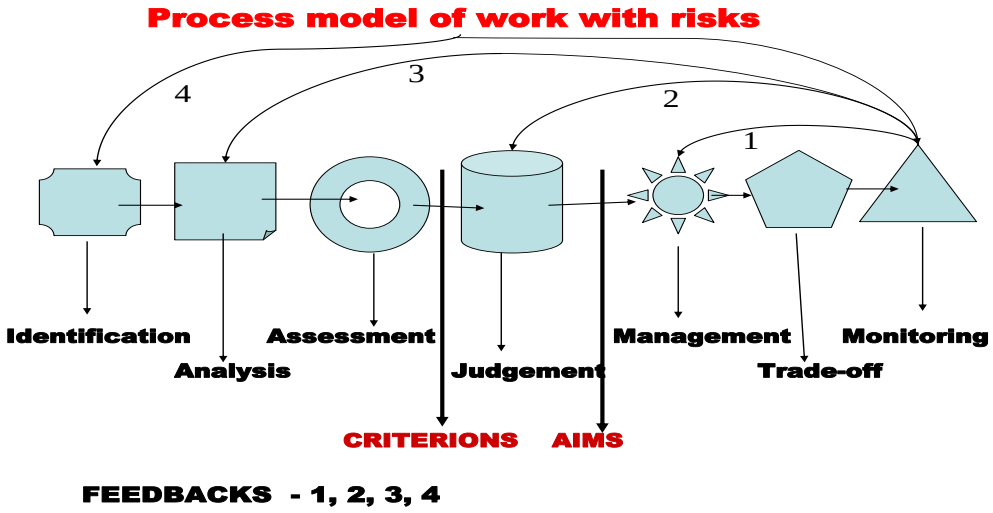

Figure 8. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks.

Risks are reduced by the reduction of vulnerability of: objects; human population; environment; State etc. (in these connections there is used the term „impact mitigation“ for impacts that cannot be averted at disaster origin). According to majority of technical norms and standards, there is performed the reduction of vulnerability at planning, designing, construction and operation of protected assets for all risks, the probability of which is equal or greater than 0.05 [13]. By this way there is formed the inherent safety of system including the human society, objects and environment (i.e. so-called design disasters ought to be get under control by design, regulations for land-use planning and construction, operating instructions, rules for response to emergencies and by instructions for response to critical situations, and therefore, their occurrence would not threaten entity sustainable development). The risk management quality depends on both, the followed risk concept and the quality of decision. The deciding can relate to

matters that are vitally important (the change of the way of life etc.), or to daily details (whether to go in an overfull metro / not to go in an overfull metro; cross a road when the lights are red / do not cross a road when the lights are red etc.). Sometimes the decision takes a lot of time for deciding (e.g. while solving the working or other problems), sometimes it is necessary to decide immediately (in the situations with a direct threatening to life, real risk of a delay and that like). We adjudicate something either on our behalf (and on ourselves, what I do, what I do not do) or on behalf of our subordinate workers / persons (in harmony with their interests, but also against their interests). The decision can only be the result of the arbitrament of one person, it can, however, be also the output of collective intellect. The decisions may be accurate but also false. The consequences of decisions can have the different rate of weight for both, the arbitrary subject and its vicinity.

30. ***Safety management*** is management of followed entity targeted to its safety formation. It is a planning, organization, allocation of work tasks and check-up of sources of organization with aim to reach requested safety level. Enhancement of safety is reached by use (application, realization or implementation) of technical, legal, organizational, educational etc. protective measures. It is also considered risks, the occurrence probabilities of which are smaller than 0.05, but impacts are fatal (severe). Safety management belongs to a common practice at planning, designing, construction and operation of technical facilities and objects such as power plants, dams, nuclear facilities etc., and it is the basement of nuclear safety, radiation protection and protection against dangerous chemical substances that is introduced by the SEVESO II directive. The safety management quality depends on both, the followed safety concept and the quality of decision. In technical slang, there is stipulated that this type of management considers beyond design (severe) accidents. Except of formation of inherent safety of system including the human society, objects and environment, this management type also promotes so called principle of precaution, because it considers disasters or their sizes, the occurrences of which are very low probable, that are unforeseen.

31. ***Emergency management*** is a management, the purpose of which is to ensure preparedness for response to possible emergency situations and to ensure the getting possible emergency situations under control with use of standard sources, forces and means.

32. ***Response management*** is management, the aim of which is the effective coping with emergency situation using the standard sources, forces and means.

33. ***Crisis management*** is a management, the purpose of which is to precede a possible critical situations, to ensure preparedness for response to possible critical situations, to ensure the getting possible critical situations under control in frame of power of crisis management authority and executing measures and tasks of line higher crisis management authorities (for getting situation under control, there is used legal measure „declaration of crisis situation“ that temporarily enables to limit rights and civil liberties of humans and use standard and beyond standard sources), to start renovation and next development.

    In some concepts, its fundamental phases are the prevention, preparedness, response and renovation. In some conceptions there is the crisis management a

part of safety management, in others the crisis management is only used for the getting critical situations caused by disasters under control and for the getting current emergency situations under control there is used emergency management.

34. ***Proactive management*** is a management type, in which there are in advance performed measures for averting or at least mitigation of some non-demanded phenomena, and ensured preparedness for the effective response to non-demanded phenomena.

35. ***Management of technical facility*** is a system of measures and activities relating to materials, technologies, design, construction, operation, staffing, organization, education, finance, and law, so as to ensure the demanded processes, which bring profit, ensure compliance with the State and competitiveness, and together to suppress the processes that bring technical facility harms and losses.

36. ***Reactive management*** is a management type, in which there are solved problems when they occur.

37. ***Safety performance indicator*** is a quantity that measures the level of safety in a given system / entity. At technical facilities, there are usually used: outcome indicators and activity indicators [13,26].

38. ***Critical infrastructure / facility protection*** means to perform strategic, systemic and proactive measures and activities so that humans can survive all emergency and critical situations and infrastructure / facility could be renovated in moderate time interval by help of moderate sources, forces and means.

39. ***The engineering*** is a set of disciplines that realise the tasks determined by management procedure into practice. With regard to complex nature of technical facilities, the present engineering types are multidisciplinary and interdisciplinary disciplines, and therefore, they use very various methods, tools and techniques because the safety management targets cannot be reached only technically. The methods, tools and techniques need to respect the logic, technological, financial and managerial data at decision-making, because their integral part is the decision-making over technical problems, human factor, costs and time planning. Some details are in Annex 2.

40. ***Good engineering practice*** (good engineering procedure) is then defined as the set of engineering methods and standards that are used during the life cycle of technical system with the aim of reaching the appropriate and cost-efficient solution. It is supported by fit documentation (conceptual documentation, diagrams, charts, manuals, testing reports etc.). In a given context the engineering expertise is the expression of the capability to:

    - apply the knowledge of mathematics, science and engineering,
    - propose and realize experiments,
    - analyse and interpret data,
    - propose components or the whole system according to requirements and under the frame of realistic limitations identify, formulate and solve engineering problems,

- ensure the effective communication,
- comprehend the impacts of engineering solutions in a broader context,
- use the advanced tools and methods in engineering practice,
- adhere professional and operational responsibilities and ethics,
- lead the interdisciplinary team.

Most of the demands gave above is directed to correct the bad manifestation of human factor.

41. ***The risk engineering*** is the systematic use of engineering knowledge and experiences for the optimization of protection of human lives, environment, property and economic assets, i.e. for the optimum reach of security and sustainable development of human system. It has a main purpose to reduce all types of harms and losses by the means of aimed and qualified trade-off with risk. It was the 20th century phenomenon and on its basis in developed countries, there was set up the groundwork for human development that is quite resistant against the traditional disasters, namely natural ones; human, animal and plant diseases; technology failures; and social disasters.

42. ***Security engineering*** is a discipline that realizes the goals of system security management, i.e. at selected concept it determines and realises the problems´ solving from their comprehension through project of solution up to implementation under given conditions. For technical facilities, its principles and implementation rules are in [27].

43. ***Safety engineering*** is a discipline that realizes the goals of system safety management, i.e. at selected concept it determines and realises the problems´ solving from their comprehension through project of solution up to implementation under given conditions. For technical facilities, its principles and implementation rules are in [13,14,26,28].

44. ***Resilience*** is a potential (capability) of the system / entity to absorb and to use the deviations and changes so that it lives through them without there might originate quality changes of its structure. It resides in a specific arrangement of the system, which keeps the functions and feedbacks of system, which include the capability of system to reorganize itself on the basis of changes induced by disorders. At technical facilities, it is created by technical and organizational measures. It is the combination of asset capability „withstanding" and "recovering" from disaster. From this it follows that the management of sustainability needs to be based on management of resilience, which has two objectives:

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

    Resilience unlike the vulnerability, answers the question "How does the system respond?". Based on the analysis of contemporary knowledge [13], there are the following types of entity resilience:

1) Engineering resilience focuses on the entity stability of the near steady state (condition), on resistance to disturbances and to speed of the return to its original state.
2) System resilience focuses on conditions remote from the steady-state equilibrium in which the disorders can switch the system from one state to another. System resilience is related to adapt (adaptability), duration and volatility.
3) Social resilience may not always be demanded, because it can promote unwanted status quo.
4) From the theory of control of systems, it follows that resilience of system is related to robustness, redundancy, ingenuity (inventiveness) and speed of response, the correct starting [13], Figure 9.

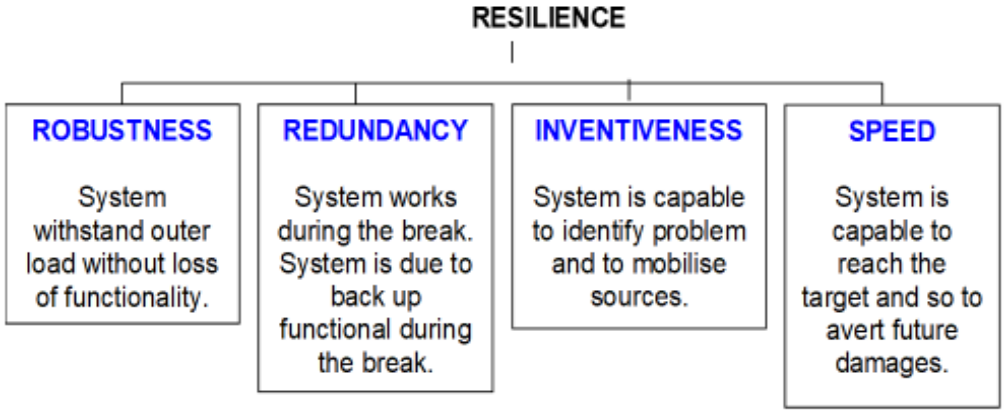

Figure 9. Context of resilience of system with robustness, redundancy, inventiveness and speed.

Resilience management process takes place in three steps, namely:

Step 1: Resilience who, what? It proposes a conceptual model of system based on specific questions: what are the spatial boundaries of the system?; What are the key system services used in the system?; What are the stakeholder groups?; What are the key components of the system, how to characterize what is their importance and dynamism?; What is the historical profile system?; What environment variables act as driving forces key system products and services?; Which factors are controllable and manageable?

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

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

45. ***Adaptability*** is a capability of system to modify its behaviour under stress (critical) situations and to ensure the system existence and functionality on expected level. It is ensured by technical, economic and organizational measures.

46. ***Functionality*** is a system capability to fulfil tasks exactly as entered.

47. ***Reliability*** is a capability of the system to provide the required functions under given conditions, in the given quality and in the given time interval. In technical domain is connected with the probability; functionality is asked to be equal or to be higher than 95 % probability.

48. ***Criticality*** denotes a limit (boundary) from which the risk impacts are significant up to eliminative for followed system, which means that appurtenant risk needs to be always mastered; details are in [21]. The criticality is mostly determined by scoring, i.e. by decision making matrix (system vulnerability vs. system importance); its scheme is shown in Figure 10.

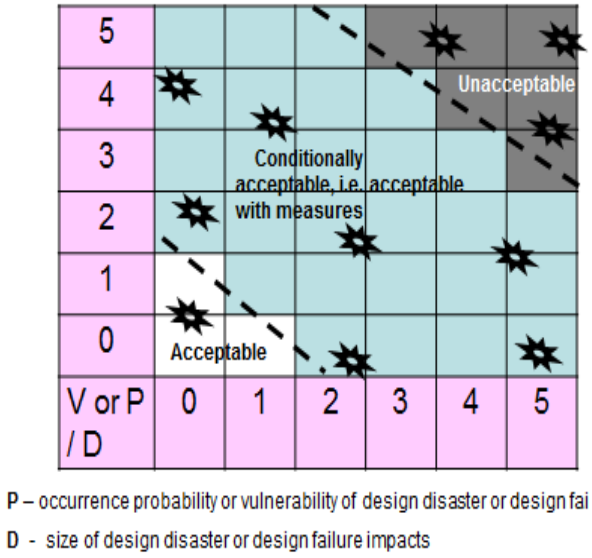

Figure 10. Criticality matrix.; scoring the vulnerability (measure of system vulnerability or system probability of failure) and the importance of system (measure of system damages).

At criticality determination, they are considered the following assets: public; technological system; territory; and the State, and the following questions:

1) How does the facility or infrastructure react to certain types of disasters?
2) How is the facility or infrastructure robust, resilient and rubbery?
3) How the behaviour of facility or infrastructure can be improved?
4) What management mechanisms in the sense of control are suitable?
5) What rules can be used for the self-regulatory or tolerable deflections?

6) Which parts of facility or infrastructure are critical?

Determining the criticality, it consistently refers to the size of the impact of the loss of functionality of each system of systems on society. When determining the criticality, it is considered:

1) Concentration of people and assets.
2) Sectors of the economy (sector analysis).
3) Types of interdependencies among the subsystems of systems:
   i. On what assets of the system depends?
   ii. What is the dependency of the assets among the systems?
4) The types of services to the public:
   iii. How long will it take to restore the provision of services?
   iv. What are the refunds / substitutes may be available and usable?
5) Public confidence in the institutions of the public administration:
   v. Can damage of the assets / public services reduce the morale of the population, the loss of national prestige, panic, riot or civil unrest?
   vi. May damage of the assets cause the impacts / changes on the environment?

Determination of technical facility criticality is based on the analyses of the hazards from the potential disasters in the given territory, from the consideration of the technical facility vulnerabilities. In theory, it has the same principle as the analysis and assessment of risks, in which there is respected the more protected assets. Therefore, one can assume that in general the process of determining the criticality can be described as follows:

1) Characteristics of the assets (assets physical, cyber, and human).
2) Determination of criticality (analysis of hazard from disasters and consideration of vulnerabilities).
3) Assessing the impact on assets (the concentration of people and assets, the economic impacts, mutual dependences, reliability).
4) Evaluation of the consequences of the losses, the victims, damages and harms to assets.
5) Prioritizing the assets according to the specified rules.

Interpretation of results for a given facility is derived from the position of the point the coordinates of which are the calculated values of serviceability (actually a degree of importance for the territory) and the degree of vulnerability. If the point falls within the sector:

- "the high vulnerability and high serviceability" mean that the condition of the facility is bad, i.e. critical, for a given territory and in terms of ensuring security and sustainable development it is the need to solve the situation by the facility backup and facility upgrade,

- "lower vulnerability and lower serviceability" mean that the condition of the facility is satisfactory and it is necessary from time to time to check this status in the territory,
- "the high vulnerability and low serviceability" mean that the condition of facility is conditionally satisfactory and it is necessary to provide sophisticated response preparedness for case of a facility failure and prevention focus on preventive and mitigation measures to reduce the vulnerability of facility to potential disasters that can cause failure,
- "lower vulnerability and high serviceability" mean that the facility condition is conditionally satisfactory and it is necessary to provide sophisticated response preparedness for the case of a facility failure and prevention focus on the reduction of the criticality, i.e. to create facilities in the territory, or to create a backup of the existing facilities.

It is true that the procedure described above shows that the assessment of facility according to two criteria, namely of the extent of services and the extent of the vulnerability is not the result of an objective calculation or process analysis, but it is rather the result of subjective estimates, which can be tolerated in the case of the determination of the basic framework. It would be more complex in the case of determining the criticality of a process.

When scoring vulnerabilities and serviceability (sometimes in the literature it is used directly the importance) of systems [13], it is necessary to consider the following items: the duration of the system recovery; the impact of the failure of system on the human lives and security; the caused injuries and losses; the impacts on the environment; and caused adverse interest.

Figure 11 shows the relationships among several characteristics of technical facility. In practice, it is often used normed relation: ***criticality rate = 1 – safety rate*** [13,14].

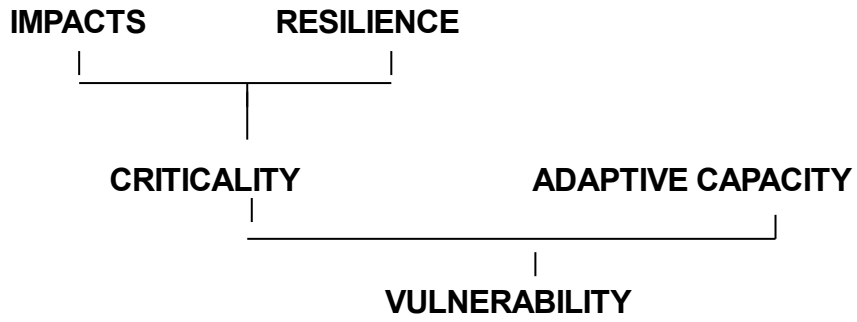

Figure 11. Links among system characteristics.

49. ***Dependability*** is a system capability to provide the required functions under the given conditions in the given quality and in the given time interval. It is measure of reliability, availability and maintainability with which the system performance is supported. It is the capability of system to provide services that can defensibly be trusted within a time-period. It is a designed property that is related not only to

normal conditions but also to abnormal and critical conditions at which through the adoption capacity of system ensures the required functions also at certain types of critical conditions.

50. ***Maintainability*** is a system capability for easy maintenance and repair. It is defined as probability of performance of successful repair within a given time.

51. ***Availability*** is a system capability to provide the required functions at the occurrence of process that uses the given function.

52. ***Integrity*** is a system capability to provide in time fair and valid report to the users on system failures. In technical facilities process safety the quantity "Safety integrity level (SIL)" is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measure of performance required for a safety instrumented function [15].

53. ***Continuity*** is a system capability to provide the required functions without interruption at the damaging process initiation.

54. ***Accuracy*** is a system capability to ensure the required system behaviour in the required range.

55. ***Interoperability*** is an interconnected systems capability to carry out the required tasks in required quality correctly and in-time in a given place and in a given time.

56. ***Durability*** is a system capability to remain functional, without requiring the excessive maintenance or repair, when faced with the challenges of normal operation over its design lifetime.

57. ***Complexity*** is a system property that denotes that system has many parts or elements that have relationships among them differentiated from relationships with other elements outside.

58. ***Complex system*** is a set of systems that have relationships (links and couplings) among them differentiated from relationships with other elements outside the relational regime [13]. Some relations are permanent and some only at certain conditions. The required ones are designed and those unrequired are consequence of disasters and are mostly unacceptable.

59. ***Integral risk*** is a risk of the complex system that includes both, the risks associated with individual assets and the cross-sectional risks that are associated with links among the assets and with the couplings among the assets realized by flows (energy, information, instructions, commands, responses to them from top to bottom and vice versa), i.e. it represents a complex risk for the qualified management.

60. ***Integral safety*** is a property of whole system; usually it is more that sum of system parts safety. It is ensured by the integral risk management. It is set of human measures ensuring the whole system safety.

61. ***Process safety*** is a property of process (e.g. production line). It is ensured by the process risk management. It is set of human measures ensuring the process safety.

62. ***Fittings / product safety*** is a property of fittings / process. It is ensured by the fittings / product risk management. It is set of human measures ensuring the fittings / product safety.

63. ***Inherent safety*** is a set of measures inserted into the entity design for reduction of hazard. Firstly, it was defined by Kletz in 1977 [15].

64. ***Limits and conditions*** are margins in which it is ensured the safety of operated system. They are tools of technical facility safety management. They are the set of positively defined conditions, for which it is proven that the technical facility operation is safe (in reality with probability ≥ 0,95). The appropriated set includes data on permissible parameters, requirements on operation capability, setting the protection systems, demands on the workers´ activities and on the organizational measures leading to the fulfilment of all defined requirements for design operation conditions. For ensuring the safety, i.e. also the reliability and the functionality, the control system of given technical facility needs to keep the determined physical quantities (parameters of appropriate subsystems) on values determined in advance. During the process of regulation, the control system changes the conditions of individual controlled systems by bearing upon the efficient quantities, with aim to reach the required state (condition) of whole system. In terms of integral safety, the following properties of control system are pursued in the order:

    - level of observance of established operation conditions and prevention of damaging (unacceptable) impacts on the system itself and its vicinity,
    - functionality (level of satisfaction of required tasks),
    - operability, i.e. level of fulfilment of required tasks at normal, abnormal and critical conditions,
    - operation stability, i.e. level of observance of established conditions during the time,
    - inherently included resilience to possible disasters.

    From above mentioned facts it follows that management and control systems determine quality and performance of systems. They have decisive influence on safety, and therefore, their following factors are considered: responsible autonomy; adaptability; integrity; and meaningfulness of tasks. Because the human behaviour is not deterministic, the main characteristics of considered systems are: the emerged properties; non-determinist behaviour; and complex relations among the organizational targets. Humans, maintenance, renewal and changes decide about each followed system. From the engineering viewpoint the followed systems are characterized by structure, hardware, procedures, surround, information flows, organization (problem of organizational accidents) and interconnections among the mentioned items.

    It is necessary to consider that all conditions different from conditions stipulated in terms of references of technical facility are mostly danger for technical facility.

65. ***All-Hazard-Approach*** is principle denoting the procedure that at ensuring the entity safety are considered all sources of risks; i.e. internal, external, human factor, organizational, diagonal. Firstly, it was defined by FEMA in 1996 [18] and for Europe it was refined in the FOCUS project [19].

66. ***Defence-In-Depth concept*** denotes special arrangements of protective barriers in entity for ensuring the entity safety [13]. Firstly, it was used in military domain. For safety of technical facilities, it was defined by the IAEA [29].

67. ***Precaution Principle*** is a strategy for approaching issues of potential harm when extensive scientific knowledge on the matter is lacking. It calls for action in the face of scientific uncertainty.

68. ***ALARA*** (as low as reasonably achievable) determines that from potential disaster impact values is acceptable for society the small value that can be achieved by applying sensible mitigation technical measures.

69. ***ALARP*** (as low as reasonably possible) expresses that the risk should be reduced to a size, which is practically achievable. This means that the cost of risk reduction measures should not be considered. It stresses the precautionary principle, which is a fundamental principle of safety management with regard to prudence. According to experts, the principle should be used at every stage of the technical facility, from preparation to the end of operation.

3. SUMMARY OF IMPORTANT KNOWLEDGE ON RISKS

From the foregoing chapters, it follows that risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an unfavourable outcome). It partly depends on the hazard that is represented by disaster (i.e. phenomena that cause damages, i.e. it is the risk source) and partly on the vulnerability of assets in a given site (i.e. on the sensitivity of each individual asset in a given place against to disaster manifestation in a given site). It expresses a possibility what it might be happen.

From this fact it follows that for each management it is important to know the risk, namely in comprehensible expression. In practice of public administration, it is certified the risk expression in a form that by risk analysis and assessment it finds that on specific section:

- there is necessary 5 million EURs a year for remedy of harms caused by existing risk,
- each ten years ten persons die in a consequence of given disaster,
- each five years the property damages caused by disaster exceed 5 billion EURs etc.

3.1. Characteristics of risk and work with risk

The typical risk properties are the random and epistemic uncertainties (epistemic uncertainties = vagueness). If we want to manage the risk, we need to identify, analyse, assess it and after this to decide, what we can do, in dependence on our possibilities – knowledge, staff, technical means and finance sources. For this, we need to use a lot of different methods, tools and techniques and also principles of good practice (good engineering practice) [15]. We divide sources of uncertainties into three groups, namely to the variations originating at:

- usual system process life cycle at normal conditions in the vicinity (uncertainties),
- real changes of system process life cycle in the time and space that affect occasional extreme values occurrences – we consider normal and abnormal conditions - (uncertainties and vagueness),
- variable system process life cycle that is caused by process changes in time and space, induced by outside causes or by critical conditions (vagueness).

The data uncertainty relates to the dispersion of observations and measurement; i.e. a random uncertainty. It may be included into assessment and prediction by mathematic statistics apparatus. The vagueness relates to both, the lack of knowledge and information and the natural variability of processes and actions that are caused disasters. For processing the vagueness, the mathematic statistics apparatus is insufficient, and therefore, it is necessary to use the recent mathematical apparatus that offers e.g.

extreme values theory, fuzzy set theory, fractal theory, dynamic chaos theory, selected expert methods and suitable heuristics based on the existence of several variants of solution processed by multicriterial methods [15,30].

In practice we work with three types of risk:

- the partial one that is only related to disaster impacts on one asset,
- the integrated one that is related to disaster impacts on several assets – e.g. sum or other aggregation of impacts´ rates,
- and the integral (systemic) one that is related to disaster impacts on the entity that is understand as a system. The last concept is necessary for solution of safety and security, the structure of which is complex.

If we want to trade-off with any risk, in the first, we need to identify it and after this to analyse it. Both steps need to be carefully performed because each inaccuracy in the given steps cannot be rectified in the following. For the steps mentioned, the professional knowledge of problem solved is the fundamental. The effective methods for work with partial and integrated risks are: What, If analysis; Check List analysis; Event Tree analysis etc.; the use of each method depends on the level of problem knowledge and on the target of risk analysis [30]. The tools for integral risk will be shown in next chapters.

Risk analysis procedure for the use in disaster prevention [15,16] contains:

- risk analysis definition and determination of study depth,
- description of considered system, object, equipment and the delimitation of its boundaries,
- identification and description of disasters, i.e. sources of risk,
- relative evaluation of disaster´ criticality (hazard assessment) and selection of relevant disasters for further study,
- identification of possible disaster impacts on considered system and its vicinity,
- compilation of possible disasters scenarios, in which unacceptable impacts can occur and selection of representative disaster scenarios,
- estimation of risk amount / size / rate,
- risk presentation.

Risk amount / size / rate is a numerical value; e.g.: the number of deaths caused by disaster (a year); numerical function giving for each N in a certain interval the probability of that as a consequence of some technological accident in a year to one or more deaths in technology vicinity originate. The function describes the relationship between the occurrence probability and consequences of given disaster that has certain nature. For risk representation, there is used e.g. risk matrix, number as one-dimensional amount, mean death measure, risk isolines (individual risk), f-N curve (societal risk) [16,30].

The acceptable risk is the amount of serious harms or jeopardy for human lives and health, home animals, environment or damages arising from existence and possible realisation of disasters that is acceptable for person / group of persons and for society.

The risk acceptability depends on social, economic and political factors, and also on a perceived profit arising from the positive activity of risk sources (disasters) from the viewpoint of analysis of costs and profits for society [4].

Because the risk is a measure of unacceptable impacts caused by an expected disaster on public assets (generally considered assets because in practice, we use different risk analysis targets) in a given site, so the risk acceptability depends on social, economic and political factors, and also on a perceived profit arising from the positive activity of risk sources from the viewpoint of analysis of costs and profits for society. In the business domain the protected assets (interests) are also a safe business, profit, competitiveness etc. With regard to these assets, the disasters are also the following phenomena:

- market failure,
- lack of finances / suitable technologies / qualified human sources,
- incompetent management of business,
- loss of competitiveness,
- external natural and other disasters that have impacts on business,
- intended damage of business outside / inside,
- and failure of links with vicinity / public administration.

In practice [15], there are distinguished the methods for:

- risk reduction in closed system only considering the technical causes of risks,
- risk reduction in closed system considering the technical and human factor causes of risks,
- risk reduction directed to ensuring the system security without respecting the system vicinity security,
- risk reduction directed to ensuring the system safety – its result is that system and its vicinity are safe,
- risk reduction directed to ensuring the system of systems (SoS) safety.

The assessment of system risk means the judgement of disasters´ impacts by help of one or more criteria that reflect the value scale of human society. Some of the criteria may be even qualitative and some of them are incommensurable [14]. Assessment process structure depends on facts:

1. What is assessed?
2. When it is assessed, to which moment in time it is assessed?
3. How, i.e. on the basis of which criteria, it is assessed?

General knowledge sets that when we want to assess something, we need to determine the assessment targets, the set of criterions and the scale used at assessment. The assessment generally represents an exertion of certain criteria, rating functions or preferences. It is used in several senses:

1. The first sense means to follow the process by help of process monitoring or observation.
2. The other sense means the comparison with some appointed limit.
3. The third sense means the comparison with some appointed limit and thinking out all the more or less probable consequences, i.e. the impacts and the profits.

The last sense supports the negotiation with risks. The system assessment means the application of certain suitably selected criteria set or rating functions to the defined system. It means that we assume and specify certain behaviour in time and space, certain responses on possible reactions etc. The criteria, we divide into:

- internal, i.e. such, that ensures the assessment of appropriate system (they take note of system only), i.e. its quality, viability, fitting the certain targets, needs, demands etc.,
- external, i.e. such, that ensures the assessment of system as a part of a broader system (they take note of system and of its vicinity), i.e. viability, material and energy demands, sources, human aspects, environmental impacts, social impacts etc.,
- criteria tied up with a time trend, i.e. with possible changes of assessment in time or with changes of a system function in time (i.e. it is considered expected dynamic behaviour of system in time).

From the given facts, it follows that the assessment has several qualitative levels, namely:

- the simplest level is the comparison of real data value, quantitative or qualitative (e.g. data on the level of quality), with a certain strictly defined limit or model (that the following phenomena aroused or did not arise). The comparison with the limit is used when the surveillance is directed to the check-up of certain item quality or to the determination whether it is necessary or not to start a specified regulation or warning measures. The comparison with parameters of certain model is more typical for observation nets that have one of aims to identify phenomena in domains, which they cover,
- the impact assessment goes partly from data and partly from collected findings. It represents a tool for the complex and systematic investigation of disasters or planned actions. For this assessment type, there is important the reference level that may be represented by: original (present) conditions; conditions that will originate without any activity; some marginal or target (covetable) conditions; ideal conditions. There are systematically followed relations described as the chain of causes and impacts (disaster scenarios) and they are determined by impacts of the first order in cases in which it is possible to directly distinguish the cause. At data processing, they are used the predicative methods (Annex 2) that are mostly based on: exact calculations; statistical formulas; experimental observation and mathematical modelling; expert approaches based on judgements, analogies and experiences; or quantities scoring, i.e. at incommensurable quantities, they are used methods of multi criteria analysis, i.e. e.g. the decision matrixes,
- the hazard assessment means the determination of disaster size on a certain level of credibility in a certain time interval and in a certain site (the time interval size and

site dimension depend on the physical nature of followed disaster). For its determination, there are used the specific methods of mathematical statistics based on the theory of great numbers; the example is in Annex1.

- the risk assessment means to use the methods by which from hazard characteristics (size and occurrence probability) and site characteristics probable size of damages is determined (Annex 2).

At work with risks, it is necessary to consider that processes under way are not only characterised by one criterion, and therefore, it needs to be used the multi criteria approach [30].

The risk assessment is possible to carry out only on the basis of real, true and tried-and-true data sets on a given phenomenon that are valid for a correctly defined system and correctly defined time interval [15]. The target is to ensure the decision-making that supports the benefit for the human system. Therefore, it needs to be used the tested set of criterions that guarantees the objectivity, the independence and the impartiality of assessment. With regard to these viewpoints we divide the criterions into:

- objective and subjective; in the objective ones, there are such criteria, the limit (comparative value) of which is created by current measurable units that are detectable by lab experiments, calculation or economic prudence,
- criterions of advantages and beneficial effect (the higher, the better) or the criterions of costs, losses and content of contaminations (the lower, the better),
- cumulative criterions that are characterised by the relation of mutual complementarities, i.e. they are mutually supplemented and supported. The higher performance of one is connected with the higher performance of the other and vice versa. The extreme cumulative criterions are such criterions, in which the performance of one is conditioned by the performance of the other; the criteria of such type warp the result, and therefore, they need to be put out of the criterion set,
- alternative criterions are given by the relation of mutual competition perhaps, they are antagonistic. The higher performance of one indicator is connected with the reduced performance of the other and vice versa. The extreme alternative criterions are absolutely eliminated, and therefore, they need to be put out of criterion set,
- independent criterions are given by indifferent or variable relations.

The assessment methods from the viewpoint of approach to matter-of-fact problem we separate to: deterministic methods; probabilistic (stochastic) methods; engineering judgement; analogy; model; and aggregation of several criterions (multi criteria assessment) [15,30].

The deterministic approach is based on a precondition that each phenomenon is the inevitable consequence of conditions and causes. The approach consists of fact that there is determined the vagueness of all input parameters, and that from the safety reasons, there are considered marginal (usually most unfavourable) values in a given real case. Just the determination of marginal values is the critical activity of this approach. By use of different data sets and the application of different assumption sets, there are mostly obtained results that are substantially different; i.e. the output value from one procedure does not lay in the interval of deviations obtained by the other

procedure. Therefore, great attention needs to be devoted to data set credibility [15]. This approach is in practice used in technical facilities designing.

The probabilistic approach is based on a precondition that the occurrence of each phenomenon has a certain random uncertainty, i.e. possibility of random phenomena occurrence is estimated with a certain value of probability. From the set of variants, the creation of which is the critical activity of this approach, there are determined representative values as median or median + σ (σ – the standard deviation). This approach is in practice used in technical facilities operation for judgement of technical facility safety level [15].

For the assessment of phenomena and processes that have random uncertainties and vagueness (i.e. the epistemic / knowledge uncertainties) they are, at present, used the computations based on the fuzzy set theory or the possibility theory [30] that combines analytical approach with expert methods. In the case of experts´ use, it is necessary to solve the problem ***who is an expert***. With regard to discussion in world conference ESREL2011 in Troyes [2], the expert is a person who:

- has the knowledge and experiences,
- is neutral,
- has the competences,
- is capable to guess with the support of object matter and to reach the acceptable consensus.

In the EU and in some countries as the USA, there is the legal rule containing the requirements that the expert needs to fulfil [16].

At multi criteria assessment, it is possible to use the methods, tools and techniques supporting the creative thinking, e.g. Delphi method, SWOT analysis, brainstorming, panel discussion, decision supporting systems etc. [15,30]. Their use needs to be prudent and careful, in order that the results bear confirmation of purpose in a value scale selected for criterions chosen for a given problem solution. For the selection of criterion sets (the order of criterions is usually important [15]), for the establishment of scale characteristics and for the judgement of correctness or inaccuracy of outputs, it is necessary to use the empirical (experience) databases.

At risk assessment there is necessary to fulfil the following requirements:

- performance of assessment in the demanded depth and quality and in harmony with the accepted methodology,
- completeness,
- to include the recent knowledge of science,
- estimation of uncertainties and vagueness at an extrapolation use,
- united expression of risk characterization,
- transparency of the process performance of risk assessment.

If the risk assessment does not fulfil these requirements, it needs to be returned to reprocessing. The involved situation arises when the risk assessment was done with the use of present scientific knowledge, but there is the lack of data for risk characterisation

or the output is burdened by too big error. In this case, it is necessary to decide to postpone the decision with note that it will be performed again as far as additional data will be obtained [15].

In practice, for risk determination we use two basis approaches, namely:

1. Determination of hazard from disaster ***H*** and return period ***τ*** (in years) is performed by methods based on the theory of large numbers, theory of extremes, theory of fuzzy sets, theory of chaos, theory of fractals etc. [30]; well-tried method is shown in Annex 1. According to a site vulnerability in an investigated land (e.g. around a given site: square 10 x 10 km; circle with radius of 5 km) the whole damage on all assets is determined for the *H* denoted by ***S*** (Figure 12)***,*** usually expressed in money. Risk ***R*** connected with the given disaster in a given site is determined by the relation

   $$R = S / \tau$$

   The result is very clear: e.g. “the risk from a given disaster in a given site is X EURs and for bigger entity it is MX EURs”, where M is number of sites.

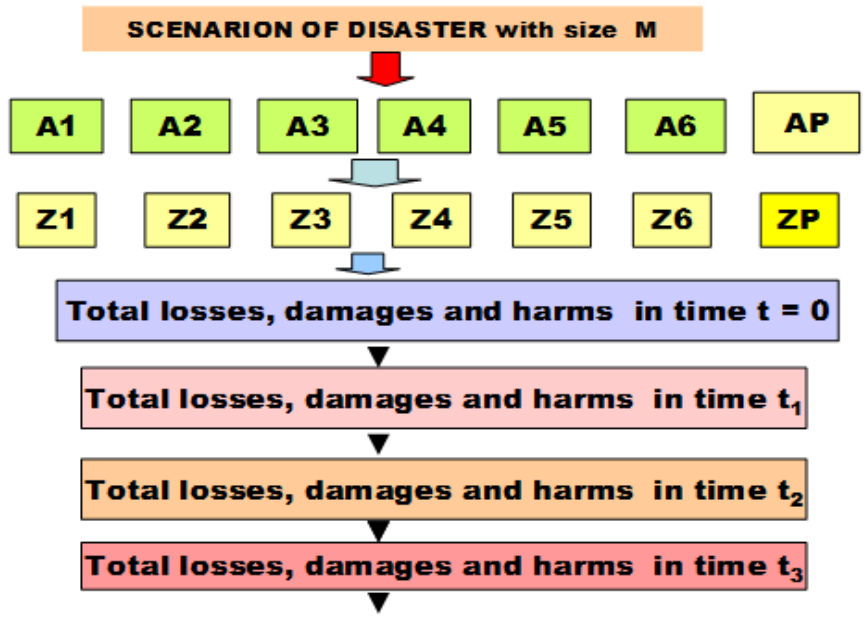

Figure. 12. Flowchart for determining the risks which is used in practice for the strategic management of safety; A – assets and Z losses, damages and harms to the assets; Description: 1-the human lives and health, 2- human security, 3 - property, 4 - the public welfare, 5 - the environment, 6 - infrastructures and technologies, P – private.

2. Determination of disaster scenario for the disaster with size corresponding to maximum expected disaster (it is possible with regard to demands of norms to use the probable size of expected disaster, or the value of standard size of determined disaster or at least unfavourable disaster) is performed; the exact scenario compilation methods [30] are used. According to data for a given land it is determined:
    - the value of whole damage on all assets in the area SS (Figure 12) is usually expressed in money according to amount of assets and their vulnerability to the impacts of a followed disaster in the affected area, usually normalised to a certain land unit ***S***,
    - the occurrence frequency of maximum expected disaster, normalised to one year, ***f*** according to the professional data from databases or expert opinions. Risk ***R*** is given by relation

      $$R = S * f.$$

    The result is in the same form as in the foregoing case. This case is often used for technological and other disasters for which we have not good long-term catalogue (this shortage the EU want to remove by paying the special attention to the compilation of the MARS database [16].

It should also be noted that the critical item is also a choice of qualitative or quantitative approach to the evaluation of risks, because with the quantification of the risks it needs to be treated with caution, since the calculations of the risk creating a false sense of security and safety. It is, therefore, always necessary to compare the originators and consequences of using quantitative and qualitative analysis. If we are talking about quantification, it is necessary to mention and compare levels of quantification: verbal (large, small), ordinal (for example, from 1 to 10), score, interval rating, probability calculation, calculating on the basis of evidence (Bayes' theorem) [30].

On the basis of previous knowledge and experience, summarised in the work [14-16,20], the following applies:

1. The reasons for supporting the quantitative analysis are: the determination of the risk is the result of objective methods and procedures, including the statistical analysis of the data; results of the analysis of the risks are also in the "managerial language" percent, finance, etc.; it is provided a sufficient basis for the analysis of costs and benefits; and it is possible to monitor and control the performance of risk management.
2. Reasons against the quantitative analysis are: the calculations can sometimes be complex and to the untrained eye may look like a black box; and to the quantitative analysis there are needed knowledge and computer programs.
3. Several recommendations for quantitative analysis: the risk as the number often fascinated, but at the same time it is blinding the perception of the context. In terms of communication with the public, it should be noted that the very low probability is difficultly related to everyday experience. For example, one/one in a million at a time is 30 seconds per year. Therefore, there is a demanded degree of analogy;

data type 10^{-5} does not represent the current risk, but are statistical upper bound of the possibility that risk could occur. Thanks to the perfect ten there are believed that reduction of the risk of the procedure or one or the two orders is simply because it is only a multiple of ten. Reduce the risk of 10^{-3} to 10^{-4} means that the risk is reduced by 90 percent. The subsequent reduction of 10^{-4} to 10^{-5} is ten times smaller, and therefore, the nine percent. Therefore, it is recommended to reduce the risk to express graphically; and quantitative approach for the risk must, therefore, be based on a simple principle: rather, measure what is measurable, than what is important. If it is important at the same time measurable, the better.

4. Reasons to use qualitative analysis are: calculations, if they do, they are simple and easy to understand; it is not necessary to quantitatively determine the frequency of the occurrence of disasters; it is not necessary to determine the cost of the measures to soften the impact of risk factors; qualitative analysis arranges and recommends areas for a deeper and more detailed assessment.
5. The reasons against the use of qualitative analysis are: results including the determination of risks are mainly subjective; it does not work with any value, and a value indicator; for the design of countermeasures there are provided only hints at the problem; it is not possible to monitor the effectiveness and efficiency of the risk management procedures, because there is no objective benchmark.
6. Several recommendations for qualitative analysis: a qualitative approach to risk should deal with only potential / opportunities of occurrence; a qualitative approach is based on friendly terms with the relative importance, so it cannot omit the following issues of the qualitative approach: how high is high risk or what is the comparability of the various risks? What are the differences between high and middle? high and low?, middle and low ?; and scoring the risk can lead to erroneous decisions, which means that the measure is doing there, where they do not, and vice versa, where should do, they do not do.

3.2. Risk engineering

Task of management and trade-off with risks is to find the optimal way how to reduce the risks evaluated at socially acceptable level, or to keep them at this level. Reducing the risk is always associated with increasing costs. Risk management is, therefore, guided by the appeal to find a border that is viable, in order to reduce risk costs incurred were socially acceptable; there are used the principles of ALARA and ALARP [15]. Therefore, it is necessary to agree on what the requirements will be output from the risk assessment meet. At the risk assessment it is necessary to try to comply with the established requirements, and any failure to comply with to justify. These are mainly of compliance with requirements [15]:

- the execution of the evaluation in demanded extent and quality in accordance with the accepted methodology of evaluation,
- the completeness of the evaluation,
- the inclusion of the latest knowledge of science,
- an estimate of the uncertainty and ambiguity in the case of the use of extrapolation,

- uniform representation of the characteristics of the risks,
- and transparency in the implementation of the risk assessment process.

Achievement of the objective means well manage and properly decide, with good management and good decision making is possible only when we have good data, and we can take advantage of the instruments that we have available [15]. From above mentioned facts, they are resulting basic principles for the work with risks [15,16], namely:

- to be proactive,
- to imagine the possible consequences,
- properly to determine priorities from the perspective of the public interest,
- to think about mastering the unacceptable impacts,
- to consider synergies,
- and to be alert,

which corresponds to the philosophy promoted at work [31].

Therefore, when determining the risk for strategic decision-making it needs to be used a hierarchical multi-criteria approach. Recent professional work used the concept of hierarchical holographic modelling (HHM) [31] and their results are of high quality, because there is considered a number of factors, which are the originators of the epistemic uncertainties.

Reduction of any risk is associated with the increasing costs, lack of knowledge, technical resources, etc. Therefore, in practice, lit is looking for the border, which is feasible to reduce the risk, so that the costs incurred were reasonable, see principles of ALARA and ALARP mentioned above. Acceptable level of risk taken as follows (certain optimization) is mostly subject to top management and the result of a political decision, at which it is in terms of ensuring the development necessary to make use of current scientific and technical knowledge and to take account of the economic, social and other conditions. Bad decisions at the top level, mainly political, tend to have large, harmful consequences, as witnessed by events from ordinary life (an attack on Iraq or Libya, and the destabilization of countries, a lack of control of pilots and the deaths of 150 people after intentional impact the aircraft to the mountain massif in the last week of March, 2015, etc. [15]).

With the perception of risks, it is related the acceptability of the risk, which needs to have a social dimension. It is necessary to consider:

- for whom it should be risk acceptable? - for the originator of the risks, for the politicians or for public administration?
- who establishes acceptability? - politicians make decisions about what is legal and, therefore, they should not decide about what is acceptable,
- whether in the determination of the acceptability of risks it was discussed currently tolerate risks, intolerant thresholds and public attitudes to risks.

When assessing the acceptability of the risk this is a comparison of the value / risk rate founded by risk analysis of the followed system with the limit of acceptability or limit of marginal function acceptability. The position of the individual to the risk depends on the perception of risk and the risk of stress, which is caused to the individuals (death, injury, loss of employment, etc.). The attitude of society to the risk also depends on the overall perception

of risk, further on the risk-averse, for example one accident with a greater number of victims in one case is less acceptable than a higher number of accidents with victims, and despite the fact that the total sum of the victims for a specific period is the same.

The society accepts, when a group of people is exposed to the risk in order to obtain benefits for different groups of people. The role is played by the ratio between the cost of increasing the safety and the number of lives saved, media attention, etc. The acceptability of the risk depends on the social, economic and political factors and the perceived benefit from the activities for which the benefits are substantially higher than the cost of the rescue and clean-up work in the realisation of the risk.

Risks were, are and will be, and constantly appear new. Management and trade-off with risk requires dimension and measure of risk, considering not only the physical damages, the victims and the equivalent of the economic losses, but also social, organisational and institutional factors. Most of the techniques on the determination of the risk do not represent a holistic approach, and not the fact that the risk is divided into local, regional and country level.

It is clear that if we are not able to identify and analyse the risk, we are not able to defend effectively against it. The error, which is allowed for the identification, analysis and evaluation of the risk is transferred to the emergency and crisis plans, business continuity plans and reduces their value in relation to the planned measures aiming in particular to the protection of human life and health, but also in the area of operational rescue forces involved in the implementation of the rescue operations. It holds the wisdom "to know means to survive, to ignore the call of the destruction's means", from which it follows that ignoring or underestimating the risk management and trade-off with risk is the reason of most problems, failures and disasters.

Due to the fact that, in many cases, it cannot well cope with epistemic uncertainties, so in practice there are used the procedures by good engineering practice, which on the basis of experience leads to a good result. On the basis of engineering principles and technical standards related to project management, it is the greatest attention paid to the risks, which may cause the greatest loss, damage and injury to the assets [15]. Therefore, components, systems, and infrastructure objects in technological systems, divided into categories; as a rule, the three with the fact that in the first category it is the risk settled up best; it performs a detailed monitoring and inspection after each realisation of the source of the risk [15].

Technically it should be primarily to assess:

- how severe (what kind of loss, damage and injury to protected assets),
- what can happen,
- what is the acceptability of impacts of direct and intermediated by a complex network of links and flows and their consequences,
- and whether the security measures and safety management system are adequate to existing threats in a given facility, i.e. whether they are such, that will ensure that in the implementation of the risk it would be acceptable.

As mentioned above, for the understanding and research of complex systems in the engineering practice there are using the chaos theory and the complexity theory, and the theory of options (possibilities), i.e. the Dempster - Shafer theory. The theory of options allows to work with uncertainties of different kinds, i.e., as with random uncertainties and epistemic

uncertainties [32]. It is a continuation of the theory of fuzzy sets, and a certain generalization of Bayesian theory of subjective probability. It assumes the existence of a number of certain conditions (variants) of the system, which have different probabilities of occurrence. It allows combining data from different sources and it is used when creating expert systems.

In the field of control, the theory of options [32] is used; according to it they are modelled variants corresponding to the different processes that are possible in the system and during them, they are considered the possible knowledge deficiencies (epistemic uncertainty). Of them, then it is selected optimal variant. In the selection of variants there are used and they are combined calculations (i.e., analytical procedures) with the practices of good practice. Practice has shown that it is not fit one expert, but it is necessary to combine the knowledge of a few experts. The combination may be ensured by using analytical methods or heuristics, for example, the Delphi, the AHP (Analytical Hierarchy Process), a panel discussion [30].

Therefore, in practice, it is used by system engineering, the main principles are:

- defining the objectives and activities of the facility for their attainment,
- the establishment and application of the criteria for the decision-making process,
- developing the alternatives,
- modelling the systems for the analysis,
- implementation of management and control.

The given principles are now widely regarded as good engineering practice. If most engineering is based on technology and science, the system engineering considers a as equivalent significant component of its practice also the management of engineering processes. The aim of the system engineering is to optimize the operation of systems in accordance with priority criteria given in proposal. The foundation of any approach for the achievement of the objectives, it is the initial assumption that system engineering optimizing the individual components, subsystems or individual partial systems does not generally warrant the creation of an optimal system. It is a known fact that improving one of the subsystems may in fact worsen the properties of the entire system. When we realize that, according to the principle of the hierarchy it is actually each system a subsystem of a larger system, so given principle represents an unsolvable problem. It is necessary to recall once again that the safety of the system of systems is not a summary of the safeties of the individual subsystems.

System approach provides a logical structure for the solution of the problem. As the first it needs to specify the objectives that the system has achieved and the criteria according to which they can be evaluated alternatives (variants) of proposals. Then it comes the phase of the creation of system that results in a set of alternative proposals. Each of these alternatives is then analysed and evaluated in accordance with the objectives and criteria and, finally, it is the best of them selected for implementation. In practice, it is a highly interactive process of mutual modification of the original objectives and criteria on the basis of the later stages of creation and elaboration of the proposal.

System engineers may not be experts in all aspects of the system, but they need to understand the subsystems and various phenomena in them enough, so to be able to describe and model their characteristics. This means that the system engineering often requires:

- the team of workers for the specification of the requirements of the system,
- the elaboration of feasibility studies,
- comparative studies,
- design,
- analysis and development of architecture of the system and analysis of interfaces of components and systems.

Due to the complex structure of systems of systems, in most cases it is not possible to eliminate all parts of the epistemic uncertainty in the processes of decision-making, because it cannot be obtained all the relevant information. Therefore, the consequences of each of the directions of procedure cannot be completely determined and for their study it originated further discipline, i.e. ***system analysis,*** which provides an organized procedure (process) for the acquisition and detection of specific information related to a given decision.

System engineering and system analysis are already de facto merged long years and are used in the formation of complex man-machine systems, in which the system analysis provides information for the decision-making process and it organises the procedures for selection of the best alternatives to the proposal. ***Listed disciplines*** **create** ***together theoretical and methodological basis of system safety***, i.e. safety of the system***.***

Due to the fact that, in many cases, it cannot well cope with epistemic uncertainties, so in practice there are used the procedures known as the good practice procedures / good engineering practice. It is a good practice in a certain area, which on the basis of experience leads to a good result. They are used in cases in which a single procedure was not approved. There are frequent when measuring in laboratories dealing with human beings, etc.

Good engineering practice (a good engineering practice) is then defined as the ensemble of engineering methods and standards that are used during the life cycle of a technical system with the aim of achieving appropriate and cost-effective solutions. It is supported by the appropriate documentation (conceptual documentation, diagrams, manuals, reports from testing, etc.).

On the basis of engineering principles and technical standards related to project management, as it was mentioned above, it is the greatest attention directed to the risks, which may cause the greatest loss, damage and injury to the assets. Therefore, facilities, objects and infrastructures are divided into categories; usually three with the fact that the first is the risk were best conducted, detailed monitoring and inspection after each implementation of the source of the risk. Design tasks are the following:

- prevention of collapse of buildings,
- to ensure the security of people,
- damages need to be repairable,
- interruption of the operation of a technical and a civilian facility needs to be acceptable,
- for objects of type power plants, water facilities, etc. continuous operation needs to be ensured,
- at the risk of technologies, it is necessary to avert disorder requiring repair, which would have unacceptable impacts on the assets.

3.3. Risk of complex systems

Because the territory and each technical facility (object / network / organization) are the complex systems of systems (set of open and mutually interconnected systems of various nature), it is necessary to consider the safety of whole complex, called the integral safety. For this purpose, it needs to work with an integral risk. The integral risk is influenced by reality that each followed entity has a range of protected assets of different nature that are interfaced by internal links of different nature and couplings created by flows.

Because the goals of assets are not always the same, it is necessary to expect the conflicts. At several conditions (caused by occurrence of special disaster with size greater than design one, which creates the boundary value that assets withstand such disaster without greater losses and damages), low assets´ resilience and interfaces among the assets are the causes of another conflicts. The entity integral risk depends on the hazards from disasters of all kinds (natural, technological, social, financial, economic, legal etc.) that can threaten the entity; the disasters affected not only the individual assets but also their links and couplings, which lead to the cascade failures.

For correct assessment of entity risk, it is important to consider all disasters that can damage the entity, and properly to determine the sizes of hazards connected with individual disasters. The risk connected with each disaster is probable size of losses, damages and harms on the entity for hazard connected with the design disaster divided to area unit and one year. The crucial is the correct determination of hazard connected with the design disaster. ***Both, the performed entity safety reports audits and the inspections after the entity accidents or failures, revealed that in evaluated cases:*** some possible disasters with potential to disrupt the entity were not considered at risk determination directed to the entity safety; and several faults in determination of correct value of hazard connected with design disaster were found (e.g. data from too short time interval on disaster, too limited knowledge).

The data [1-11] and special research results [13-17,20,21] show that risk value depend on many factors. They are shown in Figure 13. The analysis and sorting the data set revealed seven domains that influence the result of work with risks of technical facility [15,33], i.e. its safety, namely:

1. Context in which the risks, inherently connected with technical facility, are inserted.
2. List of considered sources of risks.
3. Type of risk form.
4. Ways of mastering the risks.
5. Process model of work with risks, application of the TQM approach [34] and Coase theorem [35].
6. Technique of management and coping with risks of technical facility.
7. Way of management of risks in time.

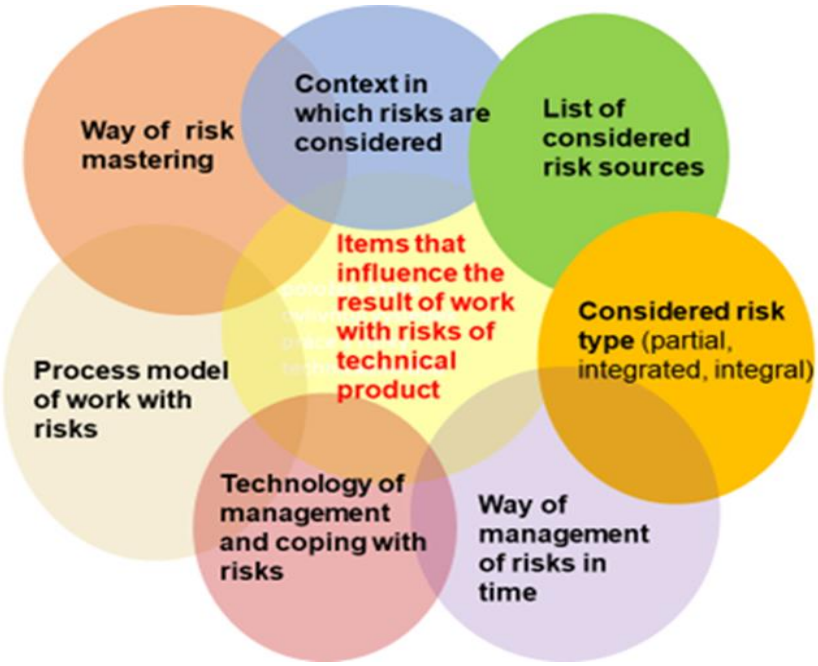

Figure 13. The factors that influence the risk size of a given entity.

On the TQM (Total Quality Management) approach [34], the ISO standards 9000, 14000 etc. had been set up. It consists in the requirement that all employees, from the plain employee up to the top management employee, are participated in the process of quality improvement. The process of quality improvement (i.e., in its top level it goes on de facto on integral safety increase) comes from the impulses which come from customer/citizen needs.

TQM comes from the assumption that the stable quality of products and services cannot be ensured by commands, supervision, partial programmes, organizational or economic measures, but it can be reached by seeking, measuring and evaluating of causes, why the productivity and quality do not improve. De facto it goes on certain safety culture (in the other words it is a way of application of measures and human activities). Attention is focused on processes ongoing in the entity. At the TQM implementation, they are considered the entity specifics, because all measures need to reflect the structure of entity from the reason of efficiency; it means they shall be site specific.

The correct outputs for needs of proper management according to the TQM are the following:

1. The risk assessment document – it contains information about the appropriate risks.
2. The list of top risks – it contains the list of selected risks, the solution of which demand big claims on resources and time.
3. The list of retired risks – it serves as the historic link for decision making in future.

The technique of only risk management from the reason of economic handling with forces, resources and funds formally before work with risks reviews both, the risk

management and the trade-off with risks in the context of benefits and costs on the outputs.

On the basis of present knowledge, the orientation to the process management leads to:

- better understanding and greater integration of entity,
- continuous management of linkages among the individual processes,
- stress on: comprehension of requirements and their fulfilment; needs to consider the processes from the viewpoint of added value; run into increase of performance and effectivity; and permanent putting forward the processes on the basis of their efficiency.

The Coase theorem in engineering practice is expressed in Figure 14. Human possibilities and sources are limited, and therefore, the acceptable entity security is near the whole cost optimum [35],

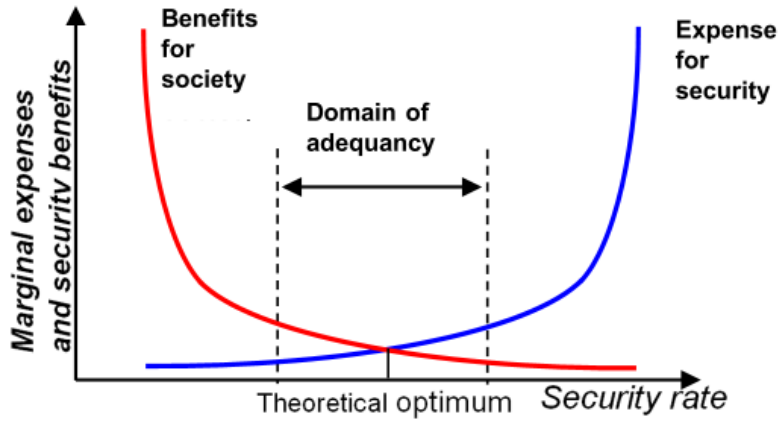

Figure 14. Security understand as economic optimum for human system.

From the practical reasons it is necessary to consider that the entity risk connected with the given disaster does not represent only the direct losses on assets but also the indirect ones; the indirect losses are caused by:

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

Due to the complex entity structure their risk is the integral risk that is expressed by following formula

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

where: ***H*** is the hazard connected with the considered disaster; A_i are the values of assets, ***i = 1,2, ..., n*** that are considered in connection with complex technical facility safety, where ***n*** is the number of monitored assets; Z_i are the vulnerabilities of assets taken under account, ***i = 1,2, ..., n***; ***F*** is the loss function; P_i is the occurrence probability of i-th asset damage – conditional probability; ***O*** is the vulnerability of safeguard measures; ***S*** is the size of followed territory / facility; ***t*** is the time that is measured from the origin of harmful phenomenon in facility; ***T*** is the time for which losses arise; and τ is the return period for the given disaster.

Because the loss function ***F*** form is not known, we use for determination of total risk (i.e. the integral risk) the scheme given above in Figure 12.

In practice, the easiest way used for estimation of losses and harms caused by disaster is to draw up the situation plan of followed entity (example in Figure 15) and to estimate the expected losses according to the distribution of assets and their vulnerability (Figure 12); e.g. a proven formula for determining the number of injured persons is

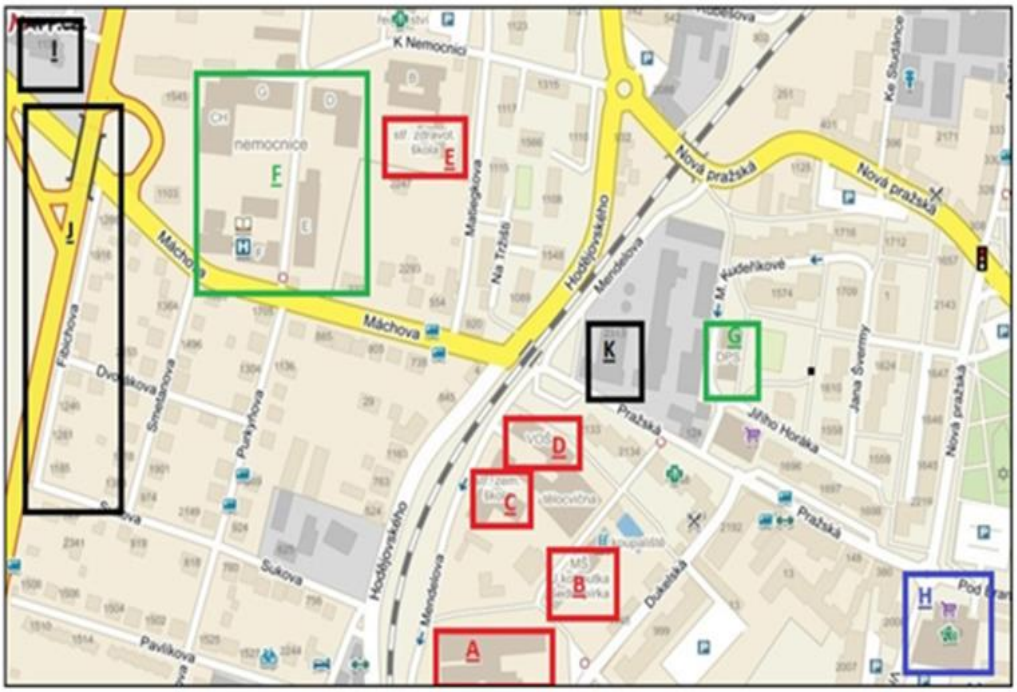

Figure 15. Example of area situation plan – blue, green and red objects – followed assets and black object domino effect source.

$$N = S \,.\, h \,.\, f$$

in which ***S*** is the affected area in ha, ***h*** is the population density given by the number of persons per ha, ***f*** is a correlation factor when only part of the territory is inhabited.

Well-tried form of registration of losses and harms is table, the model of which is in Figure 16.

Land 1	Disaster 1	0h	Impacts on	Human health and lives		Immediate causes of partial infrastructure failures and their mutual connections	Causes of the critical infrastructure failure in hierarchical order
				Property			
				Welfare			
				Environment			
				- Energy infra.			
				- Water infra.			
				- Transport infra.			
				- Finance infra.			
				- Cyber infra.			
				- Food infra.			
				- Land services			
				- Emergency services			
				- Land management			
		3h					
		6h					
		24h					
		3 days					
		14 days					
	Disaster 2						
	Disaster 3						
	.....						
Land 2							
.....							

Figure 16. Example of data registration.

Because losses and harms change with time, the impacts of monitored disaster in the selected territory is suitable to monitor:

- in time 0h (disaster origin),
- in times 3h, 6h … measured from disaster origin distinguish primary and secondary impacts; secondary ones are caused by failure of infrastructures and technologies.

Table 1 shows an example of a scale used by FEMA; description is in [15] for assessment of losses and harms on assets. In this way, additional losses caused by domino effects that mathematical models do not reveal are evaluated.

Onward, the problem is complicated by reality that the world is in dynamic development, i.e. both, the entity conditions and the risk sources are changing in time. Moreover, there is necessary to respect that the risk and safety are not complementary quantities – it holds that the risk reduction leads to safety increase but at the same risk value the safety can increase if humans perform special measures or at their behaviour use special manners following from correct safety culture.

Table 1. Auxiliary scale for assessing the risk acceptability based on the disaster impacts.

Illness - injury	**Loss on property / equipment**	**Time needed to correct impacts**	**Economic loss on equipment [$]**	**Environmental impacts**
Deaths or total permanent ineligibility	System loss, substantial damage to real estate	> 4 months	> 1 Million	Long-term environmental damage (5 years or more) or the need for more than 1 mil. $ for redress (or fine)
Permanent partial incapacity; temporary complete incapacity (over 3 months)	Substantial damage to the system; significant damage to real estate	2 weeks to 4 months	250 000 – 1 Million	Medium-term environmental damage (1-5 years), or the need for 250 thousand -1 Million $ for redress (or fine)
Minor injury; Job shift loss; Compensation for injury or illness	Minor system damage; minor damage to real estate	1 day to 2 weeks	1000 –250 000	Short-term environmental damage (< 1 year) or the need for 1 thousand - 250 thousand $ for redress (or fine)
First aid or minor medical treatment	Minor system defects	< 1 day	< 1 000	Minor environmental damage, easily remedial, requiring <1 thousand. $ for redress (or fine).

Owing to differences in individual disasters nature, the countermeasures for assets´ protection being effective to one disaster, are not effective to another and even can

increase vulnerability some of them; i.e. the countermeasures effectiveness depends on real entity and its disaster.

Therefore, at solution of practical tasks connected with both, the entity safety and the entity risk, ***it is necessary to consider that risks are normal and for the entity safety it is necessary to apply*** not only the risk prevention measures and activities determined on the basis of correct intent and correct data and methods, but also:

- the safety culture by which the human behaviour in the entity and its vicinity is targeted to safety,
- and the tools that reduced losses and damages if some important disasters occur.

Therefore, it is necessary to prepare the qualified response for important risks realizations [12-15,21], such as:

- the risk management plans for both, the entity and the entity vicinity for all relevant risks,
- the continuity plans for survive of important complex technical objects and facilities,
- and the operational crisis plans for both, the complex technical objects and facilities and their vicinities (in-site, off-site).

From the viewpoint of ensuring the human needs, namely including the human survival at critical situations, the four phases of each entity investigation are important:

- in-depth knowledge of entity (protected assets, possible disasters, vulnerabilities),
- determination of risks, determination of concept of optimising the measures and activities in entity for getting over the expected risks,
- determination of weaknesses in management and trade-off with risks and in determination of measures of response and responsibilities for case of occurrence of great damages, losses and harms on protected assets, e.g. caused by lack of finances, knowledge, technology etc.; at least it is necessary to process the risk management plans for important risks,
- constitution of capability and preparedness to ensure the survival of humans and critical technologies at critical situations (crisis plans, continuity plans).

Present knowledge shows that it is not enough to manage the risks of individual disasters but it is necessary to understand and to manage the processes that product the disasters. Due to dynamic world development, the processes originating the disasters also change, and therefore, the attention to them is logical. Safety management concept formed at certain time on the basis of integral risk is not sufficient and it is necessary continually to adapt it to changes that are caused by internal and external processes by help of proactive targeted integral risk management.

4. RISK ENGINEERING TOOLS

The basic tools for risk management and trade-off with risk directed to entity reliability, security and safety, according to knowledge summarized in [12], are:

- management (strategic, tactical, operational) based on qualified data, knowledge, professional assessments, qualified decision-making methods,
- land-use planning, correct technical facilities sitting, correct technical facilities designing, correct technical facilities building, correct technical facilities operation, correct technical facilities decommissioning and occupied territory cleaning for other civil use,
- maintenance, reparation and renovation of buildings, technologies and infrastructures,
- citizen's education, schooling and training,
- specific education of technical and management workers,
- technical standards and norms including the best practice procedures, i.e. tools for control / regulation of processes that may or might lead to disaster occurrence or to its impact increase,
- inspections and audits,
- executive security forces for qualified response,
- systems for critical situations defeating,
- emergency, continuity, crisis and contingency planning,
- safety, emergency, continuity and crisis management.

The key concepts of present risk engineering directed to security and / or safety [13,14] are:

1. The approaches are based on risk – the work intensity and documentation are adequate to a risk level.
2. The professional approach is based on reality that only the critical attributes of quality and the critical parameters of process are considered.
3. The problem solution is oriented to critical items – the critical aspects of technical systems ensuring the consistence of system operations are followed and managed.
4. Verified quality parameters are included in the project proposal.
5. The accent on quality engineering procedures – it needs to be proved the accuracy of selected procedures under given conditions.
6. The aim of a safety upgrade – permanent improving of the processes with the use of analysis of the root causes of malfunctions and failures.

For respecting these items, there need to be used relevant data sets and only verified methods that provide outputs with a designated testified competence.

4.1. Risk engineering models

The short description of procedure of risk management is shown in Figure 17 [16]. You can see basic important steps; their details are in Figure 18 [16]. Very important step is the decision if the risk is acceptable or unacceptable. Regarding the reality that the determination of the acceptability level is always very problematic and it depends on the situation in society, the risk management lean on two additional levels, namely: the insignificant one and the unacceptable one. Between these two levels, there is the domain of risk, which is acceptable with certain measures.

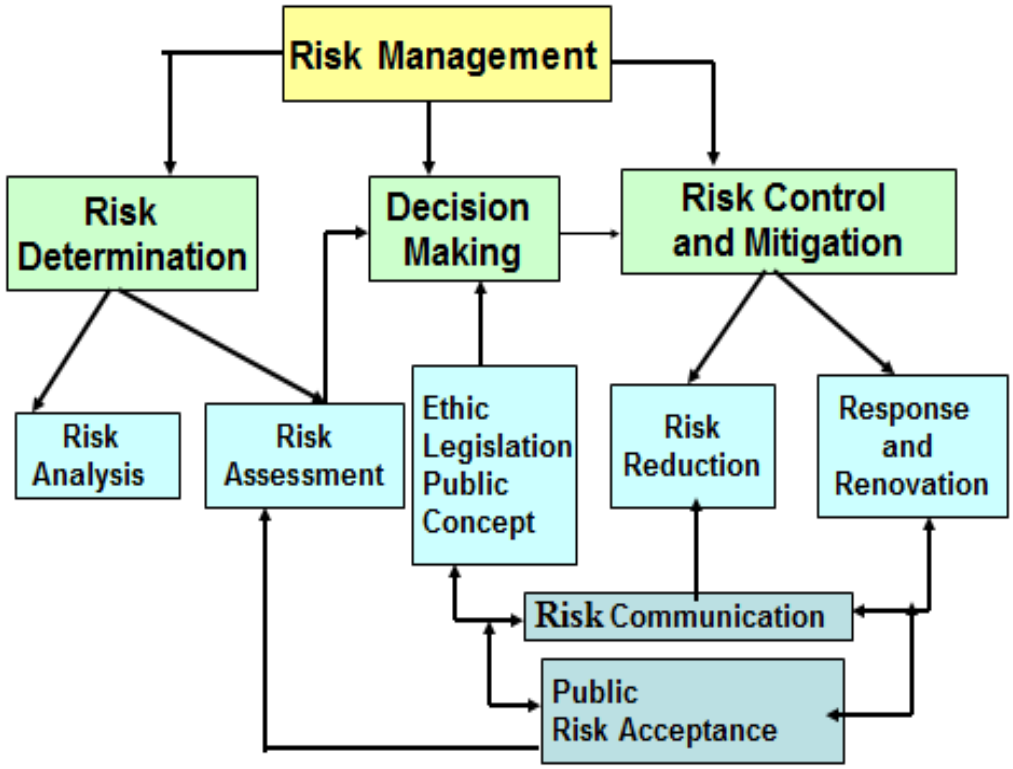

Figure 17. Model of risk management in territory.

If risk is lower than the insignificant level, no measures and activities are required, in contrary, if risk is higher than the unacceptable level, it is immediately necessary to take measures and activities for its reduction. The proposed measures and activities need to be further investigated from the viewpoint of their demands on economic, political and social domain; in particular, with the use of following analytical procedures:

- economic analysis - *"cost-benefit analysis",*
- legal analysis investigating the possibilities of the harmonisation of different variants with the legislation,

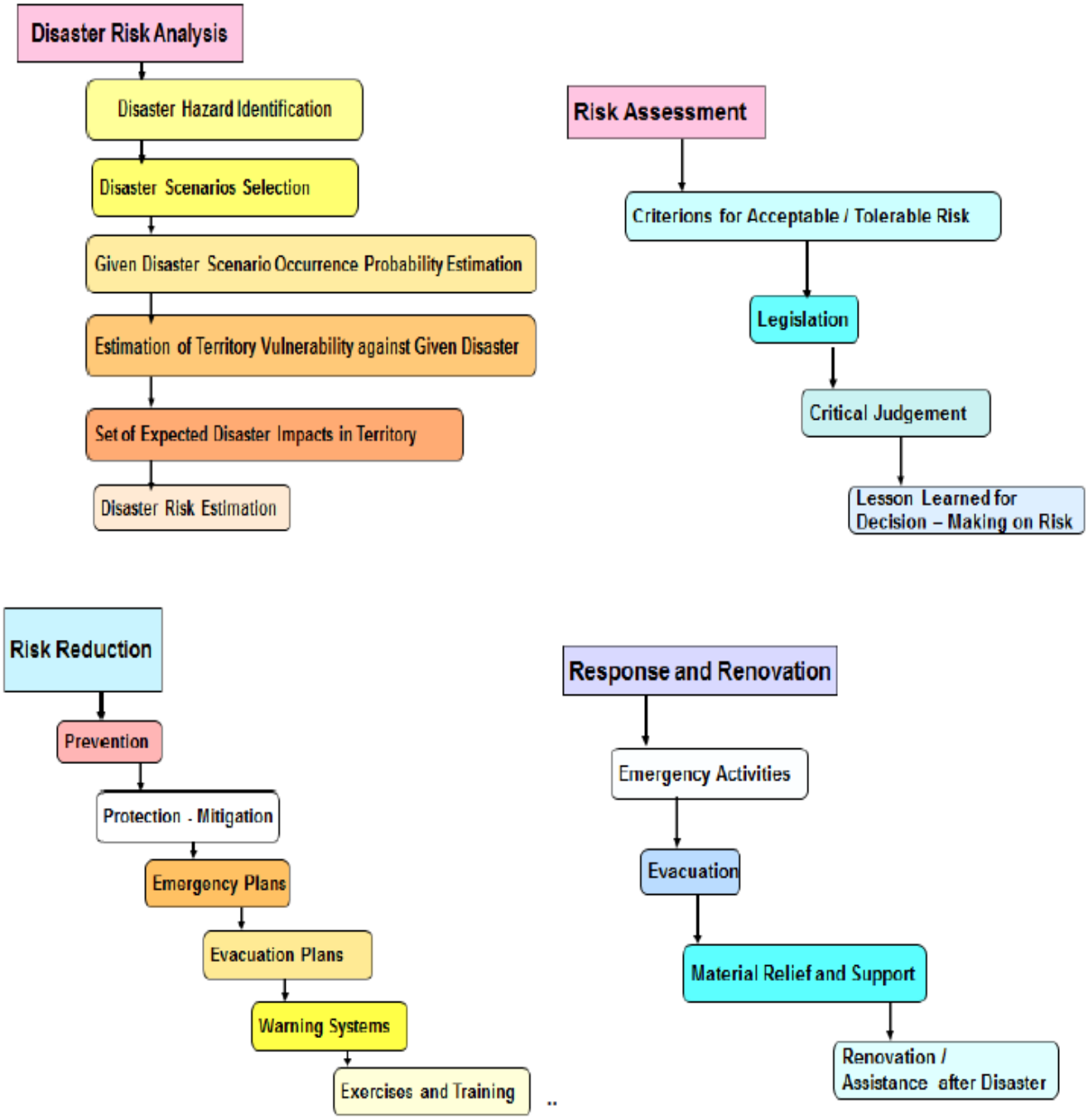

Figure 18. Detail description of processes: disaster risk analysis; risk assessment; risk reduction; and response and renovation.

- political analysis investigating the possible political consequences following from the decision,
- and analysis of the public opinion.

The analytical component of risk management is a scientific matter and its output is the proposal of several variants of a problem solution as groundwork. The part of all variants needs to be the proposal of mechanisms (Control Options) enabling the effective realisation of proposed measures. This step may be understood as the administrative one but it needs not to be underestimated or skipped because it is sufficiently known that each good mentioned executive measure without effective check-up and appropriate sanction has no effect.

The final step is the decision of the implementation of measures for risk reduction, eventually of the further following of the problem. It is necessary to accept the decision whenever, namely in case when it is evident that risk assessment will not give further results in sufficient time interval. It is necessary to accept the decision also in the case when the result of risk assessment is burden by great errors that follow from present scientific cognition and they cannot be reduced in a necessary time.

In practice two risk management models [15,16] are usually used:

- classical risk management (Figures 17 and 18),
- safety management, i.e. risk governance for security and sustainable development (Figure 19).

The Figures 17 and 18 are sufficiently expressive that we do not discuss them in details; particulars are in [15,16].

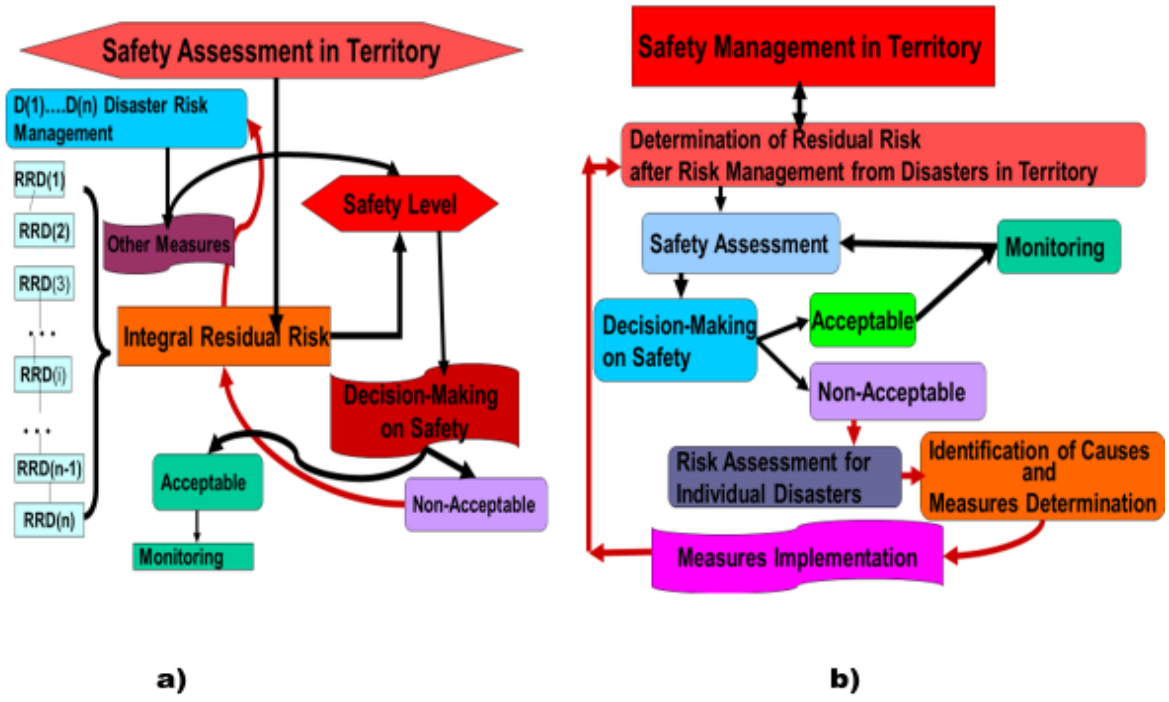

Figure 19. a) - Model of safety assessment in territory (RRD(i) – risk from the i-th relevant disaster; b) – Model of safety management in territory.

Figure 19 (part a) shows that the result of safety for followed system is a consensus for all considered disasters because each disaster type affects, owing to its nature, the system and its protected assets differently. Because the human factor failure, especially in risk management belongs to disasters, i.e. phenomena that damaged the human system from a certain size. With regard to the typical risk properties like uncertainties and vagueness, as was shown above, it is necessary at deciding on risk, to use more possible variants of real human system behaviour and multi-criteria deciding by the help of experts with verified qualification [15,16].

From Figure 19 (both parts) it follows that the result safety for followed system is a consensus for all considered disasters because each disaster type affects, owing to its nature, the system and its protected assets differently.

4.2. Demands on data and methods at risk engineering

For human safety and for human system safety (i.e. territory, organisation, plant) we need to manage the integral risk including the human factor, i.e. to find the way of cross-section risks management and to concentrate the investigation on interdependences and on critical spots with a potential to start the system cascade failures, domino effects, strange behaviour etc., and on the basis of such site knowledge to prepare measures and activities ensuring the continuity of limited infrastructure operation and of the human survival.

Evaluation of present knowledge shows that one of number of causes are interdependences inducing the cascade failures in the human system or in its part are the human errors (intentional or involuntary) in management and in deciding. Therefore, we need to do all measures in managerial and engineering activities to avert human failures, namely at decision-making. Because consequences of errors originating at decision are often huge, the great attention is concentrated to work with risks at present.

In daily practice, the getting over the risks is the duty of all participants. The qualified activities are ensured by engineers, who arrange co-ordinated implementation of measures for prevention, preparedness (directed to mitigation of severe impacts at risk realisation), response and renovation. Often used characteristic of engineering's work with the risks is:

- it considers multi-fields and cross-sectional disciplines that use both, the general and the specific methods, tools and techniques (specific ones are either simple or complex, complex ones represent well-ordered use of several general or simple methods, tools and techniques),
- it uses methods, tools and techniques logic, technological, financial, managerial and deciding because their integral part is a decision on technological problems, costs and time planning,
- it deals with tasks that connect the trade-off with risks for human system safety ensuring and the requirement of non-trivial solution of problems by use of multi-criteria methods, tools and techniques.

In all procedures it needs to be respected that assets and causes of risks have different natures that cause incommensurability of criterions and reasons, which only allows application of multi-criteria methods, tools and techniques that are suitable, i.e. correct and valid for a given problem target.

From the methodical viewpoint at selection of methods, tools and techniques they need to be respected:

- data quality,
- structure of problem that is solved and requirements on quality of results,

which means specially to test both, the data quality (accuracy, completeness, homogeneity, bearing witness to a given problem [15]), and the qualification of experts if they are used (IAEA, OECD, World Bank etc. have strict criteria for judgement of expert qualification) [16].

Methods for determination of risk size need to respect both, the nature of phenomena that are their sources (i.e. characteristics and physical nature of disasters) and the parameters of medium in which phenomena affect. There are used methods based on the mathematical statistics, theory of extreme values respecting the random, sporadic and irregular great events occurrence, fuzzy sets theory, approaches of operational analysis etc., that inherently assume the certain model of phenomena occurrence, and methods based on scenarios that are simulated or empirically obtained [15,16,30].

4.3. Organizational questions of risk engineering

For trade-off with risks of technical facilities, we use the safety management system (shortly SMS), concepts [13,14,26]. In the SMS we consider two cases, namely either the risk realisation is still substantially the same or it is significantly different. In the first case, we consider from safety reasons either the worst case (such approach is found in the standards based on a deterministic approach to safety provision) or we admit random uncertainties resulting from the momentary local and temporal conditions of assets and as a representative variable for risk management we use the mean value obtained by evaluating the possible alternatives (arithmetic mean; median; median + σ, where σ is the standard deviation).

The other procedure is now commonly considered in the preparation of documents for strategic management (the alternative scenarios for the risk realisation and their occurrence probabilities are determined; and the mean and its dispersion are derived from them by a clear mathematical approach); we can find it in the norms and standards based on a probabilistic approach. In cases when we consider the existence of vagueness in data we need to use the combination of analytical and heuristic approaches that offers different theories; overview is in [15].

Strategy of management for negotiation with risks [15,16] is:

- part of risk is reduced, i.e. the risk realisation is averted by preventive measures,

- part of risk is mitigated, i.e. the non-acceptable impacts are reduced or averted by prepared measures and activities having the mitigating effects as warning systems and another measures of emergency and crisis management,
- part of risk is re-insured,
- part of risk for which there are prepared resources for response and renovation,
- part of risk for which there is prepared contingency plan, *i.e. it is used for part of risk that is low frequent and too difficult governable.*

At present work with risk, the risk is understood as the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (a non-demanded outcome). Now in practice there are used five types of risk management / engineering of systems [15], i.e.:

- classical risk management and risk engineering,
- classical risk management and risk engineering including the human factor,
- security management and security engineering,
- safety management and safety engineering, i.e. risk governance / trade-off for security and sustainable development of system,
- safety management and safety engineering determined for system of systems (SoS).

Figure 20 shows the overview; the detail characterization is in [15] and in Annex 3.

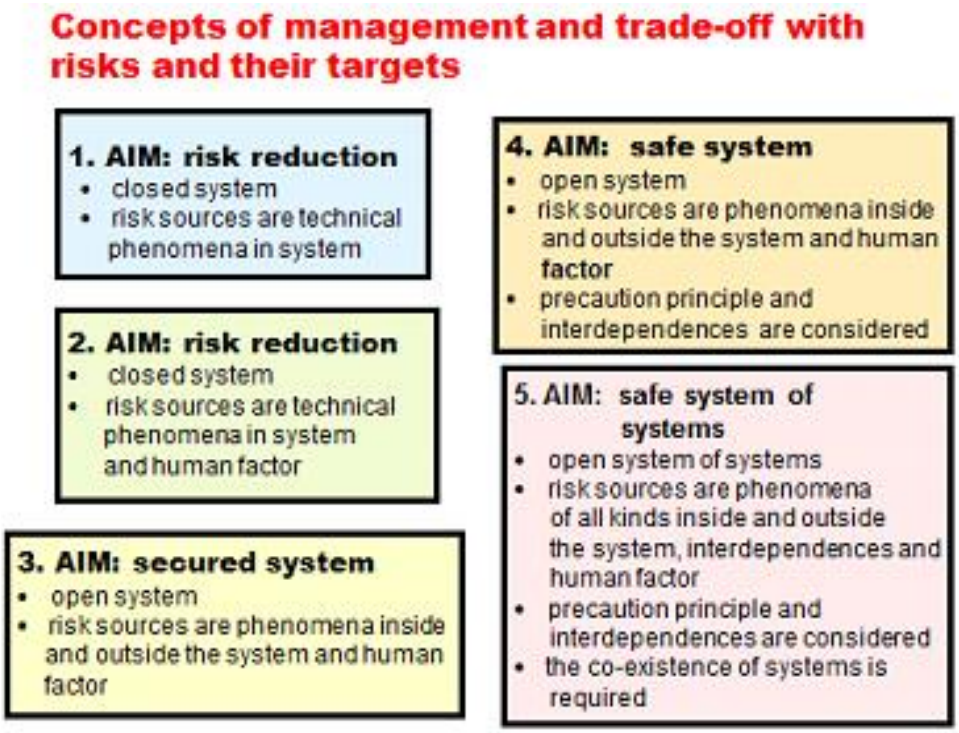

Figure 20. Concepts of management and trade-off with risks and their targets arranged chronologically according to introduction in practice.

The classical risk engineering is based on principle that: the risk was determined after the design of the system; risk determination was directed to the level of system and its components, i.e. there was not considered outer vicinity and the protection of public assets; there were only required the knowledge of system and processes, i.e. there were not required the knowledge of outer vicinity and protection of public assets; and if the risk existed then it was determined and solved but with the lack of the possibility to remove the risks connected with an inappropriate solution for a given site and system. The risk engineering leans on risk management and it searches the problem solution by way that it individually considers disaster after disaster and requires coping with all the risks the occurrence probability of which is equal or higher than 0.05. Usually it only includes disasters the sources of which are within the system and hence it very often only solves technical aspects of the problem. This risk engineering type was a predecessor of advanced risk engineering types, the standards and norms of which started to be developed in the middle of the last century [16,27,28].

The security engineering [27] ensures the system security (the security of system), i.e. it fulfils the targets of security management. It considers the risks from internal and external disasters and from human factor. It is a branch applying the methods, tools and techniques that can ensure the system security.

The safety engineering represents the further degree of engineering trading-off with risks. It is a high-powered tool that ensures the security of system and security of its vicinity. It does not deal only with technical problems but it also respects public assets in the system vicinity. It is a branch applying the methods, tools and techniques and it is based on engineering and managing approaches by way in order that the system might be safe for all public assets during their whole life cycles [28]. The comprehended safety management is particularly marked from the risk management viewpoint by these characters:

- sitting – designing – construction – project with risk reduction,
- operation with the integration of early warning systems and of procedures for the management of the acceptable level of risks,
- and defeating the abnormal, emergency and critical conditions at the operation and at putting out of the operation.

The advanced safety engineering [13] uses at risk determination the following principles:

- risk is determined during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition,
- the risk determination is directed to user’s demands and to the level of provided services,
- risk is determined according to the criticality of impacts on processes, provided services and on assets that are determined by public interest,

- unacceptable risks are mitigated by tool for risk management, i.e. according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up.

Research [36] dealing with the judgement of criticality of the concepts of management and trade-off with risks showed in Figure 20 that criticality of none of these concepts is negligible, Figure 21. Because the system safety is complementary quantity to system criticality; i.e.

safety rate + criticality rate = 1,

we obtain for safety rate values: 0,1, … ,5 and for safety rate the statement “the higher, the better”. By the use of theory of margin assessment often used in the engineering disciplines in determination of optimum solution we obtain median μ = 2 and standard deviation σ = 0.63. This means: μ + σ = 2.63; μ + 2σ = 3.26; and μ + 3σ = 4.89. This means that optimal concept for technical facility safety (i.e. the co-existence of technical facility with its surrounding) is connected with using the model “system of systems”.

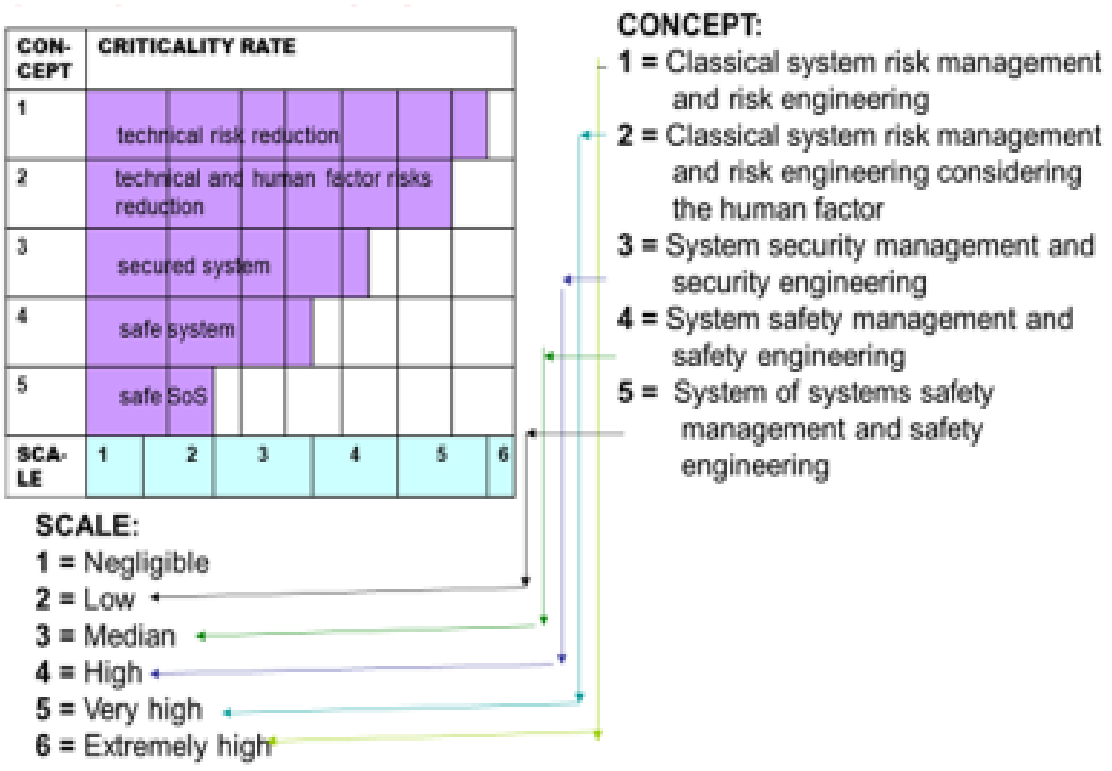

Figure 21. Criticalities of concepts of management and trade-off with risks that are shown in Figure 20.

The safety engineering as a very advanced risk engineering type respects the co-existence of systems with different nature (SoS), and so fulfils the present demands of humans [1-16,37,38]. To prepare groundwork, it is necessary to combine analytical methods with expert judgement by which we remove vagueness in data as was mentioned in chapter 3. The problems that we need to solve in this consequence consist of the acquisition of knowledge and in the assignment “who is the expert”; this was broadly discussed in world conference ESREL2011 [2]. For the first problem solution we need systematically to monitor human system and process obtained data by qualified methods [12,15,16].

It is evident that each more advanced management type in Figure 20 keeps the higher demands on knowledge, tools, times, finance, personnel qualification etc. For each management and each engineering concept there has been developed a certain set of standards and norms for its use in practice. Because the demands of various concepts are different, the standards and norms are different, the results are different and requirements on data, knowledge, material, technology, finances etc. are different. From this reason their capability to ensure human system safety, i.e. human security, existence and sustainable development, is different.

Owing to provident handle with sources, forces and means, it is necessary in real cases to decide which concept is sufficient for a given problem solution. At deciding the role plays the risk size and the level of problem solution. The results of research [13,14,36] show that at problem solution on:

- strategic level, it is necessary to use the system of systems safety management and system of systems safety engineering that fulfil demands of social engineers, technical engineers and environmental engineers,
- tactical and functional levels, it is necessary to respect the strategic concept recommendations and at site specific immediate problems´ solution it is possible to use the system safety management and system safety engineering because the character of solved problems is not so fundamental from the long-term viewpoint,
- technical level it is necessary to respect the recommendations of all higher concepts, i.e. strategic, tactical and functional ones and for site specific immediate problems´ solution it is possible to use the system security management and security engineering if character of solved problems is not so fundamental from the time viewpoint,
- political level, it might be respected the strategic solutions, because politicians usually influence the strategic issues so public interests might be respected.

At solution of emergency situation there is lack of time, information and knowledge, and therefore, it is justified the reaction using the concept of management and engineering trade-off with risk directed to secured system and at critical cases only concept of management and engineering trade-off with risks directed to technical aspects.

The assessment of criticality of individual systems (sectors) of critical complex facility parts and the whole critical complex facility is not trivial matter because under different conditions the sectors and their whole have a different role - active, reactive, critical or damping (not additive); e.g. the existence of several variants of electricity supply to one site decreases the energy facility criticality but it increases expenses etc.

With regard to knowledge summarized in [13,14], the basic principles of safety technical complex facilities are:

- to apply the principles of inherent safety,
- to create a management system that has the basic control functions, alarms and responses of operator processed in the way, so that the system was maintained in normal (steady) conditions,
- to create special control systems, which are based on safety and protective barriers that keep the system in a safe condition also at changing the operating conditions and prevent origin of non-demanded phenomena, i.e. the system carries out the objectives as well as at abnormal conditions,
- to create special safety-oriented control systems that will keep the operation also at a greater change of operating conditions or they have the capability to ensure the operation after the application of corrective measures (clean-up, repair ...), i.e. there are measures for the in-side emergency response, mitigation, and to return to normal operation, i.e. the system carries out the objectives as well as at critical conditions,
- to create special safety-oriented control systems which, in the case of loss of control of system and harmful impacts on the system and its surroundings, shall ensure the application of mitigation measures on the system and its surroundings, i.e. there are measures inserted in system to ensure that the system can be restored, and that the losses and damages caused in the area have been minimized, i.e. they provide measures for the off-side response. System supercritical conditions are the conditions for which the system was not designed, which can lead to situations that threaten the system itself and vicinity of the system.

It is necessary to apply the All-Hazard-Approach [12,15,16,18] and Defence-In-Depth concept [14,29]. In the professional area the layers mentioned above shall be regarded as protective barriers (so-called "protection in depth – defence in depth") and at the resolution of the facilities from the point of view of safety, it is used the security feature that the facility has a single stage or to a five-degree protection in depth. Individual safety management systems ensure the application of the technical, operational and organizational measures and activities that are designed to either prevent the initiation of chains of harmful phenomena, or stopped them.

4.4. Normative risk engineering

Risk engineering deals with management and trade-off with risks. Way of technical facility management and trade-off with risks determines the technical facility safety level. For high-quality risk management, it is necessary to know the risk sources and their possible impacts, and to have the necessary knowledge, available resources, forces and means for defeat the impacts so damages, losses and injuries to protected assets might be acceptable.

The fundamental facts on nature, principles, methods and tools of risk management and trade-off with risks, i.e. recent knowledge from management domain, entity structure (role of interfaces among the human system assets and human system sub-

systems), errors at decision-making and management are given in works [14,15]. As it was given above, the principles for risk management are:

- to be proactive,
- to think through possible consequences,
- correctly to determine the priorities of public interest,
- to think on overcome of problems,
- to consider the synergies,
- and to be alert.

They come out from the stipulated demands that the risk management task is the safety increase, i.e. to find the optimum way how the evaluated significant risks may be reduced on demanded socially acceptable level, or to preserve the determined safety level. From this reason, the following facts need to be respected:

- reduction of risk is practically always connected with increasing the costs,
- risk management needs to be led by effort to find the boundary to which it is endurable to reduce the risk, so the spent costs might be socially acceptable,
- on the basis of just given facts, it is necessary in each real case to establish the requirements that output from trade-off with risks needs to be fulfilled,
- at real trade-off with risks, the stipulated requirements need to be kept and in case their non-observing, the reasons need to be given.

According to ISO [38] the risk management procedure is shown in Figure 22. For the qualified risk management, it holds:

1. It creates values, because it contributes to the achievement of the objectives over the years, such as improving the health, security, environmental quality, the efficiency of the processes and activities, etc.
2. It is an integral part of the processes that take place in the system, because it corresponds to the management structure of the system and it is an integral part of all processes, of them consisting of projects in the facility, and change management.
3. It is part of the decision-making processes in the system, which helps decide according to the importance and recognize alternative ways of solving problems.
4. It is realistic, because it explicitly deals with uncertainty, random and epistemic (ambiguity) in the conditions in which the system is located, as well as in the processes that take place in and outside the facility.
5. It is a systematic, organized and timely, which ensures the effectiveness of the measures and activities.
6. It is based on the best available information, which provides the current knowledge-based solutions.
7. It is a customized system, i.e. it is locally specific, which ensures both economy and effectiveness.

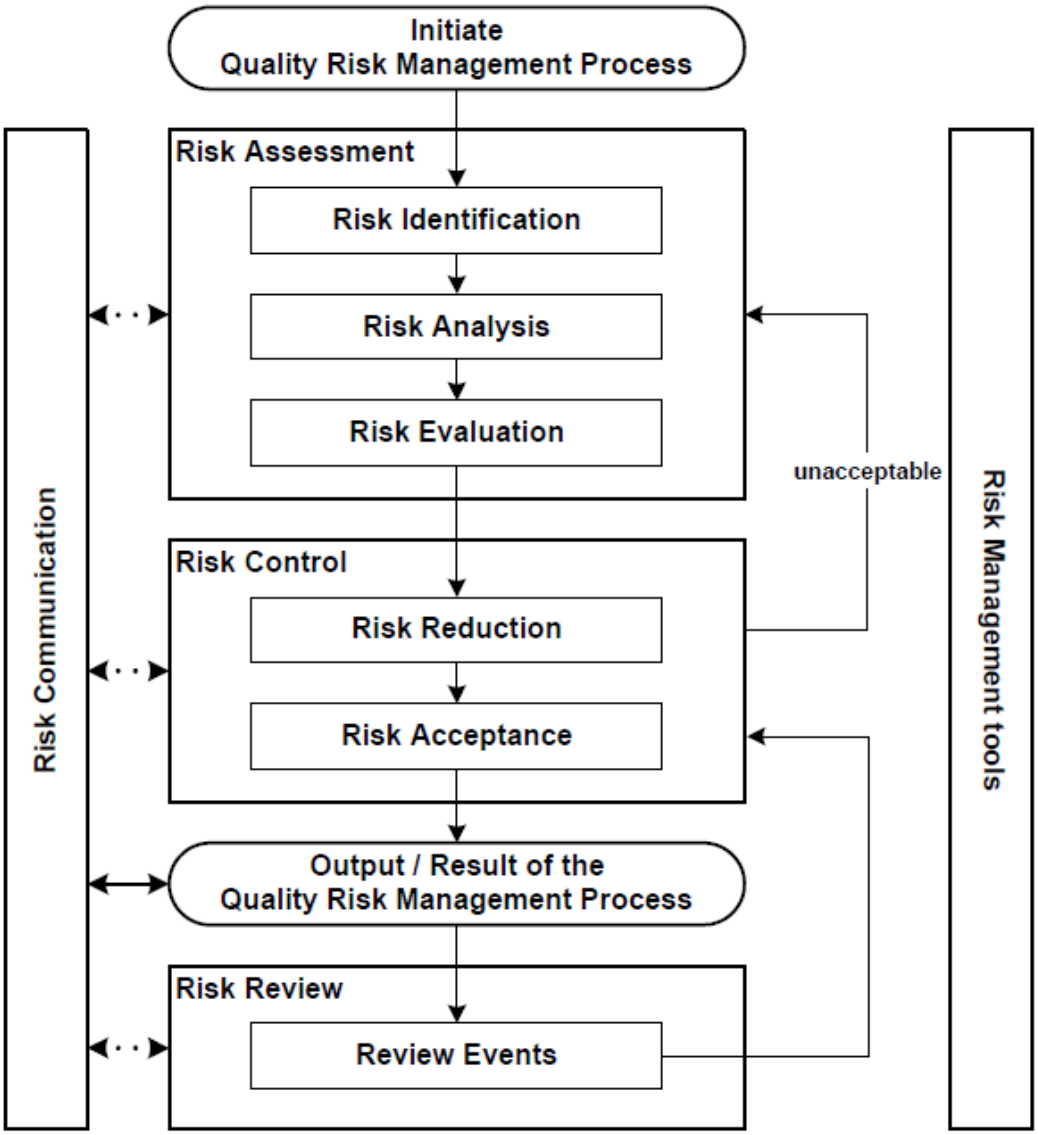

Figure 22. Risk management process; processed according to [38].

8. It considers the human and cultural factors in the system, which affects its acceptability for participating.
9. It is transparent and comprehensive, which increases its reliability.
10. It is a dynamic, repeatable, and responds to changes in the system, which guarantees its timeliness helps continuous improvement and development of the system.

The risk management framework includes:

1. Understanding of the system and its context. In the area outside of the facility it should be monitored, especially the cultural, political, legal, financial, technological, economic, and competitive aspects of the natural environ. In the area of internal it mainly goes about the quality of the resources and knowledge (e.g., capital, time, people, processes, systems, and technology), information systems, information flows and decision-making

processes (both official and unofficial), internal stakeholders, values, culture and management structure of the system.

2. The risk management policy. Risk management policy specifies the links among risk management, the objectives of the system and other policies (it is the preferred option, or is in last place in the decision-making process; how resolves conflicts; what control methods are used, what tools to support risk management, etc.).
3. The results of the integration of risk management into the management processes. So that risk management might be effective and efficient, it needs to be included in all directives and implementation processes that take place in the facility. It belongs to the strategic planning and policy development.
4. The determination of responsibility for the actions and activities related to risk management.
5. The resources required for the management of risks, including the knowledge, skills, experience and competencies.
6. Determination of mechanisms for internal communication and reporting on risks and their management.
7. Determination of mechanisms for external communication and reporting on risks and their management.

For the implementation of risk management, it is necessary to:

1. Establish an appropriate strategy and policy and include them into all the processes in the facility.
2. The risk management process to incorporate into all relevant levels and functions of the facility, i.e., it needs to be part of all regulations and directives for processes in the system.

The criteria for the risk assessment are based on:

- the nature and type of consequences that may occur, including their measurements,
- method of determining the likelihood of the occurrence of risks,
- time frame the consequences and likelihood of risks,
- how to determine the level of risk,
- the level below which the risk is acceptable or tolerable,
- the level of risk, from which it is necessary to ensure a targeted response,
- combination of options more risks.

In accordance with considerations of the current philosophers the risks in the society have their objective and subjective page, in addition they are not out the cultural and value context (even in this direction they are not "purely scientific" problem and they deserve attention from the viewpoint of civil participation). Although modern society uses a comfortable strategy for insurance and compensation, it cannot fully rely on it, since some of the risks are capable to reach the essence of the social system, which pays for certain security risks. Against the "scientism of security policy" it cannot argue, if we can be a reflexive, which mainly means to estimate the consequences of individual acts and not to the illusion about

the possibility of the "perfect solution". The reliance of the public on the experts (and institutions) can lead to a weakening of the capability to participate actively to the solutions, and accomplish so secession of the private and public (which will then be reflected as the inherent risk on that the tests will fail). According to expert concepts when balancing the risks, they have according to their possibilities the duties and responsibilities of all participants (i.e. all interest groups).

Humans, therefore, have the possibility to participate in decision-making, reflect their needs and opinions, namely without fear of penalties. Usually the aim is to involve the greatest possible number of people (even at the cost of increased costs at the beginning of the process), achieving the consensus and conformity. It is also respect for different views and clarifying positions and intentions of various groups and individuals. If we enlist the public in the decision-making process so we enlist all concerned, in accordance with other materials shareholders or the person concerned and the group. A stakeholder is the one (individual, group, organization), who can affect or who may be affected (positively and negatively) as a result of the decision, plan, program, or process that leads to the result.

The problem arises in professional matters, where the basis for decision-making are based on the assessments, which are complex and for a variety of normal citizens of the incomprehensible. The situation in these cases, it is therefore often the war of lobbyists of various groups seeking to order. Therefore, it is necessary to make the assessment procedures based on the legislation and to the selection criteria for the specific solution was focused on the public interest objectives, allow transparency of the decision-making process when choosing the right solution with regard to the resources, strength and resources of the public administration, which has available.

4.5. Challenges for getting the control over risk

Recent FOCUS project outputs [13,19,20] show that the main EU problems, i.e. the EU vulnerabilities are the following:

- All-Hazard-Approach is not systemically applied – risk from some disasters is neglected,
- some disasters are underestimated – risk is lower than it is in reality,
- systemic, strategic and proactive management is not implemented into practice – it is only determined partial or integrated risk – omission of cross-sectional risks caused by linkages and couplings in system,
- gaps in risk management – list of criterions or targets of management are incorrect,
- errors in trade-off with risks – incorrect measures are used,
- research does not determine priority orientations, its targets are influenced by politicians or lobbies,
- application procedures and orientation of strategies are not regularly verified,
- reasonable strategy for disaster management is missing,

- the disaster management does not often respect disaster life cycle; accent to problem solving is missing, still only a lot of discussions on problems,
- lack of resources,
- lack of instrument for ensuring the EU finance stability; and lack of management supporting the public protection and sustainable development.

Mentioned gaps influence the level of control of risks in daily practice. The remove of these gaps or at least the mitigation of their criticality is the challenge in improvement of get over the risks.

The most serious challenge is connected with world dynamic changes in time. This reality very significantly influences the human capability for getting the risks under control, so acceptable conditions for human lives and existence of public assets might be preserved. Since 50s of last century, the data from all prognostic polygons in the world have been showing the relevant changes in processes, the products of which are the disasters. It means that we need to concentrate to the linkage between the process variabilities and the risks.

5. TECHNICAL FACILITIES RISKS AND THEIR MANAGEMENT AND SETTLEMENT IN ENGINEERING PRACTICE

As it was said above, the technical facilities belong to public assets because they ensure products and services on which the humans are dependent [1-15]. Present knowledge shows that each public asset is open system with real time development and these developments are during the time sometimes conflicting [15]. The conflicts´ management is influenced by complex nature of all public assets which is described by system of systems models and time variability. Now we concentrate to specialities of technical facilities.

5.1. Technical facility structure and problems

Each technical facility is created by human activities and it provides products or services important to human´s lives; technical facilities only aimed at military objectives are not 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.

Currently, for needs of practice there are not sufficient individual technical systems, but there are used the files of systems. According to the type of organization, system files according to [13,14] they are divided into the following:

- simply organized units (e.g. machines),
- composite systems characterized by the higher orderliness (e.g. compound sets of machines, which together carried out the acts in a given order to ensure certain products, e.g. linked production lines with the different technologies),
- complex systems characterized by unorganized complexity and compound so as to perform certain functions (e.g. automatic systems for production, categorization and distribution of certain commodities),
- very complex systems, i.e. systems of systems, which are set of complex systems, which can also work independently and together then they perform completely unique task that is remote from the tasks of individual complex systems (such as the human body, environment, systems for production, distribution and consumption of electricity, gas, etc.).

On the basis of knowledge and experience [13,14] for the characteristics and control of:

- simply organized units and set-up units, the results of analytic solutions are used,
- composite systems that are understood as a representation of elements that are organized and connected in a certain way and because of a proper structure they fulfil certain functions, there are used results of statistical solutions based on

analytic functions, the parameters of which are variable in certain intervals, which are reflection of various possible conditions / variants of the system behaviour,

- complex systems and very complex systems, the results of simulations must be used since the given aggregates have many components (often systems too) that interact together and are organized in several levels, which causes that we observe:
  - suddenly emerged features of behaviour that cannot be obtained from the knowledge about the behaviour of components, it goes on sudden emergence,
  - hierarchy,
  - self-organization,
  - varied management structures, which all together appear like the chaos.

Therefore, while observing it is necessary to take a multidepartment and interdepartmental approach. For their management it is then necessary to use the multi-criteria approaches, the model of the system of systems and also consider the cross-sectional risks [15].

For humans´ security and development, the coexistence of technical facilities with their vicinity is necessary to be ensured throughout their life cycles [13,14]. Therefore, in line with current knowledge and experience, we need:

- to know the sources of risk at using the All-Hazard-Approach,
- 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 integral risk.

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 next parts deal with compilation of effective tools for technical facilities risk management directed to integral safety with aim to ensure their co-existences with their vicinity during their operations (life cycles).

At complex technical facilities risk management directed to safety, the system concept needs to be considered. The characteristics of this concept are to:

- see both, the whole and the details at the same time,
- focus on the dynamics of processes,
- pay attention to relations, associations and interactions,

- consider the roles of a feedback,
- consider the relativity of possible situations,
- think in a long-term way.

Management of system of systems addresses questions relating to materials, technologies, design, construction, operation, staffing, organization, education, finance, and law, so as to ensure the demanded processes, which bring profit, ensure compliance with the State and competitiveness, and together to suppress the processes that bring it harms and losses.

From the present knowledge and the facts set out above it follows that the safety of complex technological systems representing the files of open and mutually interconnected systems that are arranged so as to perform certain tasks in the interval of interoperability, mainly depends on the management of the integral risk, and especially on partial risks associated with links and flows in the system. Selecting the appropriate strategy for risk mitigation is very complex and critical task. It does not go on just the reduction of failure occurrence probability, but also on the improvement of the conditions of operating assets, the failure of which can lead to large operating costs. Incorrect strategy reduces the productivity and profitability of the technological facility. Selection of strategy for risk mitigation is, therefore, the typical multicriterial decision making problem. The best strategy needs to be selected from the possible alternatives. It needs to be considered the amounts of criterions, some of which are conflicting [14,15], e.g. Figure 23.

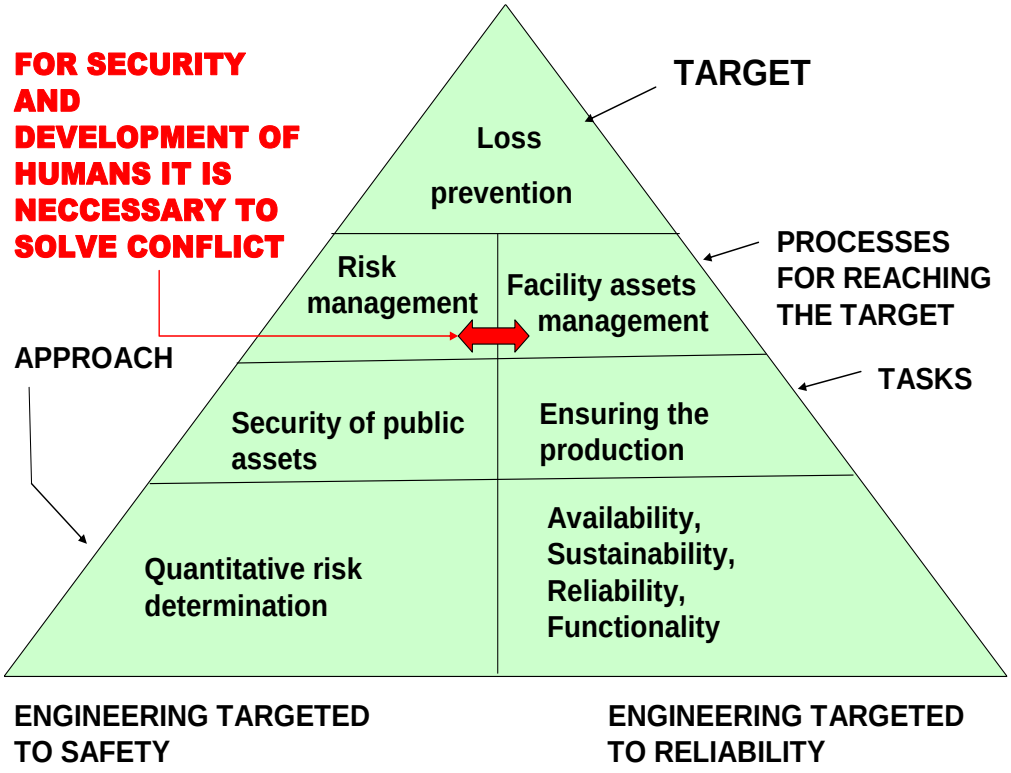

Figure 23. An example of a basic conflict in the management of critical facilities — it is compiled with consideration of ideas in [39].

To avoid the initiation of major risks that at realisation induce the great losses and damages to both, the humans and the other public and private assets, so the basic aim of control of technical facilities is not just to achieve a large number of products, but also the prevention of losses, and therefore, it is looking for a consensus between the risk management and the facility assets management. It goes on finding a way, which will not induce risks that cause losses and damages to public and private assets, which de facto will be greater than the benefits from increased production.

Because at orientation to losses prevention according to [39], it does not only go on reduction of facility failure occurrence probability, but also on improving the conditions of the operating assets, so the SMS (safety management system) of the technical facilities needs to be flexible and needs to be focused on the interoperability of public and private assets.

Heterogeneity and the tight interfaces of systems in the technical facilities are causing the rough description and emergent behaviour of the systems of systems [13-15]. Classic analytical methods do not have the capability to provide adequate sight due to the complexity of the systems of systems. This requires deep understanding and a holistic approach [15].

In addition to the inherent complexity of followed systems there are important their interfaces, known as the interdependences. Of particular importance, there are emergent interconnections that occur only under specific conditions. Just these unforeseen dependencies are the cause of the cascading failures or non-demanded domino effects and other non-demanded phenomena that are the result of different synergies and cumulating, and that are the greatest threat to today's society

Models of management of safety of complex technical facilities, i.e. particular the systems of systems are only in the beginning. They need to have inherent characteristics as a dynamic non-linear behaviour, complex rules of interactions, which are the result of their openness and high connectivity. Then, they need to respect multi-level internal dependencies and the lack of range in required: diversity of nature of services rendered; coexistence of multiple time scales; and level of resolution of the task.

Interoperability (the capability of the mutual co-operation) of subsystems means that subsystems perform specified tasks so that the system of systems fulfils the target in a demanded time, the required extent and in the required quality, namely under normal, abnormal and critical conditions. This means that the behaviour of the elements is coordinated and focused on a specific goal, i.e. by the mutual sharing of the intrinsic instructions (know-how of system), and that there are in the space-time domain ensured such synergies of elements, by which they are reached targets.

It goes on the implicit capability of process system (technology), to ensure the most efficient, high-quality, safe, environmentally sound, economically efficient, automated and integrated run of processes through the boundaries of different internal entities and their vicinity. The aim is to provide mutual services among the operating objects in accordance with the requirements of its subjects in a standardized medium. The interoperability in the context of large-scale application is the capability to collaborate with other systems without any special effort of the customer / user. It is the capability to interact and exchange information among the technical facilities and their information systems in both, the inside and the outside the facility. It needs to be addressed at least in three areas / levels: Data, Applications,

Organization. It is not only a problem of software and IT, but also about communication, technical and organisational matters.

The complexity of the systems of systems is based on the required features of the system, namely: a large-size; the use of multiple technologies; the complex functional dependencies; the great interoperability; big performance; and high safety, i.e. functionality and reliability, and a low threat to the protected assets under normal, abnormal and critical conditions. The SoS problems are heavily sub dividable into clear structure, and therefore, for support of decision making at their management they are created a DSS (Decision Support System) [15,30].

5.2. Technical facilities risk sources

Present knowledge and experiences show that technical facilities are for them beneficial and also dangerous. Humans need safe technical facilities, and therefore, they need to solve these conflicts responsibly and reasonably. Their safety and security are disturbed by phenomena are the results of five different processes in the human system that represents the world [12,17]. These phenomena (disasters) are 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 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 [12,17,20].

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.). 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 by preventive measures. 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 sizes cause damage, loss and harm on assets, i.e. they are the reasons of situations falling on a human and that is why humans have 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”* [12,15]. 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 (Figure 6 and 7) 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, and by the humans’ mistakes during the response etc.

5.3. Technical facilities risk management directed to safety

With regard to present knowledge [13-15], the technical facilities risk sources are external, internal and those connected with humans. Their risk management directed to safety needs to respect knowledge derived above for complex systems. To achieve the sufficient level of technical facility safety it is necessary well to manage and properly to decide.

As we said above, good management and good decision making are possible only when we have relevant data and when we use relevant tools. The term "*relevant data*" means: to be correct (it is known their size and accuracy); to have explanatory power for the problem (i.e. to be validated). The data files need to be representative (i.e.: complete; contain the correct particulars; have a sufficient number of particulars; the particulars need to be spread homogeneously throughout the reference period and need to be validated. In the application of models, random and epistemic uncertainties in the data need to be properly considered.

Ensuring the facility safety requires a systematic approach described in [13,14]. It is necessary to apply to the following model:

- to determine what and why it is necessary to protect,
- to provide for a minimum level of protection,
- to assess the current level of protection,
- in the case of a finding that the protection is insufficient to propose measures,
- to provide the means,
- to apply the measures for the protection,
- periodically to check the state (condition) of,
- to maintain protection at the appropriate level,
- to revise the measures depending on the developments.

Division of competences and responsibilities is an essential and important in every more complex activity of human society.

In order to ensure the safety of the facilities at siting, design, construction, and operation it is necessary to ensure that these comply with the required functions under all conditions (normal, abnormal and critical) and prevent them, in order to not carry out activities that are likely to cause unacceptable impacts to the human system, especially on human security. This means that in practice, there are implemented appropriate technical, legal, organizational, economic and educational measures aimed at ensuring the reliable operation of specific objects, infrastructures and technologies under design conditions and under beyond design conditions to limit and mitigate impacts on people and the environment, while the obligation of their use is required by law.

To the given purpose there are mapped all the possible problems of the existing facilities that can cause adverse effects on the human system. For reliable operation there are codified rules for the siting, design, construction and operation. From the engineering point of view, there are determined the conditions and limits of operation, installed safety and safety

related systems (active, passive and hybrid), and it ensures their appropriate backup [13]. ***This means that addresses questions such as:***

- what security systems and safety systems are appropriate and what it needs to be their backup?
- where / in which places the safety and safety related systems operate effectively?
- why they are just used there and not elsewhere?
- in what limits they reliably work?

In accordance with the works [13,14,21], it can be used two ***scales for the evaluation of facility*** safety***:***

1. The scale for the assessment of the severity of the losses associated with the failure of the facility:
   - degree 0: the losses of the facility do not have impact on the security and development of the territory,
   - degree 1: the losses of the facility have a small impact on the security and development of the territory,
   - degree 2: the losses of the facility have a middle impact on the security and development of the territory,
   - degree 3: the losses of the facility have a significant impact on the security and development of the territory,
   - degree 4: the losses of the facility have a very important impact on the security and development of the territory,
   - degree 5: the losses of the facility have a very substantial impact on the security and development of the territory, causing its collapse.
2. The scale for the evaluation of the degree of damage of facility according to the times, for which the damaged facility can be repaired or replaced:
   - degree 0: damaged facility can be repaired or replaced in the time interval 0 - 5 days
   - degree 1: damaged facility can be replaced in the time interval 6 - 30 days,
   - degree 2: damaged facility can be replaced in the time interval 31 to 90 days
   - degree 3: damaged facility can be replaced in the time interval 91-180 days
   - degree 4: damaged facility can be replaced in the time interval longer than 180 days,
   - degree 5: damaged facility cannot be replaced.

When we consider the complex technical facility and its interconnections physical, cyber, logical and territorial, so we may recognize that there are different types of failures, namely: cascading and escalating; and disorder of the same cause (e.g. certain disorders from a natural disaster). Their operational conditions are normal, abnormal, and critical. A measure of the tightness of their relations and the interfaces is: free; tight; and complex. ***The characteristics of the facility*** they are: time; territorially spatial; organizational; the ownership; and

institutional. As a result of mutual dependences, the disorder or failure of one subsystem will cause a malfunction or failure of another subsystem. This fact contributes to the criticality of facility in the territory / object / State.

On the basis of the results of the project [13] for assessing the facility criticality there are used questions:

1. How the facility reacts to certain types of disasters?
2. How is the facility of massive, resistant and flexible?
3. How the behaviour of facility can improve?
4. What is the appropriate facility mechanism of control?
5. What are the facility rules for self-regulation or to acceptable variation may be used?
6. Which parts of the facility are critical?

The answers to these questions are searched in six steps:

- modelling of a problem situation,
- the analysis of the layers: physical, regulation and management, organisation, strategic management,
- compilation of scenarios,
- analysis of impacts,
- planning the measures,
- and implementation of a robust and adaptive solution.

In practice, there are two types of critical items [13,14,21], namely:

- items that only cause an escalation of the impacts of disasters, either all, or just some, that are possible in a given place,
- the items, which guarantee the functionality of the facility, i.e., the safety and development of the protected assets. Their failure due to some disaster or due to operational aspects leads to serious impacts on the protected assets.

For the first type it is at the restoration carried out by upgrading the item to the disasters, which in this case cause or may cause unacceptable impacts. Implementation of their recovery has no priority from the viewpoint of the functionality of the territory. For the second type it is already in the planning, design, construction and operation carried out measures that lead to an increase in their technical reliability. Various measures are used as well as backing up the activities of the other items that lead to higher resistance against possible disasters. Therefore, at the restoration it is necessary to make measures in both, the backup and the upgrading. Because these items are life-giving for complex facility, there are priorities in the reconstruction, and it is necessary that the public interest was preferred before private interests.

From the foregoing it follows that the conditions of technical facilities are not stable, they are dependent on the internal and external processes and their dynamics. Changes to the terms, of course, give rise to the various processes in the complex technological facility. When responses to the aforementioned processes exceeds the limits and conditions for existence of elements, components and systems of the facility, so it appears not only local

disorders, but also disorders as a result of various synergies, domino effects and cascade failures.

The reality is that there are many approaches, norms and standards, the use of which ensures the safety of technical facilities but accidents still occur, and therefore, experts are looking for more new and effective approaches for their construction and management during operation.

Safety culture is designed on the basis of risk management at all levels of the administration management of facilities: the technical, operational, tactical, strategic and political (see Figure 4). Safety is measured either by using specific indicators [12,26], or by the criticality rate [13,14].

The development of technical facilities is becoming more and more to a combination of individual devices and applications to complex facilities in order to achieve an increase of production and to high profitability. There are interlinked systems of nature technical, organisational, cyber, and logical, they create systems of systems (SoS) [13,14]. Formed facilities are not the result of experts from one discipline, but they are the result of an interdisciplinary team. Especially, technical facilities that have a network structure, it holds that the individual expert is not capable to completely examine and control the large interconnected systems, and it is, therefore, necessary the cooperation of experts from many disciplines, which requires mutual understanding the objectives and capability for searching the consensus. From the need to ensure security and sustainable development of human society it is a prerequisite for the construction of the complex facilities the control of their safety. The special research [13] showed that this is present management weakness.

It is logical that in complex facilities the safety functions need to be considered in context with the other functions of the facility and its subsystems. That is not enough to solve the details (i.e. security problems within the individual subsystems), but it needs to be addressed at the same time safety of complex facility and safety of individual subsystems [13,14]. In accordance with the knowledge in [12-21] it is necessary to count with the following hazards:

- the external hazard (hazards from phenomena in the vicinity of the facility),
- internal hazards (hazards from internal phenomena and equipment of individual subsystems),
- operational hazards (hazards associated with the failure of the function of the entire facility or device or system components, i.e. the failure of subsystems),
- hazards associated with the installation,
- human hazards (hazards associated with human activities – physical and organizational).

The reality is that the safety of the individual technological sectors depends on security traditions, which developed in the sector for some time. Therefore, in the whole composite of several sectors there are carried out diverse safety measures that correspond to the knowledge and experience of the time in which they were created. Today, the reality is that when compiling the technical facilities and in creating their safety, the experts from different fields are working separately, which does not guarantee optimum safety, or even an optimal cost. It often happens that the individual subsystems are safe, because for them there are standards and norms (e.g., individual technical parts of a particular operation), but the safety of the whole, which was their interface with the cyber and other infrastructures, has not

monitored, because the evaluation and demonstration of safety is not required by the relevant legislation, and in addition to that purpose it has not been yet available the relevant professional procedure. The results are the organizational accident [15].

The management of complex facilities needs to respect the multi-level internal dependencies and the lack in interface in diversity of the nature of the services provided, in the coexistence of multiple time scales and in the level of address that are required, in order to fulfil the objectives of the analysis.

In these contexts, it should be aware of what we determine in practice and how it agrees with the integral safety. According to the current procedures, the risk from a particular activity is expressed in two dimensions – individual risk and group / social risk. The first demonstrates the likelihood that an individual will lose life as a result of the activity. The second shows the same for a group of people. The individual risk is the probability of death of a person, who is permanently exposed to certain risk in the area of agent per year. It displays using the isolines and it is used in land use planning.

To ensure the safety of complex technical facilities, it is necessary to concentrate on the serious risks (see requirements of modern methods of project management [34]), i.e., from the possible sources of risk to select sources of risks that cause serious impacts on protected assets and against them to focus preventive and mitigation measures. The objectives of the risk assessment for large technical facilities as follows:

1. To identify initiation phenomena and sequences of subsequent phenomena, which can significantly contribute to the damage and injury to protected assets.
2. To provide realistic quantitative extent the likelihood of phenomena, which causes the realisation of risk.
3. To provide a realistic assessment of the potential impacts of harmful phenomena associated with the hypothetical sequences of events that lead to the accident or failure of technical facilities.
4. To provide a reasonable basis for deciding on the sitting the design and the operation of the facility.

For the evaluation aimed to determine the priorities for the implementation of preventive and mitigation measures it is most commonly used methodology of PSA (Probabilistic Safety Assessment) [30], i.e. the analytical method for the promotion of the protection of public health and safety. The result of the evaluation is then:

- list of responses of equipment to initiation phenomena and a description of the sequence of phenomena that may follow,
- evaluation of the significance of the identified contributors to the risk. There are identified high risk sequences that lead to the accident and also the activities that lead to their mitigation.

At technical systems failure, it typically occurs a sequence of more external and internal impacts, both primary and secondary, that can be just only influenced. These impacts then affect in a different intensity and in a different time period. Therefore, in the preparatory phase of documents for the safety management of technical facilities (especially those the model of which is a system of systems), it is necessary to identify the range of relevant impacts and to determine in what context they operate, whether they are directed to political,

economic, technical, personnel, and other environ and what appropriate measures can be used to remove them, where appropriate, to mitigate them. Evaluation and management of possible hazards and risks that follow of them belong to the demanding and crucial processes of safety management. Hesitation and procrastination of solution has a very huge impact on the entire public governance, and thus on the development of human society [13-15].

In order to achieve a reasonable level of safety of technical facilities it is necessary to introduce an obligation to practice so to deterministic and probabilistic safety analysis have been carried out for all technologies with a greater risk of damage [15,30]. Because no large databases of data, so probabilistic analyses have not been sufficiently focused on the target yet. Therefore, it is necessary further development of methods for the analysis of disorders, which are directed to determination of the risks.

The good governance (proper management of public affairs) [12] also regulates the safety of technical systems, and therefore, it needs to ensure so that the safety certificates may need to be required from all technologies with increased risk. This request requires that, in practice, it had to perform a reliable risk control through preventive measures, which are economically reasonable. From the request, it follows that the technical legislation needs to be primarily oriented towards compliance with the objectives of safety, which means the only permissible / allowed risks. Only as a secondary objective the legislation may require specific technical steps for the achievement of the objectives of the safety.

Each technical system contains a number of inherent sources of risk. System failure occurs when in the system it is realised an unwanted process, which is initiated by either the expected risk or is trigger by random combinations of a few likely phenomena. In grounds for the safety management the second mentioned option has been often neglected. The proof there are usually legislative requirements on the safety reports that have be processed in developed countries for technical facilities [13,14], and in many cases, even for important civil objects.

In addition to the failure of the technologies that lead to the leakage of hazardous substances, fire and explosion, it is necessary for technological facilities to assess local impacts caused by technical facilities that cause harm to the environment, social and economic life of human society. Both types of mentioned impacts together form the potential of risk, and this is the reason for the request, that they need to be discussed in one safety analysis. At the present time, the question is how to incorporate into an environmental pollution into integral risks. In this context, it is important to know the ratio of the actual concentration of the contaminants and critical values for their concentrations. Existing support documents are not yet sufficient for the evaluation.

To ensure the safety of large technological facilities the EU issued on the basis of the recommendations of the OECD for Seveso companies following the instructions [40,41]:

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 technical 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 conditions,
   - 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. Systems on the hierarchically higher-level control 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.

Professional basis for the guidelines developed the OECD [26,41] using the principles that already from the end of the 1970s, has used by the IAEA [42].

Since the conditions of each open system depends on the vicinity conditions and both are dynamically evolving, so the safety in today's concept is concentrated on both, the security of the system, so to ensure security around the system. The set of measures and activities shall be determined on the basis of knowledge of the risks associated with possible disasters, so with the specific construction of the facility (expressed by followed assets, links and flows in the facility system), and by the specific interfaces among the facility and its surroundings or among several related facility systems and their surroundings.

For technical complex facility it holds that it performs certain demanded objectives only under certain conditions [13,14]. The aim is to ensure the coexistence of all facility systems and safety of both the individual facility systems, so the whole facility and its surroundings. For sources of risk there are taking phenomena (disasters) the sources of which are inside, including the human factor, and outside the system, and most recently, the phenomena associated with the interfaces among facility systems and their vicinities and phenomena associated with links across the facility system of systems, at manifestation of which the damages and losses occur in the system or in its assets.

The requirement in the previous paragraph is correct and logical, just its filling is not easy, and it is partly due to lack of data about the behaviour of facility in different conditions, partly because of the complexity of the facility, and because of the variability of conditions in which the real facilities are located. The application of probabilistic models allowed considering random uncertainty and thus it brought some progress. Because in addition to random

uncertainties there are still epistemic uncertainties in the behaviour of facilities caused by lack of knowledge about the facility and its behaviour under all possible conditions, it is not fully relied on the results of probabilistic models. Their major defect it is often not what they include, but what do not include. Low values of the occurrence probability of unreliable behaviour of facility simply talks about that facility does not fail by considered way, but it does not say anything about the fact that the facility can fail with far more probability in a way that was not considered [13,14]. Differentiation of risk associated with the origination of the accident from the errors, it is essential to understand the difference between safety and reliability.

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. A prerequisite it is the use of system thinking. From a theoretical point of view, it is to be:

1. To create a description of the characteristics of the technical facility, which has both, the public assets and the assets of the facility itself (which are the good condition of the subelements, reliability, and correct functionality of subsystems and the entire system), among which there are internal links.
2. To identify significant risks (in the facility system there is more protected assets, which are interconnected by internal links) for sources of risk both inside and outside the facility.
3. To establish criteria for the integral safety of the facility.
4. To establish the terms and fundamentals of communication for multidisciplinary and interdisciplinary cooperation at ensuring the facility safety.
5. To establish the principles for the management of facility safety.
6. To establish legislation on support of facility safety management.
7. To create control mechanisms for monitoring the facility safety.

Safety is a matter for all concerned. Therefore, in practice, there used the so-called. The GOLDEN RULES of ALL PARTICIPATING [12,26], which lay down for everybody the following:

- according to his / her possibilities by preventive measures to prevent the origination of natural or other disasters, or at least the origination of their unacceptable impacts, to ensure preparedness to deal with unacceptable impacts on the protected assets and the effective response,
- communicate and collaborate with others interested in all aspects of prevention, preparedness and response,
- knowing the hazard from natural or other disasters and possible risks in the territory as well as in 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 on the basis of the results of research and development, and lessons learned from the experience, respectively, to correct their activities,

- use the principles of inherent safety at design, the building and operation of facilities and their equipment,
- carefully manage change
- be prepared for all disasters that may occur,
- help others interested in performing their roles and responsibilities,
- search forever the improvement of safety,
- work in conformity with the safety culture, safe practices, and training,
- to strive constantly for all of the information and to provide information and for management staff featuring the feedback
- 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 and accordingly to plan measures for its good management,
- the use of appropriate and coherent policy for land-use planning and follow-up activities,
- be aware of the risks in the village / organisation / territory / business and know what to do in case of their realization,
- to participate in emergency planning and response.

The procedure for creating a program to increase safety in the facility [12,26] 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.

The complexity of modern technical facilities is growing. On the one hand it means the increasing efficiency of facilities, but on the other hand, it creates new sources of risk that are wrongly detectable. Some of the ways to ensure their safety (e.g. redundancy, duplication of partial components for protection against a failure of the measuring circuits or regulatory functions-backup) provides protection from accidents caused by the failure of individual parts, however, they are not equally effective against harmful phenomena that generate interactions among components in the increasingly complex and mutually interacting technical facilities today. Redundancies may in fact increase the complexity to the extent that they themselves are contributing factors to accidents [14].

Therefore, many of the new dangers are more insidious, less exposed and given out, than in the past. In addition, there is no previous experience, which could be used to overcome new dangers. A lot of experience and lessons learned from previous disasters is stored in the laws, standards and practices good practice. But the corresponding laws and standards for many of the new engineering and technology sectors are not yet developed. Many times, the lessons gathered for centuries will lose when the older technology is replaced the newer; for example, when mechanical device replaces the digital computer [14,43].

Other new dangers are only a summary such as:

- increasing exposure to danger,
- increasing accumulation of energy and risk implications,
- increasing automation,
- the growing centralization and production capacity,
- the increase in the pace of technological changes.

5.4. Methodological aspects

From reasons given above, it is necessary to continually monitor the effectiveness of the measures and activities aimed at safety and when deviations occur to apply corrective measures, or to change the concept of working with risks, as shown in Figures 8 and 23.

For the understanding of the concept of the safety solution of complex technical facilities it is given in the first the summary of the important factors, which are:

- basic knowledge to ensure the safety of complex technical facilities proven in practice,
- key concepts of safety and risk engineering,
- and the assessment of the credibility of theoretical models.

Then we will describe the concept of safety of complex technical facilities, which we designed by help of the logical synthesis of knowledge and experience in the computing and control practices, namely including the safety management procedure in time, which we verify in practice [13,14,33,36,43].

On the basis of the objective of ensuring the safe complex facility we are interested in all of the possible scenarios for the behaviour of the particular scenarios that degrade system and deplete the system and its surroundings, because there we have from the perspective of the protection of people's attention and make measures to target. On the basis of knowledge

and experience, the behaviour of each followed facility is the dynamic process, i.e. the process evolving in time, which is formally described by ordinary differential equations [44].

In practice, however, we cannot often establish analytical functions describing the behaviour of a facility, because the facility behaviour is not specified by one variable, but several variables, the values of which are interrelated, i.e. mutually dependent, and we cannot accurately describe the relationships among the variables, which provide mutual dependencies, and therefore, we use models, theoretical and physical. A good model allows describing the system, understanding its behaviour and predicting it. In the case of complex systems, we use a wide range of models and each of them provides a description and understanding of the just from the perspective of certain aspects [44]. Methods based on use of models are followed in Annex 2.

For understanding and research of complex systems it was formulated the theory of complexity, which is based on assumption that complex systems organize themselves into the emergent states (conditions), that are not predicable, as the example there are shown the genetic algorithms, cellular automata and neural networks. The theory explains the new features of systems, such as the organization itself, and its diverse specialties and moves forward the importance of properties, such as the emergence of a new feature, which is the result of a symbiotic effect of component parts, the phase space and the eligibility of circumstances cause a change [30].

In the technology practice in the given context there are used the chaos theory, complexity theory and the theory of options, i.e. the Dempster-Shafer theory [32,36,44]. The latter theory is based on assumption, that the available data and our knowledge of the system they have random uncertainty and epistemic uncertainty. In practice we often exclude the epistemic uncertainty by assumptions like "the data file for specifying the behaviour of the system is a representative"; "some analytical function describes the process of occurrence of the given phenomenon perfectly", etc.

In theory of the possibility we use a combination of analytical procedures and data from the experts, and therefore, according to it should be noted that an expert is a person who is recognized by the professional community, has an experimental experience in a given area, a number of high-quality publications, knows the essence of the uncertainties of the various concepts, the diversity of conditions, ways of compensating damages and is interested in the solution of the problem. It is necessary in this context to understand knowledge as information obtained from experiences in the application of real results in practice. For the expert, it is necessary to determine what knowledge and in which process he / she should give the data [32,44].

Each dynamic process develops over time and it can be described by ordinary differential equations for continuous systems or algebraic equations in the case of discrete time periods. A linear system is a system that can be to describe by a linear function. If they are dynamic processes of linear and time-invariant, so for their description it can be used: Laplace transformation for continuous systems; the z-transform for discrete systems, and according to the transfer function to determine whether the system is stable, unstable, or at the interface [44].

Deterministic processes are described by the analytical function of time, and therefore, they can be at any point in time to determine their values. ***Random processes*** are described by the probability function that in each time moment determines the probability of

the possible values, which can realisation of random process realization get. ***Random process is the stationary*** if the probability density function is independent on the choice of the beginning of the timeline (i.e. the mean value does not depend on time). At non-stationary processes the statistical properties are variable in time. ***Random process is ergodic***, when all of its realisations have the same statistical properties (it allows to estimate the parameters of the process from one realisation or at the long-term process by the use of data from several different starting conditions). Non-linear systems are, for example, systems with hysteresis. Under certain circumstances they exhibit a phenomenon which is characterized by sensitivity to initial conditions, the so-called deterministic chaos and, therefore, their management is difficult [30,44].

Not only in monitoring the disasters, but also in engineering practice, it holds that the available data are often only in small quantities and are not of good quality. In some cases, it is about the fundamental problems because there is no accurate models and the exact values of the parameters; the information is inaccurate, dispersed, incomplete, sketchy, vague, non-homogeneous, or just a verbal. Among the basic types of uncertainties in the engineering practice they belong:

- randomness as the natural properties of the underlying variables,
- statistical uncertainty due to limited range of data,
- the model of uncertainty caused by imperfections of computational models,
- the uncertainty caused by the inaccuracy of the limit states (conditions) definitions,
- gross errors caused by shortcomings in the activities of the persons,
- and ignorance of the actual behaviour of materials and structures.

Because of the deterministic methods have been gradually replacing by probabilistic ones also at designing critical objects and equipment. However, even these have limitations, because even the exact observance of the norms and standards does not consider all the uncertainties that exist in the real world.

Specifics of engineering methods, tools and techniques lies in the fact that it impossible separated the characteristics of the phenomena, against which the facility needs to be protected, properties of materials, structures and devices that make up the facility, the operating conditions and limits, the detection of distortion of facility when the limits are exceeded and correction measures to support the safety of the facility and its surroundings. The aim is, however, high-quality solution in the given circumstances, and therefore, it needs to fit together the exact results with results of good engineering practice, and it primarily means to use only proven procedures and verified data.

Proper engineering solutions and the selection of methods, tools and techniques depends on:

- the number and nature of the assets,
- the choice of the concept of the solution to the problem,
- and the stage of the proceedings, for which the solution is, i.e., whether it is about the measures and actions of prevention, preparedness, response and recovery.

The specifics of the safety engineering create special demands on the methods, tools and techniques, because:

1. When troubleshooting, it is considered that:
    - all of the processes are underway in the dynamically varying world, and therefore, it is necessary a special apparatus, i.e., a set of procedures that will ensure an optimal risk management,
    - disasters are many, and therefore, it needs to use All-Hazard-Approach,
    - disasters act on assets in manifold ways and, therefore, an important role is played by the vulnerability of assets and their interconnections.
2. On the basis of evaluation of available data files, the existing random uncertainties and epistemic uncertainties in the available data, it is necessary to divide the tasks of the practice, which can be addressed by way of deterministic or stochastic and or heuristically.
3. It is necessary to apply a good qualitative and quantitative approaches to risk and safety of the system in all the steps, which are:
    - definition of system and its vicinity,
    - identification of sources of risk, i.e. disasters for the system,
    - *determination of hazard for extreme events* induced by beyond design disasters,
    - evaluation of risks,
    - proposal for a corrective and remedial measures and activities according to the criteria of safety, with the aim to ensure adequate security
    - and verification of the acceptability of the risk.

The basic ***strategic approach for the safety of complex technical facilities*** is based on the realization that: nothing is absolutely safe; the elements, links and flows in the facility may fail sooner or later; and, therefore, it is necessary to a sophisticated facility safety management system. Efficient and effective safety management needs to be based on current knowledge and their correct interpretation in the context of that applies in a given territory.

For high-quality collateral listed sections are used by different standards, norms and procedures of good engineering practice, e.g.:

- EN 608 (2007) Techniques of analysis of reliability of systems-procedure of analysis of methods and the consequences of failures (FMEA),
- IEC 300-3-9 Management of reliability – part 3 – section 9: risk analysis of technological systems, January 1997,
- ISO 13824 (2009): The Bases for design of structures-General principles on risk assessment of systems involving structures.

Ensuring the complex facility safety requires a systematic approach. It is necessary to apply to the following model: determine what and why it is necessary to protect; provide for a minimum level of protection; assess the current level of protection; in the case of a finding that the protection is insufficient to propose measures; to ensure the resources; apply the measures for protection; periodically check the condition; maintain protection at the appropriate level; and revise the measures depending on the developments. Division of competences and responsibilities is an essential and important in every more complex activities of human society.

Another crucial problem is connected with the fact that at the solutions of their critical conditions they often arise conflicts of interests and, therefore, they arose the whole theories, how to resolve conflict in the management of technological facilities. According to them, a conflict management process it is seen as planning, how to achieve a mutually advantageous solution of serious problems. Tool, i.e. the risk management plan requires that both parties of the conflict have agreed in advance how they will deal with the expected contentious issues with regard to the established interests and objectives, which is to ensure the security and the development of people, namely now and in the future, and also maintaining the operability of the technology.

The costs on safe complex technical facility is not just the costs of its project and construction, but they also include the costs of operation, maintenance, repair and modernization. Therefore, the risks associated with each technological facility also need to include the risks of just being referred areas and the facility management needs to be able to deal with them. This means that it is necessary to evaluate the risks of disasters, such as: the failure of the financial market and with it associated failure of finance on the maintenance, operation, repair and modernisation of facility; corruption; misuse of powers; attacks on the integrity of the facility, etc. It is, therefore, that the criticality of facility also increases if it is not proper maintenance and regular repairs, which caused the increase of vulnerability.

On the basis of pro-active approach, which is own to project and procedural management, it can be effective to prepare for solution of conflicts in critical situations in advance; i.e. to prepare a risk management plan, which is agreed by all stakeholders, because each time delay leads to further damage.

Based on knowledge of the professional literature and experience, it is true that the basic principles of safety technological complex facilities are:

- to apply the principles of inherent safety,
- to create a management system that has the basic control functions, alarms and responses of operator processed in the way, so that the system was maintained in normal (steady) conditions,
- to create a special control system based on safety and protective barriers that keep the system in a safe state (condition) also at changing the operating conditions and prevent origin of undesirable phenomena, i.e. the system carries out the objectives as well as at abnormal conditions,
- to create a special safety-oriented control system that will keep the operation also at a greater change of operating conditions or they have the capability to ensure the operation after the application of corrective measures (clean-up, repair ...), i.e. there are measures for the in-side emergency response, mitigation, and to return to normal operation, i.e. the system carries out the objectives as well as at critical conditions,
- to create a special safety-oriented control system which, in the case of loss of control of system and harmful impacts on the system and its surroundings, shall ensure the application of mitigation measures on the system and its surroundings, i.e. there are measures inserted in system to ensure that the system can be restored, and that the losses and damages caused in the area have been minimised, i.e. they provide measures for the off-side response. System supercritical conditions are the conditions for which the system was not designed, which can lead to situations that threaten the system itself and vicinity of the system.

Sometimes it is talking about it, that each layer is the protective barrier (so-called protection in depth) and that the systems have a single stage to five stage protections in depth. Each layer contains measures which are capable to avert the occurrence of undesirable chain of phenomena or stop it, when it is triggered. The measures are technical, operational and organisational, and their goal is to reduce the risk.

The logical synthesis of data collected by research, described in the works [13,14,17] it was designed the process model for the safety management of the territory and all facilities that are located in it, targeted on security and development of the people, which take into account the survival of people in critical conditions. A generic tool for the SoS safety management consists of 4 parts, Figure 24:

1. Screening the SoS.
2. Risk assessment of the SoS.
3. Screening the existing measures and activities for the SoS risk management and for increasing the SoS safety and the evaluation of the level of negotiation with the risks.
4. Identification of the critical SoS risk management items and proposal for solution of gaps related to human survival or continuity of assets at critical disasters.

The aim of the first part denoted in Figure 24 as ***"territory"*** is to create a credible scheme and specify the properties of the territory (in the range of land-use planning documentation, as it calls for the territorial planning) - layout of objects important in terms of the protected assets (life, health and security of people; property; the public welfare; the environment; infrastructure and technology, and sources of domino effects that can increase the severity of the situation caused by the disaster; a list of potential disasters, based on the application of the principle of the All Hazard-Approach and the data on the impacts of possible disasters in the territory; and including information about the error in the data about the real disaster. Therefore, it is done the SoS screening, which consists of the following parts:

- determination of the characteristics of the SoS (in the case of the territory it goes on the characteristics in the extent of land-use planning documentation),
- classification of SoS (in the case of the territory – industrial area, agricultural area, forest, etc.),
- application of interface of the All-Hazard-Approach, and the documentation of the SoS, i.e. it is fixing the file of disasters that may have on the SoS unacceptable or conditionally acceptable impacts, i.e.,. they are dangerous for the SoS,
- identification of vulnerabilities of the SoS (e.g. using a SWOT analysis for the weak and strengths, risks and possibilities of the SoS management mechanism).

The aim of the second part, denoted in Figure 24 as ***"risk"*** is to create for each specific disaster by help of methods of What, If and case study [14] the three scenarios of disaster impacts for the size less than the design disaster and beyond design disaster. Each of the given scenarios contains a separate list of impacts on protected assets in the times measured since the origin of the disaster in a given territory: 0 h, 3 h, 6 h, 24 h, 3 days, 14 days, with the fact that from time 3 h there are separated the primary and secondary impacts and collect data on cross-sectional risks – a general and specific for the area.

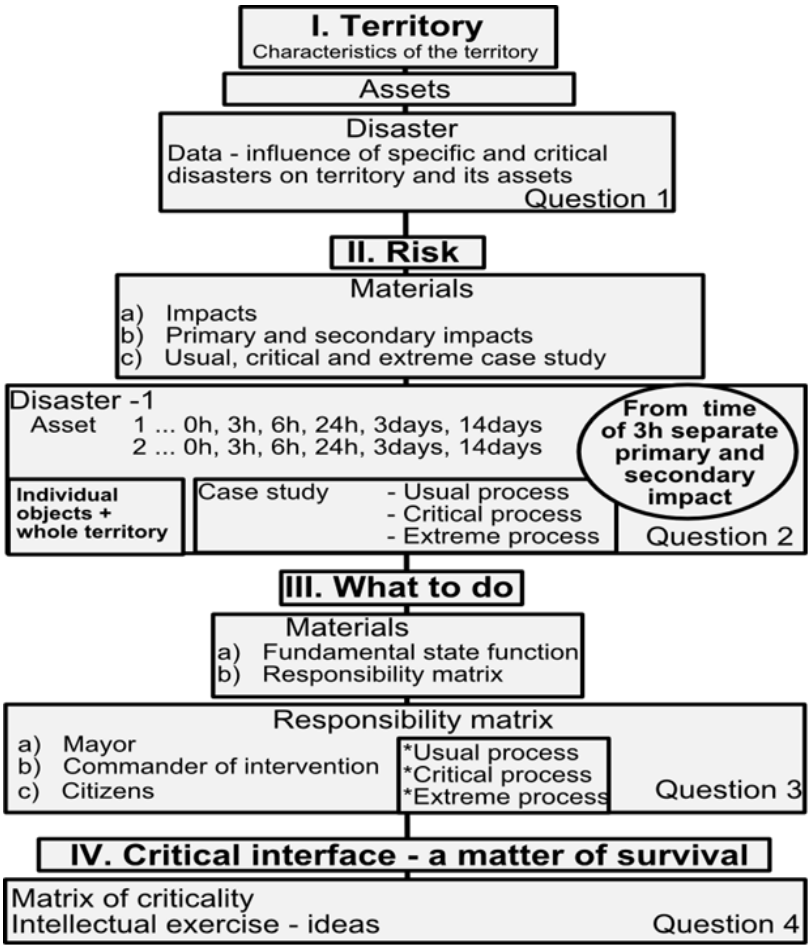

Figure 24. Process model of safety management of territory. Phases: I-the characteristics of the territory, i.e., assets, sources of domino effects and potential disasters; II-determination of risks for every possible disaster in 3 sizes; III-a cumulative assessment focused on the identification of conflicts, not covered by the serious problems and lack of responsibilities; IV-the determination of the critical situations and measures for the survival of the humans.

The objective is to obtain data for the identification of the places in which they are the necessary protective measures and measures for response - evaluation is carried out for both, the territory and the critical facility. Therefore, there are appreciated the SoS risks associated with all disasters that were identified as dangerous in the first step. With regard to the existence of random and knowledge and uncertainties in data, there are:

- process the variant scenarios of realisation of risks in the SoS for each dangerous disaster (e.g. by using a modified form of the link method, What If and targeted method of case studies [30]); with regard to the knowledge there are created the disaster scenarios for size of disasters: normal, critical, and extreme, in which there are separately followed the impacts on the SoS individual assets at defined time intervals (e.g., for the territory there are proven the simulation for periods of time

measured from the occurrence of the disaster: 0h, 3 h, 6h, 24h, 3 days, 14 days, 1 month),

- for each dangerous disaster there are evaluated secondary and higher impacts on the SoS assets, observable in the times of 3 h, 6 h, 24 h, 3 days, 14 days, 1 month, namely at scenarios of dangerous disasters of critical and extreme, and they are revealed the locations of the origin the cascading failures and possible cascades of impacts,
- by the overall evaluation of the data obtained for the disaster that are identified as dangerous for the SoS there are determined the SoS vulnerable items,
- there is determined the occurrence frequency of failures of each vulnerable item of the SoS with regard to disaster identified as dangerous for the SoS,
- it builds the criticality matrix for the SoS (for each SoS vulnerable item it is scored the occurrence frequency of failures and the severity of the failures expressed by the size of the losses on the SoS assets) and according to the appropriate value scale it shall be determined highly critical, medium-critical and critical items of the SoS.

The aim of the third part, denoted in Figure 24 as ***"what to do"*** is to evaluate the real impacts in the disaster scenarios for the disaster sizes: current, design and beyond design, compiled in part 2 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 [30] for the management of activities that support the basic functions of the territory associated with safety.

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 in consideration of all possible disasters in the sizes, which are the design disasters values. It is required the documents to 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 24 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; and to 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 is a necessary basis for choosing the right management methods; to 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.

Together with the Defence-In-Depth concept, it represents a comprehensive approach, which ensures that people and the environment will be protected, even at critical conditions in the facility with nuclear technology. It is a comprehensive philosophy of safety that has begun to apply in the 1980 of the last centuries. It includes all activities aimed at the safety of the facility and the territory in which the facility is located, namely starting from siting, through design and construction, commissioning, operation and decommissioning. To ensure the safe complex technical facility it uses the systems barriers and management modes. Its aim is to:

- to compensate the human and technological failures,
- to maintain effective barriers that avert damages to the equipment and the barriers themselves,
- to protect people and the environment, when the barrier fails to fulfil their tasks.

Present advanced management of socio-cyber- technical facilities is based on the process management; details are in Annex 4. Model for entity safety management in time [13,14] is shown in Figure 25. It is necessary to coordinate six processes: 1 - concepts and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. The main processes are further divided into sub processes:

1. The first process consists of sub processes for: the overall concept; achieving the intermediate objectives of safety; leadership / management of safety; the safety management system; personnel staff including the sections for: human resources management, training and education, internal communication / awareness and working environment; review and evaluation of the implementation of fulfilment of objectives in the safety.
2. The second process consists of sub processes for: identify of hazards from potential disasters and risk assessment; documentation of procedures (including work permits); management of change; safety in conjunction with contractors; and supervision of product safety.
3. The third process includes the sub processes for: research and development; design and mountings; inherently safer processes; technical standards; storage of hazardous substances; and maintenance of integrity and maintenance of equipment and buildings.
4. The fourth process includes the sub processes for: cooperation with the administrative authorities; cooperation with the public and other stakeholders (including the academic institutions); and cooperation with other facilities.
5. The fifth process includes the sub processes for: planning of internal (on-site) preparedness; facilitate the planning of external (off-site) preparedness (for which it corresponds

the public administration); and the coordination of the activities of the departmental (resort) facilities at ensuring the departmental emergency preparedness and at response.

6. The sixth process has sub processes for: processing of reports on disasters, accidents, near misses and other learned experience; investigation of damages, losses and harms and their causes; and the response and follow-up activities after disasters (including lessons learned and information sharing).

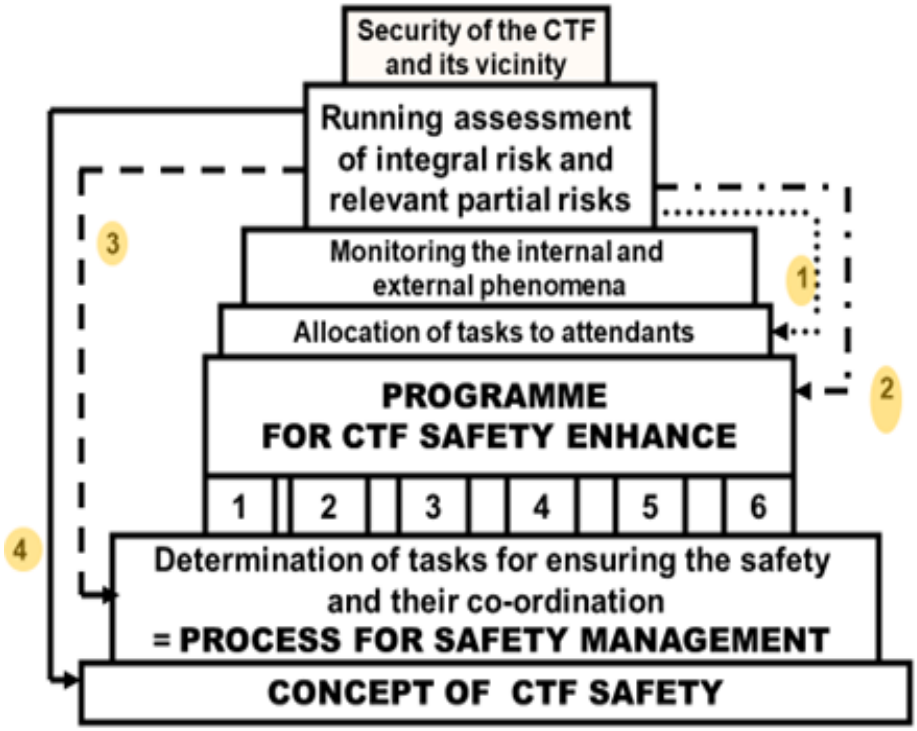

Figure 25. Model of the technical facility (CTF) safety management in time. Processes: 1 - concept and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. Feedbacks that are used to control when the risk is unacceptable - the numbers in the yellow circle.

Coordination of processes is targeted at ensuring the safe complex facilities under the conditions of normal, abnormal and critical (Figure 26).

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).

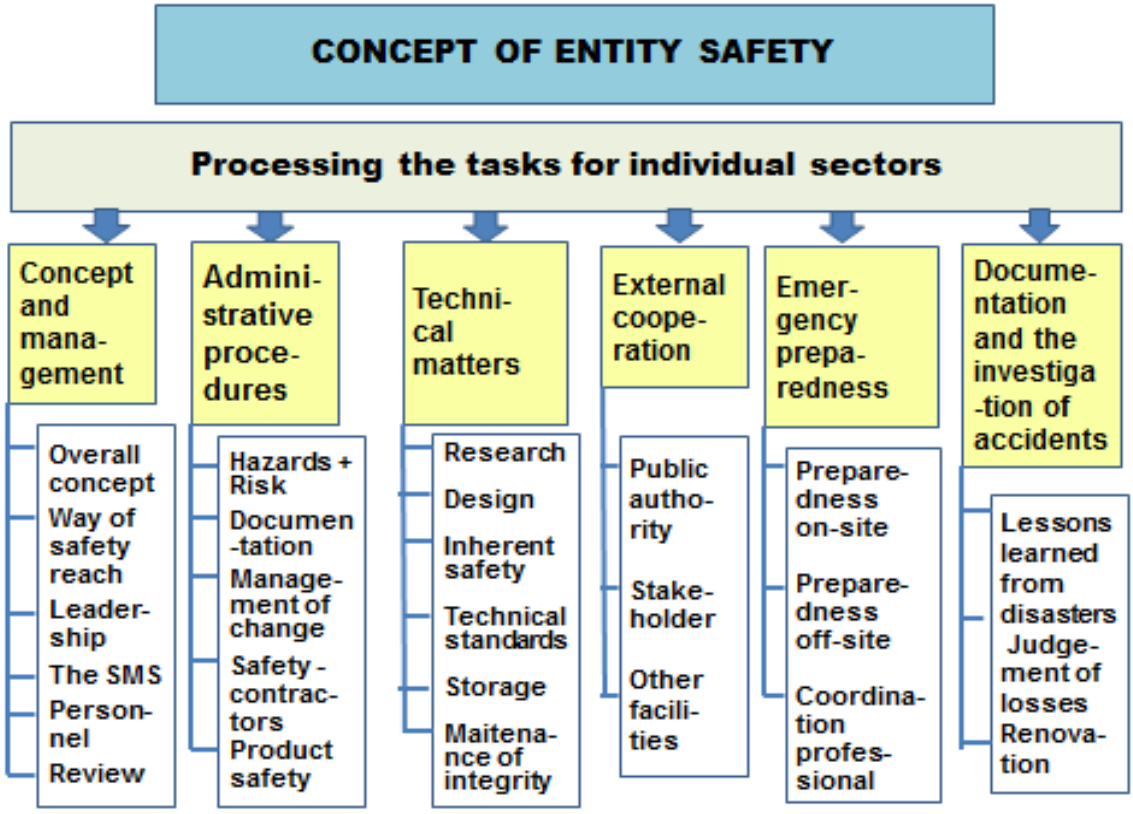

Figure 26. Concept of entity safety and its main parts.

Generally, it is possible to say that acceptable risk is determined on social and knowledge base, and that the social, economic and political factors are considered during the risk level determination. It also means that level of acceptable risk is not same for all countries.

Because the required level of safety is possible also to reach by special education, installation of warning systems, it holds that acceptable risk level is not safe risk level at which the probable losses and damages are negligible.

According to the theorization of present philosophers the risks have in society the objective and subjective features, and moreover there are not out of culture and value connections (in this direction they are not pure scientific problem and they need to be considered also from viewpoint of civic involvement). Even, if the modern society enforces the indolent strategy of insurance and reimbursement, it is not possible to rely on it fully because some risks can affect the core of social system, which it is truth for some security risks.

Against scientism of security politics nothing can be say to the extent that we prove to be reflexive, which means to reveal consequences of individual activities and we do not yield to illusion on opportunity of perfect solution. Reliance on experts (and institutions) can induce the reduction of capability to participate actively on solution and to finish the separation of private and public (which manifests as inherent risk on which the expert opinion fails). According to professional concept all participants (i.e. all interest groups) have duties and responsibilities at trade-off with risks.

From this reason the humans need to have possibility to participate in decision-making, to manifest their needs and opinions, namely without fear from punishment. It is necessary to involve many humans (in spite of great costs in the process beginning) and to try accomplishment of consensus.

Problem comes in professional matters in which the ground documents are based on evaluations that are complicated and for current humans non-understandable. The decision-making in these cases is often influenced by the lobbies of various groups that strive on commission.

From this reason it is necessary so that: all evaluation procedures need to be lean on legislative; the selection criteria need to be directed to publicly aims and need to be transparent at decision with regard to dispositional sources, forces and means of public administration. In practice we use risks of several types: partial if we consider one asset; integrated if we consider several assets and the total risk is the aggregation of individual assets risks; and integral (systemic) if we consider more assets and total risk includes also indirect impacts on assets that are caused by linkages and couplings in system.

The assignation of real work with risks in good governance is given to person or organisational part that is well prepared for such work. This approach is possible only in organization with qualified process management in which activities and measures are applied on knowledge base, namely matter-of-fact and from management domain (i.e. the activities are mutually interconnected, no errors in communication, each participant knows what to do and how to do).

Because, it does not exist the general consensus on formulation of problems of sustainability of welfare of human society in context with system utilities, each problem solution is provisional, because it continually balances among the rival interests and society goals (if they are stipulated). It is difficult to give explicit decision on problem owing to the alternating decision process character. During the decision, the following dilemmas are solved:

- relation between risks and profits (often greater benefit for human means greater risk for ecosystem),
- time conflict between needs of present and future generations,
- and social conflict (relation of needs of individuals and the society).

It is difficult to solve inverse problems owing to the systems´ complexness. If some symptoms connected with risks are stipulated and sorted out, the new symptoms will emerge. From this it follows that the real approach to sustainability management by help of risk management needs to be iterative, interactive and adaptive.

The aim of complex management is to ensure at each situation the protection of human lives and security, property, environment, infrastructures and technologies that are necessary for human survival. It means always to ensure:

- the mobilisation and co-ordination of all national sources (energy, labour force, production capacity, food and agriculture, resources, telecommunications etc.),

- the co-ordination of such activities as notification system, warning system, rescue system and first responders´ system, which reduce the disasters' impacts and supporting the public administration activities and adherence of legal rules.

The planning types that form fundamental methodical tools of individual mutually interconnected management types need to create the base in which all given aims are embedded.

For reaching the human society aims, i.e. security and sustainable development, the mutual combination of measures and activities is necessary at vulnerabilities´ reduction, resiliencies upgrade and adaptation capability; all public assets in detail and in complex need to be respected. The present tool based on knowledge and experiences means to apply on all management levels to implement the proactive safety management system based on work with risk respecting above mentioned knowledge; especially: All-Hazard-Approach, Defence-In-Depth strategy, interdependences, time and space variability.

From the critical analysis of emergency up to critical situations [17], it follows that:

- the cause of critical situations are the organisational accidents that are connected with a human factor; especially with the phenomena as corruption; abuse of power; suppress of the public interest; low respect to knowledge and engineering experiences; and low professional level of management,
- the organisational accident consequences are: government default; technologies failures; infrastructure failures; research failure; social system failure; decay of human society into intolerant groups; increasing number of impoverished people – seniors, dossiers, jobless – problem young people who are out of work and without education; disturbances of daily civil protection human needs; disturbance of daily civil protection, human security and public welfare; disuse of technology, space militarization.

From this reason we pay the attention to these phenomena that cause the disturbance of social relations, public welfare and human security – Table 2.

Table 2. Phenomena that cause the disturbance of social relations, public welfare and human security.

Domain	**Defects leading to critical situations**
Top governance	The domain management: is predetermined to political and military aspects; is short of human dimension and gives low support to the EU inhabitants; does not governed on the basis of qualified data processed by qualified methods; is often determined by fixed ideas without real assessment of their realisation; is based on image that all is stationary and it does not respect dynamic development of world that means to prepare possible extreme scenarios and measures for human's survival; and is not realised on the principle "Safety management system for system of systems".

Technical domain	In domain: no standards and norms for underground and high-rise buildings with regard to human security and public welfare; missing essential services provided to the citizens; scenarios for decision-making are prepared only by simulation without verification with use of real data – sometimes scenarios used were derived for different conditions, i.e. conditions of technology transfer were not fulfilled; no norms and standards for interoperability; no standards and norms for co-operation of diverse systems; no co-ordinated emergency plans on all levels (EU-wide to regional) – all need to be on professional level respecting knowledge and experiences, continuity and contingency plans.
Organisational domain	In domain: missing the effort directed to reduction of weakness (low number of resources, contamination of environment, work price, unemployment) and to use of strength (qualified technician population); no effective tool against to corruption, power disuse, lobbying etc.; missing the support of co-operation on mutual partner principle; missing base for mutual understanding and mutual co-existence; no effective international teams of first responders; no base for close co-operation of first responders; no norms and standards for interoperability.
Knowledge domain	In knowledge base used for decision-making: missing systematic respect to present world nature – dynamic open system of systems; low effort directed to collection of qualified data on disasters and on lesson learned from responses to extreme disasters; underestimation of disasters at disasters´ management; neglecting the creeping disasters as ground water stores, contamination of human food chain etc.; no qualified disasters´ scenarios for decision making.

The outputs of our task are created by application of methods as: the critical analysis and critical evaluation of knowledge that is gathered in professional publications and summarized in foregoing section; consideration of experiences from everyday life; logical interconnection of knowledge; classification of obtained facts; synthesis of obtained facts; application of methods of creative thinking and expert judgement (panel discussion, brainstorming, Delphi method, criticality assessment etc.) on data as:

- risk nature and features,
- risk scenarios change in time and space,
- risk management change in time and space; special attention is paid to management failures,
- trade-off with risks change in time and space; special attention is paid to failures caused by incorrect or insufficient measures.

At individual investigations the analytical and heuristic methods [15,30] are used.

The results from own direct research are based on: systematic investigation and evaluation of disasters and accidents in technological objects and facilities; judgement of impacts of real accidents on technological objects and facilities; simulations performed by the risk engineering methods (What, If and Fishbone [30]); and performed professional inspections in real technological objects and facilities.

The aim of inspections was the determination of main deficiencies in complex technological facilities. For this aim it was used the special checklist, which was compiled according to the technique described in [13]. Its form for i-th disaster is shown in Table 3.

Table 3. Identification of deficiencies for i-th specific disaster, i.e. disaster that can have important impacts on entity and its vicinity, i = 1, 2, ..., n, i.e. assessment of criticality rate of viewpoint of application of All-Hazard-Approach and Defence-In-Depth. Safety rate = 1 – criticality rate. For assessment of criticality it was used the value scale 0-5 [5] was used (0-negligible, 1-low, 2-middle,3-high,4-very high,5-extremely high) and the median of values determined by inspection members (usually 5-7).

	Question	**Assessment of criticality**	**Reasons of criticality**
i	1. Has the technical object or facility to incorporate the principles of inherent safety, i.e. safe design?		
	2. Has the control system of a technical facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technical facility in normal (steady) condition?		
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal condition to keep technical 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 condition the technical 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´ measures for emergency response that mitigate impacts on technological facility system and ensure the capability to return to a normal condition? Operation of a technological object is successful, if it is a good continuity plan ensuring 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?		

The special attention of advanced risk management and risk engineering targeted to the integral safety is targeted to the technological objects and networks that are in principle the socio-cyber-technical systems. According to knowledge concentrated in [13-15] it is necessary to use the following principles:

- the risk is followed and considered during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition,
- the risk determination is directed to user's demands and to the level of provided services,
- the risk is determined according to the criticality of impacts on facility processes, provided services and on assets that are determined by public interest,
- the unacceptable risks are mitigated by tools according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up.

The advanced risk engineering directed to human system safety respects the co-existence of systems with different nature (SoS), and so fulfils present demands of humans. To prepare groundwork it is necessary to combine analytical methods with expert judgement by which we remove vagueness in data. The problems that we need to solve in this consequence consist in acquisition of knowledge and in assignment "who is expert"; this problem was broadly discussed in world conference ESREL2011 [2]. For the first problem solution we need systematically to monitor human system and obtained data process by qualified methods.

It needs to be noted that in the real world we work at ensuring the safety of critical facilities with the non-trivial problems, i.e.:

- they have several protected assets, the objectives of which are sometimes conflicting,
- these assets vary in time and space,
- and the human system, in which the assets are and assets alone are in dynamic development.

For ensuring the safe territory and safe public assets it is necessary to apply the super process that consists from five processes (Figure 27):

Fig. 27. Structure of super process for risk management and trade-off with risk for profit of safe territory and safe public assets. The numbers denote the feedbacks that need to be realised if problems occur. From the economy reasons the firstly the feedback 1 is applied, and only if it fails the feedback 2 etc.

1. The process for obtaining the sufficient knowledge on territory includes: determination of assets in territory; determination of territory parameters and assets characteristics in the extent of land-use planning documentation; and determination of list of disasters that affected the territory (the input list of disasters being under the term All-Hazard-Approach).
2. The process of risks assessments and risk controls includes: the determination of hazards for all disasters that can have impacts on the given territory and their return periods; determination of vulnerable sites in territory and vulnerability of public assets with regard to determined sizes of hazards (ways of hazard determination are e.g. in [13]); determination of design disasters (normative determined disaster size); determination of impacts of disasters on territory and assets (it is suitable to determine the normative impact scenarios for design disasters); determination of integral risks for all important disasters (i.e. to consider the both, the direct disaster impact on assets and the indirect disaster impacts on assets through the linkages and couplings among the assets); put the work with risks.
3. Process of evaluation of quality of risk management and trade-off with risks includes: judgement of levels of effectiveness of prevention, preparedness, response and renovation with regard to integral risks connected with important disasters; determination of critical points in risk management and in trade-off with risks and determination of these points criticalities with regard to integrity and effectiveness of

applied measures and activities and their control (i.e. it goes on the reveal of sources of possible organizational accidents); proposal of corrections for high critical points.

4. Process of determination of safety management includes: determination of measures and activities for points with high criticalities and their implementation in the frame of short-term, middle-term and long-term realization plans, namely including the responsibilities for realization and sources for realizations; introduction of safety culture on the level of assets, assets´ management and on the territory safety management (from top management to individual citizens) [3, 5,14]; and determination of response procedures to emergency situations with demand that at each response to critical up to extreme situation there are solved the human survival and the continuity of critical objects, facilities and infrastructures.
5. Process of preservation and upgrade the safety includes: systematic formation of capability to perform early and effective response to critical situation, to ensure the renovation and continuity of services in territory; determination and implementation of strategic programme for safety increase in time including the monitoring the effectiveness of processes for risk management and trade-off with risks; regular detail assessment of territory safety every 10 years; and immediate territory safety judgement after critical situation occurrence.

Because the dynamic development of world it is necessary to monitor the territory and to have prepared the procedures for correction of unfavourable situations. From economy reasons it is necessary firstly to use the cheapest procedure that feedback 1 in Figure 27 shows; in case of its failure the feedback 2 etc.; at huge harms, it is immediately used the feedback 4, which means the change of territory safety concept. In each case denoted by feedback some of adjusted processes change:

- in case denoted by feedback 1, it is pursued the change of process of territory safety management (e.g. they are change the rules for territory safety management, the allocation of roles of participated persons, management priorities etc.),
- in case denoted by feedback 2, it is pursued the change of process of evaluation of quality of risk management and trade-off with risks (e.g. they are changed the ways of risk control in territory, separation of tasks of trade-off with risks among the participated persons, priorities for risk management and trade-off with risks, allocation of means for measures leading to risk reduction – it does not only rely on response but more on prevention etc.),
- in case denoted by feedback 3, it is pursued the change of process of evaluation of risk assessment (e.g. they are introduced the further criteria for risk assessment, the value scale is transformed, they are considered the contributions to integral risks from further linkages and couplings among the assets that were revealed as originators of huge damages, losses and harms on public assets etc.),
- in case denoted by feedback 4, it is pursued the change of process of knowledge on territory (they are added and introduced into practice new findings, e.g. into the set of risk sources are added the further harmful phenomena that were revealed as the sources of huge damages, losses and harms on public assets, the size of disasters criticalities changes, the size of assets´ vulnerabilities changes etc.).

For ensuring the safe technological objects or facilities (or more precisely socio-technological entity because each such entity was invented and set up by humans) that are located in real territory it is necessary to apply the super process that consists from four processes (Figure 28):

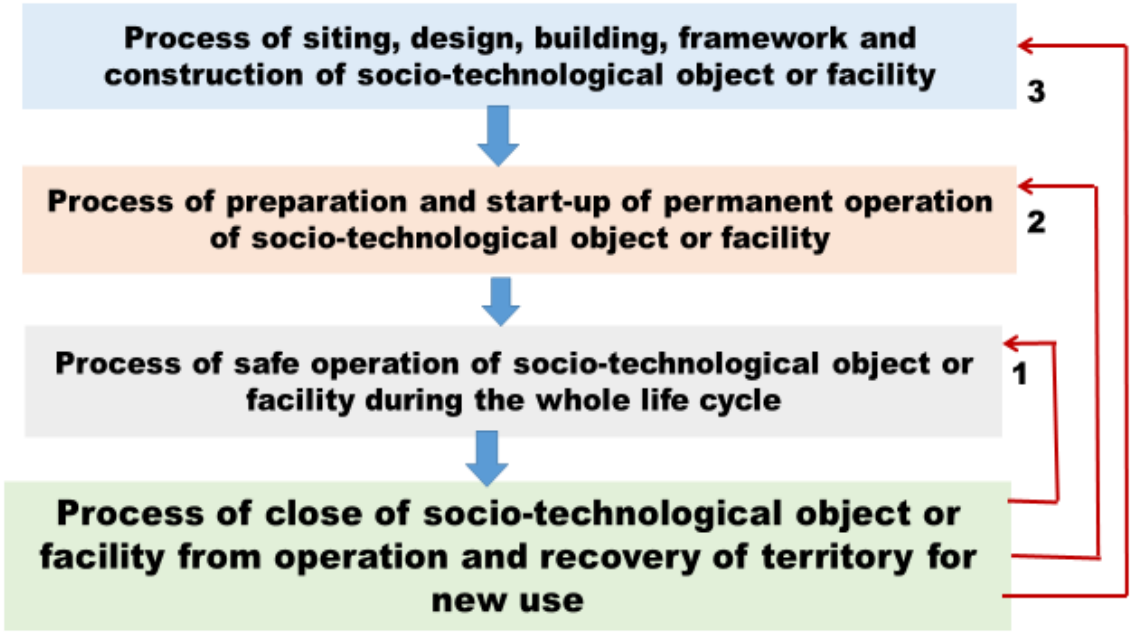

Fig. 28. The structure of super process for risk management and trade-off with risks for profit of safe technological entity during its life cycle and its safe vicinity. The numbers denote the feedbacks that need to be realised if problems occur. From the economy reasons the firstly the feedback 1 is applied, and only if it fails the feedback 2 etc.

1. Process of siting, designing, building and construction of technological entity (building, facility, network) includes: assemble of data on territory and its assets in which technological entity might be located in the extent of land-use planning documentation; assemble of data on disasters affecting the territory, their hazard sizes and their impacts character (the input list of disasters being under the term All-Hazard-Approach); determination and judgement of integral risk, and determination of vulnerability of the technological entity against to disasters affecting the territory and the estimation of integral risk increase after technological entity realization; entity siting, designing, building and constructions with regard to site risks, technology risks and human factor risks with the respecting the Defence-In-Depth principle (in detail described in [13]) and the trade-off with risks connected with linkages and couplings between entity and its vicinity; and determination of way of technological entity safety management in time during the technological entity life cycle (documentation: preliminary safety report [13]).
2. Process of preparation and start-up of permanent operation of technological entity (building, facility, network) includes: tests of functional capability of individual buildings, facilities and devices and elimination of revealed sources of technical and organizational risks; semi operation during which the risks connected with linkages and couplings (realised by different flows realizing at operation) inside and outside

the entity are traded-off; trial operation during which the risks connected with linkages and couplings (realised by different flows realizing at operation) inside and outside the entity are traded-off; realization of proposal of safety management of technological entity (processing the preoperational safety report and proposal of operational safety report [13]); and start-up of permanent operation.

3. Process of safe operation of technological entity (building, facility, network) during the life cycle includes: installation of operating procedures for normal, abnormal and critical conditions, safety culture, risk monitoring process; programme for upgrade of safety in time and procedures for continuity plan realization at critical conditions (operational safety report [13]); adjustment of optimal maintenance of buildings, facilities and devices; establishment of regular inspections of buildings, facilities and devices and rules for implementation of early repair of detected defects on buildings, facilities and devices, especially those important from safety reasons; modernization of buildings, facilities and devices; regular audits of safety of technical entity and its impacts on vicinity, which including the judgement of safety culture level, and realization of measures for getting over the detected important risks and for removing the sources of organizational accidents; and early response to critical situations and ensuring the continuity of technological entity operation after repair [13].
4. Process of close of technological entity (building, facility, network) from operation and recovery of territory for new use includes: determination of sources and responsibilities for measures and activities that are necessary for remove the entity (building, facility, and network) and decontamination works; remove of buildings, facilities and networks from the territory; performance of decontamination of territory. It goes on the process on which it is often forgotten in practice as the brownfields show, and therefore, it needs to be followed during the whole technological entity life cycle.

Because the dynamic development of world it is necessary to monitor the technical entity and to have prepared the procedures for correction of unfavourable situations. It is also necessary to consider that each technical entity has limited life cycle, and therefore, for preservation of conditions for human security and development it is necessary to forestall to depreciation of territory. From these reasons, there need to be prepared procedures and corrections in each technical entity for averting the unfavourable situation. From economy reasons, it is necessary firstly to use the cheapest procedure that feedback 1 in Figure 28 shows; in case of its failure the feedback 2 etc.; at huge harms, it is immediately used the feedback 3 that means the change of safety concept. In each case denoted by feedback some of adjusted processes change:

- in case denoted by feedback 1, it is pursued the change of technological entity safety management process (e.g. they change demands of public administration on operation of technological entity, rules for technological entity safety management, priorities in technological entity safety management – Figure 27 shows that often it is necessary to solve conflicts between security of public assets and the number of products, etc.),
- in case denoted by feedback 2, it is pursued the change of process of preparation and start-up of permanent operation of technological entity (e.g. they change ways of revealed risk management and trade-off with revealed risks and further trial

operation is performed, allocations of trade-off with risks among participants, priorities in risk management and in trade-off with risks, allocation of means for measures leading to risk reduction - it does not only rely on response and more means is given for prevention etc.),

- in case denoted by feedback 3, it is pursued the change of process siting, designing, building and construction of technological entity (e.g. they are considered further sources of risks, introduced further criteria for risk assessment, changed the value scale, considered the further contributions to integral risk from linkages and couplings among the assets that were revealed as sources of great losses, damages and harms on public assets etc.).

Due to dynamic world development it is necessary regularly to evaluate in each territory the co-existence of territory and all technological entities located in it, because it is necessary to preserve the conditions in territory that enable the safe life of future human generations. At finding the significant problems it is necessary to find sources, forces and means for removing the important impacts on future territory conditions and future generations. It is necessary to determine the measures, sources for their realizations and responsibilities for their implementation, in the frame of public interest it is necessary to use all resources for performance of remedy in acceptable time horizon.

The interface of processes for works with risks during the time, in individual parts of super processes is logical and today has support in many legal rules, norms and standards. The present problem is that it is not required the logical interface of different sectors that is very exigent. It needs the co-operation of specialists from many fields, which needs the common terms, mutual understanding, common effort at finding the consensus etc. that are missing.

With regard to results given above the super processes´ correct applications are good prevention of organization accidents. However, it is clear that the super processes application fulfils the expected targets only if all processes on lower hierarchical levels will be correctly applied and will be meaningfully interconnected and co-ordinated. It is necessary to note that problems connected with good application of both super processes, inhere in reality that neither present professional education nor present legislation do not require the connectivity of actions and measures that are important for success of super processes. The next problem is that partial processes contain subprocesses that are not interfaced in reality or their interconnections are insufficient as shown results of accidents investigation, failures of networks and conclusions from inspections of safety documentations mentioned above.

From above mentioned reasons it is necessary to introduce in education the branch of knowledge on management of hierarchically interconnected processes in vertical and horizontal structure and to prescribe the mandatory discussion of specialists responsible for management of individual sections from the level of sub-processes, over processes up to sub-processes, namely with participation of public administration and general public. The discussion needs to follow the public interest and to be performed by the suitable method of risk engineering on several professional levels (according to participants´ knowledge); the method needs to ensure the fair-mindedness and correctness; for professional discussion the more stages Delphi method [30] is suitable, according to experience the panel discussion [30] is unsuitable because at its use the special interest groups (lobby) can have chance.

5.5. Technical facilities open problems

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 [13,45]. The reason for increased number of risk sources 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, 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 [46]. 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 [46]. 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 [13,15]. However, our research shows lacks in awareness on risks, especially among managers and politicians.

Research [15,20,33] shows that at present in technical facilities, the integral risk is not considered and they are used the following choices of sources of risks:

1. Sources of risks determined either by legislative, or by experiences of worker who solves the task.
2. Only technical sources of risks in a given technological facility. Usually, it goes on:
    - risks connected with material (fulfilment of required parameters, supplier relations - alternative material etc.),

- risks connected with construction and interfaces of components and facilities (free procedures, presence of unstable hazardous substances….),
- risks connected with production procedures, e.g. at welding, specific works with millers, lathes etc.,
- risks connected with conditions that are necessary for production of quality product, e.g. certain pressure, certain temperature or certain humidity of surrounding medium etc.,

3. Technical sources of risks and human factor. To items given in point 2, they are added risks connected with false operation of workers. In this case it is also required the prevention of false technical operations in technical work.
4. Technical sources of risks and human factor the broadest most interpretation. To items given in point 3, they are added risks connected with sources of organizational accidents (i.e. bad decision-making, using the false procedures etc.).
5. Technical sources of risks, sources of risks threatened the workers lives, health and safety, sources of organizational accidents and sources of risks in working environment.
6. The sources of risks given in point 5 plus external sources of risks.
7. The sources of risks given in point 6 plus sources of risks from interfaces of facilities, components and system that disturb the technical integrity and their originators are in automatization, education and good skill. In this case it is also required the property protection, data and information protection, specific knowledge and know-how protection.
8. All Hazard Approach in the form described in [19]. This selection considers the risks from the five basic disaster sources and it is challenging on data, methods, knowledge, experience and time period. It requires the strategic system proactive approach and it has according the results of FOCUS project [13] a lot of deficits at use in practice.

Research described in [14,15,33] also shows that in technical practice there are used following ways of work with risks:

- risks are determined and mastered after technical facility creation. This way has danger that some of important risks that could be only mastered by specific technical measures in assignment of technical facility can be only reduced by organizational that are lower effective than technical measures,
- specified risks are considered from the beginning of technological facility design up to its termination from operation. This way depends on requirements of legislation, knowledge and skill of designers, constructors and operators, i.e. it does not guarantee the consideration of all risk sources,
- risks are considered from the beginning of technical facility design and it is used strategy verified in practice using the Defence-In-Depth approach that requires system thinking, multi sectoral and transdisciplinary knowledge and experiences.

6. TOOLS FOR DETERMINATION, MANAGEMENT AND TRADE-OFF WIITH RISKS AND RESPONSIBILITIES

For successful work with risks of technical facilities, they are necessary both, the correct and effective tools and the responsibilities for their correct use.

6.1.Tools

A number of specific tools have been developed to deal with risks in risk engineering. Their aim is to recognize, understand and manage the risks, thereby ensuring a safe technical facility and its safe operation throughout its lifetime. Because technical facilities are complex systems of systems, it goes on tools in which the results of analytical and expert methods are interconnected in a specific way. The most important tools and techniques are described in [15,30]. Here, based on the experience of the authors, we will mention just a few of them:

1. Benchmarking is a method of systematically comparing the processes, organizational structure, products and performance of a given technical facility department with other globally successful technical facilities with a view to achieving the excellence. It is usually used in risk management in cases, where the objective is ideal, and according to good practice principles it is good to manage risks by way as the best industry operators do.
2. Modelling is a technique by which we create a simplified picture of a real process, system or object and then we follow on it the established connections. Its aim is to determine the scenario of the process in time and space (e.g. the course of the accident, the course of the process control, the course of the response to the accident, etc.) so that we can determine appropriate measures and activities to ensure safe technical facilities (e.g., for preventing, mitigating and mastering the accidents with available capabilities, which we provide with the CBA (Cost Benefit Analysis). Based on the principle that “everything is related to everything” (regressus ad infinitum), it is necessary to validate results obtained by model; evaluations of technical facilities accidents and failures often show that kay causes were inadequate modelling the accidents. In serious cases, the care should be taken for software applications, especially where technology transfer conditions have not been verified [47].
3. A scenario is a system model that describes the evolution of a process in its various forms (variants, alternatives) depending on conditions or decisions made, containing a sequence of events that take place within it (including the prospective variants), and descriptions of interactions between the monitored assets of the system and the process [30]. Disaster scenarios are the most important for safety management because they are used to propose prevention, mitigation, response and recovery.

5. Multicriterial assessment is an assessment based on the application of multiple criteria, even incommensurable or conflicting, to a whole [30]. For the resulting solution, they need to be determined the restrictive conditions, which define objectivity (e.g. in terms of system exhaustibility, human resources or value of benefits). The exhaustibility of the system means the maximum possible level of utility (utility value) that can be achieved in a given scientific and technological development. We always judge the restrictive conditions individually, namely based on their partial evaluations. For its application in conjunction with the risks of complex systems, it has proved to be useful the application of:
   - What, If method in for of table, as it is given in Figure 16.
   - the Decision Support System (DSS) with appropriate value scales processed on the maximum utility theory [48].

Analyses of the risk management tools presented in [33,49] as well as the accumulated experience [43] show that risk management tools depend on many factors; schematically, the subject matter is also shown in Figure 13.

Whereas in a strategic management in which security and long-term functionality are concerned, two factors need to be considered:

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

In practice, it is necessary to work with risks at the lowest level (simple technical equipment - machines), as well as with risks at higher levels (components – e.g. pressure equipment; production lines, sets of production lines, whole technical facility) and at the highest level (technical facility and its surroundings). Safety at the highest level ensures the coexistence of the technical facility with the surroundings throughout the life cycle of the technical facility.

In order to ensure the safety and development of people and other public assets, the objectives of dealing with risks at all levels are the same, a reliable or secure or safe entity. Because of the current goals of human society, which have been emphasized several times, we continue to focus on the ultimate goal, which is safe entities.

At selection of risk management tools for technical equipment and technical facilities aimed to safety, they are according to arguments in [13-15] two factors important two factors:

1. The first factor is the recognition that risk is a site-specific quantity, i.e. it depends on both, the cause of the damage to the asset or pool of assets (i.e. the nature and size of the harmful phenomenon) and the characteristics of the asset or pool of assets (vulnerability) at the time of the disaster origin. E.g. an unmaintained relief valve normally does not perform its function at the pressure surge limit. Because over time there are variables, both the asset or pool of assets and the sizes of harmful phenomena or disasters, there are three categories of situations in terms of coping with the impacts of the realized risk, namely:
   - normal,
   - emergency,

- critical.

With the growing category, the professional, financial, organizational and personnel requirements for managing and settling the risks associated with these situations are increasing. Therefore, legislation that imposes requirements on owners and operators of technical facilities on risk management and public administration requirements for safety oversight in the public interest plays an important role here [12-15]. Based on analyses of legislation [13-15], current legislation is too general; it does not mention data requirements and data processing methods that fundamentally determine the quality of the result.

2. The second factor is the choice of the type of risk to be monitored in the task to be performed, which depends on the determination of:
   - the number of assets and their listing, i.e., it goes on considering which public assets and which specific assets of a technical facility in a given task are important; e.g. whether they are performance, competitiveness, profit, etc.,
   - whether links and flows between listed assets play a role in the task, i.e. a mechanical concept is not enough, but a system concept needs to be considered.

In order to ensure the safety of the entity in the short term (e.g. safe condition of simple technical equipment), it is sufficient to monitor the condition of the asset, i.e. the partial risk associated with the entity. With regard to human safety, legislation in developed countries also requires the monitoring of occupational safety and health (OSH), i.e. the monitoring of two assets (life and health of persons in the workplace, quality of the working environment), using the integrated risk (i.e. it is neglected machine - human binding).

As technical equipment, people in the workplace and the working environment are interconnected, the links and flows between these subsystems, i.e. integral risk, need to be monitored in the medium and long-term to ensure safety.

Therefore, when selecting the risk management tools (identification, analysis, evaluation, judgement, management and settlement) aimed at the safety of the selected entity, the following tasks in the technical field for technical facilities should be distinguished:

- selection of tools for work with the risk associated with the condition of technical equipment (objective - safe technical equipment),
- selection of tools for working with the risk associated with the condition of the technical component (objective - safe technical component),
- selection of tools for working with the risk associated with the production line / production process (objective - safe production process),
- selection of tools for working with the risk associated with the condition of the business process set (objective - safe business process set),
- selection of tools for working with the risk associated with the whole technical facility (objective - safe technical facility),

- selection of tools for working with the risk associated with the technical facility and its surroundings (objective - safe technical facility and safe neighbourhood of the technical facility).

Based on the work [13-15,30], focusing on technical facilities, it is not enough to ensure the safety of the human system in connection with technical facilities and technologies (i.e. coexistence of a technical facility with its surroundings during operation) and their equipment, because the choice of risk management tools depends on:

- the nature of the entity of interest (i.e. selected technical equipment or higher systems of technical facility),
- the nature of the environment in which the entity of interest (i.e. selected technical equipment or higher systems of technical facility) operates,
- the mode in which the entity of interest (i.e. selected technical equipment or higher system of technical facility) operates,
- requirements for the operation of the entity (i.e. selected technical equipment or higher systems of technical facility),
- and whether a short, medium or strategic solution is required, i.e. long-term.

By nature, [15,16,30] are risk-based tools based on four models according to the type of process they follow; it's about:

- problems that can be described by a linear model [30]; e.g.: Check list; Safety audit; Human Reliability Analysis - HRA; there is a need to be aware of the limited accuracy of the results, as only one process is monitored and the links to other processes and the environment are neglected,
- problems that can be described by the tree models [30]; e.g.: Preliminary Hazard Analysis - PHA; Quantitative Risk Analysis - QRA; Hazard Operation Process - Hazard Analysis (HAZOP); Event Tree Analysis - ETA; Failure Mode and Effect Analysis - FMEA; FMECA - Failure Mode, Effect and Criticality Analysis; Fault Tree Analysis - FTA; Probabilistic Safety Assessment - PSA; it should be noted here that the development of accidents, accidents and failures comes from a single site, i.e. models do not describe cases where impacts on a technical facility occur from one cause at several locations, i.e. combinations of harmful phenomena are not considered,
- problems that can be described by operational analysis models [30]; e.g.: critical path method; PERT; GERT; Petri nets, the last three of which are now elaborated to form “colour stochastic models”, which simulate a large number of possible scenarios that are created and assessed by experts on the basis of their experience and data presented in experience databases, the last years of the last century specifically built in developed countries,
- non-structured problems, which can be described in several ways, such as [30]: What, If, Scenario, Case Study, Multi-criteria based on Decision Support System (DSS). In these cases, experience is based; a series of scenarios will be developed through collaboration with experts, and the optimum solution is sought using maximum utility theory [48].

The experiences [15,30,43,49] show that tree models have not the capability to assess the size of technical facility integral risk because they come out from one point in technical facility. I.e., they do not express impacts of external disasters, external terrorist attacks and human factor that usually in one stroke affect many points.

For many of the above methods, software that has been derived for a particular device at a particular location is available. In order to ensure correct results in this case, it is necessary to verify, before using each software, whether the conditions of the technology transfer are met, i.e. whether the conditions for the solution and the solution are the same as for the equipment and the place for which the software was derived [30].

Based on the data and results of the research presented in [12-16,30] and the authors' experience in practice, Table 4 is compiled, listing the individual tasks recommended tools, characterized in the work [30]. According to the complexity of the entity, there are three objectives of risk management, namely:

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

Since the higher the tool type, the higher the cost (knowledge, finance, time) for its use, the table shows in each case only the lowest cost tools that, based on current knowledge and experience, have the ability to solve the task if the basic rules of safety culture, operating rules corresponding to the conditions of operation are observed; that is, no intention to damage the entity is considered.

Table 4. Tools for working with risks sorted by the objective of the task addressed[*)].

Objective of work with risks	**Tool**	**The subject of the observation**
Functional individual technical equipment / fittings (e.g. machine)	Checklist / Safety Audit / What, If	One asset
Secure individual technical equipment (the machine is functional and the operator security is ensured)	Checklist / Safety Audit / What, If	Two assets – because conflicts may occur, a rule is required for aggregation
Safe individual technical equipment (the machine does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. its operators´ security is ensured and the products are safe	DSS	Several interconnected assets – because conflicts may occur, the theory of maximum utility is most often used [48]

Functional technical component (several interconnected technical fittings)	Checklist / Safety Audit /, What, If / Tree models	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [48]
Secure technical component (several interconnected technical fittings are is functional and the operator security is ensured)	Checklist / Safety Audit /, What If / Tree models / operation analysis methods / DSS	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [48]
Safe technical component (several interconnected technical fittings do not endanger themselves even under critical conditions and do not have harmful impacts on the surroundings), i.e. its operators ´security is ensured and the products are safe	What, If / Tree models / operation analysis methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [48]
Functionality of production process (production line)	Checklist / Safety Audit /, What If / Tree models	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation
Secure production process (production line is functional and the operator security is ensured)	What, If / Tree models / operation analysis methods / DSS	Several interconnected technical and other assets and surroundings – because conflicts may occur, a rule is required for aggregation or use of theory of maximum utility [48]
Safe production process / production line does not endanger itself even under critical conditions and does not have harmful impacts on the	What, If / operation analysis methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, a rule is required

surroundings), i.e. its operators´ security is ensured and products are safe		for aggregation or use of theory of maximum utility [48]
Functionality of a set of processes in the enterprise	What, If / operation analysis methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, a rule is required for aggregation or use of theory of maximum utility [48]
Secure set of processes in the enterprise (set of processes is functional and operators security is ensured)	What, If / stochastic operation analysis methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [48]
Safe set of processes in the enterprise (set of processes does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. its operators' security is ensured and products are safe	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [48]
Functional technical facility	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [48]
Secure technical facility (technical facility is secured and functional and operators security is ensured)	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [48]

Safe technical facility (technical facility does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. its operators´ security is ensured and products are safe	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [48]

*) *In this context, it needs to be aware – functionality means reliable performance of tasks; safe means secure, reliable and functional.*

Table 5 shows the example of DSS for judgement of safety level of technical facility verified in practice. At safety audit, the answer to each question was separately formulated by 5 evaluators (technical director, security expert of technical facility, security expert of local public administration, security expert of regional public administration, author) according to documentation of technical facility. The final evaluation of each question was made as median from partial evaluations. In case of significant doubts at certain real question judgement, the note was given in special column of check list; and final results in these cases were finally obtained by panel discussion of experts. The final level of safety is determined by Table 6 in the harmony with the maximum utility theory [48].

Table 5. Check list for judgement of technical facility safety according to judgement of work with risks.

Question	**Answer**		**Note**
	yes	**no**	
Are in technical facility documentation distinguished the terms danger, hazard and risk?			
Is technical facility documentation based on context that considers only the technical facility assets?			
Is technical facility documentation based on context that considers technical facility assets and selected public assets (employee, contractors, visitors, humans in work vicinity, working setting and environment))?			
Is technical facility documentation based on context that consider technical facility assets and all public assets?			
Are only considered risk sources that are determined by expert experience?			
Are only considered only risk sources that are determined by legislative and expert experience?			

Are only considered risk sources that are connected with technical facility alone?			
Are considered risk sources that are connected with technical facility alone and human factor connected with badly performed working operation?			
Are considered risk sources that are connected with technical facility alone and human factor in the broadest concept?			
Are considered risk sources that are connected with technical facility alone, human factor in the broadest concept, workers health jeopardy and threatening the working environment?			
Are considered risk sources that are connected with technical facility alone, human factor in the broadest concept, workers health jeopardy, threatening the working environment and environment outside the technical facility?			
Are considered risk sources that are connected with technical facility alone, human factor in the broadest concept, workers health jeopardy and threatening the working environment in system context, i.e. also risk sources connected with linkages and flows in technical facility?			
Are considered risk sources according to All-Hazard-Approach?			
Are only considered partial risks?			
Are considered partial risk and integrated risk?			
Are considered partial risks, integrated risk and integral risk?			
Are risks in technical facility systematically followed?			
Are risks in technical facility systematically followed only after technical work building?			
Are risks in technical facility systematically followed for its whole life cycle, i.e. from its design?			
Are risks in technical facility systematically followed for its whole life cycle, i.e. from its design and in its design and operation used the Defence-In-Depth approach?			
Is at work with risks in technical facility systematically used the process model of work with risks?			
Is at work with risks in technical facility systematically used the process model of work with risks that possesses clearly determined criterions for risks acceptance?			
Is at work with risks in technical facility systematically used the process model of work with risks that possesses clearly determined criterions for risks acceptance, which respect public interest (i.e. they have social dimension)?			

Is at work with risks in technical facility systematically used the process model of work with risks that possesses clearly determined criterions for risks acceptance and aims of risk management?			
Is at work with risks in technical facility systematically used the process model of work with risks that possesses clearly determined criterions for risks acceptance with regard to public interest?			
Is at work with risks in technical facility systematically used the process model of work with risks that possesses clearly determined criterions for risks acceptance with regard to public interest and corrected measures in monitoring for the case that risk will happen unacceptable?			
Is at work with risks in technical facility systematically determined and followed the set of priority risks?			
Does technical facility risk management technique ensure in each phase of work with risks the review of profits and costs connected with measures for risks mastering, so economical handling with forces, sources and means might be ensured in technical facility?			
Does technical facility risk management technique ensure in each phase of work with risks the review of profits and costs connected with measures for risks mastering, so economical handling with forces, sources and means might be ensured in technical facility and in public administration?			
Are in technical facility systematically performed the preventive measures for reduction or avert of some risks?			
Are in technical facility systematically performed the preventive measures for reduction or avert of all priority risks?			
Are in technical facility systematically performed the preventive measures for reduction or avert of all risks that have potential to cause important losses to technical facility?			
Are in technical facility systematically performed the preventive measures for reduction or avert of all risks that have potential to cause important losses to technical facility and unacceptable impacts on surrounding environment?			
Are in technical facility systematically performed preventive measures for reduction or avert of all risks and prepared the mitigating measures for reduction of some highest risk impacts?			
Are in technical facility systematically performed preventive measures for reduction or avert of all risks and prepared the mitigating measures for reduction of all priority risks impacts?			

Are in technical facility systematically performed preventive measures for reduction or avert of all risks and prepared the mitigating measures for reduction of all risks impacts that can cause the significant losses to technical facility?			
Are in technical facility systematically performed preventive measures for reduction or avert of all risks and prepared the mitigating measures for reduction of all risks impacts that can cause the significant losses to technical facility and unacceptable consequences for surrounding environment?			
Is technical facility insured against risks?			
Does technical facility possess the finance, material, technical, personal and organisational for response to important risk?			
Does technical facility possess the finance, material, technical, personal and organisational for renovation after important risk realisation?			
Does technical facility possess the finance, material, technical, personal and organisational for response and renovation after extreme unexpected realisation?			
Are at work with risks in technical facility only considered the results of preliminary risk analyses?			
Are at work with risks in technical facility preferred the results of standard, fast and low precise risk analyses before results of preliminary risk analyses?			
Are at work with risks in technical facility preferred the results of detailed risk analyses in synoptic concept before the results of preliminary risk analyses and standard, fast and low precise risk analyses?			
Are at work with risks in technical facility preferred the results of individual and specific risk analyses before the results of detailed risk analyses in synoptic concept, preliminary risk analyses and standard, fast and low precise risk analyses?			
Are at work with risks in technical facility determined the criterions for assessment?			
Are at work with risks in technical facility determined the criterions for assessment technical and economical?			
Are at work with risks in technical facility determined the criterions for assessment technical and economical, external and internal?			
Are at work with risks in technical facility determined the criterions for assessment technical and economical, external and internal and socially political?			

Are at work with risks in technical facility determined the requirements for ensuring the safety?			
Are at work with risks in technical facility determined the requirements, standards and norms for ensuring the safety?			
Are at work with risks in technical facility determined the requirements, standards and norms for ensuring the safety and partial aims?			
Are at work with risks in technical facility determined the requirements, standards and norms for ensuring the safety, partial aims and methods and procedures?			
Are at work with risks in technical facility determined the requirements, standards and norms for ensuring the safety, partial aims, methods and procedures, and also limits and conditions?			
Are at work with risks in technical facility determined the requirements, standards and norms for ensuring the safety, partial aims, methods and procedures, limits and conditions and also the authorizations of persons or institutions?			
Does the technical facility administrator hold the safety management system that is compiled on the principles of process management and systemic work with risks?			
Does the technical facility administrator hold the safety management system (SMS) that contain the organizational structure, responsibilities, practices, rules, procedures and sources for determination and enforce of disaster prevention or at least for mitigating the unacceptable disasters impacts in technical work and its surrounding?			
Does the technical facility administrator hold the safety management system (SMS) that contain management of six processes: concept and management; administrative procedures; technical matters; off-site co-operation; emergency preparedness; and documentation and accident investigation?			
Does the technical facility administrator hold the SMS that contains the concept and management process with sub-processes for: overall concept; reaching the safety partial aims; safety governance; alone safety management system; personnel – human sources management, education and training, internal communication, working environment; audit and assessment of performance of safety aims?			
Does the technical facility administrator hold the SMS that contains the administrative procedures process with sub-processes for: hazard identification from possible disasters and corresponding risk assessment; documentation of procedures (including the			

work permits); changes management; safety connecter with contractors; surveillance under products safety?			
Does the technical facility administrator hold the SMS that contains the technical matters process with sub-processes for: research and development; design and montage; inherently safer processes; technical standards; storage of hazardous substances; and integrity maintenance and maintenance of equipment and buildings?			
Does the technical facility administrator hold the SMS that contains the off-site co-operation process with sub-processes for: co-operation with public administration; co-operation with public and other involved (including the academic institutions); and co-operation with other enterprises?			
Does the technical facility administrator hold the SMS that contains the emergency preparedness process with sub-processes for: on-site planning; facilitation of off-site planning (for which the public administration is responsible); and co-ordination of activities of resort organisations at ensuring the emergency preparing and the response?			
Does the technical facility administrator hold the SMS that contains the documentation and accident investigation process with sub-processes for: processing the reports on disasters, accidents, near misses and other instructive experiences; investigation of damages, losses and harms and their causes; and response and consequential activities after disasters (including the application of lessons and information sharing)?			
Does the SMS technical facility administrator contain the program for safety improvement in which there are given: roles of stakeholders; rules for safety culture improvement (golden rules); and relevant responsibilities?			
Does the SMS technical facility administrator contain the program for safety improvement in which there are given: security plans (on strategic, tactical, functional a technical levels); on-site and off-site emergency plans; continuity plans; and crisis plans?			
Does the SMS technical facility administrator contain the program for safety improvement in which there is given the risk management plan with clearly determined countermeasures and responsibilities?			
Does the SMS technical facility administrator contain the program for safety improvement in which there is given the risk management plan with clearly determined countermeasures and responsibilities that only contains the technical risks?			
Does the SMS technical facility administrator contain the program for safety improvement in which there is given the risk			

management plan with clearly determined countermeasures and responsibilities that only contains the technical and organisational risks?			
Does the SMS technical facility administrator contain the program for safety improvement in which there is given the risk management plan with clearly determined countermeasures and responsibilities that contains the technical, organisational and external risks?			
Does the SMS technical facility administrator contain the program for safety improvement in which there is given the risk management plan with clearly determined countermeasures and responsibilities that contains the technical, organisational, external and cyber risks?			
Does the SMS technical facility administrator contain the quality monitoring integral risk and all-important partial risks and corrective countermeasures for occurrence of unacceptable risks?			
TOTAL			

Table 6. Value sale for safety level determination.

Safety level	**Values v %**	**Number of answers "YES" in Table 2**
Extreme high – 5	More than 95 %	More than 68
Very high – 4	70 - 95 %	51 - 68
High – 3	45 - 70 %	33 - 50
Medium – 2	25 – 45 %	19 - 32
Low – 1	5 – 25 %	4 - 18
Negligible – 0	Lower than 5 %	Lower than 4

Based on experience, in the operational practice of technical facilities and their parts it is only applicable a tool, which is fast and not very demanding on knowledge and time. Therefore, the usefulness of risk management tools in the operation of technical facilities was monitored based on [15,43]. The result of this research shows that for:

- a not-too-complex object, it is a proven tool, a site-specific checklist with a correctly calibrated risk assessment scale,
- not very interconnected objects, it is a proven tool, a set of checklists that are site specific and have correctly calibrated risk scales, and the results of these checklists are aggregated in a specified and site-specific manner,
- complex objects, it is a proven tool DSS that consider both, the asset connectivity, the changes in time and external sources of risk.

6.2. Responsibilities

On the basis of data on risk management and trade-off with risks, there were determined by critical analysis the errors in risk management in both, the technical facility and the public administration interface and in the technical facility management itself. Their judgement shows that the risk reduction rate is also the subject to territory top management responsibility and political decision-making, at which they are used, the current scientific and technical knowledge and considered the economic, social and other conditions [14,50].

According to the TQM principles [34] and the experience of practice, it is needed in the context of problems solution in splitting the tasks and responsibilities to consider the possibilities that exist at different management levels. Options are given by both, the authority and the availability and the amount of available resources, forces and capabilities that are needed for problems solution [13,14,50]. It holds:

- at the technical facility operational management level, safety problems being well structured can be solved successfully,
- at the technical facility middle management level, they can be successfully solved safety problems being structured and poorly structured ones that are not associated with major risks,
- on the technical facility top management level, they can be successfully solved complex and unstructured safety problems that have risks that can be controlled using the tools, which are only available to top technical facility management,
- complex and unstructured safety problems of the with great extent and huge risks can be solved only by mutual deep co-operation of the public administration and the technical facility top management.

For solution of safety problems of the technical facility with transnational extent, the international cooperation is needed.

To derive the technical facility risk management responsibilities, it is required so the technical facility needs to:

- be safe throughout the lifetime,
- fulfil the tasks in demanded quality during the lifetime,
- could not endanger itself or its surroundings at its critical conditions.

It means to apply the All-Hazard-Approach developed for Europe [19], the Defence-In-Depth described for the technical facilities [13,14], and to have a program for the continuous improvement of safety and safety culture.

In complex world, the technical facility management represents the hierarchical interconnected system. According to [51], the responsibility principle paid in Europe means that for risk management are responsible both, the technical facility management and the public administration that gives permit and supervise the provision of public interest.

Therefore, from the perspective of human security and development, it is important the technical facility risk management in two areas:

- A - domain of territory administration and the technical facility management,
- B - the technical facility real safety management.

Based on critical analysis of the accidents and failures of the technical facility, there are given risk management responsibilities for the territory administration and the technical facility 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.

Real research results are in Table 7.

Table 7. Responsibilities for risk management of technical facilities; A – levels of management.

A	Requirement
A1	• to create conditions for the long-term stability of public space, which the technical facility 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 facility), • to promote the public interest and to respect the fact that the technical facility 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 realized; 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 facility operators may lead to technical facility lower quality of service, • to consider the views of specialists when deciding on the technical facility and not to prefer momentary political interests and actions of pressure groups.
A2	• 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 facility technological inadequacy and insufficient preparedness of the site for the technical facility operation (surveillance, supervision of the State), • to ensure that the liabilities associated with the technical facility may be fulfilled in good quality (surveillance, supervision of the State), • to ensure the technical facility staff training, mainly at the level of technical and technical-organizational; the relevant research, planning and legislation to support the technical facility operation, • to promote a proactive, systematic and strategic approach at working with the technical facility risks, • to pay attention to the technical facility goodwill at work with the risks, • to ensure that significant risk sources for the technical facility 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 facility management to handle the impacts of extreme disaster and to perform recovery of the technical facility and its vicinity.
A3	• to ensure that at designing, building, construction and operation of the technical facility, all serious disasters that are possible in the technical facility site are considered and properly dealt with, • to ensure so that the technical facility design documentation is correct and errors-free; the technical facility 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 facility 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 facility (to build organizational resilience.
A4	• 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 facility high-quality operation from the perspective of ensuring the material inputs and qualified personnel,

	• to create inside the technical facility, 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	• 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 facility 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 facility 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 facility operation, • to ensure the implementation of all tasks of the State (the products in the required quality, services, accessibility), • in the technical facility 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 facility 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 facility 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 facility; the external emergency plan and crisis plan (in which the clearly defined cooperation and accountability of the technical facility 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 facility.

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

- B1 - concept and way of real technical facility management - 21 requests,
- B2 - requirements for data, methods, and techniques that ensure the quality of decision-making and management of technical facility - 9 requests,
- B3 - procedures for the correct sitting, the quality of: technical facility design, building, construction and operation - 13 requests,

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

In this case, it goes on the requirements for data, methods, and ways of solving problems in the areas of technical, methodological, organizational, staffing and financial; the complete results are at work [14] . These responsibilities strongly depend on the technical facility nature, size and used technologies and on the conditions in locality in which the technical facility is located.

The keystones of good risk management on all organizational levels are knowledge and creating the permanent safety culture of all participants. It means that each human has responsibility for her personal behaviour and for actions in human society management in which he / she is found.

7. CONCLUSION

The above findings show that risk and risk sources connected with the technical facilities change with time Because the human factor at decision-making is one of important risks´ source, it proposes two super processes for management of human activities. Their adherence reduces the origin the organizational accidents and it ensures the quality management and trade-off with risks.

The research reveals a lot of deficiencies at risk management that are in practice, e.g.:

- in many entities´ concepts, on which the risks or activities connected with management or trade-off with risk, it is not considered the system nature, interconnections of individual systems, existence of some internal and external disasters and changes in time and space (usually only direct selected disaster impacts are considered). It proves series of famous failures of technological and social entities, e.g. recent finance crisis that affected the majority of world,
- continually, the managers, technicians and scientists have great confidence in power of software that were really processed on theoretically well-founded models, but are not based on sufficient amount of real data describing the behaviour of followed entity during the sufficient time interval length; i.e., the appurtenant software can just contain the measures for adaptation of entity behaviour to changes in time and space, and therefore, the have not capability to avert or mitigate great disasters impacts that are beyond their designs. From the risk engineering knowledge, such entities need to have emergency plans, continuity plans and operational crisis plans for protection of assets being in the entities´ vicinities,
- for risk assessment there are often used indistinctly determined criteria and classificatory procedures from which the real size of losses and damages on public and private assets is not recognizable (on risks they often adjudicate administrative and politicians who have low knowledge on risks and their impacts, or they have not real responsibility),
- at risk determination, it is often neglected the accent on use of relevant data and relevant methods; i.e. only exceptionally it is performed the judgement of representativeness and validity of data sets and sensibility of methods used for data processing, which in practise is manifested by errors in both, the risk determination and the measures for risks suppress,
- at ensuring the entity security and development, it is often considered to partial risks and exceptionally the integrated risks are considered. The integral (systemic) risks are considered only singularly.

For improvement, it is necessary:

- reconnaissance of important assets in real entity and its vicinity, the safety of which is the target,
- determination of disasters that can have unacceptable impacts on the studied entity, their possible scenarios at different conditions in and out of entity; it means to

consider the possible occurrence of several disasters mutually interconnected (amplification of impacts by bad maintenance, cascade effects),

- determination of processes that have capability to cause to happen the worse scenarios; determination of their criticalities and occurrence probabilities,
- evaluation of risks connected with processes with different scenarios, and mainly those that have capability to cause to happen the worse scenarios,
- judgement of human capability at copping with risks, namely critical ones, according to human possibilities and tools that are to disposal; the CBA is important tool,
- to perform correct decision on measures for coping with risks that were selected as important,
- to select the correct procedures suitable for given site for measures application in this site at prevention, mitigation and response (none of measures is suitable for all sites [13,14]),
- to determine correct procedure of realisation of measures of all kinds – technical, organizational, finance, legal and human sources,
- to ensure the prompt performance of measures,
- to introduce the monitoring that will follow the effectiveness of accepted measures and ensure the prompt correction measures.

From above concept it follows that the high-quality work with risks represents the process which is challenging on knowledge, real data and time, and therefore, it requires the relevant interface of:

- deep findings and experiences,
- independent decision-making and management for public interest benefit,
- quality implementation of measures,
- support from all participants.

In case of lack of time, detail data or professionals the method based on comparison of entity safety level with another paradigmatic entity is possible to use. ***Benchmarking*** is the method of systematic comparison of processes, organizational structure, products and power of a given entity with other globally successful entities with aim to reach the excellency. It usually uses at risk management at cases if the goal is ideal and according to the good practice principles, it is suitable to manage the risks as the best operators in the given sector carry out it.

It is important continuously to consider that for whole human society welfare, the risks need to be managed in benefit of public interest, i.e. human security and development. From epoch of F. Taylor, the founder of scientific management and his successor H. Fayol [23,24], the basic functions of management are not changed; the management goes on to lead (executors of management are people) the controlled organization or organizational part to prosperity and efficiency, and some change in this direction has not been predicted.

During the time, they have been changing the methods, the techniques and tools, how manage and lead, i.e. coordinate the human working activities so they may be

performed effectively and efficiently. The social, technical, economic and globalization changes are reflected into changes of management of businesses and regions. This trend is permanent and it will also continue in the future. It induces the need of new development strategies based on smart technologies, new ways of work with risks, use of mutual active interactions among the research and business communities at creation and dissemination of knowledge. The successful development is more and more complex and depends on level of trade-off with risks in all entities.

In all entities, it goes on achievement of conditions at which the entity has the capability to dampen famous and foreseeable internal and external disasters that can damage some entity elements (or whole entity). It mainly goes on preservation of entity structure, entity stability, entity reliability and entity behaviour that is in harmony with entity mission, i.e. strategic targeted direction. It goes on level of entity stability and on its primary and secondary adaptation. In harmony with this mission, it is possible the entity safety management to structure and to define as:

- domain of management of relatively self-reliant (independent) activities with aim preventively to precede the risks or to minimize the risks consequences if risks realize,
- institutional set of subjects – actors ensuring the safety in regions, businesses that are from public administration and private entities,
- use of methods, procedures, directions, standards, norms and tools of management including the special methods and technologies for institutional (team) cooperation of individual actors ensuring the entity safety,
- systematic, functionally arranged, recurrent cycle of interconnected activities with the accent on permanent improvement of trade-off with risks which leads to entity safety upgrade.

The human security and entity development depend on level on which we trade-off with risks in processes that are round us; if we are capable existing and foreseeable risks to identify, to analyse, to assess and to control, i.e. effectively manage. The appurtenant sources – human, finance, information and time would be also the motive power of positive human society development. But they can be limited factor or even by destructive factor if they are missing.

Generally, it is necessary to improve the safety culture and human learnedness on risks of citizens, administrators and politicians on all levels as the organizational accidents problem [13-15] shows.

From the viewpoint of responsibility for technical facility risk management and trade-off with risks towards safety, two domains need to be followed. The first domain covers the responsibilities in which the public administration responsibility scope is greater than technical facility management responsibility. Its research reveals 40 items. The other domain covers the responsibilities in which technical facility management deals with technical, economic, personal etc. items and public administration performs the surveillance from the public interest view. Its research reveals 66 items.

REFERENCES

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

[2] 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.

[3] 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

[4] 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.

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

[6] 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

[7] 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.

[8] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W. (eds). *Safety and Reliability of Complex Engineered Systems: ESREL 2015.* ISBN 978-1-138-02879-1. London: CRC Press, 4560p.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] 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

[15] 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

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

[17] 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.

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

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

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

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

[22] MASLOW, A. H. *Motivation and Personality*. New York: Haper 1954, 236p.

[23] TAYLOR, F. *The Principles of Scientific Management*. ISBN 0-415-27983-6. Routledge 1911.

[24] FAYOL, H. *General and Industrial Management: Henri Fayol's Classic Revised by Irwin Gray.* Belmont: David S. Lake Publishers 1987.

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

[26] 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.

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

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

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

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

[31] HAIMES, Y. Y. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis* 29 (2009), 12, pp. 1647–1654.

[32] CURLEY, S. P. The Application of Dempster-Shafer Theory Demonstrated with Justification Provided by Legal Evidence. *Judgment and Decision Making*, 2 (2007), pp. 257–276.

[33] PROCHAZKOVA, D., PROCHAZKA, J. Alternatives of Work with Risks Used at Technological Facilities Safety Management. *Universal Journal of Management.* ISSN 2331-950X, 6(2018), 8, pp. 287-294. ISSN 2331-9577, http://www.hrpub.org DOI: 10.13189/ujm.2018.060804

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

[35] COASE, R. H. The Problem of Social Costs. *Journal of Law and Economics,* Vol. 3, The University of Chicago Press 1960, pp. 1-44.

[36] PROCHAZKOVA, D. Optimum Concept of Management and Trade-Off with Risks. In: *Safety and Reliability: Methodology and Application.* ISBN 978-1-138-02681-0. London: CRC Press 2015, pp. 1463-1471.

[37] OECD. Assessing Societal Risks and Vulnerabilities*. OECD Studies in Risk Management*. Paris: OECD 2006, 276p.

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

[39] 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.

[40] 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.

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

[42] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2017. www.ns.iaea.org/standards

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

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

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

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

[47] OTA. *Public Law 92-484.* www.princeton.edu

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

[49] US EPA. PHA Techniques in Chemical Emergency Prevention & Planning. *Newsletter* 2008, No. 8, pp. 3-6.

[50] PROCHAZKOVA, D., PROCHAZKA, J. Complex Technical Facilities Risk Management Responsibilities. In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL);* eds: M. Beer, E. Zio. ISBN 978-981-11-2724-3. Singapore: ESRA 2019, Research Publishing 2019, pp. 1735-1742, doi:10.3850/978-981-11-2724-3_0095-cd, e:enquiries@rpsonline.com.sg

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

ANNEX 1 - DETERMINATION OF SIZE OF MAXIMUM EXPECTED DISASTERS FOR ENSURING THE TECHNICAL FACILITY SAFETY

The task dealing with determination of maximum possible or maximum expected disaster for solution of problems in real practice, in detail described in works [1-5] is of principal importance for both, the safety management and the insurance domain. Therefore, the attention has been paid to this domain for a long time.

The methodology development in time progressed conformable with the knowledge development, roughly by the following way:

- maximum expected disaster size = size of maximum observed disaster in historical period,
- maximum expected disaster size = size of maximum observed disaster in historical time + certain correction on the indeterminateness (random and knowledge uncertainties) or on the reality that extreme disaster has not had to occur yet. The correction always depended on experience and knowledge of assessor,
- maximum expected disaster size = disaster size that corresponds to intersection of graph showing the disaster frequency occurrence with the disaster size axe. Challenges to this method mainly consisted in reality that results of such assessments might be distinctly physically impossible in some cases,
- maximum expected disaster size = result of methods for extreme value determination [1-5].

Extreme value determination is widely used in many disciplines, such as earth sciences, structural engineering, finance, traffic prediction, geological engineering and biological sciences. Applications of method for extreme value determination usually go from the Gumbel distribution [6] that is a particular case of generalized extreme value distribution.

The applications for earthquakes and other disasters for needs of terms of references for nuclear power plant site locations authors started in 80s of last century and step by step they were spread for building the other complex technological complexes; the real values are in the safety documentation of these complexes. In practice connected with complex technological facilities [1,2], it was successfully tested the following relations:

$$R_t(I_0 \geq I_{0i}) = 1 - \left\{ \frac{T}{T + t.P(I_0 \geq I_{0i})} \right\}^{n+1}, \qquad (1)$$

$$P(I_0 \geq I_{0i}) = \frac{e^{-\beta I_{0i}} - e^{-\beta I_{0\max}}}{e^{-\beta I_{0\min}} - e^{-\beta I_{0\max}}}, \qquad (2)$$

in which: $R_t = (I_0 \geq I_{0i})$ is the probability that the size of disaster I_0 does not exceed the size I_{0i} in the time interval t; $P_t (I_0 \geq I_{0i})$ is the probability that the size of disaster I_0 exceeds the value I_{0i}; P is defined by the equation (2); T is the disaster observation time interval; n is the observed disaster number; I_{0min} is the minimum disaster size (from which the catalogue is homogeneous; it represents the data set homogeneity limit); and I_{0max} is the maximum disaster size in the given region.

It means that the relations hold for intensities from interval $I_{0min} \leq I_0 \leq I_{0max}$. Parameter β is determined using the numerical parameter b_c from the cumulative frequency equation

$$\log N_c = a_c - b_c I_o \,, \tag{3}$$

in which N_c is the cumulative frequency of disasters, I_0 is the disaster size, a_c and b_c are numerical parameters calculated for intensity interval $I_{0min} \leq I_{0i} \leq I_{0max}$. It holds $\beta = b_c \ln 10$. The mean value of return period η for the disaster with the intensity of I_0 is equal to time t for which it holds the relation $R_\eta = 0.633$(expressing the probable mean value of normal distribution).

The impacts of disaster on the territory and on the complex technological facility depend on the type of disaster and on the vulnerability of given assets; real data are shown e.g. in quoted works of authors.

From the safety reasons we in practice use the conservative deterministic approach for all disasters because the theory of extreme values is based on the following assumptions:

- the conditions that prevailed in the past, need also to apply in the future,
- the largest observed phenomena in a given time interval are independent,
- the largest phenomena size in a given interval will be the same in the future as in the past.

It is necessary to note that these assumptions are not in reality fully veridical [1,2,7-9], which influences the results of predictions of large (extreme) disasters.

In practice, according to the theory of extreme values there are determined two quantities the return period and the annual probability of non-exceedance by which the disaster hazard is determined.

References

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

[2] PROCHAZKOVA, D. *Principles of Risk Management of Nuclear Facilities.* ISBN 978-80-261-0173. Plzen: University of West Bohemia 2016, 56p.

[3] LUCK, P. H. *Schweizer Rueck – Sonderrisiken*. Zuerich: Swiss Re Publishing 1998, 23p.

[4] MUELLER, S. ET AL. *Safety Culture – a Reflection of Risk Awareness*. Zuerich: Swiss Re 1998, 45p.

[5] ZIMMERLI, P. *Natural Catastrophes and Reinsurance*. Zuerich: Swiss Re 2003, 46p.

[6] GUMBEL, E. *Statistical Theory of Extreme Values and Some Practical Applications.* New York: Columbia University Press 1954.

[7] BEN MENAHEM, A. *Historical Encyclopaedia of Natural and Mathematical Sciences.* ISBN 978-35-40-68831-0. Berlin: Springer 2011. 5988p.

[8] BEN MENAHEM, A. *Probability in Physics.* ISBN 978-04-86-40465. Berlin: Springer 2011. 324p.

[9] PROCHAZKOVA, D. Earthquake Pattern in Central Europe. *Acta Universitatis Carolinae - Mathematica et Physica*. 34 (1993), pp. 3-66.

ANNEX 2 - METHODS USED IN SAFETY ENGINEERING

1. Introduction

High-powered tool represented by engineering of the safety called “safety engineering” does not only deal with technical problems but it respects public assets in the system vicinity, is a branch applying the methods, tools and techniques and it is based on engineering and managing approaches by way in order that the system might be safe for all public assets during the whole its life cycle [1]. The ensuring of such comprehended safety management is particularly marked from the risk management viewpoint by these characters: sitting – designing – construction – project with risk reduction; operation with integration of early warning systems and of procedures for management of acceptable level of risks; and defeating the abnormal, emergency and critical conditions at operation and at putting out of operation [1,2]. However, the safety engineering conception was just expressed by technical terms, it holds at other domains that are important for safe human system with sustainable development; only there is necessary to use suitable transformation of terms in order that it might be comprehensible for specialists of partial disciplines that are only adapted to actual terminology [3,4].

The safety engineering is systematic use of engineering knowledge and experiences for optimising the protection of human lives, environment, property and economic affairs. From the professional view it goes on process seeking all potential conditions that could threaten favourable operation of a given system in all stages of its life cycle, and identifying the capabilities for their defeating by prevention, preparedness, response and renovation. It uses tools, methods and techniques that indicate how we could:

- texturing the problem,
- determine what we ought to solve,
- collect and create data sets so they might have a clear evidence to a given problem,
- select method for data processing so outputs might be relevant to a given problem,
- interpret the outputs in given conditions.

Therefore, it uses a family of exact methods, tools and techniques and present work contains the survey of their fine members.

From above given facts it follows that safety engineering is the branch that solves problems, i.e. it uses the methods, tools and techniques that indicate how to: texturing the problem; determine what might be solved; collect and create data set in order that it might give evidence to a given problem; select method for data processing in order that outputs might be relevant to a given problem solution aim; and how to interpret outputs of data processing from the view of human system safety that includes functionality and reliability of a given system.

From the given facts it follows that at selection of the methods, tools and techniques we need to respect that safety engineering is multi-branch and cross-section discipline that uses both, the general and specific methods, tools and techniques. The specific

ones are either simple or complex [5-7]. The complex ones represent use of several general or simple methods, tools and techniques. Individual methods, tools and techniques respect reality that aimed complex safety management of each system cannot be only reached by technical or knowledge items but by combination of possible and accessible branch tools of human activity, i.e. they must be used the methods, tools and techniques logic, technical, finance, managerial and arbitrary because integral part of safety engineering is decision-making on technical problems, human factor, costs and on time schedule etc. It means that for solution of present tasks of safety engineering that requires non-trivial problem solving to use the multi criteria methods, tools and techniques [6] in which we must respect that assets and risk source have different natures that are roots of criteria incommensurability and at their selection we must respect data quality, structure of solved problem and requirements on output quality; and specially verify both, the data quality (correctness, completeness, testified capability to problem) and also the expert competences (IAEA, OECD, USA, WB etc. have strict criteria for expert qualification verification).

According to way of data acquisition we separate the safety engineering methods, tools and techniques:

1. ***Empirical*** (based on experience). The survey of facts is made by inquiries and questionnaires. These are used at data collection on human behaviour and human society behaviour in sociology but also at acquisition of impact distribution in the case of earthquake, wind storm or other disasters in territory. In exact sciences there are used for their rapidity and modesty. Accuracy of such data is lower than those obtained by instrumental measurement but qualified statistical processing gives good and reliable information for decision-making and management.
2. ***Theoretical.*** They create findings, hypotheses, theoretical constructions on the basis of general science procedures, i.e. they are based on use of algorithms that lead to solving all tasks of a given type.
3. ***Expert.*** They use professional (professionals) for activity that requires special knowledge. They are used in many situations the common feature of which is necessity of professional (expert) judgement of problem and of its further development in future. They are also used if there is necessary to eliminate local view on a given problem and to judge it independently in new, broader or more specialised frame.

According to ways of knowledge acquisition we separate the safety engineering methods to:

- ***procedures for acquisition of fundamental (usually individual) knowledge*** – as discovery of properties and behaviour of a given substance, behaviour of nanomaterials under different physical and chemical conditions etc.,
- ***procedures for solution of simple practical tasks*** – as allocation and application of fundamental knowledge in practice, e.g. typical earthquake impact scenario for earthquakes from one focal region in a given region; way of response to chlorine release from a given building etc. In this case we need also to solve at data acquisition whether we are dependent or independent on phenomena recurrence (e.g. measurement of natural events is non-reproducible) and how inaccuracies in fact acquisition may influence uncertainties and vagueness in data and by that also in knowledge,

- and ***procedures for solution of tasks of strategic nature*** – as discovery of basic knowledge for support of capability to solve effectively present and future problems of a given object, e.g. connected with security and sustainable development of human system, with human society development in a given region. In this case we must solve how at data acquisition we are dependent on fact whether followed processes are or are not stable in space and time (e.g. processes of occurrence of floods, earthquakes etc. are not stable in time – extreme phenomena occur rarely and irregularly in time and space) and how inaccuracies in data acquisitions might influence uncertainties and vagueness in data and by that also in knowledge, and what follows from it for prediction and consecutively for management; i.e. it goes on qualified selection of optimum variant from a set of variants offering different combinations of followed parameters for problem solving.

2. Results of research of methods of risk engineering

Outputs of research of selected methods from the viewpoint of their application in domain of safety and security [8] is in Table 1.

Table 1. Way of use of engineering methods, tools and techniques and their shortages.

Method, tool, technique	**Way of use, principals for use, shortages at use**	**Evidence / proof**
Case study	Solution of non-structure problems - critical items are knowledge of experts on problem and its context. In management and engineering the safety and security the case study was verified by real data for use in following tasks: problem structure and problem context identification; forecast of scenarios / variants / alternatives; and selection of acceptable variant from the experience viewpoint.	[9-11]
SWOT analysis	Solution of non-structure problems - critical items are knowledge of experts on problem and its context. In management and engineering the safety and security the SWOT analysis was verified by real data for use in following tasks: understanding the problem; understanding the problem context; understanding the problem structure; as the source material for formation of variants of future development and for selection of optimum variant for problem solution.	[9-11]
DELPHI method	Solution of non-structure problems - critical items are knowledge of experts on problem and its context.	[9-111]

	In management and engineering the safety and security the DELPHI method was verified by real data for use in following tasks: understanding the problem; determining the problem context; determining the problem structure; determining the basis parameters of problem – e.g. occurrence probability of some phenomena; determining the process variants connected with the process manifestation; determining the occurrence probability of process variants; and determining the most probable process variant etc.	
Theory of extreme values	Solution of structure problems. In management and engineering the safety and security the theory of extreme values was verified by real data for use in following tasks: determination of size of critical disasters that can be expected in disaster focal region; determination of return period for the given disaster size; and determining the disaster scenario either by processing the empirical scenarios corresponding to disaster with a given size or by simulation based on physical disaster characteristics.	[10-12]
Multi-attribute utility theory (MUT) – version TIEQ	Solutions of non-structure complex problems - critical items are knowledge of experts on problem and its context. In management and engineering the safety and security the multi-attribute utility theory (MUT) – version TIEQ was verified by real data for use in following tasks: identification of tasks important for problems´ solving; determination of problem structure according to criteria from domain of safety, economy, environment and social (fundament for decision support systems); and selection of optimum variant of problem solved. Results can be used for prognosis of future behaviour of system under account if data on problem development are specially prepared in time series.	[9-11]
Methods of operation research (CPM, PERT, GERT, PETRI NETS, BAYESION NETS)	Solutions of non-structure complex problems - critical items are knowledge of experts on problem and its context. The application of operation research methods has the following features: problem situation is closed system or the links to vicinity are precisely defined; problem situation is represented by mathematical model; at calculation the computation technique does not insert the human behaviour.	[9-11]

	The solution is in motion in the following stages: problem formulation; model construction; solution of problem on model; analysis of solution and corrections; and implementation. The methodological shortages are: high complexity of models; and solution that cannot be implemented. In management and engineering the safety and security the methods of operation research (CPM, PERT, GERT, PETRI NETS, BAYESIAN NETS) were verified by real data for use in following tasks: identification of problems; determination of problem structure according to criteria from domain of safety, economy, environment and social; determination of problem solving variants and selection of optimum variant of problem solved; support for decision-making - i.e. retrieval of optimum results for given conditions.	
Analytical hierarchy process (AHP)	1. Solution of non-structure problems - critical items are knowledge of experts on problem and its context. 2. Decision situations to which the AHP can be applied include: 3. *Choice* - The selection of one alternative (variant) from a given set of alternatives, usually where there are multiple decision criteria involved. 4. *Ranking* - Putting a set of alternatives in order from most to least desirable. 5. *Prioritization* - Determining the relative merit of members of a set of alternatives, as opposed to selecting a single one or merely ranking them. 6. *Resource allocation* - Apportioning resources among a set of alternatives. 7. *Benchmarking* - Comparing the processes in one's own organization with those of other best-of-breed organizations. 8. *Quality management* - Dealing with the multidimensional aspects of quality and quality improvement. 9. *Conflict resolution* - Settling disputes between parties with apparently incompatible goals or positions. 10. In management and engineering the safety and security the AHP was verified by real data for use in following tasks: determination of problem structure;	[9-11]

	results for individual levels of problem in selected hierarchy; and aggregate result for the whole.	
Methods based on process models – especially methods for risk assessment, risk management, risk engineering and complex methodology for negotiation with disaster risk	Solution of both, the structure and the non-structure problems. In case of nom-structure problems - critical items are knowledge of experts on problem and its context. *Process model* is used in various contexts. For example, in process modelling, in strategic planning etc., e.g. the enterprise process model is often referred to as the *business process model*. Process models are core concepts in the discipline of process engineering. The process models are processes of the same nature that are classified together into a model. Thus, a process model is a description of a process at the type level. The targets of a process model are to be descriptive, prescriptive and explanatory. The descriptive ones are to: track what actually happens during a process; and take the point of view of an external observer who looks at the way a process has been performed and determines the improvements that must be made to make it perform more effectively or efficiently. The prescriptive ones are to: define the desired processes and how they should / could / might be performed; and establish rules, guidelines, and behaviour patterns which, if followed, would lead to the desired process performance. They can range from strict enforcement to flexible guidance. The explanatory ones are to: provide explanations about the rationale of processes; explore and evaluate the several possible courses of action based on rational arguments; establish an explicit link between processes and the requirements that the model needs to fulfil; and pre-defines points at which data can be extracted for reporting purposes. From a theoretical point of view, the meta-process modelling explains the key concepts needed to describe what happens in the development process, on what, when it happens, and why. There are following types of coverage where the term process model has been defined differently: 1. *Activity-oriented:* related set of activities conducted for the specific purpose of product definition; a set of partially ordered steps intended to reach a goal.	[9-11]

	2. *Product-oriented:* series of activities that cause sensitive product transformations to reach the desired product. 3. *Decision-oriented:* set of related decisions conducted for the specific purpose of product definition. 4. *Context-oriented:* sequence of contexts causing successive product transformations under the influence of a decision taken in a context. 5. *Strategy-oriented:* allow building models representing multi-approach processes and plan different possible ways to elaborate the product based on the notion of intention and strategy. Risk assessment, risk management and risk engineering – methods are methods that can help to solve problems and to create safety and security. For practice there are the most suitable for the first risk assessment and the fundamental monitoring the risk sizes, the following methods: check list; safety audit; what – if analysis; and relative ranking. Only for specific purposes as it is the risk determination for complex technological processes, complex objects etc. there are used more sophisticated methods as are: 1. Preliminary Hazard Analysis – PHA that is the procedure for searching the dangerous conditions (i.e. emergency situations), their causes and impacts and for their categorisation according to criteria stipulated in advance. 2. Process Quantitative Risk Analysis – QRA that is the systematic and complex access for prediction of occurrence frequency estimation, and of impacts of accidents on establishment or system operation. 3. Hazard Operation Process – HAZOP, that is the procedure based on stochastic hazard assessment and on assessment of risks followed from hazard. It is team expert complex method. The HAZOP main purpose is the identification of potential accident hazard. 4. Event Tree Analysis – ETA that is the procedure that pursues the course of the process from the initiating event over inventing the possible events always pursuant to two possibilities - favourable and unfavourable.	

5. Failure Mode and Effect Analysis – FMEA, that is the procedure based on the analysis of ways of disturbances and their impacts that enables to search the impacts and causes pursuant to systematically and structured organisation of determined arrangement faults.
6. Fault Tree Analysis – FTA, that is the procedure based on systematic retrospective event analysis with the use of chain of causes that can lead to selected top event.
7. Human Reliability Analysis – HRA, that is the procedure for the human factor influence appreciation on the disaster occurrence or some their impacts occurrence.
8. Fuzzy Set Method – FL – VV that is the method of lingual variable. It is complex multi-criterion method of decision analysis from the category of soft, fuzzy type.
9. Causes and Consequences Analysis – CCA that is the mixture of fault tree analysis and event tree analysis.
10. Probabilistic Safety Assessment – PSA that stipulates the contributions of individual vulnerable parts to total system vulnerability.

These specific methods were derived for special practical cases, and therefore, before use it is necessary to verify if conditions of technology transfer are fulfilled.

There are also *specialised methods, e.g.:* CRAMM (CCTA Risk Analysis and Management Methodology – see standards CSN ISO/IEC 13335 and ISO/IEC 17799), COBRA, MELISA.; methodologies - *@risk* (based on Monte Carlo Methods); *RiskPAC*; *Risk-WATCH.*

There is also special software as: ALOHA, SAVE I, ROZEX, CEI, TEREX, EFFECTS that are broadly used for them it also holds that it is necessary to verify if conditions of technology transfer are fulfilled and it is necessary to know if they are suitable for solution of task under account because individual versions only respect special conditions.

Note: on the address http://www.riskworld.com [12] - there is possible to find more than 1000 specialised methods that are supported by software – they were developed for specific cases, and therefore before their

	use it is necessary to verify if the conditions for technology transfer are fulfilled. Risk management methods and risk engineering methods are complex and they are described e.g. in [3,11]. *Engineering working methods* include the methods, tools and techniques used for: *disaster assessment* (i.e. site, maximum expected size, occurrence probability or occurrence frequency, distribution and size of impacts); *hazard assessment* (determination of normative disaster size – the most frequently design disaster = centennial disaster); *risk assessment* (in a given site according to hazard size and according to amount and vulnerability of assets). Complex methodology for negotiation with disaster risk is created by set of fasten (tied) methods for assessment of disasters and for risk management that is created by: - method for determination of relevant disasters in a territory; - method for determination of maximum expected disaster size (it has to modifications: root of hazard is only one source of disaster; and root of hazard is several sources of disaster); - method for determination of attenuation of disaster impact size with distance from source of disaster; - methods for determination anomalies in territorial distribution of disaster impacts; - method of determination of unacceptable disaster impacts; - method for assessment of potential damages on property caused by unacceptable disaster impacts; - method for determination of optimum corrective measures for expected disasters in a given territory; - method for implementation of corrective measures for ensuring the property renovation in a given territory; - method for determination of database of corrective measures to individual disasters; - method for determination of parametric relation between cost for renovation vs. disaster size; - method for determination of financial reserve for renovation.	

	Methods, tools and techniques for risk assessment, risk management, risk engineering and complex methodology for negotiation with disaster risk are used for determination of: hazard assessment; vulnerability assessment; disaster scenarios in variant mode; risk assessment; risk mitigation and safety management; principles of prevention, preparedness, response and renewal in dependence on accessible forces, sources and means; planning and management documents in advance; personal, financial, technical reserves in advance etc. According to way of data acquisition we separate the engineering methods to: 1. *Empirical* (based on experience). The survey of facts is made by inquiries and questionnaires. These are used at data collection on human behaviour and human society behaviour in sociology but also at acquisition of impact distribution in the case of earthquake, wind storm or other disasters in territory. In exact sciences there are used for their rapidity and modesty. Accuracy of such data is lower than those obtained by instrumental measurement but qualified statistical processing gives good and reliable information for decision-making and management. 2. *Theoretical.* They create findings, hypotheses, theoretical constructions on the basis of general science procedures, i.e. they are based on use of algorithms that lead to solving all tasks of a given type. 3. *Expert.* They use professional (professionals) for activity that requires special knowledge. They are used in many situations the common feature of which is necessity of professional (expert) judgement of problem and of its further development in future. They are also used if there is necessary to eliminate local view on a given problem and to judge it independently in new, broader or more specialised frame. According to ways of knowledge acquisition we separate the engineering methods to: - *procedures for acquisition of fundamental (usually individual) knowledge* – as discovery of properties and behaviour of a given substance, behaviour of nanomaterials under different physical and chemical conditions etc.,	

	- *procedures for solution of simple practical tasks* – as allocation and application of fundamental knowledge in practice, e.g. typical earthquake impact scenario for earthquakes from one focal region in a given region; way of response to chlorine release from a given building etc. In this case we must also solve at data acquisition whether we are dependent or independent on phenomena recurrence (e.g. measurement of natural events is non-reproducible) and how inaccuracies in fact acquisition may influence uncertainties and vagueness in data and by that also in knowledge, - *procedures for solution of tasks of strategic nature* – as discovery of basic knowledge for support of capability to solve effectively present and future problems of a given object, e.g. connected with security and sustainable development of human system, with human society development in a given region. In this case we must solve how at data acquisition we are dependent on fact whether followed processes are or are not stable in space and time (e.g. processes of occurrence of floods, earthquakes etc. are not stable in time – extreme phenomena occur rarely and irregularly in time and space) and how inaccuracies in data acquisitions might influence uncertainties and vagueness in data and by that also in knowledge, and what follows from it for prediction and consecutively for management; i.e. it goes on qualified selection of optimum variant from a set of variants offering different combinations of followed parameters for problem solving. In management and engineering the safety and security the methods based on process models – especially methods for risk assessment, risk management, risk engineering and complex methodology for negotiation with disaster risk were verified by real data for use in following tasks: problem understanding; problem context understanding; problem structure understanding; determination of aims of management and of engineering disciplines; determination of variants of problem solving and corresponding tasks for management and engineering disciplines; methodologies of risk management under different conditions; interpret results in a given conditions and formulate data for lesson learned; and plans for upgrade.	

Methods for system of systems (SoS) / systems system behaviour description and management	Solution of non-structure problems - critical items are knowledge of experts on problem and its context The methods for system of systems investigation, namely all, i.e. computational, technical and managerial must correspond to the object character. Because they have mostly several assets that are incommensurable, the more criteria must be used and all problem solution is multi-dimensional; i.e. all analysis, assessments and other procedures are multi-criteria. It means higher demand on methods, tools and techniques applied; if some problem might be decided, the managerial and computational methods, tools and techniques or managerial and technical methods, tools and techniques must be combined, i.e. heuristic approach based on good engineering practice is suitable for practice. Because we need good solution there must be applied strict rules at heuristic approach. Only in cases when the problem solved can be reduced to simple one the simple procedures can be used. For the investigation of system of systems, their behaviour and failure there are apart from analytical methods, classical methods of risk analysis, scenarios determination, deterministic and probabilistic safety analysis, security network analysis, reliability analysis, expert judgement, risk matrix, criticality matrix, Monte Carlo method etc. there are used for the SoS model construction used specific methods as: Bayesian Method; Bayesian Network; Mixed Bayesian Network; Fuzzy Bayesian Network Model; Bayesian Reliability Model; Fuzzy Rule-based Bayesian Reasoning (FuRBaR); Petri Nets (PN); Coloured Petri Nets (CPN); Stochastic Petri Nets (SPN); Coloured Stochastic Petri Nets (CSPN); Case Study (CS); Multi-Attribute Utility Theory (MAUT); Multi-Criteria Analysis (MCA); Weighted Sum Approach (WSA); Concordance, Discordance Analysis (CDA); Technique for Order Preference by Similarity to Ideal Solution (TOPSIS); Ideal Point Analysis (IPA); Aggregation Preferences (AGREPREF); Preference Ranking Organisation Method for Enrichment Evaluations (PROMETHEE); Markov Chain (MC); Multi-Objective Genetic Algorithm (MOGA); a Multiplicative Intuitionist Linear Logic (MILL). The published results on methods for system of systems (SoS) / systems system behaviour description and management are mostly in the theoretical level. We have a lot of images that were not verified on real data.	[9-11]

	The CVUT experimental investigation of electro-energy system shoved that easy application of given theoretical methods get at barriers that are formed by reality that technological, cyber, logical or territorial connections are to site specific. The results showed that the main problem consists in reality that the SoS structure is too site specific. If we applied these model construction methods in the form step by step (e.g. in some hierarchy of technological, cyber, logical or territorial connections) we can obtain by these methods: groundwork for decision-making; retrieval of critical points and items of SoS that might be sources of interdependences in which failure cascades can occur; determination of risks connected with critical points; and identification of priorities and aims that ensure the safe SoS and the whole community safety.	
Combination of methods for complex territory safety management and safety engineering	*Note:* territory safety management determines the aims fundamental and important for territory safety and territory safety engineering realised these aims in real conditions of individual sites and regions. The combination of methods for complex territory safety management and safety engineering is combination of such methods that are suitable for solution of FOCUS project tasks. It is tailored to these tasks because human cognition and experiences show that such approach gives the best results. Its assessment is concentrated to facts that are important for solution of tasks that are in the FOCUS project, i.e. the topic is not assessment of all features and variants occurring in the practice. To obtain qualified outputs from the project we only give information that was verified on real data. Therefore, we also collected information on real solutions from domains that occur in FOCUS targets. Solution of both, the structure and the non-structure problems - critical items are knowledge of experts on problem and its context The complex territory safety management method consists of four main parts that are: 1. Qualification of territory, identification of disasters that can affect the territory and determination territory asset vulnerabilities (TERRITORY SCREENING). 2. Qualification of risks, identification of possible critical situations (RISK ASSESSMENT).	[10,11]

3. Qualifications of available measures and activities used for trade-off (negotiation) with risks and identification of gaps in trade-off with risks (SCREENING THE MEASURES AND ACTIVITIES FOR RISK MANAGEMENT AND FOR TERRITORY SAFETY UPGRADE, AND ASSESSMENT OF LEVEL OF TRADE-OFF WITH RISKS).
4. Identification of critical interfaces that must be treated in a specific way to ensure human survival and possibility for further development start (IDENTIFICATION OF CRITICAL ITEMS AND PROPOSAL OF SOLUTION OF GAPS).

The details are given in publication [13]. From it follows that the real problem is too complex and that it is necessary to help experts who work with tool. If we use classical approach and we compile the representative data sets for all parts the output is relevant. Because the compilation of representative data sets is time consuming or even impossible (new problem, problem that was underestimated in past etc.), it is necessary in practice to use suitable heuristics, e.g. for territory screening the SWOT analysis; for risk assessment exact methods as extreme theory, PSA, FMEA etc., case study methodology or DELPHI method; for screening the tools for risk management and for territory safety upgrade, and assessment of level of trade-off with risks the specially directed methods as DELPHI, TIEQ, AHP, responsible matrix, risk matrix and other expert methods; and for identification of critical items and proposal of solution of gaps only expert methods. For practical purposes there were, therefore, prepared for each part of tool questions that help experts to use engineering good practice rules and not to forgot on fundamental data [13].

The results of first ca 84 practical tests showed that proposed combination of methods for complex territory safety management and safety engineering can be used in practice and confirmed the theoretical judgement that results are strongly dependent on knowledge and practical experiences of experts who are used for application.

In management and engineering the safety and security the combination of methods for complex territory safety management and safety engineering was verified by real data for use in following tasks: problem identification; problem structure and context identification;

	quantitative outputs for important disasters; identification of ways for trade-off with risks; identification of responsibilities for trade-off with risks; identification of gaps in trade-off with risks and in determination of responsibilities; determination of optimum variant with regard to a given criteria set for trade-off with risks; determination of critical items that can lead to social crisis and that would be objects of research, management and engineering. The combination of methods has potential from the viewpoint of prognosis. By help of this procedure we can obtain variants of future development of followed process but the output variants and their occurrence frequency assessment strongly depend on data quality and on human processor qualification.	

Table 1 shows that none of above described method is all-powerful, i.e. it cannot give us solution of all tasks that might be solved in the FOCUS project. Each of described method has certain principles and demands in order that its application may give qualified outputs. Each of described method is suitable for solution of one or several types of tasks. The selection of method depends on target of problem solution, on amount and quality data set, on time and techniques that we have for solution.

Even though it is possible to say that all investigated tools serve for management optimisation, so it is necessary to concentrate to reality that each method solves the problem from different view, i.e. it serves to another target. E.g.:

1. Methods for stimulation of creativity at creation of n variants (alternatives, scenarios) of solution of problems that may be decided. Among them there are belonged brainstorming, panel discussion, DELPHI method and aimed simulation techniques (NST). The DELPHI method is based on group of experts who being mutually isolated give proposals that are compared, again judged (reverse response is written) and by this way in several steps there are converged the proposed variants.
2. Methods for multi-criteria decision, e.g. process models, models based on MUT, AHP etc. The AHP is the method of multi-criteria decision for solution of non-structured problems (situations) at which the problem is separated into several levels on more simple problems and by this the hierarchical system is created. The process models in the form of arbitrary trees are mostly probabilistic arbitrary trees that serve to display and determination of optimum strategy of management of arbitrary processes with several degrees in which we can trade-off with risks.
3. Methods that serve for optimising the process courses, search of critical paths from the time viewpoint, but also sources if activities (nodes or edges) are evaluated in such way. The CPM and PERT are in principle the same. Its fundament is edge oriented graph – the edge is activity (contrary to MPM – Metra Potential Method) in which it is node-oriented graph – node is activity), The CPM works with deterministic data (values), the PERT works with stochastic values (that are obtained from pessimistic, optimistic and modal judgement, it works with the β distribution). The

Petri nets are also oriented graphs that express the structure of distribute system (two types of node – places and transitions). They are used for modelling so called parallel behaviour of distribute systems. A Bayesian network (BN) is an abstract formal model allowing one to describe cause-and-effect relations between objects and systems being investigated. Causes and effects are quantities, the nature of which is generally random, their number is considerable, and interrelations between them are multi-various. It is established that the time complexity of algorithms of analysis of such models is exponential. This determines the necessity of computerization of computational processes in many respects and also the expediency of development of new types of models and efficient algorithmic means for analysing them.

For the method selection there is important the procedure:

1. To establish the aim of problem solution and to determine what partial tasks must be solved for aim achievements (to investigate problem and to find gaps in knowledge, technical measures, legal and financial measures for problem solution).
2. To assemble accessible data on problem – recent cognition and accessible data. On the base of it to determine „roads“ (processes, plans) for aim achievement, namely including all sources and conditions (measures, actions) for ensuring their course.
3. To appreciate and complete existing data sets.
4. According to partial task and data quality to select suitable method. For generation of set of possible variants, the case study methodology or the DELPHI method may be used. For selection of sufficient good variant respecting the given criteria it is possible to use e.g. the AHP. For optimising the course of a given path it is possible to use CPM, PERT, Petri nets, Bayesian nets and for decision-making during the given path again e.g. AHP.

The experience from practice shows that the best outputs are from method that is tailored to problem solving goal.

3. Prognostic methods

Prognosis is in its wide sense the information about future. It can be seen as a forecast of future events and future development conditions. The characteristic feature of a prognosis is its variability arising from the possibility of setting the variant objectives and methods leading to their achievement, including the probabilistic character of a prognosis. The prognosis is always evaluated by its rate of reliability, which demands the specification of information requirements and requirements for data. Utilization in practice is always presumed at a prognosis setting it apart from *prediction* that *is the part of a scientific work* and from *foresight that is the general ability of a human mind for thinking about future*.

Predictive method for a certain problem is chosen depending on the amount (content) and uncertainty of input information [6]. The accessibility of the input information forms a key factor for the selection of a method. As standard method for prediction are respected: expert opinions, both implicit and explicit with the help of expert model

systems; comparison; field experiment; mathematic simulation; visual simulation (layout, photography, film, 3D model); and physical simulation (noise, air-pollution, soil column etc.).

Predictive methods are expanded to formal and informal. Formal methods recognised as proved are: exact methods; statistic methods; experimental methods; and mathematic simulation. Informal approach represents an engineer assessment and application of analogy.

Individual formal work procedures form the wide category of technically-methodical ways of prediction. In practice, *exact methods* are enabled by the formulation of a real technical idea in several variants, by the measurement of relevant values on a map basis, calculation etc. *Statistic methods* come out of the assembled data (gathered pieces of information) significant for a certain problem and area (surroundings). There are used scientific basics of prognosticating, the theory of rising curves and the assessment of probable evolution trends. By the term “prognosis” we understand a probable statement about events that arise in some spatial or time interval. *Scientific approach distinguishes 3 fundamental alternatives of a methodical approach*: extrapolation or a normative method; synthesis or a morphological method; and intuitive or a theoretical method.

However, in practise we commonly combine the extrapolation with intuition or normative method with a theoretical solution. Significant importance represents a so-called phenomenological projection of forecasts, where there are used both, the empiric experiences acquired in the field of a researched phenomenon and the information from the theory of growing models are used. If there is the evolution (i.e. rising or falling) of a certain quantity according to time without external interference, it can be supposed that the rate of evolution is a definite function of a variable. By solving of a relevant differential equation, the law of growth can be obtained.

Experimental methods and mathematical models differ in a feature that at mathematical models there is a need for a strict formulation of cause and consequence, while by experimental methods these terms don’t have to be determined. But in both cases, it is necessary to schematize (simplify) the system leading to definition of relationship ***cause ---> consequence***. Accomplishment of experiments is deemed indispensable in all cases where there aren’t basic data at a disposition. Basics in this field considered as satisfying are predicted data acquired by a mathematical simulation, laboratory experiments or experiments in situ. Favourite are comparative case studies and terrain pilot projects in similar natural and socio-ecological conditions. In the future, the gathered information of realized projects and practical testing of hypothesis (database) will be a significant help. Experimental methods are divided in: illustrative or physical models symbolizing an affected environment; terrain (field) experiments; and laboratory experiments.

Illustrative models provide, in a certain measure, only the visual forecast of a future situation, whereas physical models provide this forecast in the measure of a physical process. Laboratory experiments simulate biological and biochemical process, but

often in isolation from the overall ecosystem. The aim of the field experiments and tests is a research of the real changes in the area considered.

In mathematical models, the relations between cause and consequence are represented by one or several mathematical equations. *Mathematical models can be:* empirical, processional or mixed. Empiric models are based on experiments or a repeated measurement; they employ the knowledge of statistical analysis and show the relation between cause and consequence without explicitly formulated interrelations (a model of a black box). Beside the general models, special models applicable in a real area or the certain type of surround are used.

Process models (internally descriptive) lie in an explicit definition of process either without a reference to time (stable, constant condition) or with one (dynamic evolution). Complexity (algorithm) of models alters from simple ones that can be solved manually, to complex dynamic and stochastic models requiring a computing technology. In this context different types of models are used:

- distributional models determining a dimensional layout (e.g. source objects, protective zones, primary point field allowing the digital model of a terrain etc.),
- models of a dimensional statistic arising from the supposition that all the elements of the selective files are placed in the coordinate system; models of dimensional modifications, which are primarily represented by models of variant diffusion processes of a different type (e.g. projection of the gradient orientation and rapidity of a diffusion process by a vector field calculation from the primary point field),
- distance-decay models allowing an exact determination of so-called divided distances, safe distances, zones of an increased hazard etc., by which they simplify the resolving about the localization of other investment projects demanding a special treatment (e.g. nurseries, playgrounds etc.).

It should be noted that the behaviour of entities based on forecast models based on assumptions:

- the conditions that prevailed in the past, needs also to apply in the future,
- the largest observed phenomena in a given time interval are independent,
- the behaviour of the biggest phenomena in a given interval will be the same in the future as in the past.

Theoretical models based on the defined theories and their solution is a set of possible scenarios, with each scenario describes the behaviour of entities under certain conditions. For success in practice, it needs to know the full set of conditions in which the tracked entity can occur, the complete set of possible scenarios of the behaviour of the entity, and also the occurrence frequency of each scenario. Due to lack the knowledge, there are the possible sudden changes in conditions, which also mean sudden changes in the behaviour of the entity. This fact means that neither the probabilistic approaches applied methodically in practice since the mid-70's the years do not provide the correct prediction for the behaviour of the entities.

From observation of the real world we know that extreme changes and extreme phenomena occur irregularly and sparse in time. Therefore, modelling the extreme phenomena does not use already from the 70's years the methods of mathematical statistics, but it goes from the law of large numbers, a distribution describing the fluctuation of random maxim (it is suitable for modelling the extreme phenomena using the distribution of Gumbel, Fréchet and Weibull, which represent the limit distribution of the maximum values of random variables). The theory of extreme values needs to have a time series of phenomena and commonly is used since the mid of 80s. years for natural disasters, and in the last decade and in economy. In the area of technologies, it is based on more of the Weibull distribution.

In the area of technology, in which there are simulated situations that are partly random and partly under control of the operator, from 50th years of 20th century for support of decision targeted to the management of the possible behaviour of the entities there are used Markov´ processes based on Markov´ chains. It goes on the choice from several possible options, with each option consists of a Markov´ chain.

Bayesian network is a probabilistic model, which uses a graphical representation for displaying the probabilistic relationships among individual phenomena. It is used for the determination of the likelihood of certain phenomena which arises from the base of the theory of probability. In general, the Bayesian Networks are used for modelling across different areas, support for decision-making and for probability calculation. Bayesian statistics is a branch of modern statistics, which works with the conditional probabilities and it allows to refine the probability of initial hypothesis, how to appear more relevant realities. The core of its mathematical apparatus is the Bayes' theorem. While the classic statistics provides the probability of an event based on the known fact from the past, Bayesian statistics is used where it is not possible. Therefore, it has a very extensive use, where it works with uncertain knowledge: in finance, in management, in medicine, in criminology, and also in detecting the spam. "Bayesian approach" also has great importance in mathematical logic and the theory.

4. Scenario application

The scenario as a tool of pro-active management is a history-systemic model that describes the development of process in its different shapes (variants) dependent on conditions or performed decisions. It imitates mechanisms and processes that are under way in system. Its target is above all to determine critical phenomena or critical items in which it comes up to affection of further development, i.e. there are given alternative options among different terminative stages. Each scenario contains: sequence of events that are under way in its frame (including the possible variants); and description of interaction (communication) between user (originator) and system. For needs of planning and management of safety of followed system the following scenario types are processed in practice: scenario of disaster impacts; scenario of response to disaster; management scenario. For safety management needs the most important are scenarios of disasters because on the basis of which the proposals of response and renovation are performed.

Nowadays, it is possible to find terms such as scenarios, disaster scenarios, scenario management and other in literature and in various strategic documents. The scenario tool is frequently used technique in safety management decisions. Scenarios are compiled on the basis of empirical data or using various simulation techniques, both

analytical and heuristic [6]. Because of variability of the world represented by the human system [14] it is necessary to assemble them in variants, as the runs of relevant processes are variable.

Generally, the scenario is a set of isolated and interconnected processes or phenomena in time and space, which takes place at different spatial and temporal scales. Scenarios are used for different purposes. It is de facto succession, a chain of events in time, area, space or space-time. This chain can be deterministically given or stochastically random and the degree of randomness can in some cases be evaluated by statistical methods, by methods based on fuzzy sets and by experts [15]. In terms of present knowledge, we know that there are sets of events that seemingly have no visible internal connection, but the result of which is some specific condition of the system. In these cases, we talk about so-called deterministic chaos. In systems engineering, there exist methods to describe and understand it [6].

Scenario-as a tool of pro-active management is historical-system model which describes the development of process in its different forms (variants) depending on the conditions or decisions taken. It imitates the mechanisms and processes that take place in the system. Its aim is primarily to identify critical phenomena or points, which affect further development, i.e. which provide alternative choices between different final conditions. For the purposes of emergency planning and crisis management in practice, we put together the following types of scenarios: disaster impact scenario; response scenario; management scenario.

Hazard scenario / threat scenario is not a mathematical variable. This name is used to describe facts, on which the risk assessment is based. Above all, the source of hazard must be known, and then how it can manifest itself; in military terminology term is replaced with the term threat scenario. In the civil administration [16] the threat is understood as a probability rate of an attack (terrorist or military) in a given location; it is the probability that an event or a set of events occur, that are completely different from the required condition or development of the protected assets in terms of their integrity and functionality; it is determined by attacker capabilities, by vulnerabilities of assets protected and by intent of the attacker. Hazard scenario varies in dependence on time.

Disaster scenarios are an essential matter for safety management purposes, because designs of response and recovery (i.e. response scenarios (plans) and recovery scenarios) are performed on their basis. The term scenario is now widely overused.

However, it is necessary to further consider following views on the scenario: purpose, content, format, and life cycle. At first glance, "intention" is the answer to the question "why scenario has to be used, what are its benefits? “ The scenario can be used to project the future (this applies in particular to sustainable development); scenario can serve as decision support (description of activities for emergency response) in a hypothetical situation. The scenario for sustainable development can have three forms:

- predictive (what happens), which is associated with the "What, If" method,
- projective - exploratory (what can happen),
- normative (how to achieve specific development objectives, i.e. to specify the driving force of development).

The task of predictive scenario is to describe future development in its various forms, depending on decisions taken or on expected changes in conditions. This is mainly the identification of critical phenomena and critical points of development in which it is necessary to make major decisions or where a fundamental change can take place, affecting further development. The implications of these decisions are described in scenario as an alternative choice between the final conditions of the future.

In case of response we speak about planning and implementation scenarios using the techniques of process management. Planning scenario for a given disaster consists of a description of the emergency situation (location, possibility of occurrence, etc.) and from description of consequences of emergency situations, i.e., from estimation of damages and losses, and recommendations for prevention and mitigation of disasters impacts. Response scenario describes procedures for overcoming emergency situations aimed to mitigation of the expected impacts of the disaster, to stabilization of the situation and to start of the recovery. There is an essential difference between disaster scenario and response scenario. Disaster scenario includes distribution of disaster impacts in the territory, i.e. damages and losses to be eliminated by response. The response scenario is a set of measures and actions to be accomplished in order to overcome the disaster impacts. In Czech practice it is known under term emergency plan or flood plan. Both types of plans:

- are based on historical data and assumptions, i.e. the scenarios are only narratives (views on the problem),
- identify differences in capacities and define an action plan for response,
- identify and formalize the response teams,
- identify sources of domino effects.

Security plans include procedures for prevention, preparedness, response and recovery, have a general part which relates to the object or area and site-specific parts which depend on what disasters are important for the followed object or territory, what are territory assets and how those assets are vulnerable in case of expected disasters [14].

In the second view “content” it is necessary to answer the question: "what knowledge the scenario contains? “, which is related to the type of scenario. It is necessary to distinguish whether the scenario is a description or an analytic-synthetic approach to the facts. For the purpose of deciding the second approach is more reliable because it is based on documented facts.

In the third and most important (“format”) perspective, it is necessary to answer question "how and what the scenario expresses? “ It is necessary to distinguish whether the scenario is: narrative; descriptive table; logical sequence of events; and time sequence etc.

The chosen scenario format determines the methods, by which is processed in a particular case. It is difficult to find a scenario in a reasonable format, as e.g. it is shown in a set of scenarios in [16] - the given scenarios are just a list of facts, mostly lacking a description of the algorithm on the basis of which they were compiled. Summary of different formats is for example in [17], where the scenario is seen as a management tool. Other examples of format are in [18], in which scenarios are the basis of different

training procedures in response management (but rarely used for training planners). The work also highlights the importance of structure of scenarios, including holistic organization of knowledge. Scenarios are used today in many areas, as documented by summary performed in work [19].

In the "life cycle" it is necessary to the answer the question of "how to handle the scenario? ", i.e. how to understand, interpret, and evaluate it. E. g. at decisions based on disaster scenarios, it is necessary to know whether isolines represent the mean observed values, or some of its limit value, see, e.g. scenarios for earthquakes which are in the works [3] and are used to ensure seismic safety of buildings and infrastructures.

From all of the above it follows that the scenario is generally a set of isolated and interconnected of processes or phenomena in time and space, which takes place at different spatial and temporal scales, and that the scenarios are used for different purposes. Development of scenarios from the perspective of strategic management [14] requires:

1. Ensuring permanent monitoring of the situation in the human system from the point of view of occurrence of disasters and critical situations resulting from them.
2. Creating tools for disaster management and detection of critical situations approaching
3. Creating tools that lead to the removal of critical situations.
4. Creating tools to manage critical situations and to avert protracted critical situations.
5. Creating tools to ensure recovery after critical situations and to ensure the continued stable development.

Complex scenarios for territory management must have 4 separate parts, namely: the disaster scenario, an emergency scenario, scenario for management of response to an emergency, scenario of security management and sustainable development of the territory [14].

Following steps are important when creating scenarios:

- to identify the key assumptions or factors that affect the form of scenarios,
- to focus on factors that have a high potential impact on the shape, size, scope, etc.
- to identify factors with an uncertain nature and to try to produce alternative solution of the scenario.

A prerequisite, however, is a relatively small number of factors that could be incorporated into the possible variants.

Development of scenarios as in [6] consists of:

- gathering the prognostic information about the system and its surroundings,
- identification of targets of studied system,
- identification of internal factors, or barriers to development of the system,
- identification of external factors, or barriers to development of the system,
- identification of alternative management strategies for the system (it is necessary to consider existing management mechanism and its variants, which can be

realized in future periods, simultaneously it is necessary to formulate a strategy for development of the system - which direction is desirable),

- proper compilation of scenario,
- interpretation of scenario.

In all the steps above it is necessary to consider:

- assessment of current condition and current decisions in terms of future development,
- qualitative factors and strategies of various participants,
- the fact that the future is uncertain and multidimensional,
- the fact that each system must be examined globally and systemically,
- the fact that the information and strategies are not neutral, but biased,
- more approaches that are complementary,
- the fact that there are biases in strategies of people and prevent them.

Management scenarios can have different forms, depending on the use intended. Development of scenarios from the perspective of strategic management [13] requires:

1. Ensuring the permanent monitoring of the situation in the human system from the perspective of occurrence of disasters and critical situations resulting from them
2. Creating the tool for disaster management and detection of critical situations approaching.
3. Creating the tools that lead to the removal of formation of critical situations.
4. Creating the tools to defeat critical situations and to avert protracted critical situations.
5. Creating the tools to ensure recovery after critical situations and to ensure the continued stable development.

Based on the scenarios in a variant version there are created decision support systems that help to manage the safety of monitored system [13].

Table 2 briefly describes the differences of two categories of scenarios: gaming scenarios for disaster management and strategic scenarios for conception management [3,4]. The function of both scenarios is to face the unexpected events and test organizational readiness in condition of uncertainty and vagueness. A comparison with data shows that the gambling scenario is suitable for the type of reactive management and strategic scenario is suitable for the type of proactive management.

Table 2. Comparison of application of gaming scenario for disaster defeat and strategic scenario for strategic management

Characteristic	**Gambling scenario for disaster management**	**Strategic scenario for conception management**
Source	Job training in preparation for incidental situation as a military incident, natural disaster, industrial accident.	Long-term forecast in the frame of the policy / decision-making concepts and major investments.
Initial targets	Test of operational skills and systems aimed to create a predictable behaviour in unpredictable situations.	Notify senior managers of organizations about changes in the environment.
The nature of the scenarios and uncertainties	A simple description of the emergency event or situation with which were not previously experienced. Training for a predictable event.	Multiple descriptions of future variants (2-4) in terms of modification of social, economic and political environment. Training of mental flexibility in decision-making in an uncertain event.
The main participants	1. Entity describing the event, design and cope of risk (simulation team). 2. Participants in the field testing the crisis restrain (target audience).	1. Body forming and presenting a description of scenarios (scenario team of authors). 2. Leading managers who use and make strategic decisions according to created scenarios (target audience).
Methodological steps, including public participation	1. Persuasion of senior managers about the importance of used scenarios (simulation team). 2. Decisions about the purpose of simulation: the organizational skills to be tested? (Mutual simulation team meeting and the target audience). 3. Construction and credibility proof of disaster or emergency situation scenarios (simulation team).	1. Persuasion of senior managers about the importance of used scenarios (team of scenario authors). 2. Identification of existing assumptions (thinking), especially of senior managers. 3. Identification of important trends, uncertainties, and suggestions of the outside world that challenges the current mind-set of managers (team of scenario authors).

	4. Design of simulation exercise aimed to determine the response of the target groups to scenario (simulation team). 5. "Playing games "(Simulation Team + target audience). 6. Hearing the players and assessment of experience gained during the game (Simulation Team + target audience).	4. The arrangement of factors for a small number of scenarios (2-4) for the purpose of illustrating future variants (team of scenario authors). 5. Convincing presentation of the facts to leading managers (team of scenario authors). 6. Work with managers on conceptual management and investment decisions for each scenario (team of scenario authors + target audience).
Presentation of philosophy	Exercise and cooperation for the preparation of specific abnormal situations.	Exercise and cooperation aimed to prepare for future large uncertainty.
Presentation of objectives	Improvement of activities during a disaster or emergency situation.	Improved decision-making in policy and strategy.
Common objectives	Facing the unexpected.	Test of assumptions and organizational readiness.

The scenarios are applied in risk management, e.g. Processing Model Framework for logical model of risk management in the territory is according to [3] as follows: description of the process; defining the objectives (criteria for measuring goals, verification, hierarchy and priority objectives); generating the system structure (in a simple directed graph format, including features and links); determination of critical points of the process; defining the parameters of critical points; determining the relative importance (weight) of each parameter; aggregation of survey results and allowed simplification; interpretation of results and acceptable risk of decision-making process; definition of countermeasures in the form of response scenarios to disasters in variants; and generating the response management scenarios for the superior version, which was evaluated (selected) for the realization as socially most advantageous.

Most of these tasks is managed by standard methods of operational analysis and systems engineering, i.e. by: screening the potential risks in the territory; generating the criteria to security and sustainable development; modelling the integral risk; risk management model; catalogue of criteria; methodical processing of results of initial screening; acceptability of risk; and application of the precautionary principle.

When screening potential risks in the territory, the rating algorithm is happening in the background of a conceptual scheme for sustainable development. The system concept determines the basic paradigm, which reflects the gradual steps for the systematic risk analysis of the system, see diagrams from theoretical modelling the integral risk [3].

Development of scenarios suitable for practice requires the databases available for the respective problem and a multidisciplinary team of experts, application of suitable team expert method such as brainstorming, Delphi, panel discussion etc. From the perspective of protection of it is necessary to handle both optimistic and pessimistic scenarios, as, e.g., the conclusions drawn from work [6].

5. Process models

Management is a type of human activity that establishes and ensures the system functions. For management support there are at present used the process models and project models. Main meaning the process model is to depict the possible development tendencies as a consequence of certain phenomenon, pertinently to demark functions and role of functions, i.e. according to purpose they are separated into several types. The process models enable to compile procedures and scenarios for certain situations that have certain similar features. They are suitable for planning, response and renovation**.** We present the risk management model that has been used at present in professional practice, two simple models from daily practice and evaluation of process models for crisis management.

5.1. Selected tools supporting the management

The management is a type of human activity that establishes and ensures the given system functions. It is conscious way of application of theoretical and practical knowledge of top manager directed to identification and diagnose of problems and targets in a given system, matters of defeating the problems, determination of procedures for required targets reaching and on implementation of procedures connected with supervisory mechanisms directed to the aim in order that required targets might be optimally reached. The tasks are reliable to diagnose each problem, to decide rationally, to realise decision-making in given real conditions.

It is evident that the management is only successful if it is based on professional knowledge and on experiences. To obtain required knowledge and experiences we must in permanent way collect, process and verify data, perform qualified assessment that can only be done by qualified and experienced specialists. The fulfilment of these demands is possible to ensure on the top level, i.e. on the government level. Therefore, in developed countries there are different organisational structures, dependent on the government

administration organisation that monitor safety, disasters etc. and prepared grounds for decision making and strategic development of land.

The management consists of individual decision makings. Deciding process is logically connected useful sequence of steps of decision maker starting from problem identification up to decision making formulation. It consists of the following steps:

- assembling and processing the information with respect to fact that processing must be adequate to problem that is followed (e.g. it means that data processing methods for needs of safety management must respect that big disasters with devastative impacts occur rarely, and therefore, the procedures respecting the great

numbers law, i.e. algorithms based on extreme or marginal estimations must be used,

- recognition of solution variants,
- searching for optimal problem solution,
- own decision making.

In order that the decision making might be objective and qualified it is necessary:

- to have a sufficient number of information, its objective processing and cognition of suitable reactions,
- permanent reaction to an access of new findings,
- to understand solved problems in connection to their vicinity and in their internal structure,
- to combine the suitable knowledge, experiences and new information in order that practical way of problem solution might be obtained,
- credible data assessment.

At decision making it is necessary to consider:

- judgement of present conditions and present decision makings from the viewpoint of a future development,
- qualitative factors and strategies of different participants,
- fact that the future is multidimensional and indefinite,
- fact that each system must be investigated by both, the globally one and the systemic one,
- fact that information and strategies are not neutral but tendentious,
- more approaches that complete each other,
- fact that there are prejudices against strategies and humans and to prohibit them.

Decision making in benefit of matter decided must be objective and qualified. From the viewpoint of knowledge on problem that might be decided in systemic concept we divide the decision makings on:

- standard at which all is known and there are also known standard procedures of solution,
- well-structured at which there is a clear and quantitatively described structure of problem in systemic concept and at which the optimizing methods may be used,
- weekly structured, i.e. at several elements of structure of judged system there are not only uncertainties but also unclearness. For their putting under control there must be used methods of system analysis that join exact mathematical methods with normalised quantitative considerations (i.e. heuristic methods). Decision making heuristic methods are methods of decision-making analysis that are usually divided in:
    - decision making tree (process model),

- decision making matrix.

  It means that for decision making support there are processed either the process models or the decision-making matrixes. Assessment of process models are often performed by the Delphi method [20] and the assessment of decision-making matrixes is performed by way described in appropriate handbooks , e.g. [6],

- non-structured, i.e. at many elements, links and flows of judged system there are unclearness. Possibility for their solution only gives the expert methods. Expert methods simulate intellectual procedures of specialists. They lean on scenario of process in which decision maker is directed to gradually solution of partial problems of decision making in certain logic procedure of considerations and activities connected with generation and assessment of different variants of solution of a given problem. Expert systems are diagnosed and generative (designing) [6]. For decision making support there are processed case studies [6] that use qualitative data by way that enables to obtain idea on frequent solution of problem in certain context determined by given conditions in evaluated system and in its vicinity.

At selection of methods of decision making it is necessary to respect the nature of solved problem, determined aims of solution, criteria for solution and possibilities of collecting the necessary input information. I.e. in a domain of land safety management, it is necessary to respect that the majority of problems is connected with uncertainties and unclearness, that are induced by fact that the human system has been continuously developing in permanently changing outer medium, and that for fulfilment of safety management targets there is necessary the choice of good strategy for ensuring the human system security and sustainable development.

A strategy is a set of rules for decision making under conditions of uncertainties and unclearness. The development of strategic management accompanied by formation of effective tools started in the second half of 20 century, when there were processed methods of operating analysis based on the creation and assessment of variants of possible evolutionary tendencies of system. In 70s there was worked out the process approach on which in 80s there was linked the systemic approach that represented net interface and complex view on a given reality.

For creation of variants / alternatives of processes there are today used methods based either on the estimation or on the mathematic modelling. At selection of methods for decision making there are necessary to respect the nature of solved problem, determined aims of solution, solution criteria and possibilities of collection of necessary input information. To the first group of methods there are belonged the method of analogy, brainstorming, brain writing, panel discussion, Delphi method, Gordon methods (technique of creative thinking), application of fuzzy sets, application of fractals [6]. Methods based on mathematical modelling go out from the time series processing. Excessive exactitude at construction of exact models often leads to overestimation of theoretical viewpoints and to non-respecting the real needs and possibilities of future users. Pragmatic approach, leaning on analysis of real situation and on creation of a model suitable just for it, is dependent on methodology of model compilation – objectivity, non-prejudice and comprehensiveness of data, capabilities and competence of professionals.

In solved case there is always effort to separate problem into a whole hierarchy of sub problems of different orders, i.e. structuring the problem. Problem structuring has two dimensions, namely the problem decomposition and the level of abstraction of problem representation. According to specialised literature (e.g. [4]) there are only solved the problems that are under control of decision maker.

For management support there are at present processed the process models and the project models [4]. Main meaning the process model is to depict possible development tendencies as a consequence of certain phenomenon, pertinently to demark functions and role of functions, i.e. according to purpose they are separated into several types. The application of process model is suitable for repeated activities that can be separated and consecutively described. The typical case is the production enterprise with a serial production. The application of project approach is conversely suitable for unique projects, e.g. big buildings, software development etc. Individual projects allocate in life cycle own and external sources according to momentary need. The project approach has always higher uncertainty and is worse described by tree model [4].

5.2. Process models and their relation to management

The fundament for process management there is the creation of process models. Modelling is a specific sort of cognition of reality that is around us. It is creation of analogy of original of reality attending to its cognition or verification. It is efficiency activity that we have been using in the case of complex process / activity / object etc., when we want to investigate only certain matters, i.e. the existing reality is simplified or sometimes only reduced or magnified. During the modelling we create the model of identified reality (mathematical, thought, oral, graphical, physical (imitation)) for defined purpose, that at keeping the basic principles for model creation (following from condition of isomorphic or homomorphism representation) may give great evidence capability that is only valid in the extent of reality for each the model was created. Mathematical and physical models come from analogies among physical quantities. The model compiled according to principles for physical model has with object the same physical nature. The model compiled according to principles for mathematical model has the different nature but its function is perceived by set of equation that is identical with set of equations describing the followed items of original.

Mathematical models we can classify according to the different viewpoints. According to the character of parameters and deciding variables [3] the models are classified into:

1. Deterministic models, i.e. models in which all parameters are fixed deterministic values and in which there are only deterministic quantities and relations. I.e. they are not allowed nor uncertainties and nor unclearness.
2. Stochastic models, i.e. such models in which there is occurred at least one parameter that is a random quantity and at which there are not unclearness (i.e. deviations from reality connected with blunder error at collection or at interpretation of data, measurement or with lack of data or with non-linearity of process or with intentional or non-intentional neglecting sure actions or events). It means than at least one deciding variable in model is a random quantity. Uncertainties connected with this random quantity (or with these random quantities) may be assessed by methods of mathematic statistics. I.e. probability distribution of random variables in model is

known (in practice this distribution is deduced either from logic – theoretical considerations or by methods by mathematical statistics or by expert methods).

3. Models with unclearness we sometimes call strategic, i.e. such models at which there is at least one quantity that is random quantity but its distribution (on contrary to stochastic models) is not known and cannot be determined by logic – theoretical considerations or by methods by mathematical statistics (usually owing to low number of events) or by expert methods. We usually say that at these models we only know bottom and top limits of these quantities.

The modelling is one of the methods by which we solve tasks of practice if there are known inputs and outputs. Terminologically, clean-out models are e.g. the models: fuzzy multi-criteria; conceptual or qualitative; quantitative; dynamic and simulative; and ecological effectiveness.

Chosen typology of continuous discrete decision models leads to separation into two basic groups, namely multi criteria discrete models and multipurpose continuous optimising models. The other possible differentiation is according to so called degree or "softness" or "hardness", i.e. according to completeness and accuracy of input information. In this direction there are distinguished models of certain softness type (SOFT) and certain hardness type (HARD).

Process models belong to category of qualitative models on background of process analysis and graphical representation. During the 90s of last century there have been developed many different technologies. The most popular methods there were the OMT (Rumbaugh), the OOAD (Booch) and the OOSE (Jacobson). Each of these methods had own value and accent. The OMT emphasizes analysis, the OOAD proposal and the OOSE behaviour analysis. During the time the methodologies have been converged, however, they have been own symbols. Using the different symbols caused the problems on a market because one symbol meant different things for different people. This war of methods was terminated by origination the UML (Unified Modelling Language) that represents the unification of notations of Booche, Rumbaugh and object symbols of many others. At unification of symbols used by this object-oriented method, the UML, is a fundament / standard in domain of object-oriented analyses and of proposals based on experiences of professionals [21].

Process model supported by qualitative tool enables to describe actual conditions, to propose new processes or to optimise existing processes, to reveal unnecessary or inefficient processes, to simulate and to evaluate possible impacts of changes before their implementation. Process models are from the viewpoint of formalised process analysis the high sophisticated tools in which pure graphic representation may be misguided and it may mean unacceptable simplification of judged system.

Each process is a sequence of phenomena or activities in space and time in which we can distinguish inputs and outputs. Inside of each process there are usually parallel but distinct sub processes. Each of sub processes is bounded up to certain element in space or with certain group of elements in process under account. The process model is a representation of certain process directed to a certain target. Because targets are not same in practice there are several process models to one process.

The process models enable to compile procedures and scenarios for certain situations that have certain similar features. There are suitable for planning, response and

renovation. They are constructed according to real needs. Demand of each application of certain process model is the fulfilment of assumptions for a model construction. In other case no correct result is guaranteed. Results of process model application are the norms, standards, security, emergency, accident, crisis, continuity and other plans, disaster scenarios, response scenarios, renovation scenarios etc.

In management domain, namely in the planning there is possible for certain, strictly limited type activities to use the process models reflecting the reality type. With regard to above given theory each process model must be tested whether a given reality corresponds to model assumptions. If yes, it is possible to use this model and vice versa. With regard to the multiplicity and variety of reality it is not sufficed to use only deterministic and stochastic models but in the case of higher demands on accuracy there is necessary to apply models with unclearness in which unclearness are eliminated by expert methods or by case study methodology [6].

Just the domain of security, emergency, accident and crisis planning are the domains in which there is necessary to consider the origination of unforeseeable phenomena (human error at decision making, lack of necessary sources of all kinds, occurrence of low expected meteorological conditions, unusual combination of phenomena etc.), it is the domain in which there is necessary to use the process models based on models with unclearness because the use of:

- deterministic models that are conservative, i.e. that are for the most unfavourable conditions, is very expensive,
- stochastic models do not perceive possible situations because it is too simplified.

Also, there is come the experience from practice that a complex process model is low suitable then the set of partial process models applied in series, when after each application of partial model there is performed comparison with reality using the data from the safety monitoring and prospective correction of activities or application of corrective measures if disagreement with management purposes is found.

Process models based on deterministic approach have been used at sitting, designing, building and processing the technologies and objects because they ensure the highest level of safety with regard to present knowledge and experiences.

Process models based on stochastic approach have been most often used at inspection activities and at routine management of safety of certain processes or objects.

References

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

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

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

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

[5] ESRA. *Reliability, Risk and Safety: Theory and Applications.* ISBN 978-0-415-55509. Leiden: CRC Press / Balkema 2009, 2367 p.

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

[7] CHISA. *Prevention/Process Safety/Risk Assessment Methodology.* Pratur: CHISA 2002.

[8] EU. *The FOCUS Project - Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles*. Proposal: No.261633, topic SEC-2010.6.3-2. Brussels: EU 2011-13.

[9] PROCHÁZKOVÁ, D. *Archive of FOCUS Project*. Praha: ČVUT 2011-13.

[10] PROCHÁZKOVÁ, D. *Final CVUT Report to WP2 FOCUS.* Praha: ČVUT Archives 2011, 381p. *[It contains lists of publications in which appropriate methods were derived and used for problem solving and cases of events on which these methods were tested by author and experts for security and safety domain – these data are in the CVUT archives].*

[11] PROCHÁZKOVÁ, D. *Procedures and Methodologies of Engineering Disciplines Directed to Safety* (in Czech). ISBN 978-80-7385-111-8. Ostrava: SPBI 2012, 2 parts – book – 176p. + CD ROM – 164p.

[12] http://www.riskworld.com

[13] PROCHÁZKOVÁ, D. Tool for Compilation of Grounds for safety Management (in Czech). In: Bezpečnost a ochrana zdraví při práci 2011. ISBN 978-80-248-2424-6. Ostrava: VŠB-TU 2011, pp 157-169.

[14] PROCHÁZKOVÁ, D. *Security Planning (Land-use, Emergency and Crisis Planning)* (in Czech). ISBN 978-80-86708-80-5. České Budějovice: VŠERS 2009, 200p.

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

[16] LLOYD'S. *Realistic Disaster Scenario*. www.lloyds.com

[17] ALEXANDER, D. Scenario Methodology for Teaching Principles of Emergency Management. *Disaster Prevention and Management*, 9 (2000) 2, pp. 89 – 97.

[18] BORELL, M., ERIKSSON, K. *Learning for Safety - Improving Effectiveness of Scenario-Based Exercises.* http://www.lucram.lu.se/upload/ LUCRA M /Learning ForSafety.pdf

[19] PROCHÁZKOVÁ, D., ŘÍHA, J. Scenarios of Selected Disasters (in Czech). In: *Ochrana obyvatelstva – nebezpečné látky 2012***.** ISBN 978-80-7385-109-5, ISSN 1803-7372. Ostrava: SPBI 2012, pp. 153-157.

[20] COPPERSMITH, K. J., YOUNGS, R. R. Probabilistic Seismic - Hazard Analysis Using Expert Opinion; An Example from the Pacific Northwest. In: Krinitzsky E. L., Slemmons D. B., eds - *Neotectonics in Earthquake Evaluation.* Boulder: Am. Geol. Soc. 1990, pp. 29-46.

[21] JACOBSON, I., BOOCH, G., RUMBAUGH, J. *The Unified Software Development Process.*

ANNEX 3 – DESCRIPTION OF TYPES OF RISK MANAGEMENT AND RISK ENGINEERING

Type	Concepts of work with risks - characteristics, targets and procedures
Classical risk management / engineering	Object is a closed system. Risk sources are internal technological phenomena in system. The target is to reduce the technological risks of a system to a certain level, given by standards and norms. It originated in 30s of last century. The risk is determined after the design of the system, and therefore, there is no possibility to reduce risks connected with an inappropriate solution for a given site and system. The reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones.
Classical risk management / engineering considering the human factor	Object is a closed system. Risk sources are internal technological phenomena and human factor in system. The target is to reduce: the technological risks of a system to a certain level given by standards and norms; and risks connected with a human factor by safety instructions for danger works. It originated at the end of 70s of last century. The risk is determined after the design of the system, and therefore, for reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones.
System security management / engineering	Object is an open system. Risk sources are external and internal phenomena including the human factor. The target is to reduce risks for a system: from external and internal phenomena, a human factor, and also failures of decision-makings at risk management / engineering were to a certain level given by standards and norms; i.e. to ensure the security of a system and its assets. No interest on system vicinity. IT originated at the first half of 80s of last century. The protection of system vicinity is not solved. Unacceptable impacts on vicinity can be only mitigated by special off-site emergency plans, i.e. by organisational measures and activities if government enforces such legislation.
System safety management / engineering	Object is an open system. Risk sources are given by all hazards approach. The target is to ensure the security of a system and its assets and the security of system vicinity. The advanced safety engineering uses at risk determination the following principles: risk is

	determined during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition; the risk determination is directed to user's demands and to the level of provided services; risk is determined according to the criticality of impacts on processes, provided services and on assets that are determined by public interest; and unacceptable risks are mitigated by tool for risk management, i.e. according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up. It originated at the second half of 80s of last century. The target is the safety, i.e. it is also necessary to trade-off with risks having low occurrence frequency if their impacts are unacceptable, and i.e. precaution principle is applied. The set of standards and norms exist especially for nuclear and chemical domain. To prepare groundwork, it is necessary to combine analytical methods with expert judgement by which we remove vagueness (epistemic uncertainties) in data. Except of technical measures respecting the precaution principle, special technical problems solution there are continuity plans containing the procedures for overcoming the critical conditions in system and system vicinity, emergency plans and crisis plans. The risk management viewpoint by these characters: sitting – designing – construction – project with risk reduction; operation with the integration of early warning systems and of procedures for the management of the acceptable level of risks; and defeating the abnormal, emergency and critical conditions at the operation and at putting out of the operation.
System of systems safety management / engineering	Object is an open system of systems. The target is to ensure: the security of both, the system of systems including its assets and the system of systems vicinity; and the co-existence of individual systems creating the system of systems. Risk sources are given by all hazards approach and by interdependences among the partial systems and by those with vicinity. Formation at the beginning of third millennium. The set of standards and norms are under discussion and preparation.

ANNEX 4 – DESCRIPTION OF TECHNICAL FACILITY SAFETY BUILDING

On the basis of present knowledge, the technical (correctly socio-cyber-technical) facilities are open systems of systems, i.e. the sets of mutually interconnected open systems [1-3]. Each of these systems is made up from elements and interconnections among elements; the interconnections are set up by linkages among elements and by flows of different nature (material, energy, information, finance etc.) among elements.

The human, as a system developer, ensures that socio-cyber-technical system fulfils given tasks (it produces commodities or it furnishes a service) by using the logical linkages and the couplings set up by flows. Apart from the required interconnections, there can occur under certain circumstances the unacceptable interconnections, which lead to a lesser or higher damage of system. Such system damages cause that the system does not fulfil tasks and furthermore it endangers itself and its vicinity. Therefore, at present the technical facilities are made up as secured or safe systems.

On the basis of works [1-3], the safe system is constructed as the system that is ensured against all internal and external disasters including the human factor, i.e. to all harmful events and so that at its critical conditions it may not endanger itself and its vicinity (i.e. the place in which people live). It means that the safety is the system property, which is put above the system dependability. Therefore, the parameters which determine the system quality are arranged into the following order:

- ***safety***, i.e. the system capability to precede the critical system conditions (active safety uses the elements of control; passive safety uses the elements of protection) and even at its critical conditions does not endanger its vicinity,
- ***dependability***, i.e. the system capability to provide the required functions under the given conditions in the given quality and in the given time interval,
- ***availability***, i.e. the system capability to provide the required functions at the occurrence of process that uses the given function,
- ***integrity***, i.e. the system capability to provide the time correct and valid report on system faults,
- ***continuity***, i.e. the system capability to provide the required functions without disruption at the process initiation,
- ***accuracy***, i.e. the system capability to ensure the required system behaviour in the required range.

At the complex socio-cyber-technical systems that have the form “systems of systems” the other parameter of quality is supplemented, namely the interoperability as the interconnected systems capability to carry out the required tasks in required quality correctly and in-time in a given place and time.

As was said above, the safety is a set of measures, which are performed by human with goal to ensure the safe system, i.e. also the system security and human security in dynamically variable conditions of present world [1-3]. Origination and operation of the safe system is substantially more exigent on knowledge, sources, forces and

means, and therefore, in current practice the secured systems are mostly used. If needed, these secured systems are replenished by the organizational measures, which ensure the protection of public assets, when these systems endanger themselves and their vicinity [1-3].

The secured system is understood as the system that is secured against all internal and external disasters including the human factor, i.e. to all harmful phenomena. In comparison with the safe system, the secured system can endanger itself and its vicinity under its critical conditions. With regard to human security, it can only be operated under certain conditions – so called limits and conditions [1-3].

As it is mentioned above, the secured systems involve commonly used technical systems, which can damage themselves and their vicinities under certain conditions. From this reason we follow their special property, i.e. the ***criticality***. This quantity is consistently related to size of impacts of function losses of system or system of systems targeted to fulfilment of certain goals for society [1-3]. According to these works, the determination of criticality in the territory of serviceability goes out from: the possible disasters´ hazard analyses; consideration of territory and system vulnerabilities; and from consideration of mutual interconnections among partial systems in the territory, i.e. vulnerabilities of whole system of systems. At criticality determination they are considered the following assets: public; technical system; territory; and the State, and the following questions:

1. How does the facility react to certain types of disasters?
2. How is the facility robust, resilient and rubbery?
3. How the behaviour of facility can be improved?
4. What management mechanisms in the sense of control are suitable?
5. What rules can be used for the self-regulatory or tolerable deflections?
6. Which parts of facility are critical?

For ensuring the safety, including the functionality, dependability and stability of facility, it is necessary to know certain threshold – the criticality, which determines the conditions at which the system of systems focused on certain targets´ fulfilment, does not ensure expected functions in a required time, in a required site, and in a required quality. Therefore, with regard to results of analyses of: important and dangerous faults and failures; losses and damages caused by system malfunctions; external disasters´ impacts; failures of mitigating measures; reactions of substances in a given facility; leakage or discharge of substances (pipelines) etc., the limits and conditions of facility or infrastructure are determined [1-3].

Limits and conditions are tools for safety management of these technical facilities. Their observance ensures the safe operation of technical facility. They are the set of positively defined conditions, for which it is proven that the technological facility operation is safe. The appropriated set includes data on permissible parameters, requirements on operation capability, setting the protection systems, demands on the workers´ activities and on the organizational measures leading to the fulfilment of all defined requirements for design operation conditions [1-3].

For ensuring the safety, i.e. also the reliability and the functionality, the control system of given technical facility needs to keep the determined physical quantities (parameters of appropriate subsystems) on values determined in advance. During the process of regulation, the control system changes the conditions of individual controlled systems by bearing upon the efficient quantities, with aim to reach the required condition of whole system. In terms of integral safety [1-3], the following properties of control system are pursued in the order:

- level of observance of established operation conditions and prevention of damaging (unacceptable) impacts on the system itself and its vicinity,
- functionality (level of satisfaction of required tasks),
- operability, i.e. level of fulfilment of required tasks at normal, abnormal and critical conditions,
- operation stability, i.e. level of observance of established conditions during the time,
- inherently included resilience to possible disasters.

From above mentioned facts it follows that management and control systems determine quality and performance of systems. They have decisive influence on safety, and therefore, their following factors are considered: responsible autonomy; adaptability; integrity; and meaningfulness of tasks. Because the human behaviour is not deterministic, the main characteristics of considered systems are: the emerged properties; non-determinist behaviour; and complex relations among the organizational targets. People, maintenance, renewal and changes decide about each followed system. From the engineering viewpoint the followed systems are characterized by structure, hardware, procedures, surround, information flows, organization (problem of organizational accidents) and interconnections among the mentioned items [1-3].

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

[3] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Results of Inspections of Risk Management Quality in Facilities of Critical Infrastructure. *International Journal of Mechanical Engineering*. ISSN 2367-8968. www.iaras.org/iaras/journals/ijme

Titul:	Risk Management at Technical Facilities Type and Site Selection
Autorský kolektiv:	Doc. RNDr. Dana Procházková, DrSc., RNDr. Jan Procházka, Ph.D.
Recenzenti:	Prof. RNDr. Šárka Mayerová, Ph.D. Doc. Ing. Alena Oulehlová, Ph.D.
Vydavatel:	DSPACE ČVUT v Praze
Forma vydání	Open Access
Počet stránek:	172
Rok vydání:	2020

ISBN 978-80-01-06714-7