METES
Motivation - Education - Trust - Environment - Safety 2017
Recenzovaný zborník z medzinárodnej vedeckej konferencie, 3.máj 2017, Bratislava
Proceedings of the International Conference, Bratislava, May 3, 2017
Žilina: Strix et SSŽP. Edition ESE-34, ISBN 978-80-89753-19-2

SUPER PROCESSES FOR MANAGEMENT OF RISKS IN TERRITORY AND IN TECHNOLOGICAL FACILITIES

Dana PROCHÁZKOVÁ

SUPER PROCESY PRO ŘÍZENÍ RIZIK V ÚZEMÍ A V TECHNOLOGICKÝCH ZAŘÍZENÍCH

METES
Motivation - Education - Trust - Environment - Safety 2017

ABSTRACT
ON THE BASIS OF PRESENT KNOWLEDGE, THE WORLD AND EACH ITS ENTITY (NATURAL, SOCIAL AND TECHNOLOGICAL) MAKES UP THE SET OF OPEN AND MUTUALLY INTERCONNECTED SYSTEMS. IN THESE SYSTEMS THE PROCESSES ARE UNDER WAY THAT MAKE UP THE GROUND OF DYNAMIC DEVELOPMENT BOTH, THE INDIVIDUAL SYSTEMS AND THE COMPLEXES. WITH THESE PROCESSES IT IS CONNECTED THE OCCURRENCE OF PHENOMENA THAT HARMED HUMANS AND ENVIRONS IN WHICH THE HUMANS LIVE. FROM THIS REASON THE HUMANS HAVE BEEN TRYING TO COMPREHEND HARMFUL PHENOMENA, TO DISCOVER THEIR CAUSES AND LATER ALSO TO MANAGE THE RISKS CONNECTED WITH THEM. PRESENT TRIED-AND-TRUE MANAGEMENT IS BASED ON MANAGEMENT OF PROCESSES, AND THEREFORE, THE TARGET OF PRESENT PAPER IS TO DETERMINE THE SUPER PROCESSES FOR MANAGEMENT OF RISKS IN TERRITORY AND IN TECHNOLOGICAL ENTITIES DIRECTED TO HUMAN SECURITY AND DEVELOPMENT. TO THIS PURPOSE IT IS PERFORMED THE SYNTHESIS OF VERIFIED KNOWLEDGE AND EXPERIENCES FROM WORK WITH RISKS. ON THE BASIS OF EXPERIENCES FROM PROFESSIONAL INSPECTIONS AND FROM ANALYSES OF ACCIDENTS AND FAILURES OF TECHNOLOGICAL ENTITIES THERE ARE GIVEN THE MOST FREQUENT CAUSES OF ORGANIZATIONAL ACCIDENTS, I.E. BAD APPLICATIONS OF ONE OR MORE PROCESSES THAT BELONG TO FOLLOWED SUPER PROCESSES.

KEY WORDS: *security, development, safety, risk, risk management, process, super process, process management, territory, technological (socio-technological) entity (object or network).*

ABSTRAKT
PŘEDLOŽENÝ ČLÁNEK SHRNUJE ZÁKLADNÍ POZNATKY O PRÁCI S RIZIKY Z POHLEDU POŽADAVKŮ NA TECHNOLOGICKÁ ZAŘÍZENÍ, KTERÝMI SE ZAJIŠŤUJE PRO LIDI BEZPEČNÝ SVĚT S POTENCIÁLEM ROZVOJE. VELKÁ TECHNOLOGICKÁ DÍLA JSOU VÍC NEŽ JEN MNOŽINA TECHNICKÝCH ČÁSTÍ ZAŘÍZENÍ A SOUČÁSTEK; JDE O SOUBOR VZÁJEMNĚ PROPOJENÝCH OTEVŘENÝCH SYSTÉMŮ (TZV. SYSTÉM SYSTÉMŮ – SOS), KTERÝ SE NACHÁZÍ V DYNAMICKY PROMĚNNÉM SVĚTĚ. JEJICH POŽADOVANÉ CHARAKTERISTICKÉ RYSY JSOU: VELKÝ ROZMĚR; VELKÝ VÝKON; POUŽITÍ VÍCE TECHNOLOGIÍ; SLOŽENÍ SE Z NĚKOLIKA AUTONOMNÍCH ČÁSTÍ, KTERÉ MOHOU PRACOVAT SAMOSTATNĚ A BÝT VYVÍJENY NEZÁVISLE; VYSOKÁ BEZPEČNOST, TJ. FUNKČNOST A SPOLEHLIVOST I NÍZKÉ OHROŽENÍ CHRÁNĚNÝCH AKTIV VLASTNÍCH I VEŘEJNÝCH, A TO ZA PODMÍNEK NORMÁLNÍCH, ABNORMÁLNÍCH I KRITICKÝCH. V DANÉ SOUVISLOSTI ROZLIŠUJEME ***ZABEZPEČENÝ SYSTÉM****(SYSTÉM OCHRÁNĚNÝ PŘED VŠEMI RIZIKY) A* ***BEZPEČNÝ SYSTÉM*** *(SYSTÉM, KTERÝ JE ZABEZPEČENÝ A PŘI SVÝCH KRITICKÝCH PODMÍNKÁCH NEOHROŽUJE SEBE, ANI SVÉ OKOLÍ).*

KLÍČOVÁ SLOVA:*bezpečí, rozvoj, bezpečnost, riziko, řízení rizik, proces, super proces, řízení procesu, území, technologická (sociálně – technologická) entita (objekt nebo sí´t),*

1. INTRODUCTION

The main goal of all human effort is ensuring the human life, i.e. all human needs, interests, and wishes. Human needs, interests and wishes are fulfilled by intangible and material goods that have a utility value. Unfortunately, in the world it is not just a human society, but also other systems, which are not subordinated to the human society. Therefore, the conflicts originate: human vs. the environment; technology vs. the environment; human vs. technology; human vs. human, human vs. PC etc. Because the human kind is based on its education, as well as in the present case, it needs to realize that, in a given situation it needs to be based on knowledge, which have been accumulated by science and historical experience of life, which shows that it is a limit for the human activities, which could not be exceeded, in order to prevent the destruction of mankind.

Christianity and Eastern philosophies perceived rightly that the human basic problem is the answer to question: „How to live?" The question connected with the existence of human in today's civilization runs: „How is human going to exist?" It is necessary to state that, for example,***in minds of humans the relation between human and human society towards the nature still means the domination and exploiting of natural resources for the sake of satisfaction in their needs***. But from the view of knowledge and experiences it is necessary for the humans to realize that they are not the rulers of the Universe and they should, by their status, participate on securing the existential conditions for both, themselves and the future generations, which requires certain behaviour and certain responsibility for their manners and activities.

The strategy of sustainable development is comparable to other systems of values, which do not have a terminal form (e.g. the system of human laws and freedom). It is heading towards the securing the highest possible quality of life for the present generation and towards the creation of preconditions for quality life of following generations and with being conscious of fact that ideas of future generations concerning the quality of life can be different from ours.

From this reason the UN defined the strategic goal for human society *"safe human system"* in 1994 [1], consecutively the EU defined *"safe community"* in 2004 [2]. The present knowledge [3] shows that it is necessary to care on both, the public assets (human lives, health and security; property and welfare; environment; critical infrastructures and technologies) and their interfaces that are realised by natural and by human made linkages and couplings by help of various flows. Precisely, the interfaces among assets are the causes of permanent increase of vulnerability of present world, and therefore, today the management of entities in the world is based on the system concept [3-5].

The present world we understand as the set of open mutually interconnected systems that dynamically develop in time (the system of systems). Its foundation stones are: the environment; the human society; and the technological system [3, 4]. These principal systems and another systems and their sub-systems have own targets that they realise by help of internal processes. It is reality that all results of some of these processes are not positive for the humans, and therefore, we denoted them as disasters [3, 4].

Owing to existence of such phenomena, the humans need to try to create the favourable conditions for life. From the logical reasons, the humans need to direct their protection against phenomena that have the huge impacts on them and also on the assets that they need for the life. In this context the term "risk" is used and it is defined as the rate of probable size of disaster impacts on humans, namely directly or indirectly through the public assets on which the humans are dependent [4].

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 riskis now thedominate concept of our society.*** It is connected with complex phenomena, conditions or factors: uncertain natural hazards, technological accidents and other disasters [3]; 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 also with the human play with fear, chances and opportunities [3-5].

For quality human life it is necessary both, the co-existence of mentioned essential systems and the provision of humans needs that in hierarchical Maslow pyramid [6] (needs: physiological, security; social; sociable assertiveness, self-realization).

From this reason, the humans need to consider at management: the system interconnection 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: technical; operative (functional); tactic; strategic; and politic. For general aims´ reach, the goals on all levels need to be targeted in same direction and to be co-ordinated [3-5]. 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 [3, 5].

Basic tools of human society for provision of needs there are: correct control of human society (from urgency reason, the problem solving is divided in [3] to: management of security and development; emergency management; crisis management); and good asserting the knowledge and exercises at negotiation with risks directed to public interest respecting [4, 5]. 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 [4].

2. SUMMARY OF FINDINGS ON ADVANCED MANAGEMENT, PROCESSES AND THEIR RISKS

As it was said above, the world is dynamically developed in time and space that is manifested by different processes that are inside and across of its structural systems. The different phenomena, having the various sizes, are the products of these processes. These phenomena cause the changes that have often highly unacceptable impacts on humans, namely directly or indirectly over the public assets that humans need for quality life and development. This reality causes that the accent is put on the management type called "disaster management" in which considering all disasters is denoted as „All Hazards Approach "[7].

2.1. Disasters as processes outputs

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

- running in and out of the Earth are: *natural disasters* (earthquake, floods, drought, strong wind, volcanic activity, land slide, rock slide etc.); *epiphyte; epizootic; land erosion; desertification; fundament liquefaction; sea floor spreading etc*.
- running in the human body and in human society are: *unintentional:* illnesses; epidemic; involuntary human errors etc.; and *intentional*: robbery; killing; victimization; religious and other intolerance; criminal acts; terrorist attacks; local and other armed conflicts, bullying; religious andotherintolerance; criminal actssuch as: vandalismand illegal business, robbery and attacking, illegalentry, unauthorized use of property or services, theft and fraud, intimidation and blackmail, sabotage andd estruction, intentional disuse of technologies, such as: improper application of CBRNE substances; data mining from social networks and othercyber 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: mutualimproper 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 intointolerant 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 [3, 8-10]. Generally, it stands that the disasters have certain characteristic features, which are the origin of impacts causing the damages, losses and harms to the important assets, links or flows and that from the human point of view, because this is de facto the only thing in which a human is interested (human aim is to make human to survive).

Among the impacts it belongs e.g. vibration; directed fast air, water or soil flow; damage to a stability and cohesiveness of rocks and soil; displacements of materials; outburst of liquids; anomalies in the temperature etc. The impacts effect directly or vicariously through links and flows of human system. Humans, thanks to their intellect, deliberately create the resilience of areas, buildings, infrastructures and technologies against disasters. They do with a help of both, the choice of elements, links and flows and their interconnection; and the specific preventive measures and activities until the specific disaster extent (which is given by human knowledge, abilities, financial and technical possibilities etc.) [3]. It makes why the impacts of interconnections in the system (interdependences) appear only with beyond design disasters, which by their extent lays above the border size of disaster against which the humans systematically provide resilience [3]. Understandably, there is a big difference - rich technically developed and quality managed countries or organizations (generally entities) have the threshold of assets resilience set higher that the counties with a lower standard.

Disasters cause or from certain extend cause damage, loss and harm on assets, i.e. they are the reasons of situations falling on a human and that is why human has to handle with them. By the reason of big variety of disasters, the arising situations classified as "the emergency situations" have either the same or highly specified impacts. The relation between a disaster and an emergency situation is the relation *"cause-consequence"* [3]. This relation is not simple because the intensity (destructiveness, severity, criticality, cruelty) of emergency situation in a given place is predetermined not only by the size of disaster but also by the local vulnerability of assets, failure of implemented protective systems (e.g. the system of warning in the area, security mechanism etc.) which were created for increasing the assets resilience, the humans' mistakes during the response etc. [3, 5, 8].

2.2. Danger, hazard and risk

In domain connected with the disaster management, there are three terms that are by given way interconnected. They are not often distinguished in spoken language, which leads to misunderstanding at critical moments, and by this to huge harms. In professional terminology they have exactly the given sense, and therefore, we here deal with them; it goes on terms: danger, hazard and risk.

Danger marks the conditions of human system at which the origin of harms on protected assets has the high probability (it is almost sure that the harm will origin) [4], i.e. the term marks the rate of conditions. It means that it goes on mark of possibility of origin of harm, loss or damage of one or more assets. The danger is predetermined by substance properties that are in facility, object or territory and by properties of processes that are running in facility, object or territory. It is immediate, if the course uncontrollably goes to the disaster origin that causes the emergency situation; and it is creeping, if the course goes to disaster origin inconspicuously and without clear-cut precursors [4]. The danger for human means both, the big phenomena (e.g. natural disasters, industrial accidents, environmental or social disasters) and the seemingly small phenomena from the daily life (slump of snow, icicle or roofing from roof, rough pavement etc.) [4].

Hazard marks the disaster potential to cause the harms, losses and damages on protected assets in a given site that is prescriptively determined. It goes on prescriptive measure of danger that is connected with the given disaster. For the strategic planning needs, the centennial disaster is often considered, i.e. the hazard is size of disaster that occurs once in hundred years, or professionally exactly, the disaster size that has return period 100 years; at special buildings and facilities it is considered from safety reasons the hazard, which is connected with thousand years' disaster or ten thousand years' disaster [4].

Risk connected with a given disaster is the probable size of damages, harms or losses on protected assets that originate in given place at origin of disaster with size of normatively determined hazard, which is normalized to the certain territory unit or number of individuals and the time unit [4]. The difference between risk and danger is the following: the danger is specific (it denotes the topical conditions) and the risk is only expected opportunity.

The humans ensure the protection of human society and populated territory against the risks by the way that for each disaster they determine the certain size (so called design disaster). They perform the preventive measures to design disasters and by which they ensure so the possible risk size may be acceptable. The problem arises if disasters with size greater than design disaster occur, because great damages, harms and losses origin as the consequence of failure of man-made technological systems [3-5, 10].

2.3. Process management and risk management

The entity (territory, object, plant, state etc.) governance has been developed during the history [3]. At the beginning of the 20th century, the methods of scientific management were introduced. After the Second World War, the start-up of development of impoverished countries was need, which meant to ensure the fast

recovery of businesses and areas. For this purpose, it was needed an initiative of wide inhabitant mass and more dynamic way of management. Therefore, the special management was introduced (this type has been still used for solving the critical situations). Its fundament is the management of processes; the process is mutual interconnection of partial sets of actions (mechanisms) by which the set of events is under way.

The mentioned management type presents the targeted management (programmes are split into projects which are further divided into processes; each process manifests itself under the project coordination – new types: project management; and process management). The characteristic feature of this management type [11] is the orientation on: the priorities and the use of planning; the methods of setting the goals; and the initiative of managers / leaders.

From the 70s of last century: it comes in useful the employee participation in the management, profit and ownership; and the demands on a qualification at all professions have been increasing. The beginning the 90s is characterised by: the wide usage of automate and office technics; the flexible manufacturing system; telecommunication and informatics.

Reforms in the public governance, i.e., marking by the transition from the bureaucracy management to the targeted management, i.e. the project management based on process management, were the response to the big problems in the EU regional policy, and they were being started-up by the Maastricht treaty in 1989 [12].

At present, the goal of project management of entities from both, the profit and the non-profit (public) sector, is ensuring the safe entities with sufficient development potential, and therefore, it is strategic, proactive and systemic [3]. However, it is necessary to consider that it is not possible to use the same criteria for the management of public and private sectors, because e.g. the human protection, the education and research need the investment without consideration of profit. The main differences between public and private sectors are:

- *A difference in goals*. In the public sector that is represented by municipalities and regions, the profit or another gain for any legal or physical person is not the main goal, but the main goal is the public interest and its procuration.
- *Legislation.* The public sector has a greater connection to justice, which leads to significant constraints in domain of decision making. It is caused by the need to respect and satisfy the duties and the principles of governance, to respect the elected bodies, the adjustment and the position of state organizational units, rights and duties of their employees, requirements on financial and property management, etc.
- *A profit absence at public sector has consequences* that some benchmarks and indicators, which are used in private sector for support of more quality management, are not possible to use.

For both mentioned sectors, however, it holds that it goes on the process management, on which all stakeholders are participated. The process management leans on the partnership, it is based on negotiation with risks and at the decision making it goes from the variant assessment on the basis of qualified criterion [12].

Currently, the three types of project management are used [3], i.e.:New Public Management; Total Quality Management (TQM); and Common Assessment Framework.In our conditions, the Total Quality Management (TQM) is used [3, 12]. For its success the ISO standards 9000, 14000 etc. had been set up. The TQM approach 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.

The 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 [3]. 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 taken into account the entity specifics, because all measures need to reflect the structure of entity from the reason of efficiency [3, 12]; it means they shall be site specific.

The modern management, which leans on the project and process management, uses the general process (Problem Solving Process) that is the part of best-practice (i.e., the best experiences) and it is worldwide used [13]. It goes on the process that is universal and it exceeds the problems of project and the project management; it involves ten points: problem identification; problem definition; analysis of present conditions; looking for causes; definition of target; proposal of solutions; solution selection; solution validation; realization; and evaluation.

In real practice, we distinguish three common management levels, which are needed to be harmonized. The strategic level determines the basic development directions, from which it follows: which processes are necessary to modify or create; which organizational changes are necessary to perform; and where to obtain

know-how, financial sources, etc. The tactical level helps to sort activities, which are necessary for realization of long-term intentions. It looks for answers on questions: how to set up the processes; in which condition to maintain processes; and how the processes need to cooperate mutually. The operational management decides about the real allocation of sources in the process (human, technological, financial) and also about the execution of appropriate activities in the range of adjusted processes (how to perform the real operation). An effort is to ensure the knowledge transfer and skill transfer among workers.

The organisation can reach a competitive merit when it harmonises all three management levels. The aim is to achieve the state when the processes are defined and managed on the basis of strategy and the operational management does not mean only response to emergency conditions or other types of faults. The processes are improved on the basis of knowledge coming from the operational management. New findings coming from the management processes are then quickly reflected into the strategy and they invoke the next important change connected with the business development or another entity development.

The process management is based on the principle of integration of activities into the integral processes. It means that the partial operations are necessary to integrate. The processes are controlled by process teams. Each process team controls the processes on its level and it distributes the tasks which lead to aim achievement to subordinate groups. At the same time all process´ teams shall be motivated to achievement of optimal outcomes, and all management levels shall follow the final goal at achieving the particular aims. Within the process management, two management systems exist, namely, the functional one and the process one, which create the more complex management.

Processes for safety support need to be followed in each entity [3, 5, and 16]. Modern management types, which are the project and process managements, are only successful, when they properly deal with risks, which are inherent to human system and also to each its sub-system. If the risks are not properly managed, so it will not be possible to reach successfully targets, and therefore, the project feasibility is assessed in advance. The importance of risk role is caused by the matter that on the risk mastering it is dependent not only the project price, but overall successfulness of total project. Thus, it is needed, so that each project may own specific structure, risk separation and way of financing that corresponds to its character. Risk management deals with the risks in process, which shall be a part of each project and that shall run from the very beginning, because only by this way it can respond to originated risks.

From the logic thinking it follows that the risks have various sources [3, 5, 8, and 16] and they depend on: disasters; local vulnerabilities; methods of management and coping with risks; and they occur on the side of all stakeholders. For achievement of understanding the stakeholders and following the risks´ reductions, it is necessary properly to work with risks, it means to choice the right concept for the risk management (five concepts exist in the risk context [5,16]); risk identification, risk analysis and evaluation [4], to correctly decide about risks and to perform the right risk allocation including the risks´ coping and the risks´ negotiation to stakeholders; to get over the risks; and to introduce the permanent monitoring, in which if necessary to apply the in advance prepared corrective measures [5].

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

- The risk assessment document – it contains information about the appropriate risks.
- The list of top risks – it contains the list of selected risks, the solution of which demand big claims on resources and time.
- 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.

3. DATA USED AT DETERMINATION OF SUPER PROCESSES FOR RISK MANAGEMENT IN DYNAMICALLY VARIABLE WORLD

For determination of supper processes for risk management in dynamically variable world we use data on both, the risks´ sources and the risk management procedures directed to human safety that are used in present practice.

In the first case, we use the detailed data on disasters and the results of studies of disasters that are in special projects, e.g. Switzerland - the PLANAT project, US – FEMA projects, Canada, the Netherlands, EMA (Australia), OCHA, the Czech Republic, IAEA, OECD, UN etc. – all real references (over 1000) are given in [3-5].

In the second case for some disasters (floods, earthquakes, chemical accidents, epizootic, epidemic, electro-energy net failure, industrial accidents, traffic accidents etc.), we use practical experience with tried-and-true tools for management and getting over the risks; e.g. the plans for risk reduction for more than 5000 accidents and failure of networks [9]. These data are in further paragraphs.

Because for practical purposes, there are necessary good technical solutions based on recent findings and experiences and correctly aimed governance of public assets supported by legislative with sufficient legal force, finances, qualified human personnel and material base, these data are also followed

3.1. Knowledge on risk, risk management and risk engineering

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 [3-5, 8, 9, 10, 14, and 15]. Their summary is:

1. The principles for work with risks 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.
2. The principles of work with risks 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.

   Because the territory and each technological objects or facility are the complex systems of systems (set of open and mutually interconnected systems of various nature [3, 5]), 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 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. Therefore, the entity integral risk also depends on the hazards from disasters of all kinds (natural, technological, social, financial, economical, 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, itis 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 thatin 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).

   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 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 technological 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 in Figure 1.

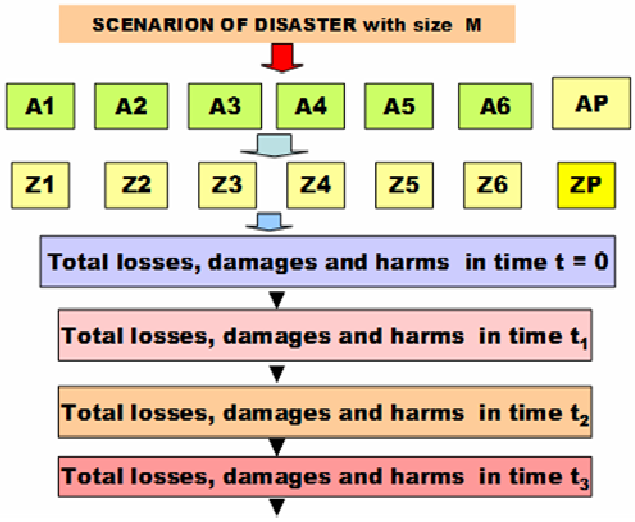


Fig. 1 - Flowchart for determining the risks for the strategic management of safety; A – assets and Z losses, damages and harms to the assets; Description: 1-the human lives and health, 2- human security, 3 - property, 4 - the public welfare, 5 - the environment, 6 - infrastructures and technologies,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

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.

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 - see the rules given in Figure 8 in chapter 1.

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, 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 technological objects and facilities; and the operational crisis plans for both, the complex technological objects and facilities and their vicinities.

3. Process model for work with risks is shown in Figure 2. 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 its security; to ensure safe system, i.e. to ensure security for system and its vicinity. The feedbacks are used in case if the monitoring shows that risk is unacceptable; firstly, it is used the cheapest feedback 1; in case of failure the feedback 2 etc.; at huge harms immediately it is used the feedback 4 that means the change of concept of work with risks.

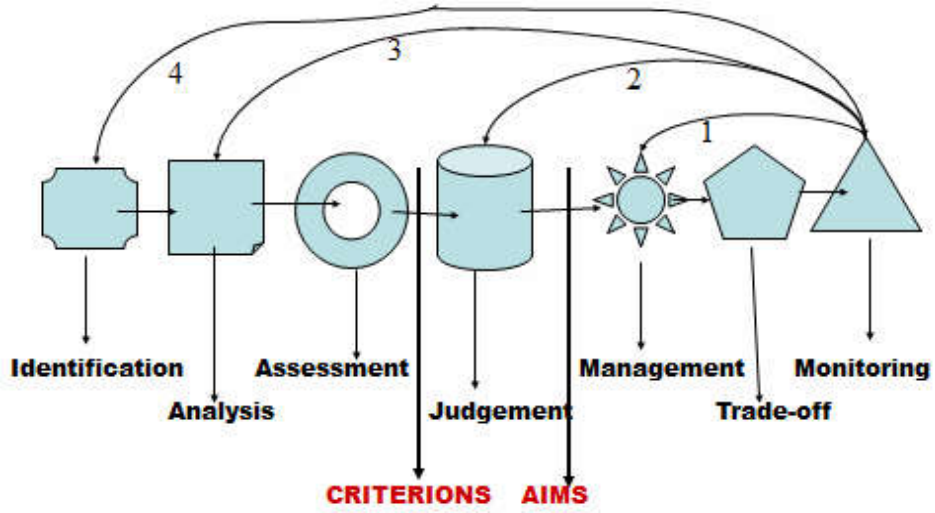


Fig.2 - Process model of work with risks targeted to safe entity.

4. The risk management is the complex process that needs knowledge, experiences and skill from many fields. Figure 3 shows fundamental separation of tasks among professionals (Risk determination), decisive sphere (Decision Making) and executive sector, i.e. engineers, technical workers and first responders (Risk Control and Mitigation); further detail specification is e.g. in [4]. If decisive sphere does not respect the public interest correctly or if it has not enough knowledge or sources, the organizational accidents occur earlier or later.

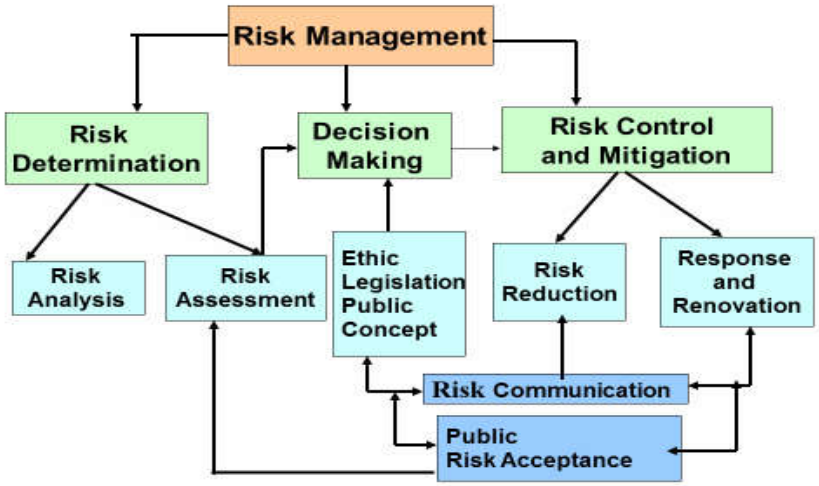
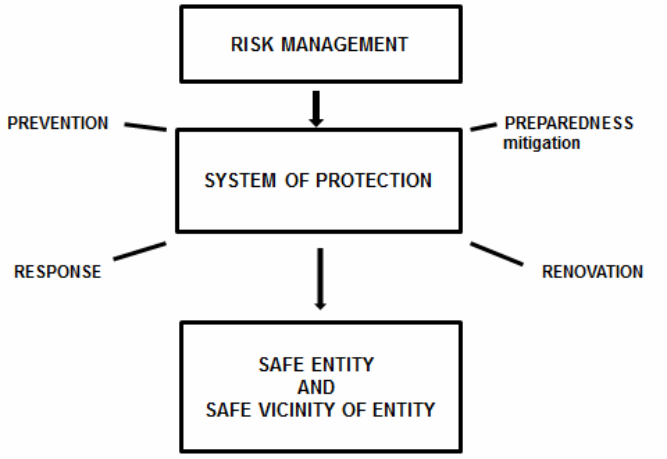


Fig. 3 - Basic structure of separation of tasks ate risk management.

5. The risk management is targeted to building the safe world. For this we perform the measures and activities during the prevention, preparedness, response and renovation, Figure 4.

Fig. 4 - Time sequence of phases in which the measures and activities for defending the risks are performed.



6. 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).
7. 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.
8. The aim of all processes for risk management is the safe world. This management type is called the safety management. Its process model is in Figure 3. The safety is a set of anthropogenic measures and activities, which lead to ensure the followed entity security and development. Since the world is dynamically changing, so the management of safety of critical installations is focused on priorities. In the first place, it means the application of All Hazard Approach [7], determining the hazards posed by individual disasters, and according to the assessment of size of threat from real disasters and vulnerabilities of a site and of critical installations against real disaster the separation of disasters into the following groups: the disasters, which cannot have impacts on critical facility; disasters that have only an acceptable impacts on critical facility, for which we use the designation "relevant disaster"; disasters that have on a critical facility only impacts that are manageable at origin by prepared prevention and mitigation measures, for which we use the designation "specific disaster"; and disasters that have an unacceptable impacts on the critical facility and, therefore, it is necessary to carry out essential preventive measures in the field of technical, organizational, legal and educational and it is necessary to have the possibility to activate all of the resources and the means to cope with their impact and jump-start further development, for which we use the designation "critical disaster". The last mentioned disasters have the potential to cause extreme emergency situations and for their defeat it is necessary to use the tools for crisis management. ***To achieve the desired level of safety it is necessary well to manage and properly to decide.***Good management and good decision making is 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.

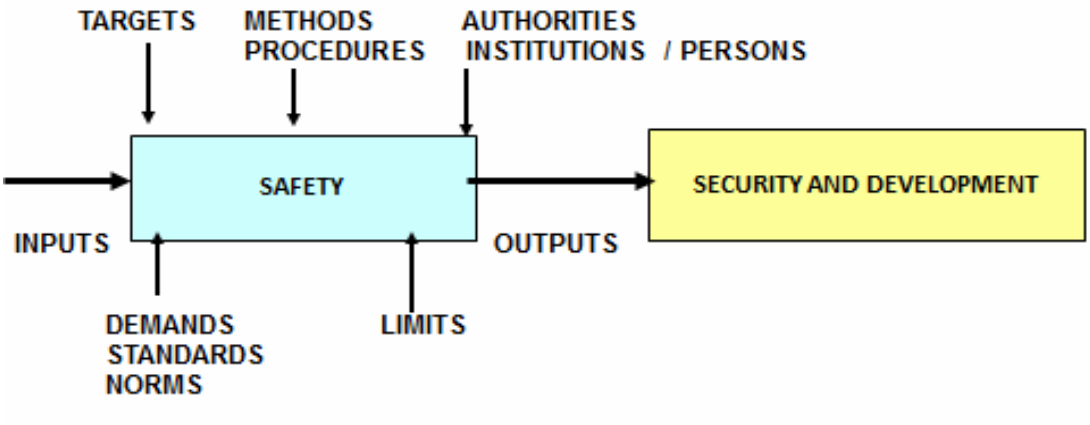


Fig. 5 - Process model for ensuring the security and development.

9. Present advanced management of socio-technological entities is based on the processes management; details are in Annex. Model for entity safety management in time [5] is shown in Figure 4. 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:
   i. 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.
   ii. 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.
   iii. 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.
   iv. 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.
   v. 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.
   vi. 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).

   Coordination of processes is targeted at ensuring the safe complex facilities under the conditions of normal, abnormal and critical (Figure 5).
10. 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).

    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.

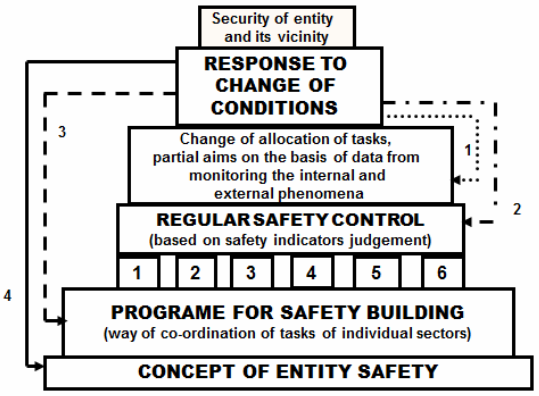


Fig. 6 - Model of management of critical complex facility safety; black block – concept for specification of important processes of critical complex facility; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4

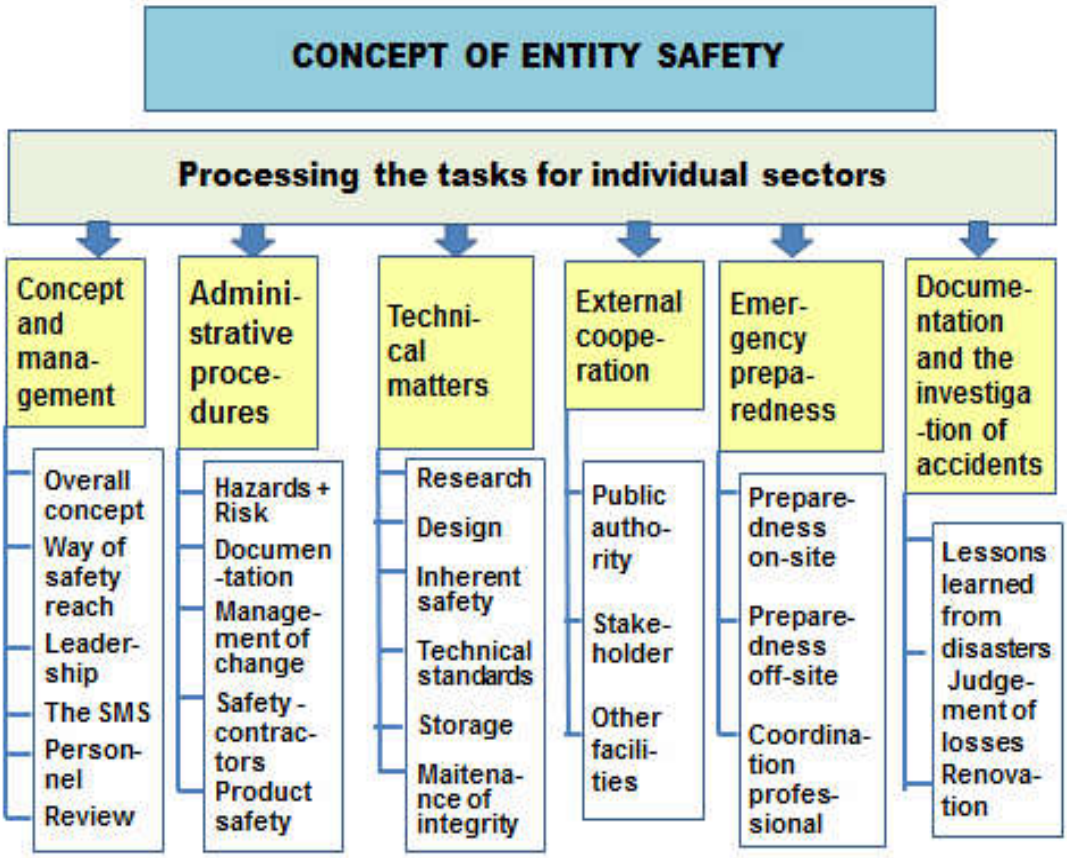


Fig. 7 - Concept of entity safety and its main parts.

11. 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.

12. 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 [3]. 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 [3, 4].
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 state 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 [4, 5].
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 [3-5].

3.2. Causes of risk management failures

Because from the critical analysis of emergency up to critical situations in human system, in detail described in [1], it followed 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,

the high attention is concentrated to such phenomena. In proposal of processes for management of risks are considered all above given knowledge and phenomena that cause the disturbance of social relations, public welfare and human security [10] – Table 1, and principles of modus operandi management, i.e. TQM (Total Quality Management) [11, 12].

Tab. 1 - 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 must 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.

4. METHODS USED FOR DETERMINATION OF SUPER PROCESSES FOR RISK MANAGEMENT IN DYNAMICALLY VARIABLE WORLD

The outputs described in the next paragraphs were created by: the critical analysis and critical evaluation of knowledge that is gathered in professional publications and summarized in foregoing chapter; the consideration of experiences from everyday life; the logical interconnection of knowledge; the classification of obtained facts; the synthesis of obtained facts; the application of methods of creative thinking and expert judgement (panel discussion, brainstorming, Delphi method, criticality assessment etc.) on: risk; risk scenarios; risk management and trade-off with risks; specific investigation of risks by analytical and heuristic methods [15, 16]. 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 [16]); 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 special the checklist, which was compiled according to the technique described in [5]. Its form for i-th disaster is shown in Table 2. All mentioned data were critically considered and synthetized according to the principles of strategic documents production [3].

All mentioned data were critically evaluated and synthetized according to the principles of compilation of strategic process models [3-5, 14], i.e. by help of procedure that is in agreement with procedure described in famous works as [17-22].

Table 2 -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 [5]. 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 technological object or facility to incorporate the principles of inherent safety, i.e. safe design?		
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?		
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).		
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions measures for emergency response that mitigate impacts on technological facility system and ensure the capability to return to a normal state? Operation of a technological object is successful, if it is a good continuity plan 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?		

5. ADVANCED PRINCIPLES OF RISK MANAGEMENT AND RISK ENGINEERING

With regard to knowledge [3, 4, and 23] the present possibilities of human society for dealing with risk are:

- part of risk is reduced, i.e. by preventive measures the risk realisation is averted in advance,
- part of risk is mitigated, i.e. by purpose-built measures, activities and by preparedness (warning systems and another measures of emergency and crisis management - response personnel, response systems, material, technical and finance reserves) at response to risk realization reduce the impacts or avert the unacceptable impacts,
- part of risk is re-insured, i.e. the insurance ensures the cover of possible loses and damages,
- part of risk for which there are prepared procedures and resources for response and renovation; i.e. the reactive measures and activities ensure the human survival, the territory protection, the situation stabilization and the renovation,

- part of risk for which there is prepared contingency plan; i.e. the reactive measures for suppress of critical unforeseeable situation (contingency plan) for case if non-controllable or too costly or low frequent risks occur.

To this it is joined the distribution of risk defeating among all stakeholders [3]. The distribution in good governance is performed according to rule that all stakeholders have responsibility for the risk defeat and that the defeat of a real risk is assigned to a subject the preparedness of whom is the best.
The key concepts of present engineering directed to human safety derived in [16] are the following:

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

For respecting these items there should be used relevant data sets and only verified methods that provide outputs with a designated testified competence. Because in the group of cases there is not well coped with vagueness in data, in practice there are used the procedures designated as good practice procedures / good engineering practice procedures. Modus operandi procedures in individual domains go on that on the basis of experience lead to a good result. The given procedure is used in cases in which there was not approved any unified procedure. It is often used at measurements in laboratories, negotiation with humans etc.
Owing to a lot of factors, including the human factor, influencing the problem solving at real conditions exist; and these factors are not only random but also epistemic, the measures, activities and procedures denoted as good engineering practice are typical for engineering disciplines.
Good engineering practice (good engineering procedure) is then defined as a 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 give above is directed to correct the human factor negative manifestation.
From given facts it follows that all considered 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 and or by mastery, but the methods, tools and techniques respecting the data logic, technological, financial, managerial and decision-making needs to be used, because their integral part is the decision-making over technical problems, human factor, costs and time planning.
The special attention of advanced risk management and risk engineering targeted to the human safety is targeted to the technological objects and networks that are in principle the socio-technological systems. According to knowledge concentrated in [5] 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 [3]. 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"; the last mentioned problem was broadly discussed in world conference ESREL2011 [23]. For the first problem solution we need systematically to monitor human system and obtained data process by qualified methods [14].

6. SUPER PROCESSES FOR MANAGEMENT OF RISKS IN DYNAMICALLY VARIABLE WORLD

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.: several protected assets, the objectives of which are sometimes conflicting. The assets vary in time and space; and the human system, in which the assets are, is in dynamic development.

6.1. Design of super processes

As above said, for ensuring the entity safety, the priority risks need to be considered. The negotiation with risks comes out from the present possibilities of human society and it consists is separation of trade-off with risks into several parts containing the measures and activities for given risk part control. The measures and activities of individual parts differ in time application. Their goals are mentioned in section 5.

As it was said above, the present knowledge shows that due to dynamic world development it is not sufficed to control the risks connected with individual disasters, but it is necessary to manage the processes that produce the disasters (the scientists have been trying to do tis since 50s of last century – e.g. technical polygons round the faults with which great earthquakes are connected - Kamchatka, Central Asia, California etc.). It means that the complex view is necessary.

Taking into account the nature of world, i.e. many open mutually interconnected systems having the proper goals that end up in conflicts from time to time, it is logic that human reaction needs to be also the process that is controlled in space and time. On the basis of logical interface of knowledge and experiences from practice by help of strategic planning principles there are proposed two super processes for management of risks in time and space. The first one is for ensuring the safe territory and the other one for ensuring the safe technological objects or facility. These super processes ensure the continual control of risks.

For ensuring the safe territory and safe public assets it is necessary to apply the super process that consists from five processes (Figure 8):

- 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 is in [10]).
- 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 [4, 5]); 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.
- 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.
- 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.

- 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 8 shows; in case of its failure the feedback 2 etc.; at huge harms immediately it is 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.).

Fig. 8 - 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.

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 9):

- 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 is in [10]); 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 [5]) 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 [5]).

- 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 [5]); and start-up of permanent operation.
- 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 [5]); 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 technological 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 [5].
- 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.

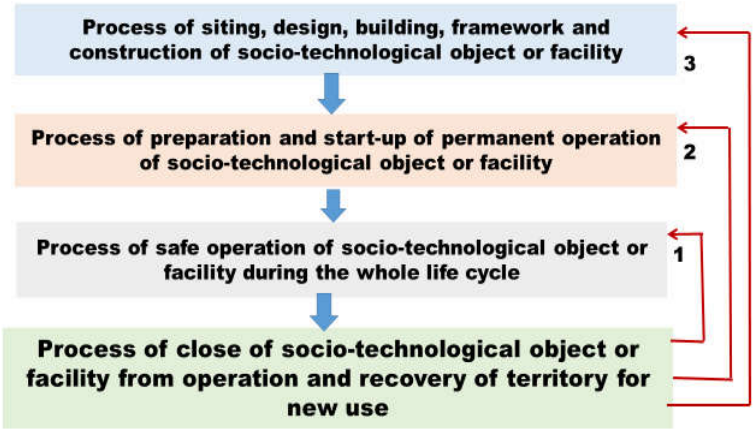


Fig. 9 - The structure of super process for risk management and trade-off with risks for profit of safe technological entity during its life cycle and its safe vicinity. The numbers denote the feedbacks that need to be realised if problems occur. From the economy reasons the firstly the feedback 1 is applied, and only if it fails the feedback 2 etc.

Because the dynamic development of world it is necessary to monitor the technological entity and to have prepared the procedures for correction of unfavourable situations. It is also necessary to consider that each technological 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 this reasons there need to be prepared procedures and corrections in each technological entity for averting the unfavourable situation. From economy reasons it is necessary firstly to use the cheapest procedure that feedback 1 in Figure 7 shows; in case of its failure the feedback 2 etc.; at huge harms immediately it is 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 10 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.),

Fig. 10 - Basic conflict in the management of technological entities from safety reasons (details in [5]).

- 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.

1.2. Deficits that reduce the effectiveness of super processes

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. This reality confirms the results obtained for:energy infrastructure in [24, 25]; drinking water infrastructure in [26, 27]; transport infrastructures (road, rail, subway, air) in [28-36]; communication, information and cyber infrastructure in [37-39]; finance infrastructure in [40]; supply chain infrastructure in [41-43]; emergency services infrastructure in [44]; public administration management in [45, 46]and other studies that are in many other publications, which are in the CVUT archives [9]. The same shows the deficits given in Table 1. These facts reveal big deficiencies in work with the risk, namely in details and in whole processes.
The results of accidents investigation and inspections that were performed in twelve complex facilities: bulk power station; metro station; important central bus station; air control operation facility, airport; waterworks facility; big chemical plant; hazardous material storage facility; important highway bridge; important road tunnel; important artificial lake; and nuclear power plant [9, 47] revealed the main causes of organizational accidents in domains, e.g.: old style of entity management concept; old style of entity safety management (omission of system structure, human resources qualification, low safety culture); omission of some disasters, too simple risk assessment, low level of safety documentation in investigated technological object or facility operation control; insufficient control of individual processes and sub-processes; insufficient technical standards and norms; low level of cooperation among sectors in entity (e.g. delay and errors in information transfer at important facts), among other entities including the public administration; missing or low level plans for on-site and off-site preparedness; no documentation on near misses and on investigation of damages, losses and harms and their causes and on the response and follow-up activities after disasters (including lessons learned and information sharing).

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 sub-processes 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 [16] is suitable, according to experience the panel discussion [16] is unsuitable because at its use the special interest groups (lobby) can have chance.

7. CONCLUSIONS

Because the ideal of today's world designated as "the safe community" can be, according to the current knowledge, reached only by ensuring the human system integral safety, it is necessary not to be afraid of new conceptions and new objectives and to start constructing the complex system safety management in the communities and other entities concentrated on all the known disasters including the corruption and other phenomena belonging to organizational accident category which is ready to transform if there is the occurrence of new risks along with a mutual respect of coexistence of various systems. As always, the problem is in humans, i.e. how to force them, so they may consider the public interest, mutual help and similar values as the top value of individuals.

It is necessary to pay attention to safety culture which means that humans in all their roles (manager, employee, citizen or the victim of a disaster) keep the safety principles, i.e. they behave in a way that they don't cause a realization of possible risks and when they become the participants of risk realization they need to contribute to the effective response, stabilisation of the assets and their renovation and to initiating of their further development. It is true that the complex of attitudes, speculations, norms and values existing in the community which is the reflection of a way of how the community is managed, i.e. these are the general principles of dividing of the power and responsibility, the managing principles and a certain relation between the stress on a work results, authority, human care, keeping the safety principles and ensuring the function of the community.

The effective culture of safety is the basic element for the safety management. It reflexes the safety conception and originates from the values, attitudes and actions of the head managers of a community and from

their communication with all the involved. It is an obvious obligation to actively participate on the solution of the safety questions and to promote among the others involved keeping of the authorized legal directives, standards and norms. The rules of safety culture must be elaborated into all the actions of a community. Their basis isn't the concentration on the delinquents'/mistakes originators' punishment but on the lesson from the mistakes and on instituting the corrective measures so that the mistakes couldn't be repeated or so that the rate of their occurrence was reduced.

On the basis of present knowledge, the world needs to be understood as the open system of systems and for security and development of humans the human communities (villages, municipalities, regions, states, association of states etc.) need to work well with risks. The work with risks targeted to human security and development is necessary to realize by super processes that are defined above. These super processes´ correct applications are good prevention of organization accidents.

Due to world variability in space and time there is necessary regularly to evaluate the conditions of co-existence of territory and all technological entities located in it from the viewpoint of human safety. Interconnection and co-ordination of super processes has not capability to ensure permanent territory safety and human safety, but it at least reduces the number of sources of organizational accidents by which it reduces the costs of human society on elimination of damages caused by technological accidents and infrastructure failures. For ensuring the correct interface and co-ordination on individual hierarchical levels, there is necessary to develop knowledge on knowledge uncertainties that are sources of risks that suddenly emerge, which of course influences the effectiveness of super processes, and causes unpleasant surprises to humans in the form of extreme disasters occurrence.

ANNEX

On the basis of present knowledge, the technological (correctly socio-technological) facilities and infrastructures are open systems of systems, i.e. the sets of mutually interconnected open systems [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-technological 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 technological facilities and infrastructures are made up as secured or safe systems.

On the basis of work [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-technological 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 [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 [3, 48].

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 [3].

As it is mentioned above, the secured systems involve commonly used technological 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 [3]. According to this work, 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; technological system; territory; and the State, and the following questions:

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

For ensuring the safety, including the functionality, dependability and stability of facility or infrastructure, 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 [3, 48].

Limits and conditions are tools for safety management of these technological facilities. Their observance ensures the safe operation of technological 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 [3, 48].

For ensuring the safety, i.e. also the reliability and the functionality, the control system of given technological facility or infrastructure 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 of whole system. In terms of integral safety [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 [3].

Acknowledgement
Author thanks to the Czech Technical University in Prague for support (grant SGS2015-17).

REFERENCES

[1] UN. *Human Development Report*. New York 1994, www.un.org
[2] EU. Safe Community. PASR projects. Brussels: EU 2004.
[3] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organisation* (In Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.
[4] PROCHÁZKOVÁ, D. *Risk Analysis and Risk Management* (In Czech). ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405p.
[5] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities.*ISBN: 978-3-659-74632-1. Lambert Academic Publishing, Saarbruecken 2015, 244p.
[6] MASLOW, A. H. *Motivation and Personality*. Haper, New York 1954, 236p.
[7] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[8] PROCHÁZKOVÁ, D. Principles of Mitigating and Managing Human System Risks. *Information & Security*, 28 (2012), No 1, 21-36, ISSN: 0861-5160, e-ISSN 1314-2119, http://infosec.procon.bg
[9] CVUT. Czech Technical University archives.
[10] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Their Control* (In Czech). ISBN: 978-80-01-05479-6. Praha: ČVUT 2014, 234p.
[11] US. *A Guide to the Project Management Body of Knowledge*. Washington: US Project Management Institute 2004.
[12] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991
[13] GLENDON, I.A et al. *Human Safety and Risk Management*. ISBN: 0-8493-3090-4. Boca Raton: CRC Press 2006.
[14] PROCHÁZKOVÁ, D. *Principles of Safety Management of Critical Infrastructure* (In Czech).ISBN: 978-80-01-05245-7. Praha: ČVUT 2013, 223p.
[15] PROCHÁZKOVÁ, D. *Methodology for Assessment of Costs on Renovation of Property Affected by Natural or Other Disaster* (In Czech). ISBN: 978-80-86634-98-2. Ostrava: SPBI SPEKTRUM XI 2007, 251p.
[16] PROCHÁZKOVÁ, D. *Methods, Tools and Techniques for Risk Engineering* (In Czech). ISBN: 978-80-01-04842-9, Praha: CVUT 2011, 369p.
[17] ARMSTRONG, J. S. Review of Corporate Strategic Planning. *Journal of Marketing*, 54 (1990), pp. 114-119.
[18] BRYSON, J. M. *Strategic Planning for Public and Non-Profit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. London: John Wiley & Sons 2011.
[19] EPPLER, M. J., PLATTS, K. W.The Systematic Use of Visualization in the Strategic-Planning Process. *Long Range Planning* 42 (2009), pp. 42-74.
[20] JUDGE, W. Q., DOUGLAS, T. J. Performance Implications of Incorporating Natural Environmental Issues into the Strategic Planning Process: An Empirical Assessment. *Journal of Management Studies*. ISSN: 1097-0266. 35 (1998), 2, pp. 241–262.
[21] MOORE, M. H. *Creating Public Value: Strategic Management in Government.* Cambridge: Harvard University Press 1995.
[22] 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.
[23] BÉRENGUER, Ch., GRALL, A., SOARES, C. G. (eds): *Advances in Safety, Reliability and Risk Management.* ISBN: 978-0-415-68379-1. London: Taylor & Francis Group 2012, 3068p.
[24] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Causes of Failure of Electroenergy Infrastructure and identification of Domains that Need Prevention and Preparedness (In Czech). In:*Rizika podnikových procesů 2015.*ISBN: 978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, pp. 114-123.
[25] KRÁKORA, J., PROCHÁZKOVÁ, D. Impacts of Electric Energy Outage on Metro (In Czech). In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 83-90.

[26] PROCHÁZKA, J., VAŠATOVÁ, L. Failure of Drinking Water Supply (In Czech). In: *Proceedings.* ISBN: 978-80-214-5336-4. Brno: VUT 2016, pp. 278-286.

[27] PROCHÁZKA, J., VAŠATOVÁ, L. Risks of Drinking Water Failures. In: *Risks of Business and Territorial Processes*. ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, pp.92-104.

[28] PROCHÁZKOVÁ, D., MOCKOVÁ, D. Impacts of Failure of Selected Elements of Transportation Infrastructure (In Czech). In: *Ochrana obyvatelstva – nebezpečné látky 2012***.** ISBN: 978-80-7385-109-5, ISSN:1803-7372, Ostrava: SPBI 2012, pp. 148-152.

[29] PROCHÁZKOVÁ, D., LÁNSKÁ, M. Case Study Simulating the Impacts of Accident in Vítkov Tunnel(In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7835-115-6. Ostrava: SPBI 2012, pp. 253-256.

[30] PROCHÁZKOVÁ, D. Principles of Protection of Transportation Infrastructure (In Czech). In: *Požárníochrana 2013*, ISBN: 978-80-7385-127-9, ISSN: 1803-1803, Ostrava: VŠB-TU 2013, pp. 214-218.

[31] PROCHÁZKOVÁ, D., PATÁKOVÁ, H., PROCHÁZKA, J., STRYMPLOVÁ, V. Problems of Hazardous Substances Transport in the Czech Republic (In Czech). In: *Crisis Management - Strategy, Safety, Research*. ISBN: 978-80-86710-79-2. Brno: VŠKE 2014, pp. 225-237.

[32] STRYMPLOVÁ, V., PROCHÁZKOVÁ, D. Results of Analysis of Critical Spots at Passengers Control at Airport (In Czech). In: *Crisis Management - Strategy, Safety, Research.* ISBN: 978-80-86710-79-2. Brno: VŠKE 2014, pp. 238-247.

[33] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PATÁKOVÁ, H. The Results of Systematic Study of Risks Associated with the Transportation of Hazardous Substances. In: *Safety and Reliability: Methodology and Application*. ISBN: 978-1-138-02681-0. CD ROM. CRC Press 2014 (London: Taylor & Francis Group 2015), pp. 1663-1670.

[34] KERTIS, T., PROCHÁZKOVÁ, D. Reduce of Criticality of Critical Infrastructure Facilities in the Railway Domain. ISBN: 978-1-4673-6727-1/15/531.00©2015 European Union. *Smart Cities Symposium Prague (SCSP).* IEEE, 2015, 8p.

[35] REMEŠ, P., PROCHÁZKOVÁ, D. Compilation of Check List for Identification of Critical Spots on Highway (In Czech). In:*Rizika podnikových procesů 2015.*ISBN:978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, pp. 151-160.

[36] PROCHÁZKA, J., PRAŽAN, M., PROCHÁZKOVÁ, D. Causes of Organizational Accidents in Civilian Skyborne Operation (In Czech). In: *Young Transportation Engineers Conference 2016*. ISBN: 978-80-01-06016-2. Praha: ČVUT 2016, 10p.

[37] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Cyber Infrastructure – Identification of Critical Spots and Impacts of Its Failure (In Czech). In: *CYTER2012*, ISBN: 978-80-01-05072-9, Praha: ČVUT 2012, 10p.

[38] SRP, J., PROCHÁZKOVÁ, D. Analysis of Cyber Networks in System Concept. In: *CYTER2012*, ISBN: 978-80-01-05072-9. Praha: ČVUT 2012, 12p.

[39] PROCHAZKOVA, D., SRP, J., PROCHAZKA, J. Analysis of Cyber Networks in a System Concept. In: *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics. Recent Advances in Systems, Control, Signal Processing and Informatics*. ISBN: 978-1-61804-204-0, Rhodes Island 2013, pp. 102-109.

[40] PROCHÁZKOVÁ, D., KOPECKÝ, Z. Problems of Bank Sector (In Czech). In: *Požárníochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 250-252.

[41] PROCHÁZKOVÁ, D., ŘÍHA, J. Selected Security problems of Supply Chains(In Czech). In: *Požárníochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 266-269.

[42] PROCHÁZKOVÁ, D. Model for Supply Chains´ Safety Management. In: *Proceedings of the 11th European Transport Congress*. Praha: CTU in Prague. ISBN: 978-80-01-05321-8, pp. 213 -219. www.etc.2013.fd.cvut.cz

[43] PROCHÁZKA, J., RETAMOZOVÁ, P. Accidents of Oil Pipeline (In Czech). In: *Rizikapodnikových a územních procesů a poznatky pro krizovéřízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 164-173.

[44] BINKOVÁ, P., HORÁKOVÁ, A., PROCHÁZKOVÁ, D. Comparison of Strategies Used in Internal Safety in the European Union and the Czech Republic in Criminal- Police Sector(In Czech). In: *Požárníochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 21-25.

[45] PROCHÁZKOVÁ, D., PEŠKOVÁ, I. Open Problems in Social Domain Management (In Czech). In: *Požárníochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 257-261.

[46] PROCHÁZKOVÁ, D., ŠENOVSKÝ, M., MOZGA, J. Problems of Public Protection in the EU (In Czech). In: *Požárníochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 270-274.

[47] 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

[48] CR. *Act. No. 183/2006 Coll., on Spatial Planning and Building Regulation (Building Law).*

ADRESA AUTORA:

Dana Procházková, doc., RNDr., PhD., DrSc.,
ČVUT v Praze, fakulta dopravní, Konviktská 20, 110 00 Praha 1, Česká republika,
e-mail: prochazkova@fd.cvut.cz

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.