Risk Management Quality in Selected Critical Facilities

DANA PROCHÁZKOVÁ, JAN PROCHÁZKA

Department of Security Technologies and Engineering
Czech Technical University in Prague
Konviktská 20, 110 00 Praha 1
CZECH REPUBLIC
prochazkova@fd.cvut.cz http://www.cvut,fd.cz

Abstract: - Series of events from recent years connected with failure of critical facilities show their high importance. The critical facilities under account represent multistage mutually overlapping systems, i.e. great complex systems, the type of which is a system of systems. Present paper shows the very advanced procedure of work with risks ensuring the safety of facilities under account that is based on the system safety management; i.e. on the combination of principles: All-Hazard-Approach and Defence-In-Depth; safety culture; and on special management procedure of work with risks in time; i.e., it shows: the concept of critical facility safety; the way of work with risks; the method of critical complex facility safety management model building; and the model for critical complex facility safety management in time. In the second part the paper summarizes the results of inspections directed to judgement of consistency of real facilities safety performance with demands of ideal model formed on the facility integral safety concept.

Key-Words:- complex critical facility; provision of territory services; security; safety; concept of facility safety formation; model for facility safety management in time; results of inspections.

1 Introduction

For ensuring the human security and development, the safe human system is necessary [1-3]; human system has different levels – village, city, region, State etc., which we further denote as communities. One of basic assets of community is the critical infrastructure, which consists of basic interfaced infrastructures [3,4]. The mentioned set of infrastructures is very important for ensuring the safe communities because it ensures for the territory the basic services which are necessary for humans´ live as energy, good quality drinking water, utility water, transport, information, rescue services etc.

Each infrastructure consists from the complex technological facilities (solid structures) and linear elements that ensure the services in the community; the paper concentrates attention to the first mentioned item. Series of events from recent years connected with failure of critical facilities show their high importance. The critical facilities under account represent the multistage mutually overlapping systems, i.e., great complex systems, the type of which is a system of systems; Figure 1.

Ensuring the safe critical facilities is not easy, because their nature is the system of systems [4], i.e. system of several mutually interconnected systems of a different nature. Consequences of interconnections (interfaces) are mutual dependences, the character of which is physical, cyber, territorial and organisational [4].

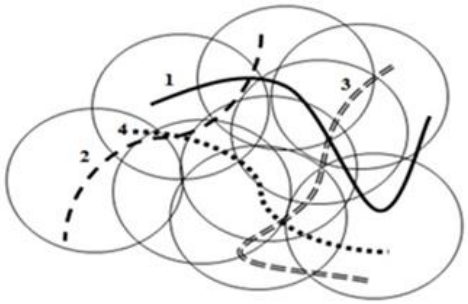

Fig.1. Scheme of complex systems – 1, 2,… are the processes being under way in mentioned entity

Above mentioned interdependences are the sources of further vulnerabilities of critical facilities, and naturally also communities in which they are located, because they magnify the integral risk of the community by increase of cross-section risks in the complex system [4]. As a consequence of growing globalisation the new sources of disasters take on force and they also cause critical complex facilities failures.

The paper deals with problems of critical complex facility in the broadest concept, i.e. not only from the viewpoint of critical complex facility itself, i.e. from the viewpoint of its structure and co-

operation of its individual parts***, but also*** from the viewpoint of its impacts and profits for a given locality in that it is in operation, i.e. for public assets in locality and region.

The paper concept includes the public protection, i.e. humans need critical complex facilities because they ensure them the high quality life, but they need to operate them very carefully because their big failures can have the long term consequences on public interest.

From the reasons of fulfilment of targets of humans (human security and development) that may be only realised if human communities are in the safe territory, the object of present paper is the critical complex facility safety that ensures the safe complex facilities that do not threaten neither themselves nor them vicinities, i.e. also another systems with which they are interconnected or which they influence.

In the first part the paper presents the very advanced procedure of work with risks ensuring the safety of facilities under account that is based on the system safety management; i.e. on the combination of principles: All-Hazard-Approach and Defence-In-Depth; safety culture; and on special management procedure of work with risks in time; i.e., it shows:

- concept of critical facility safety,
- way of work with risks,
- method of critical complex facility safety management model building,
- model for critical complex facility safety management in time.

In the second part the paper summarizes the results of inspections directed to judgement of consistency of real facilities safety performance with demands of ideal model of safe complex facility.

2 Critical complex facility safety aspects

To the term "critical complex facility" they are included the facilities that are parts of different technological systems that ensure the human society needs [4]. Each of considered systems consists of the control system and controlled systems [4], which are for company processes, social system (humans, organisational structures, assets and values, knowledge), and for own technological system (tools, equipment, procedures, technologies). It means that they are multistage systems at which among the individual stages in both directions they run flows of materials, finances, information and decisions.

From mentioned reasons the systems needs are necessary to be also analysed from the viewpoint of interactions and interdependences among the technical, human, social and organisational aspects of a system. The exception is the analysis of human survival that is either active or passive. The capability of passive survival is included in the system properties, which are based on the knowledge on defects in the real setting; the defects are mostly illustrated by causal chain. The capability of active survival is manifested by system behaviour, and therefore, it considers uncertainty in projection of future defects and failures.

From the methodological viewpoint the critical complex facility and each its partial part is a system of systems [4]. In engineering disciplines directed to risk at present we use two disciplines for trade-off with the risk [4]:

- a set of disciplines the target of which is the critical complex facility security, i.e. security of critical complex facility without regard to critical complex facility vicinity (security management),
- a set of disciplines the target of which is the critical complex facility safety, i.e. security and development of both, the critical complex facility and its vicinity.

Many professional works forever deal with ensuring the first target, which has been pursued in engineering disciplines since the beginning of 80s [4]. The other discipline target is more ambitious on understanding, accessible data and methods of engineering disciplines. It has been pursued since a half of 80s but from reasons of big demands on:

- data (there are necessary data on: system, system vicinity, linkages and flows between system and its vicinity),
- comprehension of problems and their connections in a case of open system of systems,
- methods of problem structuring, analysis and solving the problems,

it is only enforced in domain of selected fields as nuclear technologies and astronautics [4], namely in spite of it solves interconnection of targets of humans in domains social, environmental and technological [3]. According to the IAEA requirements [5] the nuclear facility safety management is realised in practice but in some aspects it needs improvement as shown results of inspections.

Regarding to present way of problem solving given above, we use two concepts for ensuring the safe entity [4]; i.e.:

- security management,
- safety management.

The first mentioned concept being simpler is more often used in practice; i.e. the target is the critical complex facility security and impacts of critical complex facility on its vicinity are out of interest.
The other ensures both, the critical complex facility security and the security of vicinity of critical complex facility.

With regards to works [3, 4] the definitions of terms connected with security and safety are:

1. Each critical complex facility is a multistage system in which among individual stages in both directions they run material, finance, information and decision flows.
2. The disasters for partial complex facilities and whole critical complex facility are the phenomena that caused damages and losses. They include phenomena belonging to the category „All-Hazards-Approach" [6] and the specific phenomena connected with humans and their behaviour that do the harm to the both, the critical complex facility owners and operators prosperity and the fulfilment of tasks for which they were established (insufficient co-ordination of activities – organising accidents, failure of outsourcing activities, intent attacks etc.).
3. The critical complex facility vulnerability is a predisposition of complex facility (its protected assets) to harm / damage origination.
4. The critical complex facility resilience is a complex facility capability to overcome impacts of a given disaster. To reach sufficient resilience, it is necessary to apply together above mentioned „All-Hazards-Approach" and "Defence-In-Depth" principle [4].
5. The critical complex facility risk is a probable size of losses, harms and detriment caused by a disaster with size of normative hazard (mostly design disaster) on critical complex facility and public assets or subsystems rescheduled on selected time unit (e.g.1 year), site unit (e.g. 1 km^2) and on the basic assets of owners and operators of critical complex facility.
6. The critical complex facility security is a situation / condition at which the probability of critical complex facility assets´ harms, damages and losses is acceptable (it is almost sure that large harms, damages and losses cannot origin).
7. The critical complex facility safety is a set of measures and activities for ensuring the security and sustainable development of critical complex facility, its assets and public assets.
8. The critical complex facility security management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded safe level of a critical complex facility (secured critical complex facility).
9. The critical complex facility safety management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded safe level of critical complex facility and its vicinity.
10. The critical complex facility safety engineering is a set of engineering measures and activities by which the critical complex facility safety is ensured in real conditions of a given site.

With regard to results from analyses of critical complex facility safety and historical experiences, performed on the data given in the professional literature [1,4] and in sources quoted in given works, it is necessary to follow systems for:

- energy supply,
- water supply,
- sewer and waste handling,
- transport,
- communication and information services,
- bank and finance services,
- emergency services (police, fire rescue service, medical rescue service),
- basic community services (food supply, waste liquidation, social services, funereal services), industry and agriculture,
- state and regional administrations, that are usually supported by the national legislative
- education,
- research.

The safety and risk are not complementary quantities (the first one depends on level of human making and the other depends on level of site danger) even though they together relate by a certain way. In each system both quantities depend on processes, acts and phenomena being under way in a given system and in its vicinity.

In advanced concept the concentration to safety has higher targets than concentration to risk because it follows system security, system development, system existence, system vicinity existence and co-existence of different systems [4]. It is the consequence of fact that the safety management is based on both:

- the high qualified trade-off with risk,
- and moreover on the human capability to penetrate into the problem of risk manifestation and in advance to prepare mitigating steps.

The risk sources are all phenomena included in the term „All-Hazards"[6], the phenomena specified in work [7] and further fulfilled during the FOCUS project (from 77 disasters followed now in 2035 the number of disasters increases to 105) [8].

The risks connected with the critical complex facilities are:

- partial risks that include risks connected with individual protected assets,
- integrated risk that include partial risks connected with several assets aggregated by a defined way,
- integral risk that includes risks connected with all protected assets, with linkages and flows among assets that cause couplings among assets, partial systems and with vicinity.

It is clear that to be able to ensure the system safety, the system integral risk needs to be considered, managed and traded-off.

3 Concept of safe complex facility set-up

With regard to the present knowledge it is necessary to give that for the complex facility safety management fundament, it is: the risk analysis, risk assessment and trade-off with risks connected with mutual interconnections in complex facility sectors and in the whole complex facility (i.e. in agreement with [4, 7] it is necessary to consider inter-dependences in a system of systems; i.e. at risk identification it is necessary also to use the cross-sectional criterions).

The procedure of work with risk is shown in Figure 2. It starts with definition of concept of work with risk (system characteristics, determination of assets, specification of aims), on the basis of which risks are identified, analysed, assessed, judged, managed, traded-off and monitored.

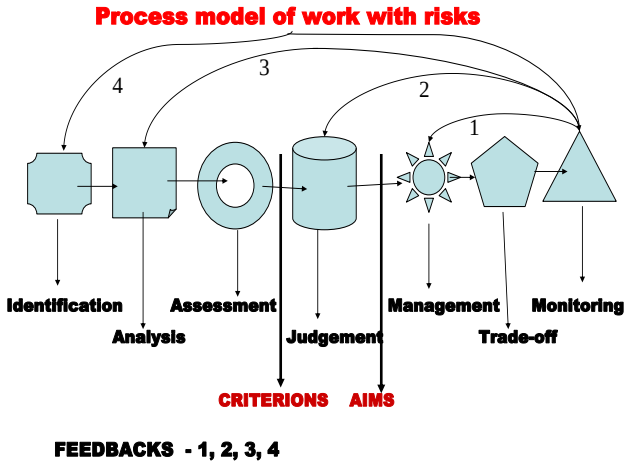

Fig.2. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks

Feedbacks denoted in the Figure 2 are used if risk level is not on required level [4] (because the costs on feedback application increase with increasing feedback order, the fourth feedback is only realised if safety concept fully fails, i.e. when basic risks were omitted when the risk identification was performed).

In the present practice we distinguish five different concepts for work with system risks, Figure 3, which are summarized and described in work [4].

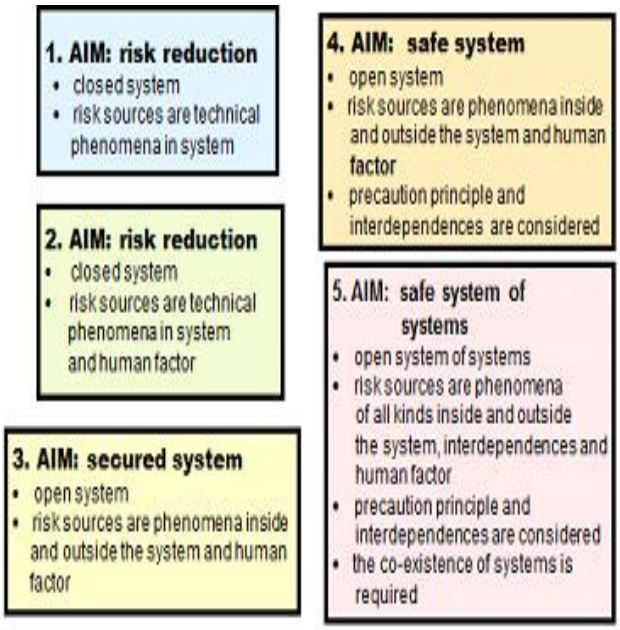

Fig.3. Concepts of risk management and engineering trade-off with risks and their objectives, arranged in chronological order according to the introduction to engineering practice

For the human safety and for the human system safety (including the territory, organisations, plants, i.e. also complex critical facilities) we need to manage the integral risk including the human factor, i.e. to apply concept 5 in Figure 3, which means to find the way of cross-section risks management, i.e. to concentrate the attention to interdependences and critical spots with a potential to start the system cascade failures, domino effects, strange behaviour etc., and on the basis of such site knowledge to prepare measures and activities ensuring the continuity of limited critical complex facility operation and of the human survival.

In Figures 4 and 5 there are shown the structures of the processes that are used in risk management and trade-off with risks in practice [7]. As the next step we also consider the relation between the territory character and the behaviour of complex facility; i.e. interdependences and their impacts on both, the territory and the complex facility and we judge the possible critical items.

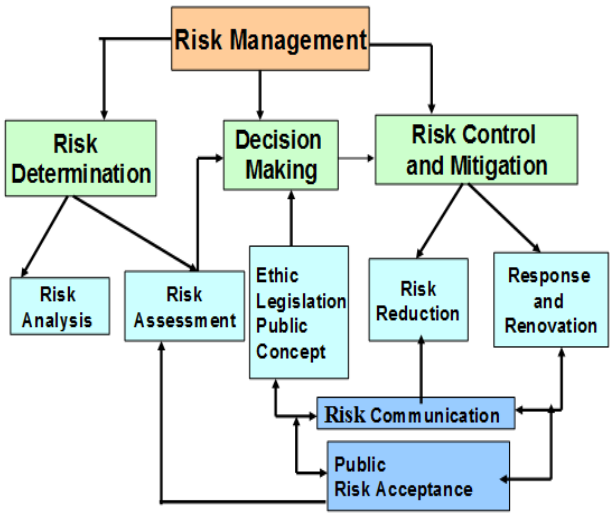

Fig. 4. Scheme of the process for the management and trade-off with the risks from the perspective of division of tasks among experts, the management sphere and implementers of specific measures and activities; the other details are in [7]

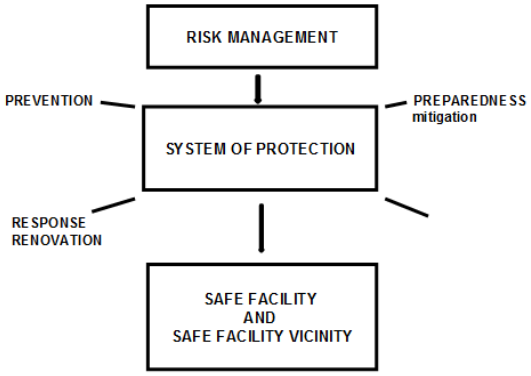

Fig.5. Scheme of the process for the management and trade-off with the risks from the perspective of formation of the protection of system aimed to a safe system and its vicinity; the other details are in [7]

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

With regard to knowledge summarized in [4] the basic principles of safety technological complex facilities are:

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

As the next step we apply All-Hazard-Approach [6] and Defence-In-Depth concept [4], the model of which is shown in Figure 6 This means:

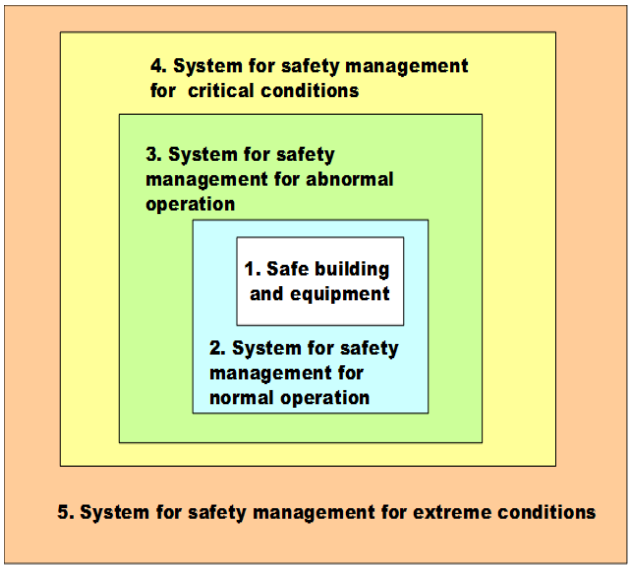

Fig.6. Way of complex facility safety ensuring in five degrees

1. In the design, construction and building of complex technological facility to use the inherent principles of safe design (approaches: All-Hazard-Approach [6], proactive, systemic considering the integral risk and also a significant partial risks associated with links and flows of material, energy, finances, and information in partial systems and across them; the correct work with risks; and monitoring, in which they are incorporated corrective measures and activities). The important thing it is the compilation of specifications (terms of references) related to the territory, that express the way of evaluation of local vulnerabilities in relation to all relevant disasters, which may affect the site and also the appreciation of all locally-specific features, which may cause specific impacts. On the basis of recent knowledge, summarised in the works [4], it is necessary to take into account for the critical complex facilities the random and epistemic uncertainties, i.e. especially epistemic uncertainties in the data, in order to avoid atypical accidents, which are a consequence of unpredictable phenomena that cannot be detected by the usual stochastic methods.
2. The control system of the complex technological facility needs to have a basic control functions, alarms and responses of operator processed by the way so that the facility was maintained in normal (steady) state under normal conditions.
3. The complex technological facility object needs to have a special safety-oriented control systems and protective barriers that keep it in a safe condition even when a larger change in the operating conditions (i.e. when abnormal conditions) and prevent the formation of undesirable phenomena, which means that it has a good resilience. The systems maintain a safe operation even under changing conditions or they have the capability to ensure the normal operation after the application of corrective measures (clean-up, repair, etc.).
4. In the event that there are occurred critical conditions that cause the loss of control of the facility, the facility needs to have a system of measures for the internal emergency response, measures mitigating the impacts for losses prevention in facility; and for return to normal operation (continuity plan and in-site emergency plan).
5. For the case that the impacts of the loss of control of the facility will affect around a facility, the facility needs to have the measures also for off-site response, mitigating measures for losses prevention in the facility; and the capacity to overcome the difficulties that it will be the capability to recover the facility.

In the professional area the layers mentioned above shall be regarded as protective barriers (so-called "protection in depth – defence in depth) and at the resolution of the facilities from the point of view of safety, it is used the security feature that the facility has a single stage or to a five-degree protection in depth. Individual safety management systems ensure the application of the technical, operational and organizational measures and activities that are designed to either prevent the initiation of chains of harmful phenomena, or stopped them [4].

Because the deterministic approach to protection in depth will not consider explicitly the occurrence probabilities of challenges or mechanisms, or does not include the quantification of the probability of success associated with the performing the elements and systems at every level of the defence in depth, the deterministic approach is added with probabilistic safety analysis (PSA) in the area of the reliability of the systems, the probable targets, etc. in order to ensure an adequate level of safety, which ensures good balanced design.

4 Management of complex facility safety in time

The purpose of model for critical complex facility safety management is to show basic steps by which it is possible to ensure critical complex facility security and critical complex facility vicinity security in time.

The model building method goes out from a system concept of critical complex facilities; it considers them as system of systems (several overlapping systems) [4, 7], which means that their complex behaviour, function and development depend on both, the number and properties of partial systems and the diversities of their interconnections, i.e. their linkages and flows among them and also across them. The linkages and flows going across the partial systems are the originators of internal dependences (interdependences). On that account we create the model by method of analogy to existing safety management models [3, 4 and 7].

At complex facility safety management we need to concentrate to critical items, and therefore, it is necessary to judge the criticality of both, the individual items and the whole. The method for judgement of criticality of individual facilities and of whole set of critical facilities is described in [9].

With regard to:

- the data and the knowledge in [3, 4, 7-14],
- the concept promoted by the OECD [15],
- the method described in works [4, 7],
- the assumption that each critical complex facility is an open system (i.e. risk sources are internal and external disasters and human factor [3, 4, 7]),

it is created a model for safety management having six processes (Figure 7), i.e.:

- concepts and management,
- administrative procedures,
- technical matters,
- external cooperation,
- emergency preparedness,
- the documentation and the investigation of accidents.

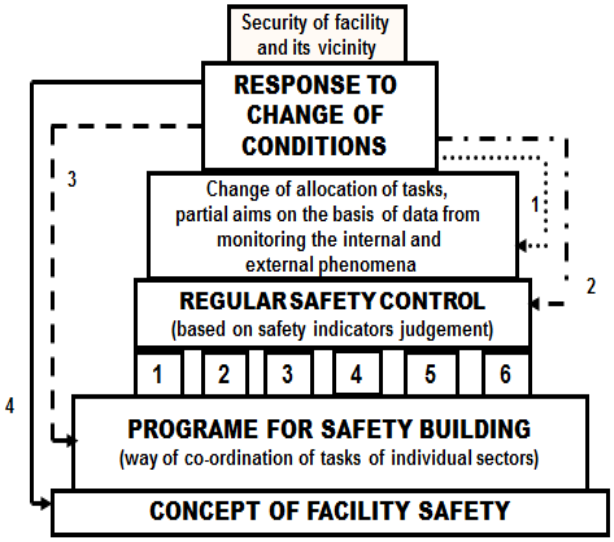

Fig.7. Model of management of critical complex facility safety; black block – concept for specification of important processes of critical complex facility; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4

The main processes are further divided into sub processes:

1. The first process consists of sub processes for: the overall concept; achieving the intermediate objectives of safety; leadership / management of safety; the safety management system; personnel staff including the sections for: human resources management, training and education, internal communication / awareness and working environment; review and evaluation of the implementation of the fulfilment of objectives in the safety.
2. The second process consists of sub processes for: identify of hazards from potential disasters and risk assessment; documentation of procedures (including work permits); management of change; safety in conjunction with contractors; and supervision of product safety.
3. The third process includes the sub processes for: research and development; design and mountings; inherently safer processes; technical standards; storage of hazardous substances; and maintenance of integrity and maintenance of equipment and buildings.
4. The fourth process includes the sub processes for: cooperation with the administrative authorities; cooperation with the public and other stakeholders (including the academic institutions); and cooperation with other facilities.
5. The fifth process includes the sub processes for: planning of internal (on-site) preparedness; facilitate the planning of external (off-site) preparedness (for which it corresponds the public administration); and the coordination of the activities of the departmental (resort) facilities at ensuring the departmental emergency preparedness and at response.
6. The sixth process has sub processes for: processing of reports on disasters, accidents, near misses and other learned experience; investigation of damages, losses and harms and their causes; and the response and follow-up activities after disasters (including lessons learned and information sharing).

From Figure 7 it follows that for each concept of critical complex facility safety it is necessary in the first to compile the programme for critical complex facility safety formation in which we establish the way how the individual sectors that manage main processes will co-ordinate their works so tasks of critical complex facility were efficient, economical and timeous, and the timetable.

Because each facility is in dynamic development the states of tasks performance need to be regularly judged by help of safety indicators (for trend and rate of target achievement) using the monitoring data. In case of abnormal deviations from targets of timetable, the corrections need to be done (e.g. allocation of tasks, partial aims, relocation of sources etc.). In the case of critical conditions (too big deviations from targets of timetable), the response to critical conditions needs to be performed. According to relevance of change of conditions the appurtenant feedback is selected; in Figure 7 you can see that the application of feedback 4

means the change of critical complex facility safety concept.

Because the costs on feedback application increase with increasing feedback order, the fourth feedback is only realised if safety concept fully fails, i.e. when the critical complex facility failure assessment shows that priority basic risks were omitted in original concept.

Coordination of processes is targeted at ensuring the safe complex facilities under the conditions of normal, abnormal and critical (Figure 8). The way of determination of tasks for individual sectors and their harmonization in time realised by process management is fundamental importance for the complex facility safety.

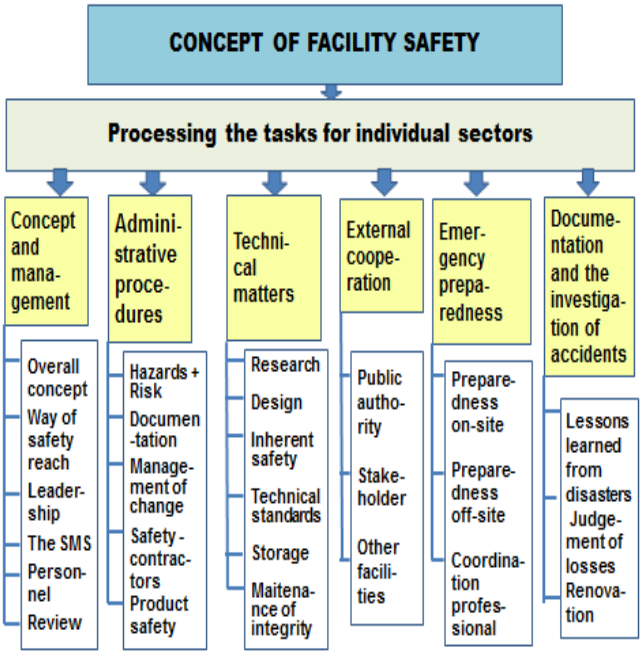

Fig.8. Concept of facility safety and its main parts

The safety management system (SMS) of facility operators includes the organisation structure, responsibilities, practices, rules, procedures and sources for determination and invoking the prevention for disasters that are results of processes inside and outside of facility or at least mitigation of their unacceptable impacts. As a rule it is connected with many aspects, apart from the organisation of employees, identification and assessment of hazard size, risk size, organising system, management of changes, emergency and crisis planning, safety monitoring, audits and scrutiny processes.

With regard to data in works [3, 15] the program for preservation and increase of complex facility safety has the following steps:

1. Determination of tasks (partial targets) and strategic goals for facility with regard to safety directed to security of both, the facility and the facility vicinity.
2. For each process that is connected with facility to determine suitable target and running indicators for safety level judgement.
3. To process dictionary for needs connected with integral safety management.
4. To harmonize standards, good practice methods and local procedures.
5. To determine set of target indicators.
6. To determine set of running indicators.
7. To determine way of assessment of target indicators specific for a given facility.
8. To determine way of assessment of running indicators specific for a given facility.
9. To determine way of assessment of all indicators together and marginal limits for a given facility.

In practice it means that for each sector of selected authority the target and running indicators are determined and they have form of limits and checklists [3, 15]. To them there are assigned criteria for assessment and scales by which it is determined if target is reached or is not reached. For creation of an effective safety management system the basic principle is that all participants need to play certain roles for safety realization.

Because the world dynamically changes it is necessary to follow continuously the safety level, i.e. the size of integral risk that includes also the cross-sectional risks connected with inter-dependences and important partial risks of critical complex facility. In case that limits and conditions are not kept, it is necessary to perform changes as shown feedbacks in Figure 7.

Because the changes requires sources, forces and needs, firstly it is realised feedback 1 and only if it does not ensure expected result the feedback 2 is realised etc. Only in the case of occurrence of extreme disaster with catastrophic impacts, the feedback 4 is immediately realised.

Safety management system for critical complex facility is lean on the concept of disaster prevention or at least of mitigation of severe disaster impacts that include the obligation to introduce and keep the safety management system [3,15] in which the following problems are taking into account:

- roles and responsibilities of persons participating in important hazards management on all organising levels and in ensuring the training,
- plans for systematic identification of important hazards and risks connected with them that are connected with normal, abnormal and critical conditions, and for assessment of their occurrence probability and severity,

- plans and procedures for ensuring the safety of all components and functions, namely including the object and facilities maintenance,
- plans for implementation of changes in territory, objects and facilities,
- plans for identification of foreseeable emergency situations by a systematic analysis including the preparation, tests and judgement of emergency plans for response to such emergency situations,
- plans for continuous evaluation of harmony with targets given in safety concept and in the SMS, and mechanisms for examination and performance of corrective activities in case of failure with aim to reach determined targets,
- plans for periodic systematic assessment of safety concept, effectiveness and convenience of the SMS and of criterions for judgement of safety level by top workers group.

It is necessary to ensure:

1. The qualified risk management of disasters, the sources of which are inside and outside of facility plus human factor; i.e. it follows facility and parameters of vicinity in which facility operates. It is composed of: assessment of expected disaster size; determination of occurrence probability of important disasters; judgement of critical complex facility vulnerabilities at important disasters; determination of impacts of important disasters on critical complex facility. It creates a base for ensuring the safe critical complex facility.
2. The designing and planning the measures and activities for ensuring the facility security at considering all important disasters [3,6]; i.e.: facility layout (structure, function, sitting, buildings, equipment); performing the measures and activities for ensuring the facility security; plan of renovation of facility after disaster; plan of training the personnel performing the facility; facility activities´ monitoring; and correcting measures and activities for a case of important deviations in facility operation.
3. The designing and planning the measures and activities for ensuring the facility vicinity security at considering all important disasters [3,6]; i.e.: facility layout by a way that it may not threaten vicinity, i.e. all public assets; performing the measures and activities for ensuring the facility vicinity security; plan of renovation of facility vicinity after disaster; plan of training the personnel performing the facility; facility activities´ monitoring; and correcting measures and activities for a case of important deviations in facility operation.
4. The harmony among the main activities connected with facility commodities, i.e.: subject of supply (its manufacture, transport and distribution); following the deviations in a process of commodity management; and operating loops. It goes on ensuring the stabilities of processes, the minimisation of delays, the quality and the other critical aspects connected with the operation.
5. The safe assets of facility, i.e. problems connected with: facilities, equipment or services; vehicles; shipping; products; and data systems. It also goes on averting the insiders' activities.
6. The safe human sources, i.e. problems connected with: acceptation of employee; understanding the employee behaviour features important for facility operation; employee training; employee self-control; implementation of procedures that ensure correct employee behaviour; and employee stimulation.
7. The good business partners, i.e. problems connected with: screening the possible partners; authentication of possible partners; producing the ways of negotiation with partners regarding to their behaviour; monitoring the partners behaviours; and audits of partners.
8. The capabilities for overcoming the impacts of extreme disasters that affect facility, i.e. problems connected with: business continuity; specific response training; investigation of causes of extreme impacts; assembling the evidences; reparation of harms; and court settlement.
9. The dislocation of criminal and illegal facilities and chains, i.e. problems connected with: formation of base for disruption (ensuring the sources, determination of means, logistics, transport of means, distribution of means); and with support of governments and customers.
10. The integral safety of critical complex facility, i.e. the coordination of all pillars, i.e. processes directing to critical complex facility safety (PSM – process safety management).

The useful tools for safety management are given in Figures 9 – 11:

1. Figure 9 shows the process safety management for facility.
2. Figure 10 shows the domains that need to be kept in harmony for achievement of facility safety.
3. Figure 11 shows the structure of plan ensuring the safe facility.

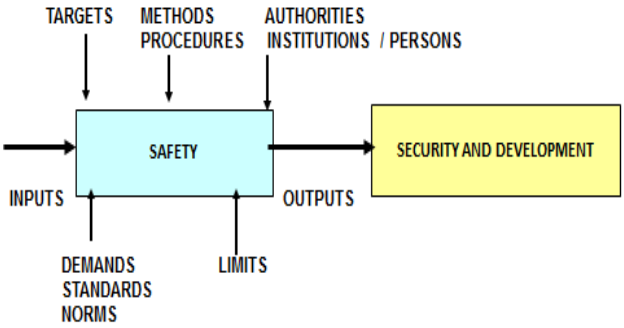

Fig.9. Process of facility safety management

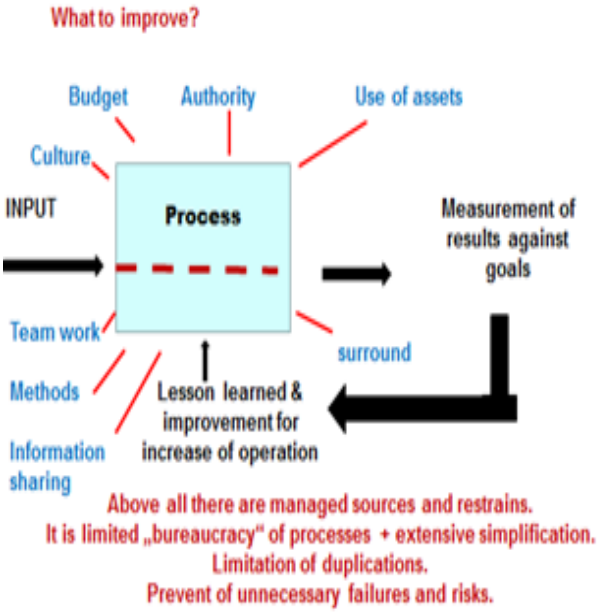

Fig. 10. The domains important for facility long-term safety achievement

5 Data and Method of Inspections

The inspections were performed in twelve complex facilities from different infrastructures belonging to the critical infrastructure:

- 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
- nuclear power plant.

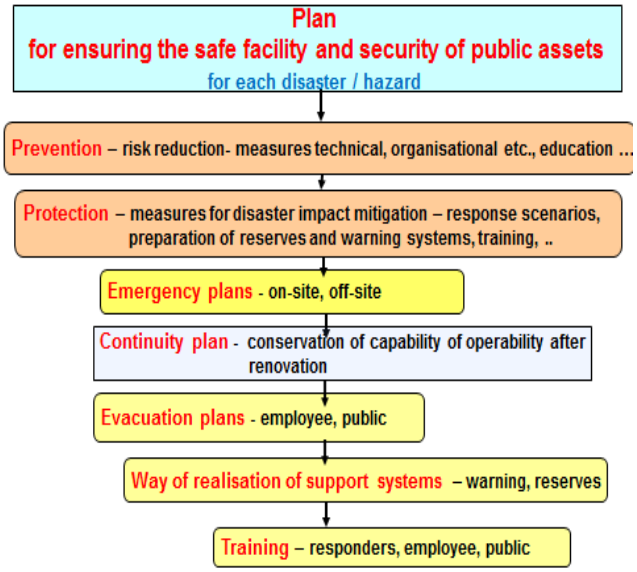

Fig.11. Structure of plan ensuring the safe facility

The aim of inspections was the judgement of safety level of selected facilities. For this purpose we used the comparison of ideal model of safe critical complex facility described in chapter 4 with data drawn from technical documentations and from walk downs of investigated complex critical facilities [16], which however, from safety reasons are not open to the public.

The comparisons were performed according the checklist (Table 1), that was compiled according to the technique described in [4].

Table 1. Identification of deficiencies for specific disasters in a given territory, 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*** [4]. For assessment of criticality it was used the value scale 0-5 [4] 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
1	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe		

	design?		
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?		
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).		
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions 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?		
2	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe design?		
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?		
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).		
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions 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?		
…….			
……..			
n	1. Has the technological facility to incorporate the principles of inherent safety, i.e. safe design?		
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?		
	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).		

	4. 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?		

6 Results of inspections directed to judgement of consistency of real facilities safety performance with demands of ideal model

The evaluation of checklists [16] obtained during the inspections in followed complex facilities, mostly show that:

1. Top safety management of complex facilities is insufficient; it is not based on use of AII-Hazard-Approach (only some disasters are considered) and integral risk at sitting, designing, building and operating the structures, components, equipment and systems.
2. Interdisciplinary communication with connection over different safety management levels of complex facility is missing.
3. Safety requirements are not solved in all domains; and therefore, some serious risks (e.g. evident risks connected with interfaces) are neglected.
4. Human faults are not often sufficiently considered (especially connected with way of deciding – no prevention of bad deciding).
5. The interdependences are not especially considered as the cause of failure of critical facilities.
6. Defence-In-Depth concept having the five layers is missing for crucial parts of complex facilities; usually only three levels were found.
7. Safety and security aspects are solved separately; mutual relations are not continually analysed.
8. Monitoring for detection of important changes in time is not systematic and complex.
9. Current legislative does not require all aspects important for facility safety, e.g. security is only respected in some domains of railway system.
10. Links and flows over boundaries of system under consideration are not solved.

The best safety rate was in the case of nuclear power plant at which the criticality rate was between low and negligible due to some opacities that can lead to organisational accidents.

7 Conclusions

Model for safety management of critical complex facilities compiled on the basis of present knowledge is the process model in which they are represented the both:

- the individual important elements of process of safety management based on qualified work with integral risk,
- the feedbacks by which it is possible to correct the cases in which demands of safety are not fulfilled owing to dynamical development of critical complex facility and its vicinity.

For application in practice the model for critical complex facility safety management is supplemented by mechanism for ensuring the capability to be effective at abnormal and critical conditions.

To ensure the critical complex facility safety during its life cycle including the human survival it is necessary to use: the mentioned concept of work with system risks directed to system of systems safety; principles All-Hazards-Approach and Defence-In-Depth; safety management programme based on model of management of critical complex facility safety shown in Figure 3; process of facility safety management shown in Figure 5; consideration of all domains shown in Figure 6; and security plan the structure of which is in Figure 7.

References

[1] UN, *Human development report.* New York:UN 1994, www.un.org.

[2] EU, *Safe Community*. PASR projects. Brussels: EU 2004.

[3] D. Procházková, *Strategic management of territory and organisation*. Praha: ČVUT 2011, 483p. ISBN:978-80-01-04844.

[4] D. Procházková, *Safety of complex technological facilities*. Saarbruecken: LAP 2015, 244p. ISBN:978-3-659-74632-1.

[5] IAEA, *Action Plan on Nuclear Safety*. Vienna: IAEA 2011,www.iaea.org

[6] FEMA, *Guide for all-hazard emergency operations planning. State and Local Guide 101*. Washinton: FEMA 1996.
[7] D. Procházková, *Analysis and management of risks*. Praha: ČVUT 2011, 405p. ISBN: 978-80-01-04841-2.
[8] EU, *FOCUS project*. Brussels: EU. www.eu.eu
[9] D. Procházková, Criticality of transport facility. *Periodica Academica*, ISSN 1802-2626, VIII (2013), No. 2, pp 112-128.
[10] W. Stein, B. Hammerli, H. Pohl, R. Posch (eds) *Critical nuclear facility protection – status and perspectives.* Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[11] J. Moteff, C. Copeland, J. Fischer, *What makes an infrastrucuture critical?* Report for Congress, 2003, CRS Web, Order Code RL31556.
[12] CISP, *Workshop on critical nuclear facility protection and civil emergency planning-dependable structures, cybersecurity, commnon standard*. Zurich: Centre for International Security Policy 2005, www.eda.admin.ch
[13] S. M. Rinaldi, Modelling and simulating critical nuclear facilitys and their interdependencies. In: *Proceedings of 37th Hawaii International Conference on System Sciences–2004.* Sandia: Sandia National Laboratories 2004 http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1265180
[14] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, Critical nuclear facility interdependencies (identifying, understanding, and analysing). *IEEE Control Systems Magazine*, Vol. 21, December 2001, pp.12-25. www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf
[15] 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.
[16] CVUT. *Czech Technical University in Prague, faculty of transportation sciences archives*.

Acknowledgement

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