Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 12, December - 2016

Model of Critical Nuclear Facility Safety Management

Dana Prochazkova
Czech Technical University in Prague,
Praha, Czech Republic
prochazkova@fd.cvut.cz

Jan Prochazka
Czech Technical University in Prague,
Praha, Czech Republic
prochazka@fd.cvut.cz

***Abstract*— The safe community is now at time of globalisation very dependent on a safety level of critical nuclear facility ensuring the territory by basic service necessary for humans´ live, which is the electric energy on which there are dependent supplies of good quality drinking water, utility water, information etc. Series of events from recent years connected with critical nuclear facility failures showed its high importance. The critical nuclear facility represents multistage mutually overlapping systems, i.e. big complex systems, the type of which is a system of systems. The paper presents the model for critical nuclear facility safety management based on the combination of principles: All-Hazard-Approach and Defence-In-Depth. It shows the way how to manage the safety of individual nuclear facility systems and the whole critical nuclear facility in time.**

Keywords—critical nuclear facility; provision of territory services; security; safety; model for nuclear facility safety management.

I. INTRODUCTION

For ensuring the human security and development, the safe human system is necessary [1-3]. Ensuring the safe human system is not easy, because the human system is a 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].

Mentioned interdependences are the sources of further vulnerabilities of human system that magnify the integral risk of a given system by increase of cross-section risks in the system of systems [4]. As a consequence of growing globalisation the new sources of disasters take on force, they also cause critical nuclear facility failures. The paper deals with problems of critical nuclear facility in the broadest concept, i.e. not only from the viewpoint of critical nuclear 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 nuclear power plants because they are clean sources of energy, but they need to operate them very carefully because nuclear accidents have 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 safe territory, the object of present paper is the critical nuclear facility safety that ensures the safe nuclear facilities that do not threaten neither themselves nor them vicinities, i.e. also another systems with which they are mutually interconnected or which they influence. The result of study, by help of methodology processed in the frame of project FOCUS [4] and the combination of principles: All-Hazard-Approach and Defence-In-Depth, is the creation of model of nuclear facility safety management in time.

II. CRITICAL NUCLEAR FACILITY

The critical nuclear facility includes 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, there are based on knowledge on defects in environs; the defects are illustrated by causal chain. The capability of active survival manifests by system behaviour, it considers uncertainty in projection of future defects and failures.

From the methodological viewpoint the critical nuclear 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 nuclear facility security, i.e. security of nuclear facility without regard to nuclear facility vicinity (security management); and a set of disciplines the target of which is the nuclear facility safety, i.e. security and development of both, the nuclear facility and its vicinity. Many professional works 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 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.

III. RELEVANT TERMS, NUCLEAR FACILITIES UNDER ACCOUNT AND SAFE CRITICAL NUCLEAR FACILITY

Regarding to present way of problem solving given above, we use two concepts for ensuring the safe entity [4]; i.e. security management and safety management. The first mentioned concept being simpler is more often used in practice; i.e. the target is the critical nuclear facility security and impacts of critical nuclear facility on its vicinity are out of interest. The other ensures both, the critical nuclear facility security and the security of vicinity of critical nuclear facility.

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

1. Each nuclear facility belonging to the critical nuclear facility and it alone 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 nuclear facilities and critical nuclear facility are the phenomena that caused damages and losses. They include phenomena belonging to the category „All-Hazards-Approach" [6] and specific phenomena connected with humans and their behaviour that do harm the both, the critical nuclear 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 nuclear facility vulnerability is a predisposition of nuclear facility (its protected assets) to harm / damage origination.
4. The nuclear facility resilience is a nuclear 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 nuclear facility risk is a probable size of losses, harms and detriment caused by a disaster with size of normative hazard (mostly design disaster) on nuclear facility and public assets or subsystems rescheduled on selected time unit (e.g.1 year), site unit (e.g. 1 km^2) and on basic assets of owners and operators of nuclear facility.
6. The nuclear facility security is a situation / condition at which the probability of nuclear facility assets´ harms, damages and losses is acceptable (it is almost sure that harms, damages and losses cannot origin).
7. The nuclear facility safety is a set of measures and activities for ensuring the security and sustainable development of nuclear facility, its assets and public assets.
8. The nuclear facility security management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded safe level of a nuclear facility (secured nuclear facility).
9. The nuclear facility safety management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded safe level of nuclear facility and its vicinity.
10. The nuclear facility safety engineering is a set of engineering measures and activities by which the nuclear facility safety is ensured in real conditions of a given site.

With regard to results from analyses of critical nuclear 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 energy from nuclear power plants for: water supply, sewer handling, transport system, communication and information systems, bank and finance system, emergency services (police, fire rescue service, medical rescue service), basic services (food supply, waste liquidation, social services, funereal services), industry, agriculture, state and regional administrations, that are usually supported by the national legislative. To them there is necessary to join the nuclear facilities for both, the education and the research, which is supported by the EU legislation.

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 nuclear facilities are: partial that include risks connected with individual protected assets; integrated that include risks connected with several assets aggregated by a defined way; and integral that include 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.

IV. METHOD OF NUCLEAR FACILITY SAFETY MANAGEMENT MODEL BUILDING

With regard to the present knowledge it is necessary to give that for nuclear facility safety management fundament, it is the risk analysis, risk assessment and trade-off with risks connected with mutual interconnections in nuclear facility sectors and in whole nuclear facility (i.e. in agreement with [4, 7] it is necessary to consider interdependences in a system of systems; i.e. at risk identification it is necessary also to use cross-sectional criterions). The procedure of work with risk is shown in Figure 1. 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. Feedbacks denoted in this Figure 1 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).

In present practice we distinguish five different concepts for work with system risks, Figure 2, which are summarized and described in work [4].

The assessment of criticality of individual systems (sectors) of nuclear facilities and the whole nuclear 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 nuclear facility criticality but it increases expenses etc.

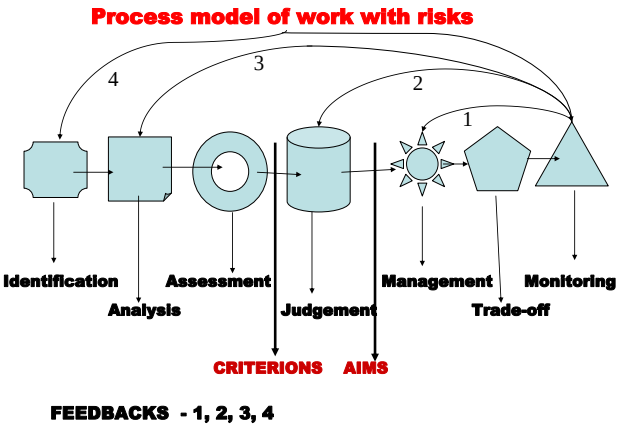

Fig.1. *Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks.*

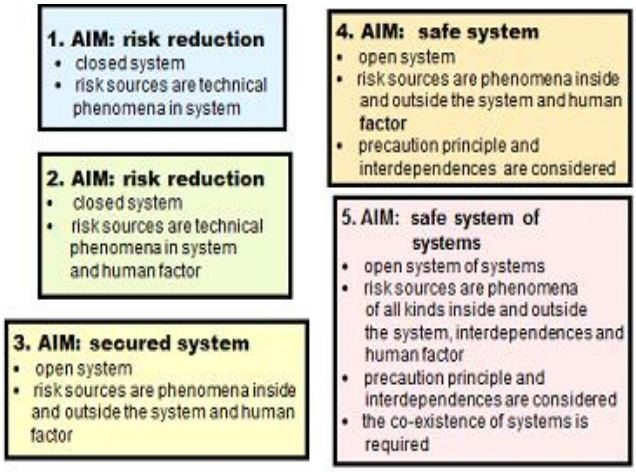

Fig.2. *Concepts of risk management and engineering trade-off with risks and their objectives, arranged in chronological order according to the introduction to engineering practice*

The purpose of model for nuclear facility safety management is to show basic steps by which it is possible to ensure nuclear facility security and nuclear facility vicinity security. The model building method goes out from a system concept of nuclear 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). The presented model is created by method of analogy to existing safety management models [3, 4 and 7].

At nuclear 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].

V. MODEL FOR NUCLEAR FACILITY SAFETY MANAGEMENT IN TIME

With regard to: data and knowledge in [3,4,7-14]; the concept promoted by the OECD [15]; the method described in works [4, 7]; and the assumption that each nuclear 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, i.e.: concepts and management; administrative procedures; technical matters; external cooperation; emergency preparedness; and the documentation and the investigation of accidents (Figure 3).

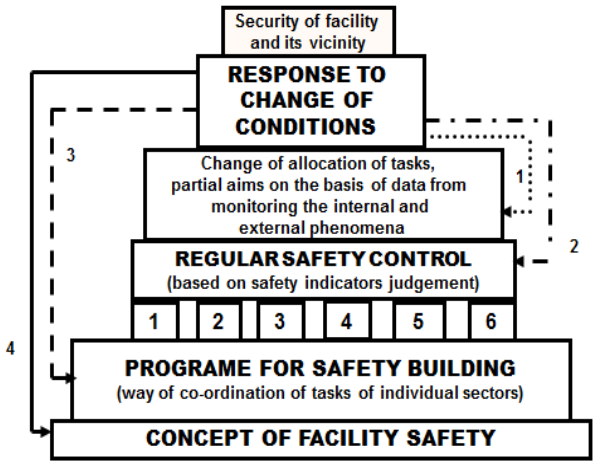

Fig.3. Model of management of nuclear facility safety; black block – concept for specification of important processes of nuclear facility; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4.

The 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).

Coordination of processes is targeted at ensuring the safe facilities under the conditions of normal, abnormal and critical (Figure 4).

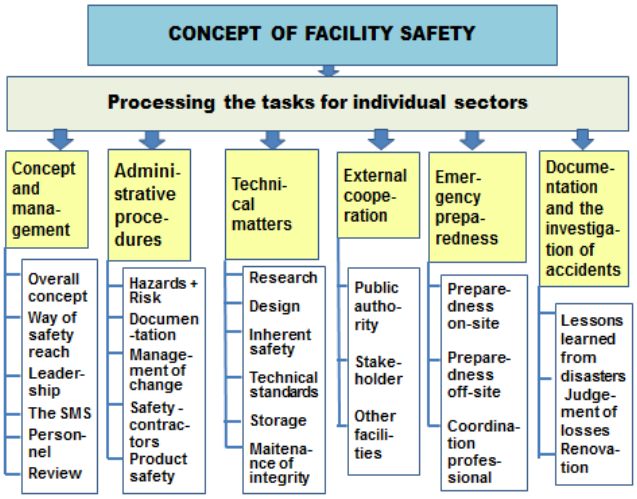

Fig.4. *Concept of facility safety and its main parts.*

From Figure 3 it follows that for each concept of nuclear facility safety it is necessary in the first to compile the programme for nuclear 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 nuclear 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 3 you can see that the application of feedback 4 means the change of 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 nuclear facility failure assessment shows that priority basic risks were omitted in original concept.

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 increase of 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 supply chain.
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 play certain roles and at safety realization they need to fulfil these roles.

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 interdependences and important partial risks of nuclear facility. In case that limits and conditions are not kept, it is necessary to perform changes as shown feedbacks in Figure 3. Because changes require 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 phenomena with catastrophic impacts, the feedback 4 is immediately realised.

Safety management system for 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 nuclear facility vulnerabilities at important disasters; determination of impacts of important disasters on nuclear facility. It creates a base for ensuring the safe nuclear 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 of 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 nuclear facility, i.e. the coordination of all pillars, i.e. processes directing to nuclear facility safety (PSM – process safety management).

Figure 5 shows the process safety management for facility. Figure 6 shows the domains that need to be kept in harmony for achievement of facility safety. Figure 7 shows the structure of plan ensuring the safe facility.

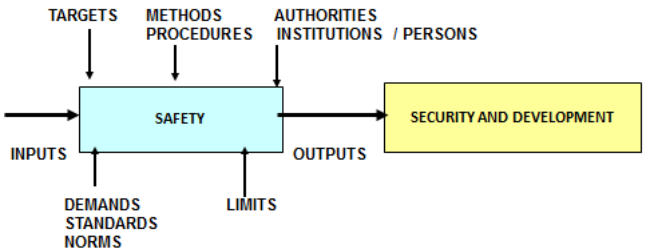

Fig.5. *Process of facility safety management.*

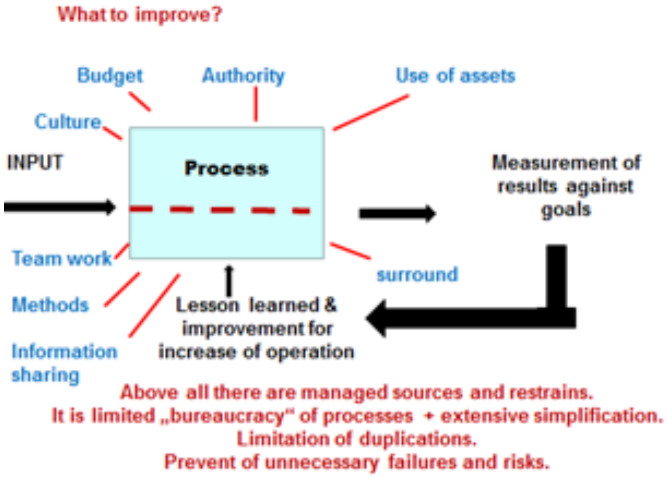

Fig. 6. The domains important for facility long-term safety achievement

Fig.7. *Structure of plan ensuring the safe facility.*

VI. RESULTS OF INSPECTIONS DIRECTED TO JUDGEMENT OF CONSISTENCY OF REAL FACILITIES SAFETY PERFORMANCE WITH DEMANDS OF IDEAL MODEL

1. The ideal model of safe nuclear facility was created by application of All-Hazard-Approach and Defence-In-Depth concept [4]. The comparisons of this model with real results of detailed inspections given in [16] show that:
2. Top safety management 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.
3. Interdisciplinary communication with connection over different safety management levels is missing.

4. Safety requirements are not solved in all domains; and therefore, some serious risks can be neglected.
5. Human faults are not often sufficiently considered.
6. The interdependences are not especially considered as the cause of failure of critical facilities.
7. Defence-In-Depth concept is missing for crucial objects in network.
8. Safety and security aspects are solved separately; mutual relations are not continually analysed.
9. Current legislative respects security only in some domains of railway system.
10. Relations and flows over boundaries of system under consideration are not solved.

VII. CONCLUSION

Model for safety management of nuclear 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,
- and the feedbacks by which it is possible to correct cases in which demands of safety are not fulfilled owing to dynamical development of infrastructure and its vicinity.

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

To ensure the critical nuclear facility safety during its life cycle including the human survival it is necessary to use: the mentioned concept of work with system risks which is directed to system of systems safety; to interface „All-Hazards-Approach" and "Defence-In-Depth" principle; safety management programme based on model of management of nuclear 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 1994, www.un.org.

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

[3] D. Prochazkova, "Strategic management of territory and organisation" (in Czech). ISBN: 978-80-01-04844. Praha: ČVUT 2011, 483p.

[4] D. Prochazkova, "Safety of complex technological facilities". ISBN: 978-3-659-74632-1. Lambert Academic Publishing, Saarbruecken 2015, 244p.

[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 (SLG) 101. Washinton: FEMA 1996.

[7] D. Prochazkova, "Analysis and management of risks" (in Czech). ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405p.

[8] EU, "FOCUS project". Brussels: EU. www.focus project.eu

[9] D. Prochazkova, "Criticality of transport facility" (in Czech). 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, "Critical facilities: What makes an infrastrucuture critical?" Report for Congress, 2003, CRS Web, Order Code RL31556.

[12] CISP, "Workshop on critical 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 facility and their interdependencies". In: Proceedings of the 37th Hawaii International Conference on System Sciences–2004. Sandia: Sandia National Laboratories 2004 http://ieeexplore.ieee.org/xpl/ freeabsall.jsp?ar number=1265180

[14] S. M. Rinaldi, J. P. Perenboom, T. K. Kelly, "Critical 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-inaldi.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.