

# Risk-Based Design of Socio-Cyber-Physical Systems

Dana Prochazkova  
Department of Energy  
Czech Technical University in Prague  
Praha, Czech Republic  
Email: Danuse.Prochazkova [AT] cvut.fs.cz

Jan Prochazka  
Department of Energy  
Czech Technical University in Prague  
Praha, Czech Republic  
Email: Jan.Prochazka [AT] cvut.fs.cz

**Abstract**— The aim of risk management of socio-cyber-physical systems at designing is the integral safety, which ensures their coexistence with their vicinity throughout their life cycles. On the basis of present knowledge and experience, part of risks that threaten socio-cyber-physical systems shall be mitigated by preventive measures during their designing and manufacturing. Due to dynamic changes of the world, the conditions of socio-cyber-physical systems at operation change. If changes exceed the socio-cyber-physical systems' safety limits which were inserted into their designs, the accidents or socio-cyber-physical systems' failures occur. The presented risk management plan is tool which ensures the prevention of such unaccepted situations and the safety.

**Keywords**- socio-cyber-physical system, design, failure, risk sources, safety, coexistence, risk management plan.

## I. INTRODUCTION

The human lives in modern society are made easier through socio-cyber-physical systems that are the result of the skill of human generations. However, all these positive consequences of technical progress on the human system functioning are redeemed by existence of a much larger number of risks that lead to: the failure of the State basic functions; safety level reduction; and disruption of coexistence of socio-cyber-physical systems (*further "SCPSs"*) with their surroundings. Coexistence generally means a common existence. The need for and the importance of coexistence is now under consideration in many technical fields [1-11]; the problem is discussed in detail e.g. in work [12].

The SCPSs consist of a series of parts that are interconnected and have object or network structures. Particular attention is currently being given to large-scale SCPSs that provide quality basic services to humans. They are complex and many of them ensure the fulfilment of the basic functions of the State, and therefore, the word critical is associated with them [13-17]. Engineering systems, from the simplest to the most complex, meet the daily needs and demands of citizens, and therefore, require targeted anthropogenic care.

Complex SCPSs belong to the different sectors management, and therefore, they greatly differ by the design and nature. Therefore, the criteria and measures for managing and settling their risks are sector-dependent, even if they have the same objective, namely safety. For reasons of great diversity, the procedures for building their safety are *site and sector-*

*specific*. Aspects important for designing the SCPSs parts and whole SCPSs are very diverse, especially those of: knowledge and technical matters, which predetermine the capacity possibilities of SCPSs; organizational and legal matters enabling the SCPS operation at a certain level of safety in the territory and over time; financial matters; personnel; social; and political at national and international level.

Based on the present findings [13,14], each engineering system is characterized by the structure, hardware, procedures, environment, information flows, organization, and interfaces among these components. The basic element of safe designing the SCPSs in the field of technical solutions is the application of safe elements (i.e. reliable, functional and non-threatening themselves and their surroundings) elements, their qualified interconnections and operating modes allowing safe (i.e. reliable and trouble-free) operation, and proper maintenance, back-up of priority parts of elements, components or systems, use of various back-up principles and thoughtful deployment of back-ups. Due to SCPS complexity, it is not enough to respects valid norms and standards, but it is necessary to apply the risk engineering principles. The paper shows the procedure of generation of risk-based design that was tested and has been already used in several cases.

## II. SUMMARY OF KNOWLEDGE ON SCPSs DESIGNING

Each territory has its own sources of risk [18], and therefore, both, the external and the internal sources of risks need to be addressed in relation to the design of the SCPS. Current knowledge shows that risks, which were not settled, cause for SCPS sooner or later losses, damage and harms in both, the public assets and on the SCPS assets [19].

SCPSs have form of objects or networks, and they represent complex systems, the form of which is a system of systems – SoS [1-12,14,20]. They include physical, cyber, organizational and social systems, i.e., individual devices, machines, components, systems, or entire production or service units. Knowledge and experience show that SCPSs are put in a certain environment, which in any case react to located SCPS. From safety reasons, these reactions need to be revealed in advance and considered in design to ensure human security.

The SCPS designing is covered by a wide range of problems, e.g.:

- theoretical analysis of critical processes, equipment and places
- proposal of practical implementation of technically and financially available countermeasures,
- selection of: materials; technical principles; construction procedures; determination of critical construction and mounting processes etc.,
- experimental verification of installed fittings and their operability under normal, abnormal and critical conditions,
- ensuring: durability, tractability of equipment and processes, required service life; quality and sufficient human resources, costs in the required amount, technical services; services etc.; and realization of buildings, structures and equipment under given conditions, etc. [12].

For human security, it is needed, so that environment reactions throughout SCPS lifetime would be adequate and its coexistence with surrounding may exist. The ensuring these aims needs to be inserted in the SCPS designing. Firstly, it is necessary to consider sources of all risks – All-Hazard-Approach [21]. To this set they also belong destructive phenomena that are results of all mutual reactions inside and outside SCPS under, normal, abnormal and critical conditions [12].

The identification of internal SCPS sources of risks associated on the one hand with individual technical equipment, their arrangement into components and systems, and on the other hand with production processes and their management, is a site specific activity which requires the risk identification at several levels, namely: technical equipment; components; systems; technical, organizational and cyber interconnections under normal operating conditions; technical, organizational and cyber interconnections under abnormal operating conditions; technical, organizational and cyber interconnections under critical operating conditions; and for high-important SCPS such as nuclear power plants, dams, etc., technical, organizational and cyber-operation interconnections under extreme operating conditions [13,14,22].

When identifying the SCPS risk sources, it is very important to consider all stable and mobile sources inside and outside the SCPS: fires (flash, pool, jet, fireball), explosions (mechanical, electrical, chemical, explosion of a cloud of gases – BLEVE or VCE, dust and, or nuclear), leakage of hazardous substances, because the damage will cause both, their impacts and their possible domino effects [6].

Each dangerous phenomenon can have different sizes and different occurrence probabilities, and therefore, it is important the hazard determination for each one. Because extreme dangerous phenomena occur rarely and irregularly, the hazard determination is one of principal steps at risk determination [20]. The hazard determination is technical-methodological method of determining the maximum expected disasters sizes. Because severe events occur randomly and irregularly and world dynamically develop in space and time (which also leads to changes in conditions that lead to disasters, and, of course, to changes in the very disasters'

characteristics), simple statistical methods cannot be used (their assumptions requiring stable processes are not fully fulfilled). Since we do not have enough knowledge of this area, we must consider existence of uncertainties, both random and knowledge-based, and to use methods based on the theory of extremes [23].

According to hazards curves we determine so call the design based disaster, which is dangerous phenomenon size, the occurrence probability of which is once during the time interval determined by legislation [20]. The parameters of design based disasters are used at technical facility project, construction, outfit by fittings, equipment components, systems and system of systems design. They create the SCPS terms of references. Their respecting ensures that SCPS has incorporate measures to prevent, mitigate and respond to unacceptable situations caused by internal, external and organizational sources of accidents and failures of elements, components and systems, namely for disasters' sizes lower than design disasters. They are key part of SCPS design documentation containing the technical, financial, time and other data determining the safe, reliable and functional SCPS. They create so called limits and conditions for safe SCPS operation [12].

According to data in [6,20], it is necessary to have in terms of references creation: knowledge of: regulations; risks in the site to which the SCPS is placed; technical system, which constitutes a SCPS; models and theories associated with accidents; methods of analysis, management and settlement of risks; and management of enterprise (finance, human resources, organization, technology, innovation...); competencies for: the application of results of methods of risk analysis and evaluation; implementation of methodology of analyzing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; transformation of policy into real actions; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; capability to find right information and lesson learned; critical analysis; designing the right solutions; communication; carrying out the synthesis and adapting the wording intended for the public; and ethics.

In terms of references creation, in the light of possible disasters in site and in connection with coexistence of SCPS with surroundings, it is necessary to specify: for each relevant disaster, size of threat according to given standards; identify critical tasks of SCPS from integral safety viewpoint; understand tasks and causes of their criticality; identified possible human failures; and propose measures for safety ensuring with regard to variable conditions.

Critical SCPS tasks from integral safety viewpoint are physical activities, by which operator contributes to: triggering the non-committed and unacceptable phenomenon; detection and prevention of phenomenon in question; management and mitigation of phenomenon in question; and response to emergency situation. At terms of references creating, it is necessary to consider that to criticality they also contribute: lack of communication (errors and interruptions in the flow of information); routine approach (certainty resulting from long-term practice in combination with risk awareness loss caused by

frequent repetitive activities and tired work); lack of knowledge (ambiguity or misunderstanding); distraction (confusion, mental chaos); lack of team collaboration (inconsistent efforts of a group of people due to a lack of belonging, fear of other mistakes, inappropriate leadership style or inappropriate communication); fatigue (it is ignored because people perceive it after it is excessive); lack of means (lack of resources, tools and materials, outdated documentation, inappropriate working conditions); coercion (from superiors or colleagues, lack of time, incorrect task settings); lack of self-esteem (inability to refuse to perform tasks resulting from lack of self-esteem, anxiety or complexes); stress (nervousness caused e.g.: time pressure, new methodology, change in the range of tasks, competitions or private factors); negligence (incorrect assessment of the possible consequences of action caused by e.g.: coercion, lack of experience or lack of knowledge); acceptability of a large number of deviations from instructions and standards in order to facilitate work.

The aim of SCPS design is to create a production process that is profitable, economic, safe and does not threaten public assets, especially humans and environment. This can be achieved by optimizing the safeguard, economic and functional criteria. SCPS design covers a wide range of problems, for example, it goes on selection of: materials; technical principles; construction procedures; framework procedures; determination of critical construction and framework processes; protection ways in domains physical, cyber etc. It, therefore, requires the participation of many different knowledge fields, i.e. the participation of a number of specialists from different fields. It should be remembered that here the human factor manifests. The low cooperation of experts leads to errors that will occur later at operation, e.g. they lead to: occurrence of organizational accidents [24]; maintenance problems [13,14]; impossibility to repair important parts [25] etc.

In each SCPS design from safety perspective, it is necessary to follow the requirements for: durability; manageability of equipment and processes; lifespan; human resources; costs; technical services; service; safety of employees, humans in surroundings and environment. Consideration and good provision of requirements in question determines the future costs of ensuring the safety and coexistence of technical facility with surroundings. E.g., non-provision of human resources for operation leads to limitation of production or service that is provided by the SCPS [12].

Designing the SCPS is a very complex activity, and in each country is regulated by national legislation (e.g. in the Czech Republic - the Act No. 183/2006 Coll.) and in some cases (e.g. nuclear installations) by international ones [26,27]. Research results [12] show: from safety viewpoint, the main goal is to avert unwanted combinations of incidents that have potential to cause accidents accompanied by major damages. To do this, proactive indicators or safety functions are used to control safety under border conditions, thereby the occurrence possibility of unlikely severe accident is reducing.

Seven principles of resilience are used: backup; to insert ability of sleek and controlled degradation; to insert ability to return from degraded state; flexibility in both, the system and

the organization; to insert ability to control limit conditions close to the performance interface; to insert optimal management models; to reduce complexity; and to reduce possible undesirable couplings. In design, it is necessary to include program for safety increase that ensures: safety and functionality of all fittings that corresponds to their missions; identification, evaluation, elimination or regulation of potential risks at acceptable level for important installations, systems and their various parts; risk management, which includes all possible disasters with resources inside and outside the SCPS that cannot be eliminated; protection of personnel, people in the vicinity, facilities and property; use of new materials or products and test techniques only in a way that is associated only with minimal risk; insertion of safety factors that ensure corrective measures that lead to improvement; consideration of all appropriate historical data on ensuring the safety generated by similar safety-enhancing programs.

From engineering viewpoint, conditions and limits of operation are established, safety systems (active, passive and hybrid) are installed and appropriate backups are ensured; it is solved: what safety systems are appropriate and what must be their backup; where / in which places safety systems operate most effectively; why they must be used just there and not elsewhere, in what limits they work reliably.

It is a fact that, at SCPS designing there are often used software based on tree models. Based on the current knowledge summarized in [20], it should be remembered that tree models do not create a basis for mastering all possible disasters that affect the whole SCPS, because they start on one point in the technical facility, for example, they do not consider impacts of external disasters, attacks and human factor.

According to [10,11,30-33], for the SCPS safety during the lifetime, it is necessary at designing to consider at each critical process the problems connected with: given process; designing a process; process management; operational staff and signaling its condition; safety management system; other technical systems promoting the safety; external active and passive systems for mitigating the risks leaded to process failure; SCPS emergency response; and SCPS surrounding response.

According to knowledge summarized in [14], it is important so that the processes risk management strategy may use: principles of inherent safety, e.g. [30,31]; and passive safety systems, active safety systems and different barriers types, procedural procedures that are proven or thoroughly tested in such a way that they do not contain latent sources of danger under possible conditions [12].

To ensure the important SCPS safety, the Defense-Depth principle is used [32]. The principle in question is implemented using a combination of several subsequent deeply independent levels of protection. The basic condition is - when one level of protection or barrier fails, the subsequent level must be available. When approach is well applied, so individual technical, human or organizational failure should not lead to devastating impacts, and a combination of several failures

leading to devastating impacts should have a low occurrence probability. Special attention must be paid to pressure equipment with dangerous substances [12,25].

From a professional viewpoint, safety document shall contain answers to questions: what may break down; what may not work (hazard identification and its analysis); how serious consequences (risk assessment) can be; what measures need to be taken to avoid this (risk management); what needs to be done when this occurs (emergency measures).

### III. DATA AND METHODS USED IN RESEARCH

For research, the original database of SCPS accidents and failures from world data was compiled [25] and several case studies were analyzed in great details in [12]. The database contains 7829 events from the whole world sources that were accessible in last 35 years to authors; 521 events originated due to mistakes in designing.

To reveal the event roots (risk causes), the collected data were processed by risk engineering methods: e.g. What, If; Checklist; Fishbone diagram; Case studies; Event Tree; FMECA; etc. [33]. Their results were critically assessed and separated into classes according similarity of causes and create the basis for Decision Support System enabling to multicriterial assessment of possible SCPS risks [12]. The results obtained from lessons learned from the risk impacts suppressions were also critically assessed and separated into classes according similarity of response tools and created the basis for Risk Management Plan that is based on the TQM management method [34] and it is recommended by ISO 31000 [35].

### IV. RISK CAUSES IN DESIGN

The causes of SCPS failures and accidents in database [25] were split up into categories: deficits in SCPS designing; deficits in performance of supervision by public administration; legislation deficit; and other. These categories were further subdivided; e.g.: the first one was designated into: errors in terms of references (e.g. omitting the critical disaster); errors in design (e.g. mistakes in concept of barriers; omitting of important norms and standards etc.); or legislation deficits into: low authority of public administration supervision; very general requirements on design, construction, outfit by technology equipment, testing and commissioning, etc.

The specific identified causes of SCPS failures and accidents found in a designing are omissions, errors and deficiencies in:

#### 1. SCPS design - factual area:

- errors in terms of references (e.g. not used the All Hazard Approach procedure; incorrectly determined hazard sizes of disasters; not applied Defense-In-Depth principle etc. – further ones in [12],
- errors in the project (an inappropriate building model used for calculations with regard to the conditions in the site, either too theoretical or general or not to settle

uncertainty and uncertainty; not properly used principle Defense-In-Depth principle),

- omitting the site vulnerabilities as e.g. large populations, existence of objects such as hospitals, schools, etc.,
- insufficient capacity sources of energy, water and sewerage,
- insufficient capacity of transport routes, lack of staff to operate, etc.,
- the non-determination of critical building sites, which led to omission of measures for risk management towards safety at normal operation – as barriers, on the basis of an assessment of the risks to their safety, i.e. barriers, backups – further ones in [12],
- the non-determination of critical building sites, which lead to omission of measures for risk management towards safety at abnormal operation conditions, – on the basis of an assessment of the risks to their safety, i.e. the risk assessment of their safety, i.e. barriers, backups – further ones in [12],
- the non-determination of critical points of technology and production processes, which led to omission of measures for risks management to safety, protection and dependability under abnormal and critical conditions - barriers, advances, principles to increase safety,
- they have not been considered and adequately addressed critical points of technology (pressure vessels and their equipment in which dangerous substances are or carry out hazardous reactions or pressured pipes, mainly those with hazardous substances) and places in which there is a risk of operator failure from the point of view of potential risks,
- failure to comply with good practice standards or the application of erroneous standards (which has led to the project being designed: inappropriate materials; inappropriate technical principles; inappropriate construction procedures; inappropriate design procedures; critical construction and construction processes have not been established and specific measures have been proposed for their quality design; equipment, machines, components and systems did not meet the safety, reliability and long-term functionality requirements, i.e. the safety, reliability and long-term functionality of the equipment, machinery, components and systems; durability and easy handling of equipment and processes; ergonomic requirements of the operator, service requirements, maintenance and financial costs associated with them are not respected; inappropriate placement of protective equipment and safety support systems; inappropriate technologies of construction, construction and assembly),
- in creation of design of automatic and semi-automatic control systems, there were deficiencies caused by insufficient knowledge or lack of cooperation of specialists from different disciplines or the use of faulty or imperfect IT tools,

- non-incorporation of technical measures for the basic physical and cyber protection of technical facility,
  - not considering the possibilities of changes in: laws during construction; system of taxation during the construction; interest system during construction; market situation – inflation, deflation, demand changes, etc.; support for technical facility by the State (e.g. when changing political representation); supplies of essential materials and technologies and relied on only one supplier, leading to problems in construction and operation – e.g. due to the lack of finance or unavailability of the material, some buildings and equipment were then ripped off.
2. Supervision of public administration over SCPS design:
- lack of public administration supervision, e.g. it did not ask for documentation on certification of SCPS safety in all important six stages of the SCPS referred to above,
  - neglecting the solution of sufficient capacity of local sources of energy, water and sewerage, transport routes and personnel in SCPS facility sitting and design,
  - neglecting the assessment of investor financial capacity in granting the relevant authorizations.
3. Inadequate legislation:
- insufficient public administration supervisory power,
  - insufficient legislation governing the design of SCPS (too general, incomplete, allows for several interpretations,
  - insufficient enforceability of the right to safety, employee protection, public protection and the environment.
4. Other:
- the State has not professional institution which has been able to professionally assess the process of making the SCPS in all aspects,
  - haste in design and construction due to pressure from politicians,
  - the State has not developed a system of supervision under design of SCPS,
  - the State did not have criteria for assessing the accuracy of the design of SCPS,
  - contractor and investor did not cooperate with the public administration during the design of the SCPS,
  - natural disaster occurrence as: earthquake; landslide; flood; fire,
  - occurrence of phenomena as: corruption; insider´ attack; hackers´ attack; terrorist attack.

## V. RISK MANAGEMENT PLAN

The risk management plan for design process is after prevention principles the second important tool for the SCPS design. For creating this top-quality safety management tool, they are considered both, the current knowledge and experience on risks associated with SCPS and their surroundings summarized in [12], and the new real knowledge, which were obtained from study of compiled original database of SCPS failures and accidents, among the causes of which they were found defects in the area of design; totally 521 cases were identified.

The aim of risk management plan is to ensure the SCPS coexistence with surroundings. Two actors are considered - public administration, which supervises activities in the territory including the SCPS with aim to ensure the safety of territory and citizens, and designer, who is responsible for the safety of design of SCPS, which also includes the protection of the surroundings and inhabitants. It is prepared in the form of table; Table 1 shows example for designing; complete table is are in [12].

TABLE 1. RISK MANAGEMENT PLAN FOR SCPS DESIGNING DIRECTED TO COEXISTENCE OF OPERATED SCPS WITH ITS SURROUNDING.

Risk area	Risk description	Probability of occurrence Risk impacts size	Risk mitigation measures
Public administration	As a result of absence of a State strategy on SCPS design focused on safety, it is possible to enforce current political interests, requirements of coercive groups or the failure to cope with extreme political situations (war, terrorist attacks), which in turn leads to reduction in human living standard and safety of citizens, economic instability, etc.	Probability: Large Impacts: Large	<b>Measures:</b> To develop the relevant State strategy and adapt the Building Act <b>Execute:</b> Prime minister <b>Responsibility:</b> Parliament chairman
	Due to lack of competence of public authority in overseeing the SCPS design there is an extension of construction, problems in commissioning, accidents accompanied by enormous expenditure from the public budget, disruption of citizens security.	Probability: Large Impacts: Large	<b>Measures:</b> To adapt the Competence Act and the laws associated with it. <b>Execute:</b> Prime Minister <b>Responsibility:</b> Parliament chairman
	As a result of errors in the authorized designer selection, the project is of poor quality, which sooner or later will disrupt the construction or operation and lead to accidents accompanied by enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	<b>Measures:</b> Change of designer <b>Execute:</b> Authorized investor worker <b>Responsibility:</b> Investor director
Future operator	As a result of a poor estimate in the field of supplier – customer relations, the project is based on unrealistic data, which sooner or later will lead to disrupts the construction or operation of a SCPS, enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	<b>Measures:</b> To force investor to perform remedy <b>Execute:</b> Authorized future operator worker <b>Responsibility:</b> Future operator director
Authorized designer	As a result of a poor quality or non-cooperative team of project processors, the project is of poor quality and it leads sooner or later to disruption of construction or operation, enormous expenditure, citizens safety and problems with public administration.	Probability: Medium Impacts: Large	<b>Measures:</b> To introduce rules for team cooperation <b>Execute:</b> Authorized designer team worker <b>Responsibility:</b> Authorized designer team director

Table 1 serves for protection against problems that impede to building permit issue. Table shows that big role plays the human factor, namely at way of execution of critical tasks of designing (terms of references compilation, use of knowledge on compilation of safe design etc.) and at professionalism of supervision performed by the public administration directed to public interest.

Risk management plan was tested with success at six medium SCPS [25]; their site-specific compilation and application in practice are ambitious on experts' knowledge and time, and it requires the access to detail SCPS and public administration documents, which is connected with respecting the certain legal rules.

## VI. PROCEDURE OF SCPS RISK-BASED DESIGN GENERATION

Based on the above facts, we have compiled a procedure for SCPS risk-based design compilation to respect applicable standards, practices of good practice and the above principles for working with risks. Since in many cases it is necessary also to consider the opposite criteria when deciding on a problem, we used both simple methods (linear and tree) and multi-criteria tool – the DSS in the work [36] when working with risks, for each component, the process of production and the entire facility, i.e. socio-cyber-physical system.

When deciding on specific items, we used both partial risks of critical components and systems and their interconnection, as well as integrated process risks and integral risk of the whole. We considered all the risk sources listed in chapter above, determined their sizes for the above items that had the

parameters required by the standards. For all relevant risk sources (in accordance with focus, we have considered the eight most common combinations of external risk sources) we have identified the threat size for the 1000-year interval for quiet sites (the size of risk sources of all kinds is acceptable and calculated in all construction and design standards), places at risk (with one to two larger sources of risk not foreseen in building and design standards) and critical sites (multiple sources of major risks, which is not foreseen in building and construction standards).

In the case of the second and third cases, the designer needs to think as follows:

1. Can I eliminate the hazard?
2. Can I reduce the size of this hazard?
3. Cannot I create a new hazard with the proposed measures to manage this hazard?
4. What technical and control systems are required to manage the hazard that is left?

In order to manage the SCPS safety according to [12,19] within the design it is necessary to create:

- conditions for shaping the culture of safety in the operation of the SCPS, which is implemented by: compliance with safety rules and procedures; the responsibilities of the managers; workplace running reporting systems; workplace audits; communication with employees; a proactive approach to risk management; taking care of a safe workplace, communications on safety, and training the employees.,
- the right loss prevention policy implemented by safety management (higher priority than reliability),
- a clear division of responsibilities (consistency between competences and responsibilities is important),
- the distribution of equipment, components and systems according to criticality,
- operating regulations for normal, abnormal and critical conditions,
- correct modes for the operation of equipment, components and systems, especially critical ones,
- summary of critical assets - their limits and conditions and requirements for risk based inspections (RBI),
- maintenance plan (preventive and forecasting for critical equipment, components and systems),
- modernization and renewal of equipment, components and systems, especially critical ones,
- a program of non-destructive tests of critical equipment,
- emergency (contingency) plans,
- a continuity plan that ensures the survival of the SCPS (mainly its critical items) under extreme conditions.

On the basis of above knowledge and experiences from practice [25,37], the technique for compilation of a risk-based design we propose by such way:

1. To establish a list of components and systems that comply with the standards and will be combined into sub-units.

2. For all items in the list of components and systems (point 1), to determine the limits and conditions from the point of view of their operation in a particular territory with regard to: the material from which they are made; demands on up-time; the working mode in which they will work; human factor; and possible other risks (internal fire or explosion and external risks).
3. For all items in the list of components and systems (point 1), to determine for the site-specific sources of risks determined by considering the All-Hazard-Approach, the sizes and characteristics of the partial risks.
4. For all risk sources (point 3) to determine impact scenarios; and when some risk impacts are not acceptable, it is necessary to increase the material and construction requirements so that these risks may be acceptable.
5. To establish the component interconnections and model of their interconnections, which meets standards and inherent safety requirements.
6. For all interconnections (point 5) to determine the limits and conditions from the point of view of their material composition, method of execution (loose, tight, or complex), methods of interconnection (welds, screws, rivets, seals, etc.) and the realization of possible other risks (internal fire or explosion, human factor and external risks).
7. For the risk sources (point 3) to determine impacts scenarios of partial risks for all interconnections and integrated risk for whole made up from jointed components; when the partial risks and integrated risk of whole made up from jointed components are not acceptable, it is necessary to increase requirements on material and construction of components interconnections so that these risks may be acceptable.
8. For the risk sources (point 3) to determine for the entire production process the process impact scenarios showing the integrated risk manifestation. In the case that the integrated risk is not acceptable, to increase the demands on design of: components of production process; working regime; and operators, so that the risks may be acceptable.
9. For the risk sources (point 3) to determine integral risk. If the risk is only conditionally acceptable (ALARP), then make modifications to the technology that will allow an immediate quality response that will ensure a return to normal state. In case of unacceptable risk, it is necessary to return to the adjustment of partial risks of components, systems and their interconnection (planned and even those that arise in the realization of sources of major risks) and the introduction of the principle of fail safely.
10. Considering the risk sources (point 3) to specify requirements for the steering system, that is for both, the I&C and the operators under normal, abnormal and critical conditions.

The above procedure of generation of SCPS risk-based design was tested with success at seven medium SCPS [25,37].

## VII. CONCLUSION

The quality of SCPS design predetermines its safety throughout the operation. Examples from practice show that some errors, such as underestimation of foundation conditions

or some errors in terms of references, cannot be removed after the construction completion and commissioning. They pose a danger under certain conditions (e.g. at flood or earthquake) and can only be mitigated by organizational measures that entail additional costs and do not have the ability to ensure safety level as correct measures at design stage [13,14,25].

The above-summarized knowledge and results of study of SCPS accidents and failures show that basis for ensuring the facilities safety at required life cycle is knowledge of: regulations (legislation, norms, standards) in context; risks in the site to which the technical facility is placed; technical system, which constitutes a technical facility; models and theories associated with accidents; methods of analysis, management and settlement of risks; and way of management that operator might use after commissioning (finance, human resources, organization, technology, innovation...).

Furthermore, it is necessary for all those involved to respect the public interest, to participate in building the safety culture and for managers to motivate employees to do quality work, even by their own example, as shown by the so-called "golden rules of safety" [29]. The grounds need to be inserted into the design.

An analysis of environmental development as well as development of political, social and economic situation in the world shows the need to be prepared for the resolution of cases and actions that will cause critical situations with impacts intensities higher than these today. In order to manage realization of risks which are inherent in present world using the adequate forces, resources and means, it should be had: principles for managing the emergencies and critical situations, especially those of a large range; allocation of resources; and allocation of responsibilities. The risk management plan is tool that gives overview on measures, the person who execute them and the responsible person for execution.

Since the design of a SCPS is complex, the Process Safety Management (PSM) should be required for rational management of each process and for complete management is required the Safety Management System (SMS) [13,16,29] for rational management of each process. For practice, twelve methodologies for public administration are presented at work [33]. Most of these methodologies can also be used for SCPS in the event of external risk sources. For internal sources of risk, specific investigations should always be carried out or procedures should always be applied to analogue SCPS where the conditions for technology transfer are met [38].

The results of the study [12,36,37] show that designer's competences are very important for: the application of the results of methods of risk analysis and evaluation; implementation of the methodology for analyzing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; the transformation of policy into a real action; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; finding the right information and learning; critical analysis; designing the right solutions; communication; carrying

out synthesis and adapting the wording intended for the public; and ethics.

At each decision in favor of safety it should be remembered: all factors and processes that can be dangerous and how often they can occur; how large their impacts can be; how the size of the impacts or frequency of occurrence can be reduced; whether the proposed measures cannot be a source of new hazards; and which technical and control systems can be controlled by hazards that cannot be prevented.

Finally, it should be noted that, in line with the results at work [14], it is essential what is the political will to create a system to protect against unacceptable impacts of harmful phenomena, i.e. natural and other disasters. An analysis of environmental development as well as the development of the political, social and economic situation in the world shows the need to prepare for the resolution of cases and actions that will cause critical situations by the intensity of impacts, and these are phenomena that do not today have such cruelty (severity) in the followed territory. Therefore, in terms of human security, the development of the human system, the existence, stability and development of the State, the concept of human safety and the subsequent concept of development must be codified and implemented through the management of safety into practice. In order to manage the realization of the risks, which are inherent in the present world using adequate forces, resources and means, it should be had: management principles for managing emergencies and critical situations, especially those of a large range; allocation of resources; and allocation of responsibilities.

The research showed that:

- each technical facility design has a certain danger. The designer art is to select such solution that is optimal, i.e. it is sufficiently safe and it is possible to realize with regard to investor and public administration options. The near the same holds for manufacturer's skill (craftsmanship) at realization,
- impressive and low robust designs with insufficient safety margins often fail sooner or later,
- wrongly determined limits and conditions for critical technical facility parts lead to frequent disturbances up to serious accidents; they are not able to react to condition changes.

The analysis of accessible legislations [25] revealed that rules in force do not require to follow operation process safety in designing, and this occasionally leads to problems at operation, which is revealed e.g. in [19]. Based on authors' experiences from practice [25,37], they compiled procedure for generation of SCPS risk-based design. There is continued the procedure implementation in practice and its improvement.

#### ACKNOWLEDGEMENT

Authors thank for the EU grant; project RIRIZIBECZ.02.2.69/0.0/0.0/16-018/0002649.



REFERENCES

- [1] B. Ale, I. Papazoglou, E. ZIO, "Reliability, Risk and Safety". London: Taylor & Francis Group 2010, 2448p.
- [2] M. Beer, E. Zio, "Proceedings of the 29<sup>th</sup> European Safety and Reliability Conference". Singapore: ESRA 2019, e:enquiries@rpsonline.com.sg
- [3] C. Bérenguer, A. Grall C. Guedes Soares, "Advances in Safety, Reliability and Risk Management". London: Taylor & Francis Group 2011, 3035p.
- [4] R. Briš, C. Guedes Soares, S. Martorell, "Reliability, Risk and Safety. Theory and Applications". London: CRC Press 2009, 2362p.
- [5] M. Cepin, R. Bris, "Safety and Reliability – Theory and Applications". London: Taylor & Francis Group 2017, 3627p.
- [6] S. Haugen, J. Vinnem, A. Barros, T. Kongsvik, A. Van Gulijk, "Safe Societies in a Changing World". London: Taylor & Francis Group 2018, 3234p.; <https://www.ntnu.edu/esrel2018>.
- [7] IAPSAM, "Probabilistic Safety Assessment and Management Conference". Helsinki: IPSAM & ESRA 2012, 6889p.
- [8] T. Nowakowski, M. Młyńczak, A. Jodejko-Pietruczuk, S. Werbińska-Wojciechowska, "Safety and Reliability: Methodology and Application". London: Taylor & Francis Group 2014, 2453p.
- [9] L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger, "Safety and Reliability of Complex Engineered systems: ESREL 2015". London: CRC press 2015, 4560p.
- [10] R. Steenbergen, P. Van Gelder, S. Miraglia, A. Vrouwenvelder, "Safety Reliability and Risk Analysis: Beyond the Horizon". London: Taylor & Francis Group 2013, 3387p.
- [11] L. Walls, M. Revie, T. Bedford, "Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016". London: CRC Press 2016, 2942p.
- [12] D. Prochazkova, J. Prochazka, J. Lukavsky, V. Beran, V. Sindlerova, "Management of Risks of Processes Connected with Manufacturing and Commissioning Technical Facility". Praha: CVUT 2019, 207p. <http://hdl.handle.net/10467/84466>
- [13] D. Prochazkova, "Safety of Complex Technological Facilities". ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244p.
- [14] D. Prochazkova, "Principles of Management of Risks of Complex Technological Facilities". ISBN 978-80-01-06180-0, e-ISBN 978-80-01-06182-4. Praha: CVUT 2017, 364p. <http://hdl.handle.net/10467/72582>
- [15] D. Procházková, "Critical Infrastructure Safety". ISBN 978-80-01-05103-0. Praha: CVUT 2012, 318 p.
- [16] D. Procházková, "Principles of Management of Critical Infrastructure Safety". ISBN 978-80-01-05245-7. CVUT, Praha 2013, 223 p.
- [17] D. Procházková, "Challenges Connected with Critical Infrastructure Safety. ISBN 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.
- [18] D. Procházková, "Risks Connected with Disasters and Engineering Ways of Their Managements". ISBN 978-80-01-05479-6. Praha: CVUT 2014, 234 p.
- [19] D. Procházková, J. Procházka, J. Lukavský, V. Dostál, Z. Procházka, L. Ouhřabka, "Management of Risks of Processes Connected with Technical Facilities Operation during Life Cycle". ISBN 978-80-01-06675-1. Praha: CVUT, 465 p. <http://hdl.handle.net/10467/85867>  
doi:10.14311/BK.9788001066751
- [20] D. Prochazkova, "Analysis and Coping with Risks Connected with Technical Facilities". Praha: CVUT 2018, 222p. <http://hdl.handle.net/10467/78442>
- [21] FEMA, "Guide for All-Hazard Emergency Operations Planning". State and Local Guide (SLG) 101. Washington: FEMA 1996.
- [22] M. Rausand, "Reliability of Safety-Critical Systems: Theory and Applications". John Wiley & Sons 2014.
- [23] W. Epstein, "Not Losing to the Rain: What I Learned when I Learned about Onagawa". In: Safety and Reliability of Complex Systems. London: Taylor & Francis Group 2015, pp. 365-371.
- [24] J. Reason, "Human Error". Cambridge: University Press 1990.
- [25] CVUT, "Database on World Disasters, Technical Entities Accidents and Failures – Causes, Impacts and Lessons Learned". Praha: CVUT 2021.
- [26] EU, "Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities". Brussels: EU 1982.
- [27] IAEA, "Safety Guides and Technical Documents". Vienna: IAEA 1954–2020. [www.ns.iaea.org/standards](http://www.ns.iaea.org/standards)
- [28] COMAH, "Safety Report Assessment Manual: COMAH". London: UK – HID CD2 London 2002, 570 p.
- [29] 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.
- [30] A. M. Heikkilä, "Inherent Safety in Process Plant Design. An Index-Based Approach". Helsinki: VIT 1999, 132 p.
- [31] T. Kletz, "Process Plants: A Handbook for Inherently Safer Design CRC". London: Taylor & Francis Group 1998.
- [32] INSAG, "Defence in Depth in Nuclear Safety. INSAG-10". Vienna: IAEA 1996.
- [33] D. Prochazkova, "Methods, Tools and Techniques for Risk Engineering". Praha: CVUT 2011, 369p.
- [34] M. Zairi, "Total Quality Management for Engineers". Cambridge: Woodhead Publishing Ltd. 1991.
- [35] ISO, "Risk Management – Principles and Guidelines". ISO 31000:2009.
- [36] D. Prochazkova, J. Prochazka, "Risk Management at Technical Facilities Designing, Building and Commissioning". ISBN 978-80-01-06716-1. Praha: CVUT 2020. [dSPACE.cvut.cz http://hdl.handle.net/10467/87491](http://hdl.handle.net/10467/87491), <https://doi.org/10.14311/BK.9788001067161>
- [37] D. Prochazkova, J. Prochazka, "Tool for Risk Reduction at Specific Component Aircraft Engine Welding". Proceedings of International European Safety and Reliability Conference, ESREL2018. ISBN 978-0-8153-8682-7 (Handbook). London: Taylor & Francis Group 2018; ISBN: 978-1-351-17466-4 (eBook); <https://www.ntnu.edu/esrel2018>; pp. 3135-3142
- [38] D. Procházková, "Examination of Core of Complaints and Conflicts Concerning Technical Solutions: Kontrola MSK CR, v. 5, No 6, 1992. MSK CR Praha, 95p.