Tool for Risk-Based Operation of Socio-Cyber-Physical Systems

DANA PROCHAZKOVA, JAN PROCHAZKA
Department of Energy
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6

Abstract: - The aim of risk management of socio-cyber-physical systems at operation is the integral safety which ensures their co-existence with their vicinity throughout their life cycles. On the basis of present knowledge and experience, part of risks that threaten socio-cyber-physical systems is coped by preventive measures during their designing and manufacturing. Due to dynamic changes of the world, the conditions of socio-cyber-physical systems at operations 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 correct response to such unaccepted situations and fast ensuring the safety.

Key-Words: - Socio-cyber-physical system, operation, failure, risk sources, safety, coexistence, risk management plan.

1 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.

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 [1-5]. 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, 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 operation of SCPSs parts and whole SCPSs are very diverse, it especially goes on 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 [1,2], each engineering system is characterized by the structure, hardware, procedures, environment, information flows, organization, and interfaces among these components. The safe SCPSs operation means operation which is reliable, functional and does not threatening themselves and their surroundings. The basic element of safe operation of SCPSs in the field of technical solutions is the application of safe technical 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 technical fittings, components or systems, use of various back-up principles and thoughtful deployment of back-ups.

Paper concentrates to ensuring the complex SCPSs´ safety during their operation and puts the tool, i.e. the risk management plan for operation

2 Summary of knowledge on complex SCPS

Large and complex SCPSs include: power plants, industrial plants, dams, airports, railway stations, warehouses, hospitals, large shopping centres, banks, information networks, large cultural or sports centres, etc. (including the complex systems as health protection system, banking system, legal system etc.). These SCPSs belong to the management of various sectors and their aim is to ensure the quality of life of humans. As already mentioned, they include physi-

cal, cyber, organizational and social systems, i.e. individual equipment, machines, components, systems or entire production or service units.

Due to SCPSs complexity the behaviour of the whole cannot be inferred from the behaviour of individual parts, and under certain conditions there are unexpected phenomena that lead to the destruction or failure of the functionality of a given of SCPSs [1,2]. It is about: suddenly emerging features of behaviour that cannot be derived from knowledge about the behaviour of components (it is so-called emergence); hierarchy; self-organization; and a diversity of management structures that together resembles chaos.

Therefore, in order to ensure the safety of complex SCPSs, it is necessary to use approaches from many branches and interdisciplinary [1,2,4] so it would be ensured: their existence (ability to ensure balance); their efficiency (ability to cope with resource shortages); their freedom (ability to handle challenges from around); their security (ability to protect yourself from phenomena inside and outside); their adaptation (ability to adapt to external changes); and their integral safety which ensures the coexistence (the ability of system to change its behaviour so that the behaviour responds to the behaviour and orientation of other systems and so that it may not endanger them, and they may not endanger it).

The applications of technical norms, standards and best practices procedures reduce the vulnerability of buildings and infrastructures, and by this the risk size. The main problem of our times are complex SCPSs, which represents a system of systems (i.e. the set of open overlapping systems) for which we today only look for measures to reduce their vulnerabilities with respect to individual elements. From safety reasons of the whole, it is necessity to find principles to reduce vulnerability across different systems and across systems of systems [6], i.e. to increase their resiliencies.

The problem of the complex system vulnerability in a certain area is however dependent on local conditions, and therefore, it is not possible to outline its general solution [16].

From the point of view of current knowledge [1,2,4,5], there are now at least two tasks:

- to solve the problem of the functionality of a set of interconnected (i.e. dependent) objects and infrastructures under normal, abnormal and critical conditions,
- to look for critical conditions of complex SCPSs that are unpredictable or are the result of a serious operator errors, and under certain conditions they may go to highly non-demanded, i.e. highly unacceptable situations, i.e. situations in which the very existence of SCPS, or even humans, is threatened, and which we usually refer to as crisis.

The SCPSs safety as a whole is the level of measures and activities by which risks are managed and settled [7,8]. The SCPS risk management is a structured, consistent, and continuous process across the whole SCPS for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the safety, which is strategic goal. On opportunities and priorities at decision-making on risks, the context and way of work with risks play main role. The aspects playing the main role at risk management are shown in Figure 1.

Safety needs to be an integral part of the business activities of the SCPS owners. All SCPSs shall be managed in such a way that the occurrence of accidents affecting the safety is minimal. It is about integral safety [6] - all activities and efforts of managers and employees need to be directed towards this. The key elements for the objective in question are mutual cooperation, open communication and regular monitoring of the achievement of safety objectives [1,2,4,9,10]. On the basis of the current requirements enshrined in the legislation of developed countries, owners and operators of technical facilities need to:

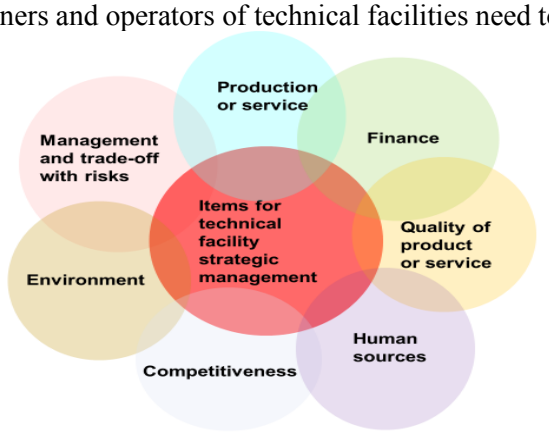

Fig. 1. Items determining the SCPS safety and development (i.e. also competitiveness during the life cycle).

1. Safety needs to be an integral part of the business activities of the SCPS owners.
2. All SCPSs shall be managed in such a way that the occurrence of accidents affecting the safety is minimal.
3. It is about integral safety [6] - all activities and efforts of managers and employees need to be directed towards this. The key elements for the objective in question are mutual cooperation, open communication and regular monitoring of the achievement of safety objectives [1,2,4,9,10].

On the basis of the current requirements enshrined in the legislation of developed countries, owners and operators of technical facilities need to: promote

safety as a whole part of their business activities and promote safe activities; actively search for safety information; cooperate with administrations and other entrepreneurs in order to improve safety; create, together with other SCPSs, the conditions for joint response and mutual assistance; and create professional organizations to provide a platform for the exchange of knowledge and experience.

Public administration needs to set safety objectives, to establish a clear and holistic framework for safety management and, through appropriate inspections and enforcement measures, to ensure that all relevant safety requirements are met.

The safe operation of SCPS depends on a number of diverse aspects [9-11], such as the training of the serving staff, the organization of technological components and their interconnections, the process of works, cooperation and how to understand the situation of the service personnel.

In view of the current knowledge, it is necessary to monitor in the SCPS internal dependencies, which mediate the secondary and other impacts of disasters on the protected assets of SCPS and its surroundings. To achieve this, it is necessary [1,2,9,10], to:

- put into practice safety monitoring,
- develop and codify methodologies for data collection, their professional processing necessary for risk management in the system of systems,
- develop risk decision-making methodologies and linked control-list systems to support decision-making,
- develop for employees sets of measures on what to do before, at and after the occurrence of the risks, which in the technical facilities belong among specific or even critical risks,
- develop plans for the strategic SCPS management aimed to security and development, emergency plans, continuity plans and crisis plans of the technical facility, which shall be interconnected and in which safety and development management tasks are underpinned at all times,
- ensure support systems for the qualified SCPS safety management because skilled solutions always save money, strength and resources. The knowledge so far shows that simplified solutions are only possible sometimes, but even in cases where they are possible, it is necessary to know what simplifications have been made, why they could be applied and whether there is no need to take further action after some time.

In the case, in which there is no effective defence of SCPS against a disaster, i.e. against realization of significant risk, SCPS management need to be prepared to response. It means that the SCPSs need to have prepared procedures in place to ensure a response to the situation aimed at stabilizing the affected part of SCPS and restoring the critical processes and resources for their implementation [6].

Emergency planning does not reduce risks and needs to be tailored to whose, who perform both, the response and the follow-up recovery. It is by no means a cheap thing. It is about ensuring that the knowledge set is organized and each responsibly managed institution had a security concept. This shall be based on the classification of emergencies and a risk analysis aimed at determining expectations of what impacts are likely in the event of a disaster of expected (legally defined) size [6].

3 Technical facility operation conditions

Each SCPS and its surroundings change over time, these changes are not all over synergic, and therefore, they also change their mutual interactions. From the human security and development viewpoint, it is important so these interactions throughout the SCPS life cycle should be adequate. They may not only cause new sources of risks that would significantly undermine the conditions necessary for the human lives, but also cause the situations that human society would not have the capacity to deal to its advantage.

The humans already find out that due to the SCPSs´ and the world´ complexities and time changes in conditions, that they do not have the ability to influence this fact. Therefore, the SCPSs accidents and failures are a reality with which the anthropogenic management needs to deal [12].

In order to ensure security for human society and other public assets, it is, therefore, necessary to have the tools to reveal risk sources and to manage emergencies so that their impacts on public assets and on SCPS itself may be minimal. It should be remembered that in critical situations, the solution is not a " to sacrifice the technical facility", i.e. to carry out measures and activities that completely destroy it, since the SCPS supplies products or provides services, employs humans and is a source of economic capital for given territory. Therefore, serious risks should be managed with targeting the SCPS safety in all possible conditions [7,8]. However, our research shows lacks in awareness on risks, especially among managers and politicians [6].

Because SCPSs are complex systems, their behaviours cannot be inferred from the behaviour of individual parts and, under certain conditions, there might occurred unexpected phenomena that lead to the destruction or failure of the SCPS functionality. They are result of: a sudden emerging the behaviour

feature that cannot be derived from knowledge of components´ behaviour; hierarchy; self-organization; and diversity of management structures, which together resemble chaos [1,2].

Due to SCPSs complexity, it is necessary to understand integral safety. Great attention needs to pay to interconnections and existing flows among different parts and sectors that manage partial subsystems. At one system failure, interconnections can have unforeseen the consequences in form of chain reactions (cascades) and domino effects accompanied by failure, or by gradually failing other important systems and services; e.g. power outages can cause outages in drinking water supplies, food supplies, heat supply, fuel, failure of transport infrastructure, failure of management and information technologies for the functioning of the banking sector, state administration and emergency services, etc. [1,2].

The suitable solution offers the use of SCPS risk-based design (integral safety concept) [13], the root of which is: to consider the priorities in assets and all phenomena that can damage the territory and SCPS; and at each reducing the costs clearly to determine what risks can been neglected by fact that facility, fittings or equipment is only considered as a secure system or only a reliable system [2,13].

Risk-based SCPS operation [6] requires to: monitor priority risks and conditions of critical fittings, components and personnel; keep rules for safe operation at all organization levels; permanently increase safety by help of special strategic program; perform risk-based inspections on critical fittings, components and systems; realize condition-based maintenance; systematically improve safety culture; be prepared for response to all expected emergencies in all aspects connected with response and for ensuring the operation continuity under abnormal and critical conditions; use optimal working modes; motivate personnel; have necessary reserves in all important items; systematically co-operate with public administration, organizations using the same technology and research organizations; be able to install technological changes if necessary; and have risk-management plan for responses to all kind critical situations.

Analyses of risk engineering tools summarized at [6] and the experience gathered [14] show that risk management tools depend on many factors. At SCPS strategic management, it is necessary to consider both, the safety and the long-term functionality. This means that two facts need to be considered: SCPSs are complex multi-level systems; and the specific sources of some risk are not the same at all technical facility levels.

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

In terms of needs and economic use of resources, it is true that in a number of practical tasks it is sufficient to consider only certain sources of risk, because the aim is a safe machine and not the whole SCPS and its surroundings safety. Therefore, for each risk-related work task, it is important to determine the risk management objective. At the same time, it is important to follow that certain technical equipment (insurance valves, drain valves, etc.) or certain SCPS components (pressure vessels, reactors, control systems, etc.) are essential for integral SCPS safety, and therefore, at them it is not sufficient at them to work with risks only from the point of view of entity itself, but it is necessary to work with risks that are also important in terms of whole SCPS safety. It goes on critical elements, critical equipment, critical components and critical technical facilities systems [1,2,4,5,15] that require special work with risks in sitting, designing, construction and operation.

Depending on SCPS complexity, four risk-related objectives are distinguished: fittings safety; operation safety; process safety (component operation, production line); and entity integral safety.

4 Risk sources

For research, the original database of SCPS accidents and failures [14] from the world data was compiled and several case studies were analysed in great details [6]. The database contains 7829 events from the whole world sources that were accessible in last 35 years to authors; more than 90% events originated during the technical facilities operation. To reveal the event causes (risk realized), the collected data were processed by risk engineering methods: e.g. What, If; Checklist; Fishbone diagram; Case studies; Event Tree; FMECA; etc. [16] in dependence of data quality and amount. They were also considered get-at-able results of other authors [6,17-22].

The results of these methods were critically assessed and separated into classes according similarity of causes and created the basis for Decision Support System enabling to multicriterial assessment of possible technical facility risks [6]. The obtained results on lessons learned from risk impacts suppressions were also critically assessed and separated into classes according similarity of response tools and created

the basis for risk management plan, which is shown hereafter.

Detail database accident and failure study [6,14] shows that causes of technical facilities accidents and failures belong to categories: natural disasters; outages of external infrastructures that are important for technical facility operation; internal disasters as outages of internal critical infrastructures, critical fittings malfunctions, bad maintenance etc.; top management errors; project management errors; process management errors; low level of operation provisions; errors in technical fittings operation regime and maintenance; insufficient control of fittings and component conditions; bad safety culture; insufficient training, motivation and workmanship of workers; bad working conditions or regime; errors in cyber concept, fittings and nets in automatic and semiautomatic systems supporting the management decision; bad public administration supervision; insufficient legislation with regard to technical facilities safety; attacks of hackers, terrorists, insiders etc. The scheme is in Figure 2. Detail division of individual categories is in [6].

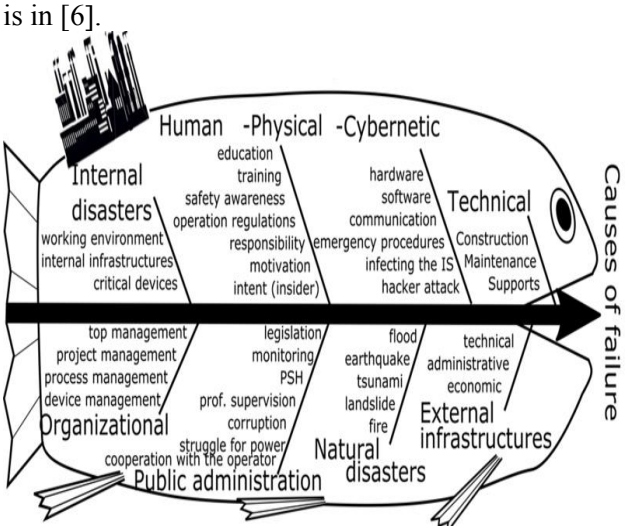

Fig. 2. Basic categories of risk sources associated with the technical facilities operation which lead to the failures of the coexistence of technical facilities with surrounding areas during their operation; IS = information system; PSH = personnel safety and health.

The SCPSs accidents and failures research [6,23] shows that their originators except of great natural disasters are:

- large mistakes in risk prevention made in technical facility terms of references, designing and operation,
- origination of small mistakes, the nearly contemporary realization of which in short time interval is dangerous.

It means that both these factors need to be managed. For management improvement, two tools were developed, namely decision support system and risk management plan [6].

5 Method of risk management plan construction

The risk management plan is risk engineering tool that ensures SCPS and public administration preparedness for emergency situations. For each serious risk source, it shows not only risk characteristics and impacts but also real mitigation measures for response that are prepared in detail in all important domains, including the real persons who perform measures and also persons who are responsible for measures application.

The risk management plan is recommended by ISO 31000 [24]. It is based on the TQM facility management method [25]. In monitored SCPS, they are considered priority risks that could not be settled and that have the potential to significantly damage SCPS at their realization.

To develop a risk management plan that meets the management requirements required by the TQM, it is necessary to know in detail: disasters, i.e. sources of risks; local vulnerabilities that determine the severity (criticality, relevance) of critical situations; and possibilities of response in critical situations.

The plan itself is drawn up in the form of a table, in which they are followed:

- domains of risk causes (technical, organizational, internal, external, cyber, legal, education, training etc.),
- description of risk,
- risk assessment results: the probability of risk occurrence and the expected magnitude of the impacts of the risk on the protected assets (basic public assets should also be considered based on legislative requirements),
- risk mitigation measures, which are clearly identified, and at each of them it is given responsible person for their implementation.

Due to reality that for SCPS safety, they are responsible both, the SCPS and the public administration, so that they are distinguish according to duty to ensure qualified response: interface of public administration and SCPS management; and SCPS management. They are followed: internal sources of risk of SCPS related to its construction, construction, equipment and operation; errors of SCPS management; errors of SCPS personnel; external sources of risk of SCPS associated with natural disasters; external sources of SCPS risks related to public administration behaviour, competition, market, etc.; attacks on

SCPS; cybernetic risks associated with networks; and war.

For construction of risk management plan, we use the DSS [6], which revealed root risk sources that led to accidents and failures at SCPSs operation.

6 Risk management plans for SCPS operation

Research described in [6,14] showed that in order the risk management plan would fulfil its role, it needs to be based on quality data processed by experts using quality methods and it shall have a foothold in legislation that ensures properly distributed competences and forces accountability, thereby contributing to the building of safety culture in society. The risk management plan helps to resolve conflicts, because in the event of an expected conflict of interest, it can be in advance: agreed the objectives of solving the problems caused by risk realization; established the relevant responsibilities; and codified the resolution procedures.

The SCPS good management is based on the openness, accountability and efficiency of SCPS management and public administration in decision-making and other processes. It means transparency, accountability, integrity, the appropriate type of governance, efficient and affordable services, a commitment to partnership and the continuous development [11]. It has five basic features: openness; public involvement in decision-making; responsibility; efficiency; and the coherence of strategies and real activities. In management, it holds that the manager (officer) on higher position has higher responsibility on solving the problems connected with the organizational, technical, economic, operational and other matters.

The essence of good integral SCPS safety management lies in the combination of different levels of decision-making as opposed to the almost exclusive role of the State. As a result, decision-makings shift to multi-level structures and both, the SCPS management and the public administration management, represent the hierarchical interconnected systems [6]. At management execution, project and process managements are applied; both are based on the strategic development plan [4].

Risk management plan is a tool for ensuring the SCPS preparedness management of risks directly related to it and risks associated with interconnection of SCPS – the territory; and for public administration pays the same. Therefore, the compiled risk management plan is linked to continuity plan [6].

The SCPS continuity plan is a plan for such SCPS response which ensures the limited operation of the SCPS and its survival in such a condition (state) that it can be gradually restored [4-6].

On the basis of the data collected (data on the causes of accidents and failures of technical facilities during operation, and relevant lessons learned from SCPS responses [6,14]), the risk management plan for the SCPS operation is compiled. In it, two areas are considered: sources of risks in territory which have potential to cause SCPS accident or failure; and sources of risks within SCPS which have potential to cause SCPS accident or failure with impacts that they may cause loses and damages in surroundings. From these facts it follows that plan is site specific. Table 1 shows examples of selected parts of this plan; the complete plan is in [6].

Table 1. Risk management plan to ensure the coexistence of operated SCPS facility with its vicinity.

Risk source	**Description of risk**	**Occurrence probability Size of impacts**	**Measures for risk mitigation**
Beyond design natural disasters	Losses, damages and harms connected with public assets and technical facility assets – big accident in technical facility that worsen losses, damages and harm in surrounding.	Probability: low Impacts: Great	***Measures:*** Crisis plan of State, region and municipality. ***Execute:*** Government chairman / Region chairman / Municipality mayor. ***Responsibility:*** Region chairman
Broad fire outside the SCPS	Fire can affect the SCPS and cause big accident.	Probability: medium Impacts: Great	***Measures:*** Crisis plans of municipality. ***Execute:*** Municipality mayor. ***Responsibility:*** Region chairman .

Failure of critical infrastructures in SCPS vicinity	In case that sufficient internal sources are missing, the SCPS accident or failure can occur or emergency regime would be necessary.	Probability: medium Impacts: great	***Measures:*** Crisis plan of region and municipality. ***Execute:*** Region chairman / Municipality mayor. ***Responsibility:*** Region *chairman.*
Lack of labour force for SCPS	Due to lack of qualified labour forces, the SCPS cannot fulfil tasks and services, which leads to discontent and losses, also in state budget.	Probability: medium Impacts: Great	***Measures:*** Recruitment of workers abroad. ***Execute:*** Government chairman. ***Responsibility:*** Parliament chairman.
Insufficient political culture (manifestation of fight on power among political rivals)	Conditions for SCPS are unfavourable, because support for its activities misses.	Probability: great Impacts: Great	***Measures:*** Introducing the clear rules for safety culture in public sphere. ***Execute:*** Government chairman. ***Responsibility:*** Parliament chairman.
Pressure groups	Conditions for SCPS are unfavourable, because its good will is continuously impaired and permanently it is necessary realized counter-actions with aim to disprove untruths.	Probability: great Impacts: Great	***Measures:*** Introducing the clear rules and safety culture in public sphere. ***Execute:*** Government chairman. ***Responsibility:*** Parliament chairman.
Terrorist attacks	Huge losses for SCPS and its surrounding (human, material, finance).	Probability: great Impacts: Great	***Measures:*** Implementation of effective safety concept and protection in the State. ***Execute:*** Government chairman / Region chairman / Municipality mayor. ***Responsibility:*** Parliament chairman.
Corruption	Huge losses for SCPS and its surrounding (social, material, finance). It goes to loss of authority of State.	Probability: great Impacts: great	***Measures:*** Implementation of effective safety concept and protection in the State. ***Execute:*** Government chairman / Region chairman / Municipality mayor. ***Responsibility:*** Parliament chairman.
Conditions for SCPS safe operation (legislative, taxes, interests etc.)	Huge losses for SCPS and its surrounding (material, finance).	Probability: great Impacts: great	***Measures:*** Stable strategy of development and public budget. ***Execute:*** Government chairman. ***Responsibility:*** Parliament chairman.
Wrong or insufficient technical legislative	Due to wrong and insufficient legislative (e.g. incorrectly determined requirements on technical facility operation with regards to ensure the co-existence of technical facility with surrounding at operation; at accidents the State has enormous costs from public budget, it comes to disruption of humans ´security and State stability.	Probability: great Impacts: great	***Measures:*** Adjustment of legislation connected with technical facilities and education. ***Execute:*** *Government chairman*. ***Responsibility:*** Parliament chairman.
……..			
In SCPS it is discrepancy with OSH requirements	Frequent injuries at work. High valetudinarianism. Discontent of workers.	Probability: medium Impacts: great	***Measures:*** Ensuring the adherence of requirements of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
SCPS contaminates environment (under allowable limits)	Penalties from public administration. Damaged SCPS good will.	Probability: medium	***Measures:*** Corrections according to demands of legislation in force. ***Execute:*** responsible technical facility project managers, responsible technical

		Impacts: great	facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Non-cover finance obligations to public administration	Penalties from public administration. Damaged good will.	Probability: medium Impacts: great	***Measures:*** Corrections according to demands of legislation in force. ***Execute:*** Technical facility finance manager. ***Responsibility:*** responsible technical facility top manager.
……..			
Occurrence of natural disaster higher than design one	Disruption of SCPS operation or accident in SCPS.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Aircraft crash on SCPS or in its close vicinity	Disruption of SCPS operation or accident in SCPS.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Failure of external critical infrastructures	Disruption of SCPS operation or accident or failure in SCPS.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Lack of qualified labour forces	Insufficient of SCPS operation up to its accident or failure.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager for labour forces. ***Responsibility:*** responsible technical facility top manager.
Consumption crisis	Unmarketability of products or services, i.e. economic losses.	Probability: low Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** responsible technical facility manager for sale. ***Responsibility:*** responsible technical facility top manager.
Critical technical fittings or components are wearied down	Low or disrupted performance, danger of failure or accident of SCPS.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant development plan. ***Execute:*** responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Missing funds on maintenance, repairs and modernization of equipment	Low or disrupted performance, danger of failure or accident of technical facility.	Probability: medium	***Measures:*** According to continuity plan; especially appurtenant development plan. ***Execute:*** responsible technical facility project managers, responsible technical

		Impacts: great	facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Internal fire	Losses and damages, disrupted performance of SCPS. Unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in hardware of information system supporting the SCPS control and management	Accident or failure of SCPS, which means loss of fulfilment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insufficient maintenance	Frequent disruption of performance, accident or failure of SCPS and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions for SCPS.	Probability: great Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong reaction of technical equipment to change of conditions	Frequent disruption of performance. Danger of origination of accident or failure of SCPS and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Ineffective safety management system	Frequent disruption of performance, accident or failure of SCPS and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially plan for safety ensuring. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insider	Frequent disruption of performance, accident or failure of SCPS and their impacts on assets.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical

	Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions for SCPS.		fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of top management in section of strategy, conception, supervision and check-up	Frequent disruption of performance, accident or failure of SCPS and their impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Wrong operating rules for normal operation	Frequent disruption of performance up to accident or failure of SCPS and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions for SCPS. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan; especially appurtenant response plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors in working regime	Overload of personnel which lead to frequent disruptions of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions.	Probability: medium Impacts: great	***Measures:*** According to continuity plan and legislation in force. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Insufficient motivation of key personnel	Neglecting the co-operation, frequent disruptions of performance up to accident or failure of technical facility and its impacts on assets. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** According to continuity plan. ***Execute:*** Appurtenant responsible technical facility project managers, responsible technical facility process managers, responsible persons for technical fittings operation, operator of technical fittings. ***Responsibility:*** responsible technical facility top manager.
Errors of critical personnel at work with risks connected with technical equipment, production, transport of material and products	Frequent disruptions of performance due to incidents up to accidents or failures of technical facility. Due to disrupted performance it gets to unfulfillment of commitments to third party. Sanctions. Loss of competitiveness.	Probability: medium Impacts: great	***Measures:*** Continuity plan. ***Execute:*** Appurtenant responsible technical facility operator of technical fittings. ***Responsibility:*** Appurtenant responsible technical facility responsible persons for technical fittings operation.
……			

From real data [14], it follows that errors of top levels of management, namely at both cases, the public administration and the SCPS, mean far greater losses, damage and harms to the public assets and assets of the technical facility than errors at the lower levels of management. This is due to the fact that top management has greater possibilities (power, resources, finance) to influence safety-targeted risk management than lower ones.

The continuity plan used for SCPSs is a strategic plan for the management of security and development of SCPSs enshrined in the SCPS safety management system. The plan is based on the method of managing the integral safety [6]. The plan lists not only data relevant to the SCPS operation, but also a way of solving problems that can seriously impair the SCPS operation and competitiveness. It includes:

- a way of resolving the risks that have a source outside SCPS and will seriously affect the SCPS with appropriate responsibilities and procedures for resolving the conflicts between the public interest and the SCPS interest,
- procedures to ensure safe SCPSs over its intended lifetime so that the SCPS provides quality products or services, is competitive and does not endanger itself and its surroundings,
- due to the dynamic development of the SCPS and the surrounding, which are not necessarily synergic, the reactions to the change in conditions, including emergency and crisis management measures, which are elaborated in detail and ensured in all respects for all levels of management of the SCPS, in addition, for critical SCPS that are vital to ensuring the basic functions of the State, there is also a crisis preparedness plan containing the measures and way of their ensuring to support the State at response to critical situations.

In order to the risk management plan may fulfil its role, it needs to be based on quality data processed by experts using the quality methods and be backed by legislation that ensures well-divided competences and enforces responsibilities, thereby contributing to building a safety culture in society.

7 Conclusion

The analysis of database of the SCPS accidents and failures shows that in spite of a lot of knowledge on SCPSs´ structures, interdependences, risks and safety, the SCPS accidents and failures have been forever occurred. Very significant source of accidents and failures is the human factor, especially in areas associated with: management on all hierarchical levels; the highest on the top level; maintenance of critical technical fittings and components; risk-based inspections, the frequency of which needs to correspond to fittings and components criticality; critical fittings, components and personnel working modes; and critical personnel education and training.

The causes of this reality are several: world dynamic variability; insufficient human knowledge and capabilities; slow application of knowledge and lessons learned into practice; and unsatisfactory awareness on risks and their consequences for technical facility and public interest.

Based on a detailed analysis of documentation on accidents and failures of SCPS [14], it can be concluded that very often an accident or failure occurs because:

- to date, outdated methods of risk assessment are used for complex technical facilities, e.g. tree models that do not consider confluences of phenomena,
- the operators or owners are mainly oriented towards performance (i.e. profit) and the public administration allows them to do so,
- personnel in contact with the causes and impacts of the risks do not have sufficient competence to implement proactive measures and operating regulations adapted to current conditions (normal, abnormal, critical),
- technical decisions are due to products of various particular, political or economic pressures and do not consider the specific risks that arise during operation.

The basic reasons why operators of SCPSs are not willing to influence the risks are usually:

- lack of awareness of the risks and their impact on and around the technical facility,
- subjective feelings of the responsible person, who does not consider the risk to be important,
- the idea that the risks relate to the distant future,
- the steps leading to the identification of the risk and its reduction are mostly contrary to the immediate (mostly economic or political) interests of the operator or owner,
- a particular competent worker is usually not the one, who can make direct decisions about the steps to reduce the risk.

Incorrect settlement of risks in technical facilities is due to:

- decision-making processes directly in technical facilities tend to be multi-level. At a level, on which increasing risk symptoms can be realistically identified and the risk involved is appreciated, it is not possible to decide on the additional costs of eliminating that risk,
- it is insufficient awareness on risks, their management and settlement. Working with risks is understood to be an activity consisting in compliance

with standards and regulations, which is not true, as the rules in place cover only 68.4 % of the possible conditions [2]. Programmes of the vast majority of training courses taking place often exacerbate this inadequacy,

- engineers in operation and its management has narrow understanding the safety; the orientation on the technical safety of the equipment is prevalent in such a way that the technical equipment does not pose a hazard during the service life,
- there is a lack of cooperation among professions – builders, engineers, economists, chemists, computer scientists, recruiters, etc. – each profession works separately, which does not allow to solve interdisciplinary and multidisciplinary problems,
- many top managers are convinced that everything is eternal, i.e. they do not consider changes in technical equipment over time and with changes in conditions, thereby underestimating the maintenance, repair, skill and compliance with work regimes that respect physical, chemical and biological regulations.

Due to dynamic world development, technical facilities parts ageing, wear and tear, and limited human knowledge, sources and capabilities, technical facilities´ managements and public administration need to be prepared for important risk realizations in next time. For this purpose, we propose to use above given tool "Risk Management Plan" that respects present knowledge on technical facilities´ response and the lessons learned from past responses to accidents and failures, the causes of which were connected with their operation. Its example for SCPS, which was tested in practice [14], is shown above

Acknowledgement: Authors thank for the EU grant; project RIRIZIBE-CZ.02.2.69/0.0/0.0/16-018/00026 49.

References

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

[2] PROCHAZKOVA, D., *Principles of Management of Risks of Complex Technological Facilities* (in Czech). ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/ 10467/72582

[3] PROCHÁZKOVÁ, D., *Critical Infrastructure Safety* (in Czech). ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

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

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

[6] PROCHAZKOVA, D., PROCHAZKA, J., *Risk management and settlement at technical facilities operation.* ISBN 978-80-01-06713-0. Praha: ČVUT 2020. dspace.cvut.cz . http://hdl.handle.net/10467/87552

[7] PROCHÁZKOVÁ, D., *Analysis, Management and Trade-off with Risks of Technical Facilities* (in Czech). ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. http://hdl.handle.net/10467/78442

[8] PROCHÁZKOVÁ, D., PROCHÁZKA, J., *Analysis, Management and Trade-off with Risks of Technical Facilities.* ISBN 978-80-01-06714-7. Praha: ČVUT 2020, 172p. http://hdl.handle.net/10467/87451

[9] 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.

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

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

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

[13] PROCHAZKOVA, D., PROCHAZKA, J., *Risk Management at Technical Facilities Designing, Building and Commissioning.* ISBN 978-80-01-06716-1. Praha: ČVUT 2020. dspace.cvut.cz. http://hdl.handle.net10467/87491

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

[15] PROCHAZKOVA, D., PROCHAZKA, J., Tools for Risk Management of Technical Facilities Operation. *European Journal of Engineering research & Science (EJERS).* ISSN 2506-8016. 5 (2020), 4, pp. 494-500. doi10.24018/ejers.2020. 5.4.1854

[16] PROCHÁZKOVÁ, D., *Methods, Tools and Techniques for Risk Engineering* (in Czech). ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369p.
[17] HEINRICH, H .W., *Industrial Accident Prevention: A Scientific Approach*. New York, NY, US: McGraw-Hill 1931.
[18] LEES, F. P., *Loss Prevention in the Process Industry*, *Volumes 1-3.* Oxford: Butterworth-Heinemann 2001.
[19] PAUL SCHERRER INSTITUTE, *Database ENSAD.* Zuerich: Paul Scherrer Institute 2019.
[20] BURGHERR, P., HIRSCHBERG, S., A Comparative Analysis of Accident Risks in Fossil, Hydro, and Nuclear Energy Chains. *Human and Ecological Risk Assessment.* 14 (2008), 5, pp. 947-973.
[21] BURGHERR, P., ECKLE, P., HIRSCHBERG, S., Comparative Risk Assessment of Severe Accidents in the Energy Sector Based on the ENSAD database: 20 years of Experience. In: *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013.
[22] BIRD, F. E., GERMAIN, G. L., *Damage Control.* New York: American Management Associations, Inc. 1966.
[23] GEYSEN, W., The Acceptance of Systemic Thinking in Various Fields of Technology and Consequences on Respective Safety Phylosophies. In: *Safety of Modern Systems. Congress Documentaion Saarbruecken 2001*. ISBN 3-8249-0659-7. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.
[24] IRM, *A Risk Practitioners Guide to ISO 31000*: 2018. London: IRM 2018. www.theirm.org.
[25] ZAIRI, M., *Total Quality Management for Engineers.* Cambridge: Woodhead Publishing Ltd. 1991.