Tool for Determination of Risk for Risk-Based Operation of Socio-Cyber-Physical Systems. Applications in Engineering Education.

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

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 paper contains the Decision Support System for determination of risk rate of socio-cyber-physical systems. Its regular application shows present-day risk rate and allows to reveal danger situations and in time to apply mitigation measures.

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

Received: September 10, 2020. Revised: March 10, 2021. Accepted: March 25, 2021. Published: April 10, 2021.

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], [2], [3], [4], [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 physical, 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 [6].

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.

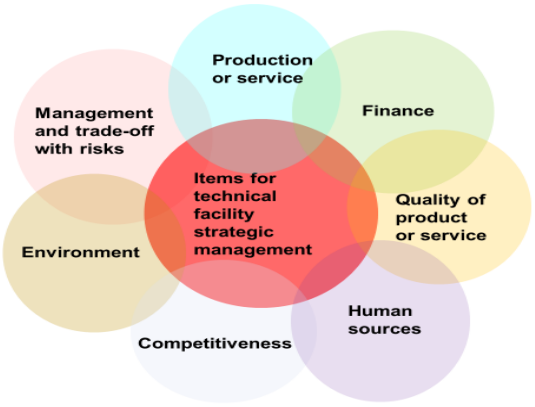

Fig. 1. Items determining the SCPS safety and development (i.e. also competitiveness during the life cycle).

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:

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], [1], [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.

The present problem is that university education mostly contains separate teaching the individual subjects, however, for understanding the complexity problems it is necessary to consider the problems on interfaces: human-technology, human-cyber, technology-cyber and human-cyber-technology.

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], [18], [19], [20], [21], [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].

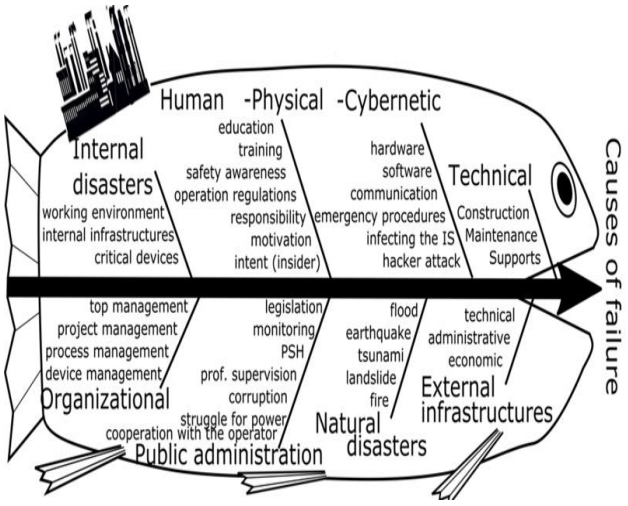

Fig. 2. Basic categories of risk sources associated with the technical facilities operation which lead to the failures of the coexistence of technical facilities with surrounding areas during their operation; IS = information system; PSH = personnel safety and health.

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].

The database research also shows significant role of human factor at origin of the SCPS accidents and failures (ca 80%). Big manifestation of human factor is at the SCPS management. Managers: do not solve errors in design; tolerate bad maintenance; underestimate response preparation; do not create acceptable conditions for workers; underestimate risks; and prefer profit.

5 Method of decision support system construction

The Decision Support System (DSS) [6], [8], [16] is a special technique for obtaining data for deciding the complex problems. It generally consists of the following components:

- data management module,
- model of management modules (model library),
- module for management of dialogue with user; and knowledge core (Knowledge engine).

There are different DSSs, or they have different conceptual starting points:

- model-based DSS (it using statistical simulation),
- communication DSS (it is for cooperation on a number of decisions),
- document DSS (it uses different types of documents to support decisions),
- knowledge DSS (it contains defined rules).

The decision support system (DSS) helps to solve the problem by supporting an analytical style of decision making against heuristic decision making. This means that:

- it organizes information for decision-making situations,
- it interacts with the decision-maker at various stages of decision-making,
- it extends the information horizon of the decision-making body,
- it facilitates multi-criteria evaluation, because it has built-in multi-criteria methods without the user knowing their mathematical structure.

Decision support systems use a general model for the certain case, reflecting the real situation. When specific parameter variables are substituted, they provide results for the given problem. The aim is to ensure that the result corresponds to the optimal solution. In their creation and application are used:

- knowledge and data from experts who know the technical parameters, limits and conditions of the technical facility and the local vulnerabilities,
- the principle of maximum utility theory [24], i.e. "the greater, the better" or "the greater, the worse".

Decision support systems are divided into special ones that provide support for solving the specific problems; and general, which are based on adaptive and flexible decision-making models. Obviously, the use of a specific DSS is only possible when verification establishes that the conditions for technology transfer are met [25]. Otherwise, the method must be adapted to local conditions. It should be noted that the adaptation of the method to specific conditions cannot be done by IT specialists, but by technical experts, who know the technical parameters, limits and conditions of the technical work and local vulnerabilities.

Applications of sophisticated DSS based on multi-criteria evaluation give good solutions. In our case, we will compile a DSS in the form of a checklist [4], [5] supplemented by a rule for evaluating questions in terms of [4] and assigning a logical value scale.

DSS application aims are:

- identifying, managing, eliminating or minimizing unforeseen events that have an adverse impact on critical elements, critical components, critical processes, critical functions, critical infrastructure and critical technologies in the technical facility,
- the process of comparing the estimated risks against the benefit and / or cost of possible countermeasures and establishing an implementation strategy in the context of integral (systemic, overall) safety,
- determining which disasters (harmful phenomena) the technical facility is exposed to, what are the risks from individual harmful phenomena, what damage may arise, which measures will eliminate or minimize the occurrence of harmful events,
- the procedure consists of: the assets are defined and their safety requirements are defined; identification of vulnerabilities, potential impacts and risks; estimated the amount of potentially caused damage; estimated the cost of appropriate safety measures; adequate safety measures selection.

For critical items, limit values (limits) shall be established to ensure acceptable security. This means that the task of their managing is to ensure compliance with the limits, and therefore, the basis is thorough monitoring and qualified DSS.

Tool “Decision Support System” respects present knowledge on technical facilities´ safety and lessons learned from past technical facilities accidents and failures, the causes of which were connected with their operations. Its base goes out from critical assessments of all findings collected and the results of engineering tools as compiled What, If tables, Case studies, fault trees etc. [16].

In system entity understanding, each technical facility is socio-cyber-technical (physical) system of systems, i.e. it has a lot of interfaces of different nature and relevance under certain conditions that in each place changing with time. From this reason, at DSS compilation, attention is concentrated to aspects that assess:

- way of consideration of risks and their sources,
- achieved level of safety in technical facility design,
- measures on technical levels – maintenance regime,
- risk based inspection performance etc.,
- material and energy demandingness,
- measures implementation speeds,
- demands on staff education and training,
- information security demands,
- financial demands,

- claims of liability,
- and as well as claims on management of all interested parties (i.e. in technical facility and territory).

Because the humans are creators of the SCPS, and at origin of the SCPS accidents and failures they play big role as was shown above, we started with tasks that they fulfil in connection with the SCPS risk management. Owing to the SCPS complexity, the capability of the SCPS to respond to accidents and failures is also considered, and therefore, this is also considered. Since the risk management realisation needs competence, skill personal, money etc., the economic, personal etc. manners are also considered. Due to role of country government in ensuring the public interest, the public responsibility for the SCPS safety (supervision the SCPS safety) is considered.

6 Decision support system for SCPS operation

On the basis of the requirements for technical facilities risks summarized in detail in [1], [2], [26]; data on accidents and failures descripted above and summarized with related lessons learned in [1], [14], [26], the DSS in the form of checklist for the operated technical facilities risks assessment was compiled – it has 302 criteria [6]. Example is in Table 1.

TABLE 1: EXAMPLE OF CHECKLIST FOR ASSESSMENT OF OPERATED TECHNICAL FACILITIES RISK.

Criterion	Rate	Note
The degree at which the technical facility top management understands and realizes responsibility for the risk management to technical facility integral safety; i.e. by other words level of safe operation in the case / level of coexistence.		
The degree at which the technical facility top management and operation management documents consider the impact of disasters under the All-Hazard-Approach, which are possible in the territory and carry out the correction of deficiencies; i.e. by other words level of safe operation in the case / level of coexistence.		
The degree at which the technical facility top management and operation management documents consider impacts of possible beyond design natural disasters in given territory and remedy the deficiencies; i.e. by other words level of safe operation in the case / level of coexistence.		
…….		
The degree in which the top management of the technical facility impacts of lack of qualified labour forces, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The degree in which the top management of the technical facility and managemental documents for operation consider impacts of high change in interest change, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
The degree in which the top management of the technical facility and managemental documents for operation consider impacts of rejection of state grant, and carry out improvement of defects; i.e. rate of level of ensuring the safe operation of technical facility.		
…….		
The degree in which the top management of the technical facility and managemental documents for operation consider impacts of hacker attack from surrounding, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
The degree in which the top management of the technical facility and managemental documents for operation consider impacts of pressure gangs from surrounding, and carry out protective measures; i.e. rate of level of ensuring the safe operation of technical facility.		
…..		
The degree in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of ensuring: - the quality working conditions for personnel, - the quality regime measures for operation of machines, fittings, components and systems, considering real personnel possibilities,		

and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The degree in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of protection of lives, health and security (OSH) at under all conditions (protective aids, tools, shelters, evacuation), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The degree in which the higher management (project leaders) of the technical facility and managemental documents for project realization consider the impacts of errors of higher management in section of operating rules for critical operation (activity), and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
……..		
The degree in which the middle management (process leaders) of the technical facility and managemental documents for process realization consider the impacts of errors of middle management in section of: - quality of personnel working conditions, - quality of regime measures for operation (activity) of machines, fittings, components and systems that considering the personnel possibilities, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
……		
The degree in which the technical management (technical fittings leaders) of the technical facility and managemental documents for technical fittings consider the impacts of errors of technical management in section of warning system, and carry out improvement of defects; i.e. rate of level of ensuring the adequate safe operation of technical facility.		
……..		
The degree in which the critical technical personnel responsible for real operation task in the technical facility operation consider and realize responsibility for safety of operations (activities); i.e. rate of level of ensuring the adequate safe operation of technical facility.		
The degree of education level of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
The degree of training and skill level of the critical technical personnel responsible for real operation task in the technical facility operation; i.e. rate of level of ensuring the safe operation.		
……..		
The degree in which public administration performs supervision under technical facility integral safety.		
The degree in which public administration enforces the operator to implement measures supporting the technical facility integral safety.		
The degree in which public administration checks-up the adherence of OSH requirements.		
The degree in which public administration checks-up the adherence of environment protection requirements.		
The degree in which public administration checks-up the adherence of user protection requirements.		
The degree in which public administration co-operates with technical facility operator at ensuring the safety at critical situations.		

The check list is in the form so it may be possible to use classification scale 1 to 5 with the philosophy "the higher number, the higher risk" which means lower safety and lower coexistence of technical facility with its surrounding. For DSS application, the auxiliary scale Table 2 derived in [4], [5], and the second scale for the evaluation of the entire checklist based on the principle that was introduced into standards in the 1980s, Table 3.

The assessment of Table 1, hereafter given, assumes that all criteria have the same weight. Practical examples [14] show that in many cases some criteria are more important than others, and therefore, it is necessary to assign them higher weight, and to change data in Table 3 by appurtenant way.

TABLE 2: SCALE FOR DETERMINATION OF RATE OF RISK; P – annual insurance, ABT-the annual budget of territory governance.

Domain	**Risk rate**	**Classification criterion**
Social	*By accident or failure of technical facility, it is affected:*	
	0	less than 50 humans
	1	50 - 500 humans
	2	500 - 5000 humans
	3	5 000 – 50 000 humans
	4	50 000 – 500 000 humans
	5	more than 500 000 humans
Technical and Economic	*Accident or failure of technical facility causes damages:*	
	0	less than 0.05 p
	1	equal to p
	2	between p and 0.05 ABT
	3	between 0.05 ABT and 0.075 ABT
	4	between 0.75 ABT and 0.1 ABT.
	5	higher than 0.1 ABT.
Environment	*Accident or failure of technical facility causes:*	
	0	very low damages of environment
	1	damages of environment with which the nature cope during the acceptable time
	2	moderate damages of unrenewable resources of nature and natural reservations.
	3	medium damages of unrenewable resources of nature and natural reservations
	4	unreturnable damages of unrenewable resources of nature and natural reservations
	5	devastation of landscape, unrenewable resources of nature and natural reservations

TABLE 3: VALUE SCALE FOR DETERMINING THE RISK RATE.; N = five times the number of criteria in Table 1; N = 1510.

The level of risk	**Values in % N**
Extremely high – 5	More than 95 %
Very high – 4	70 - 95 %
High – 3	45 - 70 %
Medium – 2	25 – 45 %

Negligible – 0	Low than 5 %

The evaluation of real cases according to Table 1 needs to be performed by a team of specialists from different fields independently; in practice [2], [3], [4], [5], it comes in useful team consisting of:

- worker of public administration responsible for territory safety,
- worker of public administration responsible for the development of the territory,
- representative of technical facility,
- representative of the professional institution for the technical facility safety assessment, for example from the technical inspection,
- representative of the Integrated rescue system.

The resulting value is the median for each criterion, and in cases of great variance of the values in one criterion it is necessary, so that the worker of public administration responsible for territory safety may ensure further investigation, on which each assessor shall communicate the grounds for his / her review in the present case, and on the basis of panel discussions or brainstorming session, the final risk rate value is determined.

At the technical facility risk management based on data in Table 1 we consider the responsibility principle that is general in Europe [27]. It means that in the followed technical facility phase (operation) both, the operator (owner) and the public administration are responsible for the technical facility safety.

Considering:

- the ALARP principle as in works [27], [28], [29], [30],
- the integrated approach as in works [31], [32],
- and the assumption that all risk sources have the same occurrence probability, we obtain the requirement for tolerable risk measured by the technical facility maximum annual losses $\boldsymbol{RZTD}$

$$\boldsymbol{RZTD} < 0.1 \sum_{i=1}^{n} \frac{k_i \, \boldsymbol{HTD}}{5 \, \boldsymbol{T}},$$

where $\boldsymbol{HTD}$ is the technical facility utility value, $\boldsymbol{k_i}$ are result evaluations of risk sources in Table 1, n is the number of risk sources (in our case 302) and $\boldsymbol{T}$ is the technical facility lifetime in years. When this condition is not fulfilled, so the proposed technical facility may not be accepted for realisation because the coexistence will be violated. It means that either a new option or other risk reduction measures should be requested, followed by a further assessment of the proposal.

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 need regularly to determine risk and in time to apply mitigation measures to avert failure of critical parts or accident. Its example for SCPS, which was tested in practice in seven cases [14], is shown above . These concepts are also very useful for Education and especially for Engineering Education.

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, 244 p.

[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, 364 p. 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, 218 p.

[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, 172 p. 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 2002,191 p.

[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, 483 p.

[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 Philosophies. In: *Safety of Modern Systems. Congress Documentaion Saarbruecken 2001*. ISBN 3-8249-0659-7. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.

[24] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569 p.

[25] PROCHÁZKOVÁ, D. Examination of Core of Complaints and Conflicts Concerning Technical Solutions (in Czech). *Kontrola MSK ČR 1992*. MSK ČR Praha, 95 p.

[26] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Management of Risks of Processes Connected with Technical Facility Operation at Life Cycle* (in Czech). ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. http://hdl.handle.net/10467/85867. doi:10.14311/BK.9788001066751

[27] DELONGU, B. *Risk Analysis and Governance in EU Policy Making and Regulation.* ISBN 978-3-319-30822-1. Springer 2016, 288 p.

[28] ALE, B. Tolerable or Acceptable. A Comparison of Risk Regulation in the United Kingdom and in the Netherlands. *Risk Analysis*, 25 (2005),2, pp. 231-242.

[29] BOULDER, F., SLAVIN, D., RAGNAR, E. *The Tolerability of Risk: A New Framework for Risk Management.* ISBN 978-1-84407-398-6. London: Taylor & Francis 2007, 160 p.

[30] EU. *Land Use Planning Guidelines in the Context of Article 12 of the SEVESO II DIRECTIVE 96/82/EC as Amended by DIRECTIVE 105/2003/EC*. Brussels: Joint Research Centre 2006.

[31] LEVITT, R. E., LOGCHER, R. D., QUADDUMI, N. H. Impact of Owner-Engineer Risk Sharing on Design Conservatism. *ASCE Journal of Professional Issue in Engineering.* 110 (1984), pp. 157-167.

[32] BRUCE, J. F. *Investment Performance Measurement.* ISBN 0-471-26849-9. New York: Wiley 2003, 748 p.