Tools for Risk Management of Technical Facilities Operation

Dana Prochazkova, Jan Prochazka

***Abstract*—The article shows the results of research directed to detection of technical facilities accidents and failures sources at their operation. The research aim is to create the effective tools for management of risks so the coexistence of technical facilities with their vicinity would be ensured throughout their life cycles. The problems solution way is based on the simultaneously preferred concept, in which the safety is preferred over the reliability. Respecting the present knowledge on technical facilities´ safety and the lessons learned from the past technical facilities accidents and failures, the causes of which were connected with their operation, two tools are developed: Decision Support System and Risk Management Plan that were reviewed by experts and tested in practice.**

***Index Terms*—Decision Support System, Operation, Risk, Risk Management Plan, Safety, Technical Facility.**

I. Introduction

Technical facilities belong to public assets because they ensure products and services on which the humans are dependent [1-11]. Present knowledge shows that each public asset is open system with real time development and these developments are during the time sometimes conflicting [12]. The conflicts´ management is influenced by complex nature of all public assets which is described by system of systems models and time variability.

For humans´ security and development, the coexistence of technical facilities with their vicinity is necessary to be ensured throughout their life cycles [13,14]. Therefore, in line with current knowledge and experience, we need:

- to know the sources of risk at using the All-Hazard-Approach [15],
- to appreciate their harmful potential (i.e. identify the sizes and distribution of their impacts on public assets) in individual places, and the size of their potential losses and damages depending on the distribution of public assets, i.e. to determine the risk [12].

Depending on the concerned human society possibilities, the risks are divided into acceptable, conditionally acceptable and unacceptable. In the case of risks which are:

- unacceptable, the application of effective preventive measures against their resources should be ensured,
- conditionally acceptable, the mitigating, reactive and renewing measures for the monitored assets should be prepared,
- acceptable, the risk monitoring over time should be installed with aim to reveal an increase of their harmful impacts over time.

In this way, we carry out activity which we call "risk management". The activity effectiveness depends on tools. The article deals with compilation of effective tools for technical facilities risk management directed to integral safety with aim to ensure their co-existences with their vicinity during their operations. The problems solution given hereafter respects that the safety is preferred over the reliability.

II. Technical Facilities Risks

Each technical facility is created by human activities and it provides products or services important to human´s lives; technical facilities aimed at promoting policy objectives only are not subject to research. Technical facility architecture is object or network. Each technical facility type has its specifics; e.g. there is a significant difference between the control of stable ones and moving ones.

The human lives in modern society are made easier through technical and cyber systems. 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 technical facilities coexistence with their surroundings

[13,16]. The reason for increased number of risk sources is existence of a large number of different types of complex systems, their elements and interconnections on which the human system depends.

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

As the world dynamically evolves, the progressive anthropogenic management already notes that due to the technical facilities´ and the world´ complexities and time changes in conditions that humans do not have the ability to influence, the accidents and failures of technical facilities

Published on April 26, 2020.

D. Prochazkova is with Czech Technical University in Prague, Fac-ulty of Machinery, Technicka 4, 166 00 Praha 6, Czech Republic. (danuse.prochazkova@fs.cvut.cz)

J. Prochazka is with Czech Technical University in Prague, Faculty of Machinery, Technicka 4, 166 00 Praha 6, Czech Republic. (jan.prochazka@fs.cvut.cz)

are a reality with which the anthropogenic management needs to deal [17]. It needs to go on such technical facilities managing that performs well-established tasks during their lifetimes for their safety. Due to the existence of dynamic transformations, the management is foreseen that situations may arise where technical facility becomes dangerous to itself and its surroundings [17]. 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 technical facility 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 technical facility 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 technical facilities safety in all possible conditions [12,13]. However, our research shows lacks in awareness on risks, especially among managers and politicians.

III. Aspects of Management of Risks of Technical Facilities Safety at Operation

Technical facilities are physical, cyber and organizational (including personnel) interconnected systems. Examples of physical/technical systems are buildings, technical equipment for the production or transmission of energy, networks, means of transport, material equipment. Examples of cyber systems are computer systems for the management of production and other processes, information sources, etc. An example of organizational systems are economic and organizational units.

Due to technical facility complexity, their safety is necessary to understand in integral sense. 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 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. [13,14]; examples of failures impacts are also in [17,18].

Because technical facilities are complex systems (system of systems - SoS), their behaviors cannot be inferred from the behavior of individual parts and, under certain conditions, there are occurred unexpected phenomena that lead to the destruction or failure of the technical facility functionality. It goes on:

- a sudden emerging the behavior feature that cannot be derived from knowledge of components´ behavior,
- hierarchy,
- self-organization,
- diversity of management structures,

which together resemble chaos [13,14]. Therefore, to ensure complex technical facilities safety, it needs to be used multi-disciplinary and interdisciplinary approach [12], which ensure their:

- existence (ability to ensure balance,
- efficiency (ability to cope with resource shortages),
- freedom (ability to handle challenges from the surroundings well),
- security (ability to protect itself from phenomena inside and outside),
- adaptation (ability to adapt to external changes),
- coexistence (the ability to change its behavior so that it may responds to the behavior and orientation of other systems and so that the systems do not endanger each other).

In terms of current knowledge, at least two tasks are ahead today:

- to solve the functionality of set of interconnected (i.e. dependent) objects and infrastructures under normal, abnormal and critical conditions
- to search critical conditions of complex fitting, equipment or facility that are unpredictable or are result of serious operator´ error, and that may, under certain conditions, go to highly non-demanded, i.e. highly unacceptable conditions, i.e. situations in which the very existences of facility or even humans are threatened, and which we usually refer to as crisis.

Therefore, they are followed specific characteristics such as:

- interoperability (i.e. ability of technical facility as a whole to perform quality tasks under normal, abnormal and critical conditions),
- safety integrity (SIL), which is mostly tracked in conjunction with human errors (at specification, design, installation, maintenance, modification, etc.),
- criticality (i.e. extent to which personal injury, material destruction, damage or other asset losses may occur – threshold below which monitored equipment condition is demanded and vice versa),
- dependability (operational reliability), which ensures that system meets specified requirements and its operation complies with specified conditions (it extends to two basic characteristics, which are vulnerability and durability).

In this context, we divide technical facilities into reliable, secure and safe systems [13]. Reliable system is system that performs required functions at 95% probability level. Secure system is reliable system that is protected from all risks. Safe system is secure system that, even in its critical conditions, does not endanger itself and its surroundings. In creation and operation of all these system types it is:

- worked with risks; applied on Defense-In-Depth principle,
- and required management using the technical facility safety management system – SMS [13,14].

When at the technical facility designing, creation and operation, it is not clarified what objective is pursued in practice, confusions arise in prioritization, and it leads to conflicts, and therefore, the optimization of measures [13,19] must be carried out. Misplaced priorities bring harm, e.g. five girls lost their lives in an escape game in Poland because they were in a secure room; pilot Andreas, from Germanwings, could have led the plane to the Alpine

mountain massif because the cockpit was secured - the armored door could not open from the outside, etc. [12].

The possible action is using the integral safety concept, which: considers the priorities in public assets; is based on consideration of all phenomena that can damage the territory and technical facility, i.e. the All-Hazard-Approach [15]; and which at reducing the costs clearly determines what risks can be neglected by fact that facility, fittings or equipment is only considered as a secure system or only a reliable system [14]. Its application 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 base 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; and be able to install technological changes if necessary [18].

IV. Data and Methods Used

For research, the original database of technical facilities accidents and failures [20] from the world data was compiled and several case studies were analyzed in great details [18]. 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. [21].

Their results 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. 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.

V. Results of Analysis of Database of Technical Facilities Accidents and Failures

Detail database study shows that causes of technical facilities accidents and failures are:

- 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.

See Fig. 1.

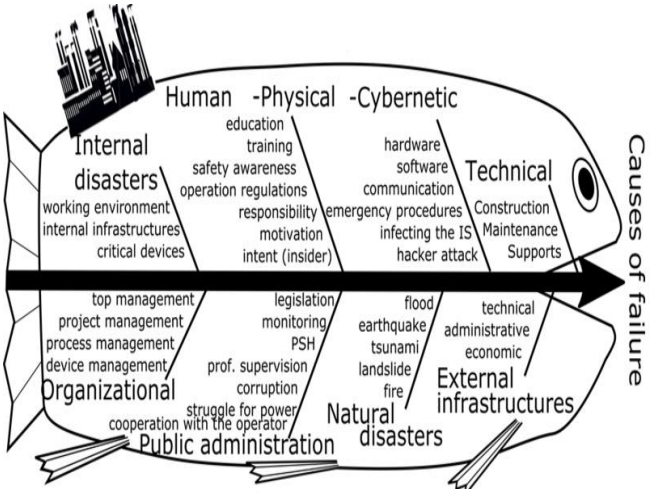

Fig. 1. Basic categories of risk sources associated with the technical facilities operation which lead to the failures of the coexistence of technical facilities with surrounding areas during their operation; IS = information system; PSH = personnel safety and health.

The database analysis shows that in spite of a lot of knowledge on technical facilities´ structures, interdependences, risks and safety, the technical facilities accidents and failures have been forever occurred. Very significant source of accidents and failures is the human factor, especially in areas associated with:

- maintenance of critical technical fittings and components,
- risk based inspections, the frequency of which must 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.

The technical facilities accidents and failures research show that originators of technical facilities accidents and failures are:

- large mistakes in risk prevention made in technical facility terms of references and designing,

- and origination of small mistakes, the realization of which in short time interval is dangerous.

Both these factors need to be managed. For management improvement, two tools were developed, namely decision support system and risk management plan.

VI. Verified Tools for Facilities Risk Management

Analyses of tools for working with risks summarized at [18] and the experience gathered [20] show that risk management tools depend on many factors. At technical facilities strategic management, it is necessary to consider both, the safety and the long-term functionality. This means that two facts need to be considered: technical facilities 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) and with risks at higher levels (e.g. pressure vessels; production lines, sets of production lines, whole technical facility) and at the highest level (technical facility and its surroundings). Safety at the highest level ensures the coexistence of technical facility 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 technical facility 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 components of a technical facility (pressure vessels, reactors, control systems, etc.) are essential for integral technical facility safety, and therefore, it is not sufficient for 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 technical facility safety. It goes on critical elements, critical equipment, critical components and critical technical facilities systems [14,18] that require special work with risks in siting, designing, construction and operation.

Depending on entity complexity, three risk-related objectives are distinguished:

- operation safety,
- process safety (component operation, production line),
- and entity integral safety.

Because the higher the tool type is used, the higher the demands (knowledge, finance, time) are connected with its use, so in practice they are preferred tools with the lowest demands, which, based on current knowledge and experience, have the capability to solve a task if they are respected the safety culture basic rules and the operating regulations corresponding to operation conditions; i.e. it is not considered intent to damage the entity.

Based on experience in practice from technical facilities operational practice [14,18], it is an applicable tool that is fast and not very demanding for knowledge and time. The evaluation of usefulness of risk management tools in the technical facilities operation performed in cited book is that at:

- simple entities, a proven tool is checklist that is locally specific and has a properly calibrated scale for risk assessment,
- not very interconnected entities, a proven tool is a set of checklists that are locally specific and have properly calibrated risk assessment scales, with the results of those checklists are aggregated in a designated and locally specific manner,
- and at complex entities, a proven tool is decision support system (DSS) that consider both, the asset connectivity and the time changes and external risk sources.

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. The important role plays technical facilities organizational structure, which is mechanism used to coordinate and control technical facilities operation. According to [22], it constitutes a hierarchical arrangement of relationships of superiority and subordination and addresses mutual competences, links and responsibilities. Of course, large financial and other means releases on risk management is only at the highest hierarchical level. Complex technical facilities have several hierarchical levels. According to experience from practice [20] we assume at the DSS creation the organizational structure as follows: top management; higher management – responsible for projects (e.g. the result of a set of several production lines); medium management – responsible for processes (e.g. one production line); technical management – responsible for individual technical equipment operation; personnel (critical and supportive) – responsible for technical activities.

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

On the basis of the requirements for technical facilities risks summarized in detail in [14,18]; data on accidents and failures and related lessons learned in [20], the DSS in the form of checklist for the operated technical facilities risks assessment was compiled – it has 302 criteria; its example is in Table I.

TABLE I: CHECKLIST FOR ASSESSMENT OF OPERATED TECHNICAL FACILITIES RISK; NUMBER OF CRITERIA N = 302. AIM IS TECHNICAL FACILITY AND ITS SURROUNDING SAFETY

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.		

At application in practice, individual criteria in Table I are evaluated by scale 1 – 5 with concept "the higher the value, the higher the risk" [23]. The scale for the evaluation of whole checklist is in Table II; it was introduced into standards in the 1980s [24].

TABLE II: VALUE SCALE FOR DETERMINING THE RATE OF COEXISTENCE OF PLANNED TECHNICAL FACILITY AND ITS SURROUNDINGS; N = FIVE TIMES OF NUMBER OF CRITERIA IN TABLE I; N = 1510.

The level of coexistence disruption (risk) between TF and surrounding	Values in % N
Extremely high – 5	More than 95 %
Very high – 4	70 - 95 %
High – 3	45 - 70 %
Medium – 2	25 – 45 %
Low – 1	5 – 25 %
Negligible – 0	Low than 5 %

The evaluation of real cases according to Table I needs to be performed by a team of specialists from different fields independently; in practice, 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

[25]. 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. The DSS was tested with success at five medium enterprises [20]; its site-specific compilation and application in practice are is ambitious on experts´ knowledge and time, and they require the access to detail enterprise and public administration documents, which is connected with respecting the certain legal rules.

Procedures for assessment of technical facility risk acceptability for both parties, the technical facility and the public administration is described in [24]. It is based on comparison of losses caused by mean annual technical facility risk and benefits for both, the technical facility and the public administration.

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, it was developed 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.

Since technical facility and its surroundings are interconnected, two important players are considered – technical facility management and public administration. Risk management plan in question needs to be concerned with preparation of technical facility for management of risks directly related to it and risks associated with interconnection of technical facility – the territory; and for public administration pays the same. Therefore, the compiled plan is linked to: safety (strategic) technical facility plan; security (strategic) roadmap for territory development; on-side emergency plan; off-side emergency plan; technical facility continuity plan for critical conditions; the territory's crisis plan; and territory recovery plan [13,18].

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 risk management plan contains four basic items:

- area of risk causes from all areas (technical, organizational, internal causes, external causes, cyber, etc.),
- description of risks causes of the risk,
- occurrence probability and assessment of risk impacts,
- risk mitigation measures and responsibilities for their implementation.

The management type TQM [26] and its principles are considered when drawing up a risk management plan.

From the viewpoint of responsibilities, two cases need to be distinguished, namely risk management in following areas: connection between public administration and management of technical facility; and technical facility management [14].

In line with the TQM, responsibilities for the following functions are considered in public administration: Parliament President; Minister of the Sector, which includes the technical facility (industry, energy, health, agriculture, transport, communications, etc.); Region Chairman; Municipality Mayor; responsible public administration

officer for territory safety; responsible public administration officer for territory development; responsible authorized inspector; and responsible representative of civil protection.

For dealing with risks in technical facility are considered statutory representatives of: top management; higher management – projects leaders; medium management – processes leaders; technical management – responsible for technical equipment operation; personnel (critical and supportive) – responsible for technical activities.

On the basis of the data collected (data on the causes of accidents and failures of technical works during operation, and relevant lessons), the knowledge described above, a priority risk management plan for the field of operation of the technical work is drawn up by 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; and representative of the Integrated rescue system [18]; its example is in Table III.

TABLE III: RISK MANAGEMENT PLAN TO ENSURE THE COEXISTENCE OF OPERATED TECHNICAL FACILITY WITH ITS SURROUNDING

Risk area	Risk description	Occurrence probability Risk impacts size	Risk mitigation measures
CONNECTION OF PUBLIC ADMINISTRATION AND TECHNICAL FACILITY MANAGEMENT			
Sources of risks in the territory			
Beyond design natural disaster occurrence	Losses, damages and harms on public assets as well as on the technical facility assets – the result may be also be accident of technical facility that will worsen situation in territory	Probability: Small Impacts: Large	***Measures in the territory:*** Regional and municipality crisis plans ***Execute:*** Region Chairman and Municipality Mayor ***Responsibility:*** Region Chairman ***Measures in technical facility:*** Continuity plan ***Execute:*** Higher management representatives ***Responsibility:*** Statutory representative of top management
TECHNICAL FACILITY MANAGEMENT			
Sources of risks in the territory			
Beyond design natural disaster occurrence	Interruption of operation, failure or accident in technical facility	Probability: Small Impacts: Large	***Measures:*** Continuity plan ***Execute:*** higher management representatives in co-operation with representatives of medium and technical management and staff ***Responsibility:*** statutory representative of top management
Pollution of environment (above the permitted limits)	Fines from the public administration. Good will damage	Probability: Medium Impacts: Large	**Measures:** Respect the requirements of valid legislation **Execute:** Statutory representatives of top management **Responsibility:** Technical facility owner
Insufficient safety culture	Overloading of operators, non-cooperation, frequent interruptions of technical facility performance, occurrence of incidents, accidents and failures. Due to the interrupted performance it goes to failure to fulfil obligations to a third party, the risk of penalties	Probability: Medium Impacts: Large	***Measures:*** Continuity plan ***Execute:*** higher management representatives in co-operation with representatives of medium and technical management and staff ***Responsibility:*** statutory representative of top management
Failure of emergency communication system	Accidents or failures of technical facility and their impact on assets. Due to interrupted technical facility performance it goes to failure to fulfil obligations to a third party, Penalties	Probability: Large Impacts: Large	***Measures:*** Continuity plan ***Execute:*** representative of higher management, who is responsible for information system ***Responsibility:*** Statutory representatives of top management
Inadequate maintenance	Frequent interruption of performance. Accidents or failures in technical facility and their impact on assets. Due to the interrupted performance it goes to failure to fulfil obligations to a third party, Penalties	Probability: Large Impacts: Large	***Measures:*** Continuity plan ***Execute:*** representative of higher management, who is responsible for technical facility conditions ***Responsibility:*** Statutory representatives of top management
Weaknesses in critical staff education	Interruption of performance. Accidents or failures in technical facility and their impact on assets. Due to the interrupted performance it goes to failure to fulfil obligations to a third party, Penalties	Probability: Medium Impacts: Large	***Measures:*** Continuity plan ***Execute:*** representative of technical management responsible for technical equipment operation **Responsibility:** Statutory representatives of top management in cooperation with the higher management representative, who manages the project to which the production process belongs and with the medium management representative, who manages the process to which the relevant technical equipment belongs

In plan, two areas are considered: sources of risk in territory which have potential to cause technical facility accident or failure; and sources of risks within technical facility which have potential to cause technical facility accident or failure with impacts that they may cause loses and damages in surroundings. From these facts it follows that plan is site specific. The Risk Management Plan was tested with success at five medium enterprises [20]; it is ambitious on experts´ knowledge and time, and it requires the access to detail enterprise and public administration documents, which is connected with respecting the certain legal rules.

VII. Conclusion

Technical equipment and technical facilities belong to the different sectors management and are very diverse 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 safe technical equipment or safe technical facility. For reasons of great diversity, the different procedures are site and sector-specific. Aspects important for operation of technical equipment and whole technical facilities are very diverse, especially those of: knowledge and technical, which predetermine the capacity possibilities of technical facilities and technical equipment; organizational and legal matters enabling the technical facilities operation and technical equipment operation at a certain level of safety in the territory and over time; financial, personnel, social and political at national and international level.

The findings obtained by research of technical facilities accidents and failures show that in the prevention of accidents and failures, the following should be avoided: major risk prevention errors (e.g. underestimating the size of external risk sources or sources of organizational accidents); and occurrence of minor errors, realization of which in short time period is dangerous, although the impacts of separate individual errors are manageable by prepared response measures. To this aim the 'Decision Support System' tool is developed and recommended for practice

Due to world dynamic development, ageing and wear of parts of technical facilities and limited human knowledge, resources and possibilities, the technical facility management and the public administration must be prepared for future occurrence of risks. To this aim 'Risk Management Plan' tool is developed and recommended for practice.

Both tools respect current knowledge of technical facilities safety and lessons learned from their past accidents and failures, the causes of which have been linked to their operation. They must be compiled as sector and site specific in order to be effective and effective.

Acknowledgment

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

References

[1] B. Ale, I. Papazoglou and E. Zi, "*Reliability, Risk and Safety"*. London: Taylor & Francis Group, 2010, 2448p.
[2] M. Beer, M. and E. Zi, "*Proceedings of the 29th European Safety and Reliability Conference"*. Singapore: ESRA, 2019, e:enquiries@ rpsonline.com.sg
[3] C. Bérenguer, A. Grall and C. Guedes Soares, "*Advances in Safety, Reliability and Risk Management"*. London: Taylor & Francis Group, 2011, 3035p.
[4] R. Briš, C. Guedes Soares and S. Martorell, "*Reliability, Risk and Safety. Theory and Applications"*. London: CRC Press, 2009, 2362p.
[5] M. Cepin, and R. Bris, "*Safety and Reliability – Theory and Applications"*. London: Taylor & Francis Group, 2017, 3627p.
[6] S. Haugen, J. Vinnem, A. Barros, T. Kongsvik and A. Van Gulijk, "*Safe Societies in a Changing World"*. London: Taylor & Francis, 2018, Group 3234p.; https://www.ntnu.edu/ esrel2018.
[7] IAPSAM, "*Probabilistic Safety Assessment and Management Conference"*. Helsinki: IPSAM & ESRA, 2012, 6889p.
[8] T. Nowakowski, M. Mlyńczak, A. Jodejko-Pietruczuk and S. Werbińska-Wojciechowska, "Safety *and Reliability: Methodology and Application"*. London: Taylor & Francis Group, 2014, 2453p.
[9] L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio and W. Kröger, "*Safety and Reliability of Complex Engineered systems: ESREL 2015"*. London: CRC press, 2015, 4560p.
[10] [R. Steenbergen, P. Van Gelder, S. Miraglia and A. Ton Vrouwenvelder, *"Safety Reliability and Risk Analysis: Beyond the Horizon"*. London: Taylor & Francis Group, 2013, 3387p.
[11] L. Walls, l., M. Revie and T. Bedford, "*Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. London: CRC Press, 2016, 2942p.
[12] D. Prochazkova, "*Analysis and Coping with Risks Connected with Technical Facilities"*. Praha: ČVUT, 2018, 222p. http://hdl.handle.net /10467/78442
[13] D. Prochazkova, "*Safety of Complex Technological Facilities"*. Saarbruecken: Lambert Academic Publishing, 2015, 232p.
[14] D. Prochazkova, "*Principles of Management of Risks of Complex Technological Facilities"*. Praha: ČVUT, 2017, 364p., http://hdl.handle. net/10467/72582
[15] FEMA, "*Guide for All-Hazard Emergency Operations Planning"*. State and Local Guide (SLG) 101. Washington: FEMA, 1996.
[16] OECD, "*Machine-to-Machine Communications: Connecting Billions of Devices"*. OECD Digital Economy Papers, No. 192. Paris: OECD, 2004. http://dx.doi.org/10.1787/5k9 gsh2gp043-en
[17] C. Perrow, "*Normal Accidents: Living with High-Risk Technologies"*. Princeton: Princeton University Press, 1999.
[18] D. Prochazkova, D., J. Prochazka, J. Lukavsky, V. Dostal, Z. Prochazka and L. Ouhrabka. "*Management of Risks Connected with Technical Facility Operation"*. http://hdl.handle.net/10467/85867. doi:10.14 31/BK.97 88001066751
[19] S. Sagan, "*The Limits of Safety"*. Princeton: Princeton University 1993.
[20] CVUT, "*Database on World Disasters, Technical Entities Accidents and Failures – Causes, Impacts and Lessons Learned"*. Praha: CVUT, 2020.
[21] D. Prochazkova, "*Methods, Tools and Techniques for Risk Engineering"*. Praha: ČVUT, 2011, 369p.
[22] J. Dedina, "*Management and Organizational Behaviour"*. Praha: Grada, 2005.
[23] R. L. Keeney and H. Raiffa, "*Decision with Multiple Objectives"*. Cambridge: Cambridge University Press 1993, 569p.
[24] D. Prochazkova, J. Prochazka, J. Riha, V. Beran and Z. Prochazka, "DSS for Ensuring the Coexistence of Technical Facility with Its Vicinity during the Type Selection and Sitting" In: *Proceedings of the 29th European Safety and Reliability Conference*. Singapore: ESRA, 2019, e:enquiries@rpsonline.com.sg
[25] D. Prochazkova, "*Critical Infrastructure Safety Management Rules"*. Praha: CVUT, 2013, 223p.
[26] M. Zairi, "*Total Quality Management for Engineers"*. Cambridge: Woodhead Publishing Ltd., 1991.

Dana Prochazkova was born in Pardubice (Czech Republic) in 1945. She studied the Faculty of Mathematics and Physics, Charles University at Praha - physics (RNDr.). She worked in Czechoslovak Academy of Sciences (P.D., D.Sc.), State Office for Nuclear Safety, and in Czech Technical University in Prague (Assoc. Prof.).

The objectives of professional works have been engineering, nuclear engineering, crisis management, risk and safety management, critical facilities safety etc. She published more than 500 professional papers in the English, in the Czech, in the Russian, in German and one in the Chinese; 25 professional books and 17 textbooks for Universities. She solved and successfully co-ordinated 47 national research projects, 17 international research projects (for the EU, IAEA, UN).

Jan Prochazka was born in Praha (Czech Republic) in 1982. He studied the Charles University in Praha, Faculty of Mathematics and Physics (RNDr., Ph.D.). He has been working in the Czech Technical University in Praha.

The objectives of professional works have been quantum physics, optoelectronic, material properties, hazardous materials, protection against hazardous substances, engineering problems, emergency management, crisis management and risk management. He published 25 professional papers and participating on 15 professional reports containing the real problems solution.