Optimum Risk Engineering Tools Depend on Technical Facility Complexity

Dana Prochazkova
Department of Energy
Czech Technical Univerisity in Prague
Praha, Czech Republic
danuse.prochazkova@fs.cvut.cz

Jan Prochazka
Department of Energy
Czech Technical Univerisity in Prague
Praha, Czech Republic
jan.prochazka@fs.cvut.cz

***Abstract*—The study of accidents and failures of complex technical facilities has shown that in many cases, these phenomena occur when the technical facility integral risk exceeds the certain criticality rate, i.e. also if larger number of small risk sources executes in technical facility in a short period of time and their impacts are specially interconnected. The present risk engineering tools are diverse and have different requirements for data, knowledge, processing time, i.e. finance, and practice is of course interested in the least demanding tools. The article shows optimum risk engineering tools working with risks for achievement of main three targets of technical facility (reliability; security; safety), which depend on the technical facilities´ complexity rate.**

***Keywords*— technical facility; complexity; risk; risk engineering tools; safety; security; reliability; risk management.**

I. Introduction

Each technical product or each technical facility (further only technical facility) is the result of human activity with aim to ensure the products and services supporting the human lives and development. To ensure the technical facility safety, it is necessary to work with risks of all kinds [1]. The coexistence of technical facility with the surroundings (i.e. with public assets, which include the human lives, health and security, property, public welfare, the environment, other technical facilities) is ensured if the technical facility integral (i.e. total) safety is successfully managed [2,3]. Level of integral safety depends on quality of work with integral risk [2,4]. For successful work with risks of all types, they are necessary both, the correct and effective tools and the responsibilities for their correct use [1-5]. The paper deals with the first item; the second one was solved in [2,6].

A number of specific tools have been developed to deal with risks in risk engineering [2,4,7-9]. Because in practice, they are different aims of risk engineering (safety of machine, safety of process, safety of whole facility etc. [3,9]) and used tools in practice have different requirements on knowledge, data, time and finance, it is necessary in real case to use such tool that fulfil the given aim and it is feasible. Real practice requires the tools that have the lowest demands [10]. Next, they are specified such tools for selected tasks, which are solved in practice.

II. Summary of Knowledge

The coexistence of technical facility with its surroundings during the whole technical facility life cycle is ensured if integral safety of technical facility is kept on certain level by qualified risk management [1]. The integral safety is understood as an attribute on the level of the whole technical facility, and it is determined by the quality of the file of anthropogenic measures and activities aimed at the safe technical facility, and even at its critical conditions [4].

The main present aim is to recognize, understand and manage the risks, thereby ensuring a safe technical facility and its safe operation throughout its lifetime. Because technical facilities are characterized by open systems of systems (SoS), it goes on choice of tools in which the results of analytical and expert methods are interconnected in a specific way [4,5,7].

Technical facility architecture is object or network [1,2]. Each technical facility type has its specifics; e.g. therefore, there is a significant difference between the control of stable technical facilities and moving ones. Currently, in practice there are not used simple technical systems, but there are used the files of systems. According to the type of system files organization [1,2], they are distinguished:

- simply organized units (e.g. machines),
- composite systems that are understood as a set of elements that are organized and connected in a certain way and because of a proper structure they fulfil certain functions, they are characterized by the higher level of configuration (e.g. compound set of machines – production line, which carried out in a given order tasks, to set up certain product),
- complex systems characterized by organized complexity and compound so as to perform certain functions (linked production lines with the different technologies, e.g. automatic systems for production – for example so called digital factories, categorization and distribution of certain commodities),
- very complex systems representing the mutually interconnected complex systems in horizontal and vertical structure, which mark out by great variability, which appears like unorganized complexity, i.e. systems of systems. Individual complex systems can work by both, independently and together. At common work, they perform completely unique task that is remote from the tasks of individual complex systems (systems for production, distribution and consumption of electricity, gas, etc.).

On the basis of knowledge and experience [1,2] for the characterization and control of:

- simply organized units, the results of analytic solutions are used,
- composite systems, there are used the results of statistical solutions based on analytic functions, the parameters of which are variable in certain intervals, which are reflection of random conditions / random variants of the system behaviour,
- complex systems, the results of simulations need to be used, because random uncertainties are great and

cause that behaviour of scenarios are in broader range, than include the randomness, i.e. the methods of operations research are used [7].

- very complex systems, the multicriterial methods are need to be used, since the given aggregates have many systems, which are organized in several levels. The systems interact together in dependence of internal and external conditions, which causes that we observe:
- suddenly emerged features of behavior that cannot be obtained from the knowledge about the behavior of components, it goes on sudden origin of phenomena, which were not expected,
- various hierarchies,
- self-organization,
- varied management structures, which all together appear like the chaos.

These systems have random uncertainties and knowledge uncertainties, and therefore, for their characterization, it is necessary to use the expert and heuristic methods [7]; sometimes it is necessary to consider many criteria, some of which are often opposing (conflicting) [4,5].

To describe the type of technical facility organization, we introduce the quantity, called "complexity". According to [4], the complexity is a system attribute that denotes that system has many parts or elements that have mutual relationships that are different from relationships with other elements outside and their behaviours depend on many internal and external parameters. It characterizes the behaviour of system, the parts of which interact in variable ways in dependence on momentary conditions in a given site and in a given time [1]. For its description, it is necessary to use multidisciplinary and interdisciplinary approach and for its management it is then necessary to use the multi-criteria approaches, which enable to consider the cross-sectional risks [5]. A number of specific tools have been developed to deal with risks in risk engineering, and therefore, it originates the problem, which tool is this true in a given conditions.

According to present knowledge, they are used in practice three different targets of technical facility management, namely: reliability; security; and safety. Because these aims go out from different concepts, the technical facilities risk values obtained for individual aims are not the same; they are strongly dependent on concept [2,5]. With regard to present knowledge given above, the integral risk rate depends on both, the risk management target and the technical facility´ complexity rate [2-5].

The risk engineering tools are diverse and have different requirements for data, knowledge, processing time, i.e. also for finance, and practice is of course interested in the least demanding tools [1-5]. According to results summarized in [3,8], the useful methods in practice for complex technical facilities are:

- Benchmarking is a method of systematically comparing the processes, organizational structure, products and performance of a given technical facility department with other globally successful technical facilities with a view to achieving the excellence. It is usually used in risk management in cases, where the objective is ideal, and according to good practice principles it is good to manage risks by way as the best industry operators do.
- Modelling is a technique by which we create a simplified picture of a real process, system or object and then we follow on it the established connections. Its aim is to determine the scenario of the process in time and space (e.g. the course of the accident, the course of the process control, the course of the response to the accident, etc.), so that we can determine appropriate measures and activities to ensure safe technical facilities (e.g., at preventing, mitigating and mastering the incidents, accidents and failures) with available capabilities and possibilities, which we execute with the CBA (Cost Benefit Analysis). Based on the principle that "everything is related to everything" (regressus ad infinitum), it is necessary to validate results obtained by model, because evaluations of technical facilities accidents and failures often show that key causes were inadequately considered at modelling the accidents. In serious cases, the care should be taken for software applications, especially where technology transfer conditions have not been verified [11].
- A scenario is a system model that describes the evolution of a process in its various forms (variants, alternatives) depending on conditions or decisions made. It contains a sequence of events that take place within time, territory or other entity (including the prospective variants), and it descripts interactions among the monitored assets of the system and the process [7]. Disaster scenarios are the most important for safety management because they are used to propose measures for prevention, mitigation, response and recovery.
- Multicriterial assessment is an assessment based on the application of multiple criteria, even incommensurable or conflicting, to a whole [7]. For the resulting solution, they need to be determined the restrictive conditions, which define objectivity (e.g. in terms of system exhaustibility, human resources or value of benefits). The exhaustibility of the system means the maximum possible level of utility (utility value) that can be achieved at a given scientific and technological development. We always judge the restrictive conditions individually, namely based on their partial evaluations. For maximum utility application in conjunction with the risks of complex systems, it has proved to be useful the application of: What, If method in form of table, Table 1; and the DSS (Decision Support System) with appropriate value scales processed on the maximum utility theory [12].

Analyses of the risk management tools presented in [9,13] as well as the accumulated experience [10] show that risk management tools depend on many factors; schematically, the subject matter is shown in Figure 1.

It is evident that the technical facility strategic management, in which security and long-term functionality are concerned, needs to consider two factors:

- technical facilities are complex multi-level systems,

- specific sources of risk associated with technical facilities are not the same at all levels of the technical facility.

TABLE 1. Standard model for applying the What, If method.

Asset		**Potential impact of disaster on asset**
Human lives and health		
Human security		
Property		
Welfare		
Environment		
Infrastructures and technologies	Energy supply sector	
	Water supply sector	
	Sewerage sector	
	Transport sector	
	Communication and information sector	
	Bank and finance sector	
	Emergency services	
	Basic territory services (industry, agriculture, supply service, health service, waste management, social services, funereal services)	
	Public administration	
Technical facility	Critical fittings	
	Critical components	
	Critical links	
	Critical internal infrastructures	
	Critical couplings	
	Critical stocks	
	Critical personnel	
	Waste management	
	Critical processes management items	
	Critical projects management items	
	Critical integral management items	
………..		

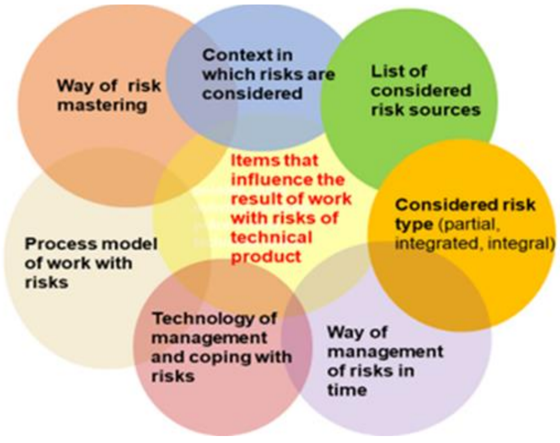
Way of risk mastering
Context in which risks are considered
List of considered risk sources
Items that influence the result of work with risks of technical product
Considered risk type (partial, integrated, integral)
Process model of work with risks
Technology of management and coping with risks
Way of management of risks in time

Fig. 1. The factors that influence the risk size of a given entity.

Due to technical facility complexity, in practice, it is necessary to work with risks at the lowest level (simple technical equipment - machines), as well as with risks at higher levels (components – e.g. pressure equipment; 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 the technical facility with the surroundings throughout the life cycle of the technical facility.

In order to ensure the safety and development of humans and other public assets, the objectives of dealing with risks at all technical facility levels are the same, a reliable or secure or safe entity. Because of the current goals of human society, which have been already emphasized several times, we above all focus on the ultimate goal, which are the safe entities.

III. RISKS USED IN PRACTICE

In practice, they are used three types of risk: partial (related to one asset); integrated (sum of risks related to several assets); and integral [4,5]. The integral risk is systemic risk that depends on momentary conditions in a given site and a given time. Therefore, its determination is very difficult for complex technical facilities, where a great variability of linkages and flows exists. In these cases, its analytical expression is difficult due to existence of many random and epistemic uncertainties [4,5]. And therefore, they need to be used the specific engineering tools as special What, If form (Table 1) for each possible scenario and Decision support system [4,5,7], the combination of which have the ability to identify the integral risk size in advance.

At selection of risk management tools for technical equipment and whole technical facilities aimed to safety, they are important two factors according to arguments in [1,2,5]:

- The first factor is the cognition that risk is a site-specific and time-specific quantity, i.e. it depends on both, the cause of the destructive phenomena (i.e. the nature and size of the harmful phenomenon) and the characteristics of the entity (vulnerability, resiliency) at the time of the phenomena origin (e.g. an unmaintained relief valve does not perform its function at the exceedance of pressure limit). Because over time there are variables, both the asset or pool of assets and the sizes of harmful phenomena or disasters, there are three categories of situations in terms of coping with the impacts of the realized risk, namely: normal; emergency; and critical. With the growing category, the professional, financial, organizational and personnel requirements for managing and settling the risks associated with these situations are increasing. Therefore, important role here plays the legislation that imposes requirements on owners and operators of technical facilities on risk management and on the public administration for technical facilities safety oversight in the public interest [1,2,5]. Based on analyses of legislation [1,2,5,10], current legislation is too general; it does not mention data requirements and data processing methods that fundamentally determine the quality of the result.

- The second factor is the choice of the type of risk, which should be monitored in the task, which depends on the determination of:
  - the number of assets and their listing, i.e., it goes on considering which public assets and which specific assets of a technical facility in a given task are important; e.g. whether they are performance, competitiveness, profit, etc.,
  - whether links and flows between listed assets play a role in the task, i.e. a mechanical concept is not enough, but a system concept needs to be considered.

In order to ensure the safety of the entity in the short term (e.g. safe state of simple technical equipment), it is sufficient to monitor the condition of the asset, i.e. the partial risk associated with the entity. With regard to human safety, legislation in developed countries also requires the ensuring the occupational safety and health (OSH), i.e. the monitoring of two assets (life and health of persons in the workplace, quality of the working environment), at using the integrated risk, it is neglected machine - human linkage, which influences the machine condition. Since technical fittings, people in the workplace and the working environment are interconnected, the links and flows between these subsystems, i.e. integral risk, need to be monitored in the medium and long-term to ensure safety of the whole.

Therefore, when selecting the risk management tools (identification, analysis, evaluation, judgement, management and settlement) aimed at the safety of the selected entity, the following tasks in the technical field for technical facilities should be distinguished:

- selection of tools for work with the risk associated with the condition of technical equipment (objective - safe technical equipment),
- selection of tools for working with the risk associated with the condition of the technical component (objective - safe technical component),
- selection of tools for working with the risk associated with the production line / production process (objective - safe production process),
- selection of tools for working with the risk associated with the condition of the business process set (objective - safe business process set),
- selection of tools for working with the risk associated with the whole technical facility (objective - safe technical facility),
- selection of tools for working with the risk associated with the technical facility and its surroundings (objective - safe technical facility and safe neighbourhood of the technical facility).

Based on the works [1,2,5,7], focusing on technical facilities, it is not enough to ensure the safety of the human system in connection with technical facilities and technologies (i.e. coexistence of a technical facility with its surroundings during the operation) only by concentration to technical facilities´ safeties, because the choice of risk management tools depends on:

- the nature of the entity of interest (i.e. selected technical equipment or higher systems of technical facility),
- the nature of the environment in which the entity of interest (i.e. selected technical equipment or higher systems of technical facility) operates,
- the mode in which the entity of interest (i.e. selected technical equipment or higher system of technical facility) operates,
- requirements for the operation of the entity of interest (i.e. selected technical equipment or higher systems of technical facility),
- and whether a short, medium or strategic solution, i.e. long-term, is required.

IV. Data used

For task solution, the original database of technical facilities accidents and failures [10] from the world data was compiled and several case studies were analyzed in great details. The database contains 7829 dangerous events from the whole world sources that were accessible in last 35 years to authors; more than 90% dangerous events originated during the technical facilities operation. To reveal their causes (risks realized), the collected data were processed by risk engineering methods: e.g. What, If; Checklist; Fishbone diagram; Case studies; Event Tree; FMECA; etc. [7] in dependence of accessible data quality and amount [10]. They were also considered get-at-able results of other authors [14-19].

The study of accidents and failures of complex technical facilities [3,10,20] has shown that originators of technical facilities accidents and failures except of great natural disasters are:

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

- cumulation of small unfavourable phenomena, the realization of which in short time interval is devastating.

The second case is more frequent. It occurs when integral risk exceeds the certain criticality rate. In many cases at technical facilities with great complexity, the criticality rate exceedance is caused by combination of larger number of small risk sources activated in technical facility in a short period of time. To manage the technical facility behavior in these cases, the integral risk needs to be followed [1,2].

V. Method for evaluation of tools´ effectiveness

Risk engineering disciplines by nature use tools based on four models [2,7] according to the type of problems, which they follow; it goes on:

- problems that can be described by a linear model [7] (simply organized units and set-up units) – rate of complexity 1; e.g.: Check list; Safety audit; Human Reliability Analysis - HRA; there is a need to be aware of the limited accuracy of the results, as only one process is monitored and the links with other processes and the environment are neglected,
- problems that can be described by the tree models [7] (composite systems that are understood as a representation of elements that are organized and connected in a certain way) – rate of complexity 2; e.g.: Preliminary Hazard Analysis - PHA; Quantitative Risk Analysis - QRA; Hazard Operation Process - Hazard Analysis (HAZOP); Event Tree Analysis - ETA; Failure Mode and Effect Analysis - FMEA; FMECA - Failure Mode, Effect and Criticality Analysis; Fault Tree Analysis - FTA; Probabilistic Safety Assessment - PSA; it should be noted here that in this case the development of incidents, accidents and failures comes from a single site, i.e. models do not describe cases where impacts on a technical facility occur from one cause at several different locations, i.e. combinations of harmful phenomena are not considered,
- problems that can be described by operational research models [7] (complex systems that are understood as a representation of elements that are organized and connected in a certain way and their behaviour manifests in certain range and may be expressed by variants of statistical function) – rate of complexity 3; e.g.: critical path method; PERT; GERT; Petri nets; for the last three ones are now elaborated to form "colour stochastic models", which simulate a large number of possible scenarios that are created and assessed by experts on the basis of their experience and data presented in experience databases, have been compiled at the last years in developed countries,
- non-structured problems, which cannot be described simply due to great variability of possible configurations, which cause hardly foreseeable behaviour modes [7] – rate of complexity 4: specific What, If form; Scenarios; Case Studies; Multi-criteria methods based on Decision Support System (DSS). In these cases, experience is the ground; a series of scenarios is be developed through collaboration with experts, and the optimum solution is sought using the maximum utility theory [12].

The experiences from world-wide practice [5,7,10,13] show that often used tree models have not the capability to assess the size of technical facility integral risk because they come out from one point in technical facility. It means that they do not express impacts of external disasters, external terrorist attacks and human factor that usually in one stroke affect many points, and they do not consider interfaces with surroundings.

The Decision Support System (DSS) [7] is a special technique for obtaining data for deciding the complex problems. It helps to solve the problem by supporting an analytical style of decision making against heuristic decision making. It 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.

Its 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 and another parameters, limits and conditions of the technical facility and the local vulnerabilities,
- the principle of maximum utility theory [12], i.e. "the greater, the better" or "the greater, the worse".

For many of the above methods, there are software that has been derived for a particular device at a particular location is available. In order to ensure correct results in this case, it is necessary to verify, before using each software, whether the conditions of the technology transfer are met, i.e. whether the conditions for the solution and the solution are the same as for the technical facility and the place for which the software was derived [7].

Considering the facts that:

- individual tools of risk engineering have different aims and different requirements on knowledge, data, experience, time, and thus also on finance,
- in practice they are preferred tools with the least demands,
- the integral risk determination of technical facility is very dependent on its complexity,

by the critical evaluation of ability of individual engineering tools (given above) to reveal the most of defects that led to accidents and failures (111 cases from [10] would to be used due to demands of considered methods on data), we determined the least demanding tools depending on the technical facility complexity rate and on target of technical facilities risk management.

Based on years of experience, we used the scoring method for the data described above to determine the optimal methods for tasks related to technical facilities in which the risk management objective, complexity of the technical facility, the duration of the solution and the existence of uncertainties should be considered for the data described above [7]. Its application we have acquired 4 basic categories of conditions for valuing the effectiveness (capability) of methods to give an acceptable solution at the smallest cost (knowledge, time, finance); Figure 2:

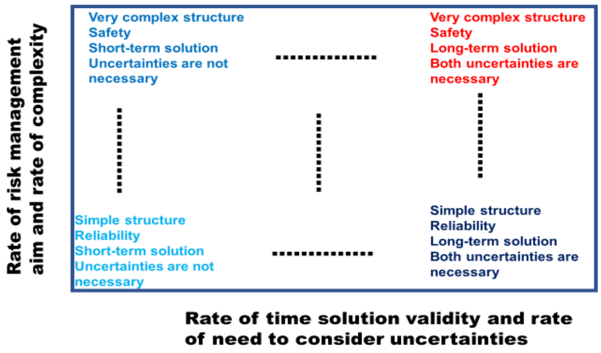
Rate of risk management aim and rate of complexity
Very complex structure
Safety
Short-term solution
Uncertainties are not necessary
Very complex structure
Safety
Long-term solution
Both uncertainties are necessary
Simple structure
Reliability
Short-term solution
Uncertainties are not necessary
Simple structure
Reliability
Long-term solution
Both uncertainties are necessary
Rate of time solution validity and rate of need to consider uncertainties

Fig. 2. Scoring the important aspects for working with the risks of technical facilities.

- task is based on a simple structure of a technical facility, it is focused on the reliability of a technical facility, it requires short-term validity of the result and it does not need to consider either random or knowledge uncertainties,
- task is based on the very complex structure of the technical facility, it is focused on the integral safety of the technical facility, it requires the short-term validity of the result and it does not need to consider either random or knowledge uncertainties,
- the task is based on a simple structure of the technical facility, it is focused on the reliability of the technical facility, it requires the long-term validity of the result and it needs to consider both random and knowledge uncertainties,
- the task is based on the very complex structure of the technical facility, it is focused on the integral safety of the technical facility, it requires the long-term validity of the result and it needs to consider both random and knowledge uncertainties.

The rate of the entity's risk management goal and complexity for each task was determined by the sum as follows:

- risk management target: reliability – 1 point; security – 2 points; safety – 3 points,
- entity structure complexity: point – 1 point; linear – 2 points, tree – 3 points, area – 4 points, spatial – 5 points.

The rate of time in validity of the solution and the need to consider the uncertainties for each task was determined by the sum as follows:

- need for consideration of uncertainties: no need – 1point; only random – 2 points; random and knowledge-based - 2 points,
- solution validity: short-term – 1 point; medium- to 2 points; long-term – 3 points.

VI. Optimal Methods for Risk Management Dependent on Complexity Rate and Management Target

Based on the results of described way of evaluation of methods by help of data on the technical facilities´ accidents and failures [2,7,10] and the authors' experience from practice, Table 2 is compiled. It contains optimum risk engineering tools suitable for different targets of technical facility and its parts, dependent on two variables. In addition to the complexity of the entity, there are considered three objectives of entity risk management, namely arranged according to growing demandingness of target procuration [2,7,10]:

- entity reliability ensuring the operation safety of entity,
- entity security ensuring the process safety of entity (component operation, production line),
- entity safety, i.e. integral safety, ensuring the safety of both, the entity and its surroundings.

Since the higher the tool type, the higher the cost (knowledge, finance, time) for its use, Table 2 shows in each case only the lowest cost tools that, based on current knowledge and experience, have the ability to solve the task if the basic rules of safety culture, operating rules corresponding to the conditions of operation are observed; that is, no intention to damage the entity is considered.

TABLE II. Tools for working with risks sorted by the aim of the followed task$^{*)}$.

Objective of work with risks	**Complexity rate**	**Tool**	**The subject of the monitoring**
Reliability of individual technical equipment / fittings (e.g. machine)	1	Checklist / Safety Audit / What, If	One asset
Security of individual technical equipment (the machine is reliable and its security and the operator security are ensured)	2	Checklist / Safety Audit / What, If	Two assets – because conflicts may occur, a rule is required for aggregation
Safety of individual technical equipment (the machine does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. its operators´ security is ensured and the products are safe	3	DSS	Several interconnected assets – because conflicts may occur, the theory of maximum utility is most often used [9]
Reliability of technical component (several interconnected technical fittings)	2	Checklist / Safety Audit /, What, If / Tree models	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [9]

Security of technical component (several interconnected technical fittings are reliable and their securities and the operator security are ensured)	3	Checklist / Safety Audit /, What If / Tree models / operation research methods / DSS	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [9]
Safety of technical component (several interconnected technical fittings do not endanger themselves even under critical conditions and do not have harmful impacts on the surroundings), i.e. it is safe and the products are safe	4	What, If / Tree models / operation research methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, a rule is required for aggregation or use theory of maximum utility [9]
Reliability of production process (production line)	2	Checklist / Safety Audit /, What If / Tree models	Several interconnected technical and other assets – because conflicts may occur, a rule is required for aggregation
Security of production process (production line is reliable and it is ensured its security and the operator security)	3	What, If / Tree models / operation research methods / DSS	Several interconnected technical and other assets and surroundings – because conflicts may occur, a rule is required for aggregation or use of theory of maximum utility [9]
Safety of production process / production line does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. its operators´ security is ensured and products are safe. and the products are safe	4	What, If / operation research methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, a rule is required for aggregation or use of theory of maximum utility [9]
Reliability of a set of processes in the technical facility	3	What, If / operation research methods / DSS	Several interconnected technical and other assets - because conflicts may occur, a rule is required for aggregation or use of theory of maximum utility [9]
Security of set of processes in the technical facility (set of processes is reliable and its security and operators security are ensured)	4	What, If / stochastic operation research methods / DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [9]
Safety of set of processes in the technical facility (set of processes does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. it is safe and products are safe	4	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [9]
Reliability of technical facility	4	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [9]
Security of technical facility (technical facility is secured and operators security is ensured)	4	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [9]
Safety of technical facility (technical facility does not endanger itself even under critical conditions and does not have harmful impacts on the surroundings), i.e. it is safe and products are safe	4	DSS	Several interconnected technical and other assets and surroundings - because conflicts may occur, it is required use of theory of maximum utility [9]

*) In this context, *it needs* to be aware – reliability means *correct* performance of entity tasks with probability equal or higher than 0.95; *security means reliability and provision of entity protection; and* safety means security (including the reliability) and *provision of protection of entity and its surrounding*.

VII. Conclusion

A critical analysis of the dependence of the tools on data shows that the higher the type of risk management tool is used, the higher are the costs (knowledge, finance, time) to use it. By critical evaluating the data on specific accidents and failures of technical facilities of varying complexity, the lowest cost-effective tools were identified, which, on the basis of current knowledge and experience, should have the ability to solve the tasks by complying with the basic rules of the safety culture, operating regulations corresponding to the conditions of operation; i.e. it was not considered intent to damage the technical facility.

Based on experience, in the operational practice of technical facilities and their parts, it is only useful broadly applicable a tool, which is fast and not very demanding on knowledge and time. Therefore, the credibility of risk management tools for the operation of technical facilities was judged [5,13]. The result of this research showed that for:

- a not-too-complex entity, it is a proven tool, a site-specific checklist with a correctly calibrated risk assessment scale,
- not very interconnected entities, it is a proven tool, a set of checklists that are site specific and have correctly calibrated risk scales, and the results of these

checklists are aggregated in a specified and site-specific manner,

- complex entity, it is a proven tool DSS that consider both, the asset connectivity, the changes in time and external sources of risks.

Table 2 shows separation of risk engineering tools for optimal solution of practical task in dependence on the technical facilities´ complexity and their risk management aims.

Acknowledgment

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

References

[1] D. Prochazkova, *Safety of Complex Technological Facilities.* Saarbruecken: Lambert Academic Publishing 2015, 244p.

[2] D. Prochazkova, *Principles of Management of Risks of Complex Technological Facilities*. Praha: ČVUT 2017, 364p.

[3] D. Prochazkova, J. Prochazka, "Tools for Risk Management of Technical Facilities Operation. *European Journal of Engineering research & Science (EJERS).* ISSN 2506-8016. 5 (2020), 4, pp. 494-500.

[4] D. Prochazkova, J. Prochazka, *Analysis, Management and Trade-off with Risks of Technical Facilities*. Praha: ČVUT 2020, 172p. http://hdl.handle.net/10467/87451

[5] D. Prochazkova, *Analysis and Coping with Risks Connected with Technical Facilities.* Praha: ČVUT 2018, 222p. http://hdl.handle.net/10467/78442

[6] D. Prochazkova, J. Prochazka, "Complex Technical Facilities Risk Management Responsibilities". In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* Singapore: ESRA 2019, pp. 1735-1742, doi:10.3850/978-981-11-2724-3_0095-cd,

[7] D. Procházková, *Methods, Tools and Techniques for Risk Engineering.* Praha: ČVUT 2011, 369p.

[8] D. Prochazkova, J. Prochazka, "Risk Management Plan for Technical Facility Designing, Manufacturing and Commissioning". *International Journal of Economics and Management Systems.* ISSN: 2367-8925**. 5 (**2020), pp. 75-85. https://www.iaras.org/iaras/home/caijems/risk-management-plan-for-technical-facility-designing-manufacturing-and-commissioning

[9] D. Prochazkova, J. Prochazka, "Alternatives of Work with Risks Used at Technological Facilities Safety Management". *Universal Journal of Management.* ISSN 2331-950X, 6(2018), 8, pp. 287-294. ISSN 2331-9577, http://www.hrpub.org DOI: 10.13189/ujm.2018.060804

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

[11] OTA: *Public Law 92-484*. www.princeton.edu

[12] R. L. Keeney, H. Raiffa, *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569p.

[13] US EPA, "PHA Techniques in Chemical Emergency Prevention & Planning". *Newsletter* 2008, No. 8, pp. 3-6.

[14] H. W. Heinrich, *Industrial Accident Prevention: A Scientific Approach*. New York, NY, US: McGraw-Hill 1931.

[15] F. P. Lees, *Loss Prevention in the Process Industry, Volumes 1-3.* Oxford: Butterworth-Heinemann 2001.

[16] Paul Scherrer Institute, *Database ENSAD.* Zürich: Paul Scherrer Institute 2019.

[17] P. Burgherr, S. Hirschberg, " A Comparative Analysis of Accident Risks in Fossil, Hydro, and Nuclear Energy Chains". *Human and Ecological Risk Assessment.* 14 (2008), 5, pp. 947-973.

[18] P. Burgherr, P. Eckle, S. Hirschberg, "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*. London: Taylor & Francis Group 2013.

[19] F. E. Bird, G. L. Germain, *Damage Control.* New York: American Management Associations, Inc. 1966.

[20] W. Geysen, "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*. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.