Alternatives of work with risks used at technological facilities safety management

D. Prochazkova, J. Prochazka

***Abstract*—**The aim of all people is human security and development. Therefore, they need technological facilities, which ensure energy, services and products for life. Present cognition shows that safety of technological facilities is based on copping with risks. Human cognition contains a lot of knowledge and experiences with risks, but in reality only part of them are used in practice. The aim of research, the results of which are presented, was the judgement, how in practice connected with complex technological facility safety it is used the present human cognition on work with risks.

With regard to world dynamic development it is necessary the priority risks to monitor and to cope with them during time, and also to measure the respective safety. At measure of rate for safety level we use the known experience that the better coping with relevant risks, the higher facility safety level is. The analysis of based publications and data from real practice shows that seven domains at work with risks are important. The paper shows the results of critical judgement of individual techniques that are used at work with risks in technological facilities in practice.

Keywords— Safety culture; systems of systems; technological facility; work with risks.

I. INTRODUCTION

On the basis of present level of knowledge that is e.g. represented by publications from the ESREL conferences [1], [2], [3], [4], [5], [6], [7], [8], [9], the main results of which are summarized in works [10], [11], we perceive each technological facility as open complex system of systems, i.e. as several open systems that are mutually penetrated and are interfaced with vicinity.

The interfaces ensure the fulfilment of important operations and services, but on the other side they are the cause of dependences that make up specific vulnerabilities. In consequence of these vulnerabilities, under specific conditions they originate highly unfavourable interfaces that lead to technological facility failure, which at certain circumstances distinctly also damage the technological facility vicinity.

Therefore, at ensuring the technological facility safety it is necessary to consider that technological facilities have various assets that are altered in dynamically variable world. The multiplicity and variability of assets cause that under certain conditions the measures that ensure the individual assets´ safety are conflicting, which means that methods using at risk management aimed to technical product safety need to be multi criterial [11]; but in practice this is not often fulfilled [11].

Human cognition summarized in [10], [11] contains a lot of knowledge and experiences from work with risks with aim to ensure the safety of technological facilities and their vicinities. Generally, from safety reasons it is necessary:

1. To control the processes that lead to significant risks.
2. To reduce the vulnerabilities of public assets.
3. To rise the human society resilience. Resilience is the combination of asset capability „withstanding" and "recovering" from disaster.

The aim of our research, the results of which are presented, was the judgement, how in practice connected with complex technological facility safety, the present human cognition on work with risks is used. I.e., how they are used pieces of knowledge on:

- risk sources,
- ways of work with risks that have potential to ensure:
  - human security,
  - safe technical facility and its safe vicinity.

The data for research create the information that is given in publication from the ESREL conferences since 2009 and data summarized in [10], [11] and [12]. These data were separated into seven domains which determine approaches to the risks. In individual domains the information was processed by critical analysis method and the elicited ways of work with risks connected with technological facilities in each domain were arranged from the worse one to the best one.

II. SAFETY AND RISKS OF TECHNOLOGICAL FACILITIES

At present in advanced engineering disciplines described in works [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] the safety is understood as the property that emerges on the system level. It represents the set of measures and activities, which ensure that system is safe, with validity of following connections:

Dependable (reliable) system is a system that performs required functions at a given place, a given time and in a given quality during the whole life cycle.

Secure system is the dependable system that is protected against to internal and external disasters of all kinds.

This work was supported by the EU and the Czech Ministry for Education.

The paper was prepared in the frame of the RIRIZIBE project, CZ.02.2.69/0.0/0.0/16_018/0002649.

Dana Prochazkova & Jan Prochazka are academician workers of the *Czech Technical University in Prague, Faculty of Transportation Sciences, Czech Republic; phone. 420 224355027; email: prochazkova@fd.cvut.cz*

Safe system is the secure system that not at its critical conditions does not endanger itself and its vicinity.

Risk je is understood as the probable size of losses, damages and harms on protected assets in real system that is calculated for unit of space and time. It is dependent on the disaster size and on the local assets vulnerabilities.

Safety and risk are in certain relation but they are not complementary quantities. The risk reduction means the safety increase but it is not always valid inversely [10], [11]. The complementary quantity to safety is the criticality; in some legislation, e.g. in the SEVESO directive, it is used the term recklessness instead of criticality.

Criticality denotes the limit (boundary) from which the risk impacts are significant up to eliminative for followed system, which means that appurtenant risk needs to be always mastered.

III. INFORMATION, PROCEDURES AND IMPORTANT DOMAINS CONNECTED WITH TECHNOLOGICAL FACILITY SAFETY

For compilation of important aspects for technological facilities safety management we use data given in publications [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] and in Archives [12]. By help of their critical comparison, classification and judgement it was derived that for technological facility safety it is necessary to consider seven domains (Fig. 1) that influence the result of work with risks of technological facility, i.e. its safety, namely:

1. Context in which the risks inherently connected with technological facility are inserted.
2. List of considered sources of risks.
3. Type of risk form.
4. Ways of mastering the risks.
5. Process model of work with risks, application of the TQM and Coase theorem.
6. Technique of management and coping with risks of technological facility.
7. Way of management of risks in time.

IV. CHARACTERISTIC FORMS OF DOMAINS USED IN PRACTICE

In the first domain it holds that the best context, in which the risks of technological facility are inserted, has the assets and process model ensuring the human security and development that are shown in Figure 2 [10].

On the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], in the technology

Fig. 1 Items that influence the result of work with risks of technological facility

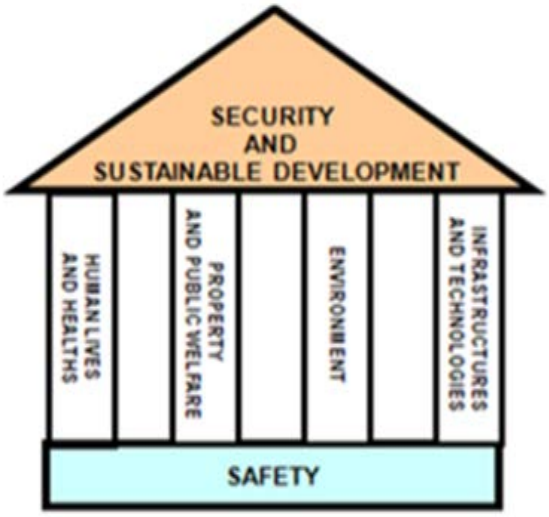

Fig. 2 Assets of human system and process model for ensuring its security and development [13]

sector it is often considered only the context of technological facility or context of enterprise that administrate the technological facility, and in many cases only the context of production facility or line.

It is understandable that the use of more limited context means the higher neglect of reality. In practice it means that the appurtenant solution does not consider some of sources of risks and the impacts of risks´ realization on public and firm assets; very often it goes on:

- elimination of harmful phenomena: from the followed technological facility; and phenomena that are caused to

happen by bad decisions of management of firm or administrative bodies,
- neglecting the risks impacts on human, properties and environment in the technological facility vicinity.

In the second domain, on the basis of results of investigations given in [10], [11], [13] and data obtained directly in practice [12], it holds that in technical practice there are used the following choices of sources of risks:

1. Sources of risks determined either by legislative, or by experiences of worker who solves the task.
2. Only technical sources of risks in a given technological facility. Usually, it goes on:
   - risks connected with material (fulfilment of required parameters, supplier relations - alternative material etc.),
   - risks connected with construction and interfaces of components and facilities (free procedures, presence of unstable hazardous substances….),
   - risks connected with production procedures, e.g. at welding, specific works with millers, lathes etc.,
   - risks connected with conditions that are necessary for production of quality product, e.g. certain pressure, certain temperature or certain humidity of surrounding medium etc.,
3. Technical sources of risks and human factor. To items given in point 2, they are added risks connected with false operation of workers. In this case it is also required the prevention of false technical operations in technical work.
4. Technical sources of risks and human factor the broadest most interpretation. To items given in point 3, they are added risks connected with sources of organizational accidents (i.e. bad decision-making, using the false procedures etc.).
5. Technical sources of risks, sources of risks threatened the workers lives, health and safety, sources of organizational accidents and sources of risks in working environment.
6. The sources of risks given in point 5 plus external sources of risks.
7. The sources of risks given in point 6 plus sources of risks from interfaces of facilities, components and system that disturb the technical integrity and their originators are in automatization, education and good skill. In this case it is also required the property protection, data and information protection, specific knowledge and know-how protection.
8. All Hazard Approach in the form described in [13]. This selection considers the risks from the five basic disaster sources and it is challenging on data, methods, knowledge, experience and time period. It requires the strategic system proactive approach and it has according the results of FOCUS project [10] a lot of deficits at use in practice.

In the third domain, on the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], it holds that in technical practice there are used there are used partial, integrated and integral (systemic) risks.

Partial risk is risk connected with one asset. The partial risks are various, e.g. health risks, technological risks, risk of fire etc. For their determination, many legal rules and supporting software exist [13].

Integrated risk represents the sum or other aggregation of partial risks. It is used e.g. in protection of workers lives, health and safety [13].

Integral (systemic) risk is based on system concept of entity and it also includes the interfaces among the assets and components of technical work [10], [11]. It is given by relation

$$R(H) = \left[\sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int_S F(H, A_i, P_i, O, t) \mathrm{d}S\mathrm{d}t \right] \cdot \tau^{-1}$$

in which H is the hazard connected with given disaster in site of technical work; A_i are values of followed assets for i = 1,2,…, n; Z_i are vulnerabilities of assets for i = 1,2,…, n; F is the loos function; P_i are the occurrence probabilities of damage of assets for i = 1,2,…, it goes on conditioned probabilities; O is vulnerability of protective measures; S is the size of followed space; t is time measured from the disaster origin; T is the time period of losses origin; and τ is the disaster return period. The problem is unknowing the form of loss function, and therefore, special strenuous procedure need to be used in practice [10].

It is evident that for long-term ensuring the safe technical work, it is necessary to consider the integral risk. Because in above given formula, the loss function is not known, so in publications [10], [11] there are given procedures used in practice for estimation of integral risk; they are based on the analysis of real and simulated disasters´ scenarios. The procedure given in Figure 3 is used.

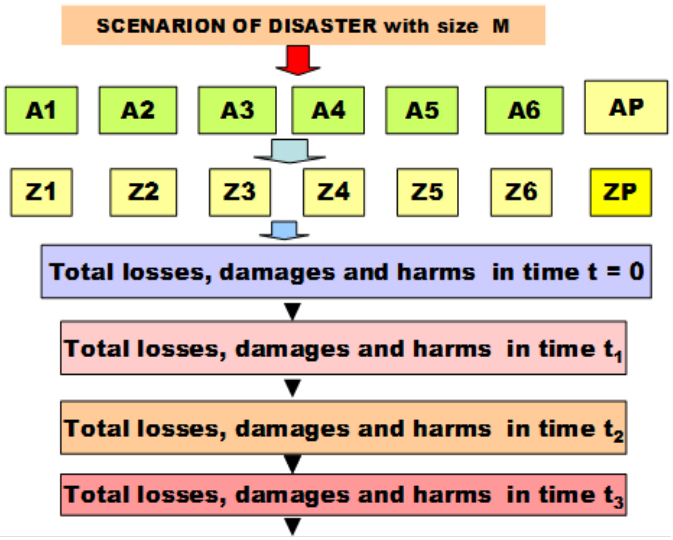

Fig. 3. Procedure of determination of losses caused by technological facility failure based on scenario.

It is necessary to note that determination of individual types of risks also differ in exactingness on data and methods of their processing [11], [13]; the lowest challenging is the

determination of partial risks, and therefore, these are mostly used in practice, although their validity compatibility with regard to total technical work safety is very limited.

In the fourth domain, on the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], it holds that in technical practice there are used:

- risks are determined and mastered after technological facility creation [10]. This way has danger that some of important risks that could be only mastered by specific technical measures in assignment of technological facility can be only reduced by organizational that are lower effective than technical measures [10], [11], [12],
- specified risks are considered from the beginning of technological facility design up to its termination from operation. This way depends on requirements of legislation, knowledge and skill of designers, constructors and operators, i.e. it does not guarantee the consideration of all risks sources,
- risks are considered from the beginning of technological facility design and it is used strategy verified in practice using the Defence-In-Depth approach that requires system thinking, multi sectoral and transdisciplinary knowledge and experiences [10], [11], [12].

The ensuring the technological facility safety and all others entities depends on quality of work with risks and on accessible possibilities of both, the technological facility management and personnel and the public administration [12]. The mastering the risk in a given time and in a given site requires: knowledge; compatibilities; finance; material, technical and human sources. Therefore, we need to deal not only with alone work with risks but also with practical procedures that are used at decision-making on the risk mastering.

In the fifth domain, on the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], it holds that in technical practice it needs to use the process model shown in Figure 4 [10], [11].

It is evident that if we are not able to identify and analyse some risk, so we are not capable effectively to defend against it. The error, which we do at risk analysis, is transferred to emergency, continuity and crises plans, and it reduces its value in relation to planned measures directed above all to protection of human lives and health, and also in operation of rescue units participating in performance of rescue operations.

The aim of risk management is to find the optimum way, how to reduce the founded risks on required socially acceptable level, possible to keep up on this level. The risk engineering aim is then the proposed measures and activities for risks mastering by way determined by risk management to realize and to ensure their reliability and function. The risk reduction is almost always connected with increase of expenses and claims on knowledge. The risk management is led by effort to find the boundary to which it is endurable the risk reduction so the spend expenses would be socially acceptable.

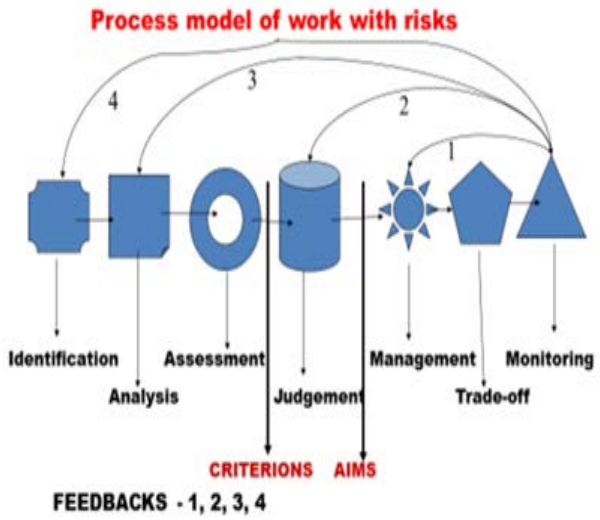

Fig. 4 Process model of work with risks Criterions = conditions that determined when the risk is acceptable, conditionally acceptable or unacceptable. Aims denote required states. Numbers 1,2,3,4 denote feedbacks that are used if the monitoring shows that followed requirements on safety are not fulfilled [10]

Important role at work with risks it plays both, the risk assessment and the risk judgement. According to requirements given in [13], the assessment means: the carrying out of certain operations in demanded extent and quality in harmony with accepted assessment methodology; completeness of assessment; considering the advanced science findings; evaluation of uncertainties in case of extrapolations use; unified expression of risk; transparency and reproduction of risk assessment.

At risk judgement it goes on correct judgement of risk acceptance and on choice of correct reaction to risk. The risk acceptance is in reality the result of several types of acceptability – technical acceptability (dependability and complexity of technologies, technical works, machines and facilities); economic acceptability (expenses) and socially-political acceptability (perception of risks) [10], [11], [13]; for risk judgement the risk matrixes are often used.

In harmony with the public interest it is necessary so the risk acceptability might social dimension. Therefore, it is necessary to consider:

1. For whom the risk could be acceptable; for risk originators, for politicians or for public?
2. Who determines the acceptability; politicians adjudicate on that, which is legal, and so they could not adjudicate on that, which is acceptable.
3. If at risk determination there were discussed actually permitted risks, intolerant threshold values and attitudes of public to risks.

Risks are inherent factors of human system, i.e. they were, are and will be, and in addition to present ones, new ones will occur. Therefore, the management of risks requires risk dimension and measurement of risk, which consider not only

the physical damages, harms, victims and economic losses bulk, but also the social, organizational and institutional factors. Therefore, it is used the risk definition given above.

Group of present techniques for risk determination does not represent the holistic approach, and most of them do not consider the linkages and flows among the system elements as the vulnerable system items, that intensify the damages, losses and harms. Often at allocation of tasks connected with risk mastering, it forgets on reality that mastering the risks connected with the technical work needs to be split up among the all technical work management levels and also on local, regional and state level of public administration [11], [13].

In our conditions the Total Quality Management (TQM) [14] is used. For its prosperousness the series of ISO norms 9000, 14000 etc. were created. The TQM approach lies in requirement that in the process of entity quality increase the all employee participate, from normal employee up to top managers. The process of quality increase (i.e. at the highest level it goes on integral safety increase) comes out from impulses from needs of customer / citizen.

The outputs from risk management process for needs of good governance according to TQM are:

1. *Risk assessment document* – records on all appurtenant risks.
2. *Top risks list* – list of selected risks, the mastering with them ha the highest claims on sources and time.
3. *Retired risk list* – serving as the historical reference for future decision-making.

Technique of alone risk management from the point of provident handle with forces, sources and means formally reviews before at each phase of work with risks the results of management and mastering the risks in the context of profits and expenses on outputs. The Coase theorem [15] is used for determination of economic optimum in expenses on mastering the risks.

In the sixth domain, on the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], it holds that in technical practice it needs to understand that technological facility risk management and risk mastering are not task of individual, not one organisation or one sector. It goes on the collective effort of all participants. It is evident that: professionals who have knowledge, data and capability to apply suitable methods can only determine the risk; and only persons who have appropriate competence can decide on handling with risk, i.e. legally determined representative of public administration or technical work; and risk mitigating and control could be performed only by professionals who have appropriate knowledge, capabilities, skill, equipment, sources and means. The public is lawful participant at risk mastering because it goes on its security and quality of life. Because risk sources are always more and countermeasures for their mastering are often conflicting, it is necessary to use the risk management aimed to safety [14].

The negotiation with risks goes from present possibilities of human society and it lies in splitting the measures and activities for risk mastering into categories with following aims:

- part of risk is reduced or averted by preventive measures,
- for part of risk the mitigating measures are prepared for prospective response (warning systems, measures of emergency and crisis management,
- insurance for cover of expected losses and damages at risk realization,
- systematic production of reserves for successful response to risk realisation and for renovation,
- preparation of contingency plan for realisation of low frequent risks realizations.

In practice, we use several levels of risk analysis: A – preliminary risk analysis; B – standard risk analysis, i.e. fast and low precise risk analysis; C – detail risk analysis in overall context; and D – individual and specific risk analysis. The individual levels differ by demands on qualification of data and processing methods; the highest demands are required at strategic planning directed to safe system in long term time scale.

According to the aims of negotiation with risk, it is necessary to differentiate the methods that are suitable for: risk identification only; determination of risk value that is needed for strategic decision-making; determination of risk value for checking the risk of real process in certain time and place, when it is possible to use only verbal scale for fast and tactical decision-making. So the risk values might possess the clear validity, it is important to use not only the tool, but also clearly defined value scale for both, the partial items classification for risk level determination and the set of these items.

So the executive body of organisation could effectively work with risks, it is necessary to determine the procedure for risk determination by legal rule, and simultaneously to determine the value scales by which the outputs of tools for determination of risks in organization are interpreted; i.e. it is necessary to determine which risk value is acceptable, which one is conditionally acceptable and which one is unacceptable. In tools for risk determination, it is necessary to distinguish the sophisticated tools for professional sphere and tools for administrative bodies for which the check lists are the most suitable.

In the seventh domain, on the basis of results of investigations given in [10], [11] and data obtained directly in practice [12], it holds that in technical practice it needs to understand that from system viewpoint the ensuing the technological facility safety is the requirement on the complex system, not on its components, and from this view the scheme of safety management shown in Figure 5 is valid. From this figure it follows that selection of measures for system safety building predetermines the level of security as measure of system condition and its sustainability in time.

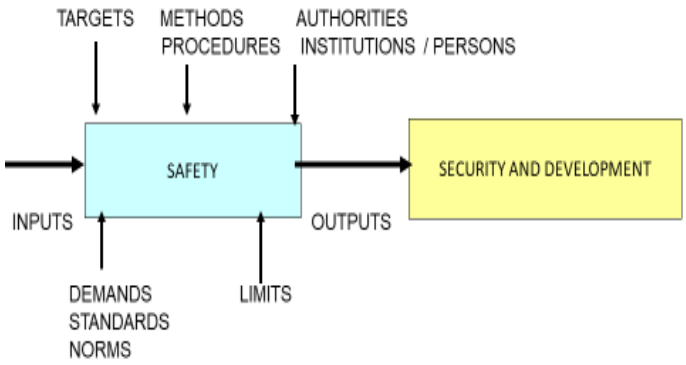

Fig. 5 Process model for ensuring the actual entity safety formation, its inputs and outputs [10]

Knowledge from physics and other exact disciplines shows the properties of materials and their interfaces depend on conditions in which they are situated. It means that required properties and required behaviour of technical works can be only ensured in certain interval of conditions; i.e. the technological facility safety has limits.

Risks are inherent attribute of human system and each technological facility, and therefore they need to be managed during the whole technological facility life time (Fig. 6). The aim of risk management is to ensure the safe technological facility, i.e. also their competitiveness today and in future, i.e. it goes on determination the priority risks and their correct management. The risk management needs to ensure the technological facility safety at conditions normal, abnormal and critical. The model of technological facility safety management is shown in Figure 6.

On the basis of present knowledge given in [10], [11], [13], the safety management system (SMS) of complex object is built on principles of process management and it includes the organization structure, responsibilities, practices, regulations, procedures and sources for determination and assertion of prevention of disasters or at least the mitigating their unacceptable impacts. Usually, it deals with many questions, apart from also the organisation, workers, identification and assessment of hazards and risk that follow from them, organization management, change management in organization, emergency and crisis planning, safety monitoring, audits and review.

The process safety management is concentrated to six processes: concept and management; administrative procedures; technical matters; external co-operation; emergency preparedness; and documentation and investigation of accidents. These processed are further divided into sub processes that are in detail described in [10], [11].

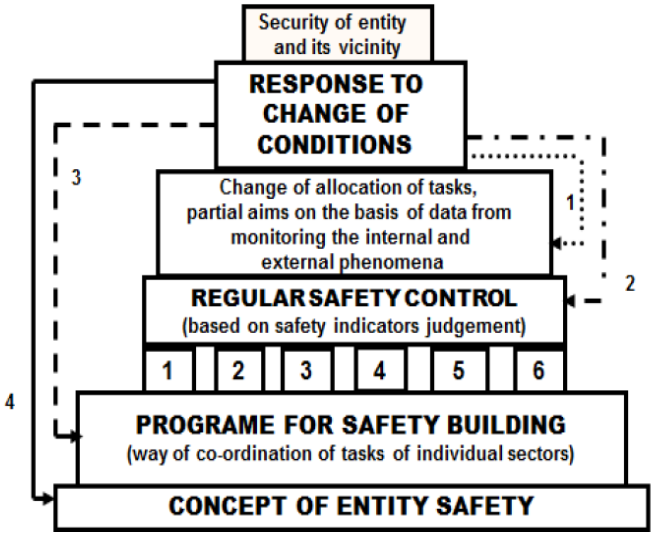

Fig. 6 Safety management system of technological facility [11]

The processes coordination is aimed to ensuring the safe object at conditions normal, abnormal and critical. The coordination in this context is understood as the controlled process, the aim of which is to create and to operate the technological facility in required quality; it follows the processes in spheres as: space and time, personnel, material, finance and documentation [10], [11].

For support of safety management system, it is necessary to process the series of remedial tools as: security plans; on-site and off-site emergency plans; continuity plans; crisis plans; in practise the risk management plans for priority risks have been very came in useful [11].

V. Conclusion

The results in [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] and [12] show that at present practice the alternatives of work with risks used at technological facilities safety management are often very simple. In all important domains they are still predominated the techniques of work with risks that do not respect the system nature of technological facilities and the dynamics of world development. From the study of followed technological facilities documentations [12] it is obvious that at creating their safety, the experts from different fields work separately, which of course does not guarantee optimal safety, or even the optimal cost.

The research showed that in practice there are not used all knowledge and experiences which we have for risks, risk management and trade-off with risks directed to safety.

Big role plays the reality that work with risks may not be only limited to mathematical computations. The correct work with risks requires: logic system thinking; technical knowledge; and experience from practice.

Discussion with more than 100 technological facilities workers [12] showed that there are used simplified procedures because:

- the workers in broad professional and management spheres do not have appurtenant knowledge on work with risks; they rely on software and often they have problems with technical thinking,
- qualified procedures of work with risks have high demands on data, the collection of which is expensive and time consuming,
- qualified procedures of work with risks have high demands on special processing methods (as Decision Support Systems for specific site conditions) because problems are multi criterial,
- laws and technical norms and standards do not specify demands on works with risks, especially real demands on data and methods,
- quality management and trade-off with risks is also time consuming.

Because for human security, the high qualified work with risks is necessary, it is needed:

1. To teach physics, technical knowledge, principles and skills.
2. To teach multi criterial methods and their principles.
3. To ensure the data sets for risk assessment in real territories and real technical facilities.
4. To force facility owners and managers to trade-off with risks in the frame of public interest.
5. To teach rules for risk management and trade-off with risks in complex world in which there are: non-homogeneities, anisotropies, leap changes, non-linearity's etc. It is necessary to use multi criterial approaches, expert experiences and rules for conflict management.
6. To specify the demands of risk management and trade-off with risks by laws, norms and standards.

ACKNOWLEDGMENT

Authors thanks for grant to EU and Czech Ministry for Education; CZ.02.2.69/0.0/0.0/16_018/0002649 - project RIRIZIBE.

REFERENCES

[1] R. Briš, C. Guedes Soares, S. Martorell (eds), *Reliability, Risk and Safety. Theory and Applications.* ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362p.

[2] B. Ale, I. Papazoglou, E. Zio (eds), *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448p.

[3] C. Bérenguer, A. Grall, C. Guedes Soares (eds), *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035p.

[4] IAPSAM (eds), *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (and Annual European Safety and Reliability Conference).* ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889p.

[5] R. Steenbergen, P. Van Gelder, S. Miraglia, A. Ton Vrouwenvelder (eds), *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387p.

[6] T. Nowakowski, M. Mlyńczak, A. Jodejko-Pietruczuk, S. Werbińska-Wojciechowska (eds), Safety *and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453p.

[7] L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger (eds). *Safety and Reliability of Complex Engineered Systems: ESREL 2015*. ISBN 978-1-138-02879-1. London: CRC Press, 4560p.

[8] L. Walls, M. Revie, T. Bedford (eds), *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. ISBN 978-1-315-37498-7. London: CRC Press, 2942p.

[9] M. Cepin, R. Bris (eds), *Safety and Reliability – Theory and Applications.* ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627p.

[10] D. Procházková, *Safety of Complex Technological Systems.* ISBN: 978-80-01-05771-1. Praha: ČVUT 2015, 208p.

[11] D. Procházková, *Principles of Management of Risks of Complex Technological Facilities.* ISBN: 78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/10467/72582

[12] ČVUT. *Archives of Solved Tasks from Safety Management and Crisis Management.* Praha: ČVUT 2017.

[13] D. Procházková, *Analysis and Management of Risks*. ISBN: 978-80-01-04841-2. Praha: ČVUT, Praha, 2011, 405p.

[14] M. Zairi, *Total Quality Management for Engineers.* Cambridge: Woodhead Publishing Ltd, 1991.

[15] R. Coase, "The Problem of Social Costs". *Journal of Law and Economics*, Vol. 3, The University of Chicago Press 1960, pp. 1-44.