RISK OF PROCESSES AND THEIR MANAGEMENT

Dana Procházková and Authors´ Team

Praha 2017

Reviewers:

Prof., Dr., Dipl. Ing. František Holešovský
Assoc. Prof., Dipl. Ing. Václav Jirovský, PhD.
Assoc. Prof., RNDr. Miroslav Rusko, PhD.
Dipl. Ing. Karel Dach, PhD.

Ústav bezpečnostních technologií a inženýrství
Assoc. Prof.,RNDr. Dana Procházková, PhD., D.Sc.

ISBN 978-80-01-06186-2

CONTENT

PREFACE

Publication „*Risks of Processes and Their Management* "is released on the basis of information and recommendations from two international conferences (Risks of business processes 2015 and 2016), which held in Děčín on the Czech Technical University ground and were organised in co-operation with the Jan Evangelista Purkyně University located in Ústí nad Labem. Papers presented on both conferences showed the new findings connected with: identification and analysis of risks in territory and in businesses; management of important risks; and trade-off with risks under conditions of security systems with accent to solution of safety of businesses, infrastructures and territory.

By this way, it was collected the sum of new theoretical, technical, organisational and methodical findings for support of effective, practical and powerful systems for pulling off the risks at conditions normal, abnormal and critical. This was supplemented by information on crisis management and on experiences from putting off the critical situations (operation crisis plans for response to emergency and crisis situations, problems of adequacy of maintenance, qualified response to businesses´ accidents, natural disasters etc.) that showed the change of targets and management structure at critical situations.

Evaluations of mentioned papers and their conclusions showed that the powerful public protection is intimately connected with safety of entities technological and social, and in particular with critical infrastructure safety that ensures pursuing the basic State functions, namely at crisis conditions. ***Therefore, on their ground it originates the project*** with the goal to summarize the relevant results, to underline new knowledge and to show the road forward. The project result is the present book that contains seventeen chapters split to fifth parts.

Great thanks belongs to authors of chapters for effort to apply integrated view on risks in different sectors of human activities and their partial domains, which enables to compare approaches, methodologies and key techniques and procedures that are connected with work with risks. From human security and development reasons it does not go on different make-believes with risks based on theories, but on effective procedures targeted to risks´ control so they might not cause serious damages to humans and decline of human civilisation.

Great thank belongs to reviewers ……., who help me to improve the present book.

Specific acknowledgement and thank I express to Dipl. Ing. Lucie Povolná from the Jan Evangelista Purkyně University in Ústí nad Labem for help with groundworks collection and to Mgr. David Borovička from the Czech Technical University in Prague for technical works connected with the publication issue.

I am indebted to the Czech Technical University in Prague, and especially to the Associate Professor, Dipl. Ing. Václav Jirovský PhD., the head of department of security technologies and engineering for chance of present book processing.

Praha, March 25, 2017 *Dana Procházková*

Chapter 1

OUTLINE ON RISK, RISK MANAGEMENT AND TRADE-OFF WITH RISKS*

1. Introduction

For ensuring the human security and development, the safe human system is necessary [1-3]; the human system has different levels – village, city, organization, business, region, State etc. For ensuring the humans´ lives in a safe space there is necessary to manage and trade-off with risks properly on all mentioned levels, i.e. to apply the measures and activities targeted to the existence, security and development of human system. The basic tools of human society for achievement of these objectives are the human society governance and the correct application of knowledge and experiences connected with trade-off with risks respecting the public interests. In this respect the great role plays the management and engineering disciplines, the aim of which is to arrange the human security and sustainable development.

The present cognition [3, 4] shows that humans need to take care on public assets: human lives, health and security; property and welfare; environment; critical technologies and infrastructures, Figure 1. The tool that is aimed to mentioned targets is an integral (complex) safety. To reach just mentioned targets, the problems on several levels: technical, functional (organisational, operative), tactical, strategic and political (Figure 2) have been solved by a way that solutions on all levels have been interconnected.

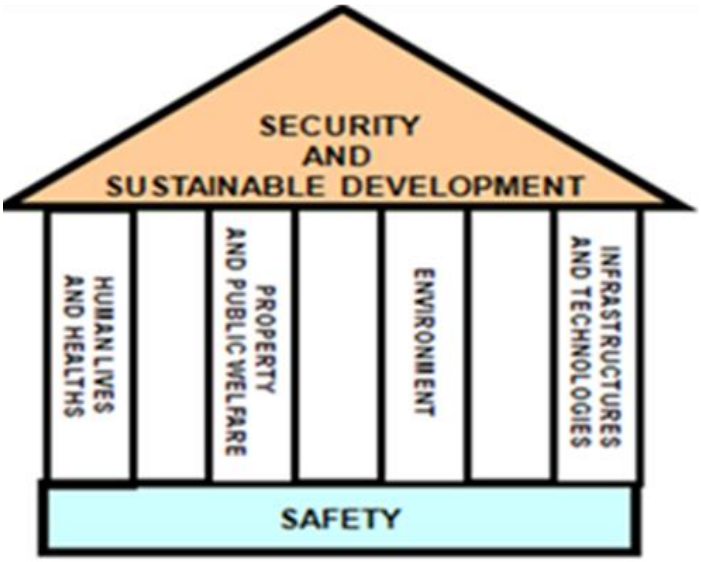


Fig. 1. Human system public assets.

Author: Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc. Czech Technical University in Prague, Praha, Czech Republic, prochazkova@fd.cvut.cz

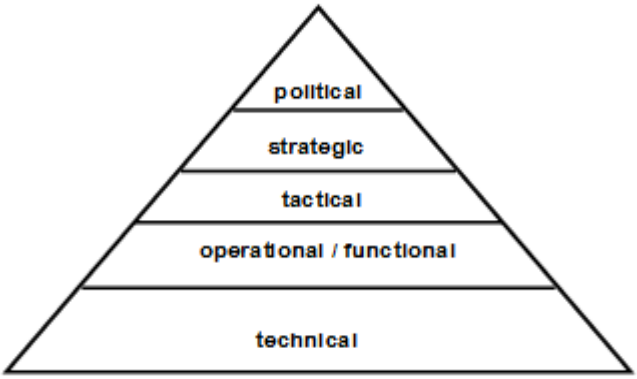


Fig. 2. Levels on which security problems should be addressed.

State of art of problems´ solution, according to knowledge, summarized in works [4-6], is the following:

- each object under consideration is a system, i.e. it is characterized by elements, linkages and flows,
- the system vulnerabilities are also caused by linkages and mainly by flows of energy, information, material, finances etc. among the system elements that cause couplings; mentioned couplings create often interdependences that are often the causes of failures and often by a cascade failure of several partial systems at occurrence of extreme (beyond design, severe) disasters, Figure 3. The nature of interdependences is physical, cyber, organizational and territorial [5].

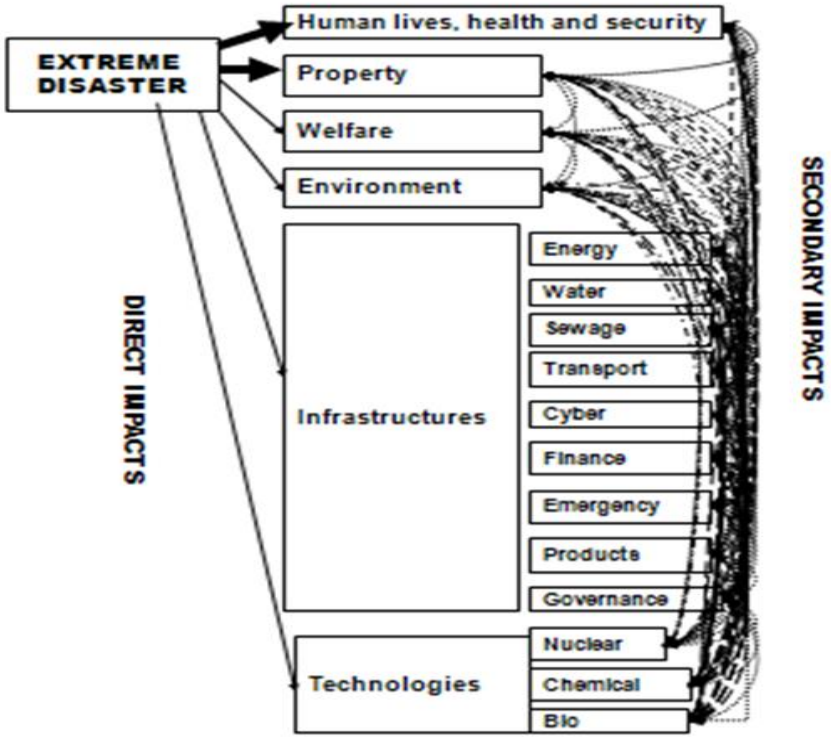


Fig. 3. Impacts in the human system at extreme disaster; anthropogenic measures and activities ensure the protection of public assets only for disasters with size smaller than design disaster; only at defined nuclear facilities there are carried out measures and activities against selected beyond design disasters.

The recent cognition [3-6] shows that the present world and its objects are represented by a model denoted as a system of systems i.e. several overlapping systems that are open and fulfil certain functions. They are interconnected by linkages and flows which create mutual interdependences that under some conditions cause specific vulnerabilities. A system according to its core means more than only a sum of parts, and therefore, the stress is put on: a study of interactions and associations; non-linear thinking; interactions; inductions; feedbacks; and experiments or realistic simulations. E.g. feedbacks cause the non-linearity in the system behaviour and cause that the behaviour is not predictable, and therefore, it is not possible to use the common prognostic methods for the identification of possible system states. The consequence is an occasional occurrence of unexpected situations that threaten the humans, and it is difficult to get over them.

The complexity of systems with which we work in practice is different. According to work [6] four types of system configurations are used; they are: simply organized units; composite systems; complex systems; and set of overlapping systems.

Behaviour of simply organized units is clearly given by structure and properties of units and it is described by analytic functions. The composite systems are understood as a representation of elements that are organized and connected in a certain way and because of proper structure they fulfil certain functions. Their behaviour is described by results of statistical solutions based on analytic functions, the parameters of which are variable in a certain interval, which are a reflection of various possible states / variants of system behaviour.

The complex systems have many components (often systems too) that interact together and are organized in several levels [6], which causes that we observe: suddenly emerged behaviour features that is not possible to obtain from the knowledge of components' behaviour, it is the so-called emergence; hierarchy; self-organization; and various management structures, which all together seems as a chaos, and therefore, in their description there are random and epistemic uncertainties. The complex systems behaviour is described by results of simulations taking into account the existence of epistemic uncertainties.

The system of systems (SoS), i.e. a set of several overlapping systems (often complex systems). It is very complicated, and therefore, its behaviour can be only obtained if a multidimensional and inter-dimensional approach is applied and it is based on simulation of variants by multi-criteria procedures.

Since the solution of many problems in practice means to consider the complex systems and the SoS, the system thinking is the fundamental principle of research if we deal with safety. The system thinking means: to see both, the whole and the details at the same time; ***to focus on the dynamics of processes;*** to pay attention to relations, associations and interactions; ***to take into account the roles of feedbacks;*** to consider the relativity of possible situations; and to think in a long-term way.

At management and engineering solution of complex systems and systems of systems, it is then *necessary to use the multi-criteria approach and in a case of system of systems, it is also* necessary to consider the cross-sectional risks that are the causes of emergent interdependences originating at certain conditions, and therefore, to their detection the attention of engineering disciplines is concentrated at system design. At their problems´ solution the tools are based on: the theory of chaos; theory of fuzzy sets; complexity theory; and theory of possibilities – set of references to their derivation is in books [5, 6].

In case of SoS management, we need also to respect the basic requirements, i.e. co-existence of overlapping systems [7]. For human goals fulfilment, it is necessary to

arrange the co-existence of important systems, minimally social, environmental and technological systems that create the human system.

Regarding to present view of the UN, EU and public interest [1-3], the ground for human being is a conservation of existence, security and potential for development for humans. In this context in practice, the following terms are used:

Security is the state of system at which the occurrence of harm or loss on system assets (protected public interests etc.) and the system itself has an acceptable occurrence probability (it is almost sure that harm and loss do not arise). It means that it ensures a certain stability of system in time and space, i.e. a sustainable development which means that the system is well protected against internal and external disasters of all kinds.

Safety is a set of human measures and activities for ensuring the existence, security and sustainable development of system and its assets. Its measure is the effectiveness of appropriate measures and activities at ensuring the system assets security and sustainable development.

Secured system is the system, in which the system and its assets are not threatened by disasters, the origin of which is inside and outside of system, including the human factor.

Safe system is the system, in which the system and its assets are not threatened by disasters, the origin of which are inside and outside of system, including the human factor, and the system does not threaten itself and its vicinity not at its critical conditions.

Human system safety management is the management of human system directed to human system safety, the product of which is the security and sustainable development of all public assets.

The engineering is a set of disciplines that realise the tasks determined by management procedure into practice. The risk is for engineering practice expressed as probable size of losses, damages and harms on followed assets that are caused by a given disaster with specified size (the size of normative hazard) and that are rescheduled for a certain time unit (usually 1 year) and a certain object or a certain site. The risk engineering was the 20^{th} century phenomenon and on its base there was set up in developed countries the groundwork for human development that is quite resistant against to traditional disasters, namely natural ones; human, animal and plant diseases; technology failures; and social disasters.

According to definitions used by the UN, Swiss Re, World Bank etc. the risk engineering:

- is the systematic use of engineering knowledge and experiences for the optimization of protection of human lives, environment, property and economic assets, i.e. for the optimum reach of security and sustainable development of human system,
- has a main purpose to reduce all types of harms and losses by the means of aimed and qualified trade-off with risk.

It is necessary to note that at present practice the risk engineering has not yet been interpreted by an explicit way and different concepts are not often distinguished.

It is necessary to consider that risk engineering is not a static discipline because it has been developed in time. ***The problem of present specialists, mainly oriented to calculations***, is that they do not distinguish the different concepts, and in some cases such ignorance is a cause of incorrect solutions (e.g. if they use standards and norms for secured system and the correct solution of problem requires standards and norms for the safe system because the failure of system has a great potential to damaged assets being in system and in system vicinity); see lessons learned from recent important accidents [6, 8].

2. Risk

The term “risk” has origin in the middle Ages. There are different definitions of risk for each of several applications [4]. The widely inconsistent and ambiguous use of the word is one of several current criticisms of methods to manage risk. Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an unfavourable outcome). The notion implies that a choice having an influence on the outcome exists (or existed). Potential losses themselves may also be called "*risks*".

The present concept has been developed since 30s of last century. According to present standards for strategic management, the risk expresses the probable size of unfavourable and unacceptable impacts (losses, harms and detriment) of disasters with size of normative hazard on system assets or subsystems related to a given time interval (e.g. 1 year) and a given site; i.e. it is always the site specific [4].

The risk partly depends on the hazard and partly on the vulnerability of assets in a given site (i.e. on the sensitivity of each individual asset in a given place against to disaster manifestation in a given site). It expresses a possibility what it might be happen [4]. From this fact it follows that for each management it is important to know the risk, namely in comprehensible expression. In practice of public administration, it is certified the risk expression in a form that by risk analysis and assessment it finds that on specific section:

- there is necessary 5 million a year for remedy of harms caused by existing risk,
- each ten years ten persons die in a consequence of given disaster,
- each five years the property damages caused by disaster exceed 5 billion EURs etc.

The typical risk properties are the random and epistemic uncertainties (epistemic uncertainties = vagueness). If we want to manage the risk, we need to identify, analyse, assess it and after this to decide, what we can do, in dependence on our possibilities – knowledge, staff, technical means and finance sources. For this, we need to use a lot of different methods, tools and techniques and also principles of good practice (good engineering practice) [4].

In practice we work with three types of risk: the partial one that is only related to disaster impacts on one asset; the integrated one that is related to disaster impacts on several assets – e.g. sum or other aggregation of impacts´ rates; and the integral (systemic) one that is related to disaster impacts on the entity that is understand as a system. The last concept is necessary for solution of safety and security, the structure of which is complex, i.e. the system of systems, Figure 4.

As we said above, the principal attributes of each risk are ***uncertainty and vagueness***. We divide their sources into three groups, namely to the variations originating at: usual system process life cycle at normal conditions in the vicinity (uncertainties); real changes of system process life cycle in the time and space that affect occasional extreme values occurrences – we consider normal and abnormal conditions - (uncertainties and vagueness); variable system process life cycle that is caused by process changes in time and space, induced by outside causes or by critical conditions (vagueness).

The data uncertainty relates to the dispersion of observations and measurement; i.e. a random uncertainty. It may be included into assessment and prediction by mathematic statistics apparatus. The vagueness relates to both, the lack of knowledge and information and the natural variability of processes and actions that caused disasters. For processing the vagueness, the mathematic statistics apparatus is insufficient and therefore, it is necessary to use the recent mathematical apparatus that offers e.g. extreme values theory,

fuzzy set theory, fractal theory, dynamic chaos theory, selected expert methods and suitable heuristics based on the existence of several variants of solution.

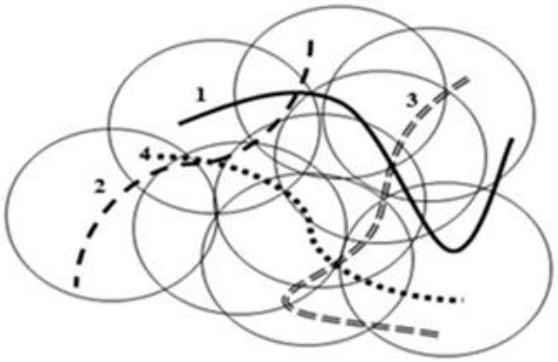


Fig. 4. Scheme of complex systems – 1, 2,… are the processes being under way in mentioned entity.

Because in each entity: several disasters are the sources of risks; each disaster scenarios depends on the entity momentary conditions and on the real disaster properties that pre-determine the real forms of disasters´ scenarios. These facts need to be considered when we want to ensure the safety and the security.

Let k is the number of possible disaster scenarios for the object / location / area, p_i is the occurrence probability of the i-th disaster scenario, i = 1,2,..., k, c_i is the overall impact of the i-th scenario disaster, i = 1,2, ..k. to the assets, then the risk R associated with the disaster with respect to the assets in a given place is determined by relationship

$$R = \sum_{i=1}^{k} p_i \, c_i \, .$$

If we relate the risk to just one asset, i.e. human life and we consider that today's acceptable probability of human casualty is 10^{-5} in case of individuals and $10^{-3} \cdot N^{-2}$ in case of group of persons, where N is the number of affected individuals [4].

In the selection of specific measures and actions to ensure the safety objectives we are considering contemporary targets, which means to achieve likelihood of occurrence of human casualties at 10^{-6} at individuals $10^{-4} N^{-2}$ at groups of people, where N is the number of affected individuals [4]. Number of vulnerable people is calculated according to formula

$$N = S \cdot h \cdot f_s \, ,$$

where S is the affected area in ha, h is the density given by the number of persons per ha, f_s is the correlation factor when only part of the territory is inhabited.

In terms of risk as a proportion of total damage, the total values of assets´ risk are dimensionless quantities (a number between 0 and 1 or between 0 and 100, depending on the chosen scale) related to the chosen time unit. On the basis of representative set of empirical disaster scenarios and corresponding calculations of losses and damages in a particular area it is possible to calculate the average total risk associated with disaster in a given area [4].

3. Present work with risk

Work with risk is expressed by model shown in Figure 5 [4, 6]. It starts with definition of concept of work with risk (system characteristics, determination of assets, specification of aims), on the basis of which the risks are identified, analysed, assessed, judged, managed, traded-off and monitored. The criterions determine the conditions at which the risk is acceptable, conditionally acceptable or unacceptable. The aims in real case are selected from further given possibilities: to reduce risk to certain level; to secure the system, i.e. to ensure system security; to ensure safe system, i.e. to ensure security for both, the system and its vicinity. The feedbacks denoted in Figure 5 are used in case if the monitoring shows that the risk level is not on required level; firstly, it is used the cheapest feedback 1; in case of its failure the feedback 2 etc.; at huge harms immediately it is used the feedback 4 that means the change of concept of work with risks.

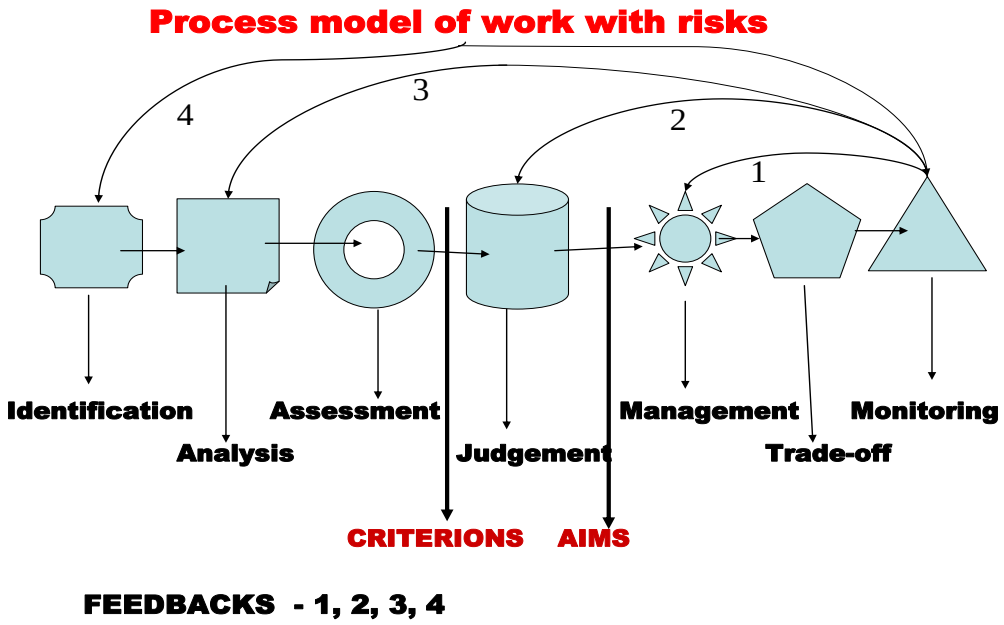


Fig. 5. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks.

If we want to trade-off with any risk, in the first, we need to identify it and after this to analyse it. Both steps need to be carefully performed because each inaccuracy in the given steps cannot be rectified in the following. For the steps mentioned, the professional knowledge of problem solved is the fundamental. The effective methods are What, If analysis, Check List analysis, Event Tree analysis etc.; the use of each method depends on the level of problem knowledge and on the target of risk analysis [4]. E.g. risk analysis procedure for the use in disaster prevention contains according to the following parts:

- risk analysis definition and determination of study depth,
- description of considered system, object, equipment and the delimitation of its boundaries,
- identification and description of disasters, i.e. sources of risk,
- relative evaluation of disaster´ criticality (hazard assessment) and selection of relevant disasters for further study,
- identification of possible disaster impacts on considered system and its vicinity,

- compilation of possible disasters scenarios, in which unacceptable impacts can occur and selection of representative disaster scenarios,
- estimation of risk amount / size / rate),
- risk presentation.

Risk amount / size / rate is a numerical value; e.g.: the number of deaths caused by disaster (a year); numerical function giving for each N in a certain interval the probability of that as a consequence of some technological accident in a year to an M or more deaths in technology vicinity. The function describes the relationship between the occurrence probability and consequences of given disaster that has certain nature. For risk representation, there is used e.g. risk matrix, number as one-dimensional amount, mean death measure, risk isolines (individual risk), f-N curve (societal risk) [4].

The acceptable risk is the amount of serious harms or jeopardy for human lives and health, home animals, environment or damages arising from existence and possible realisation of disasters that is acceptable for person / group of persons and for society. The risk acceptability depends on social, economic and political factors, and also on a perceived profit arising from the positive activity of risk sources (disasters) from the viewpoint of analysis of costs and profits for society [4].

The risk is a measure of unacceptable impacts caused by an expected disaster on public assets (generally considered assets because in practice, we use different risk analysis targets) in a given site. In the business domain the protected assets (interests) are also a safe business, profit, competitiveness and the like. With regard to these assets, the disasters are also the following phenomena: market failure; lack of finances / suitable technologies / qualified human sources; incompetent management of business; loss of competitiveness; external natural and other disasters that have impacts on business; intended damage of business outside / inside; and failure of links with vicinity / public administration.

The assessment of human (or other) system risk means the judgement of disasters´ impacts by help of one or more criteria that reflect the value scale of human society. Some of the criteria may be even qualitative and some of them are incommensurable [4]. Assessment process structure depends on facts:

1. What is assessed?
2. When it is assessed, to which moment in time it is assessed?
3. How, i.e. on the basis of which criteria, it is assessed?

General knowledge sets that when we want to assess something, we need to determine the assessment targets, the set of criterions and the scale used at assessment. The assessment generally represents an exertion of certain criteria, rating functions or preferences. It is used in several senses:

1. The first sense means to follow the process by help of process monitoring or observation.
2. The other means the comparison with some appointed limit.
3. The third one means the comparison with some appointed limit and thinking out all the more or less probable consequences, i.e. the impacts and the profits.

The last sense supports the negotiation with risks. The system assessment means the application of certain suitably selected criteria set or rating functions to the defined system. It means that we assume and specify certain behaviour in time and space, certain responses on possible reactions etc. The criteria, we divide into:

- internal, i.e. such, that ensures the assessment of appropriate system (they take note of system only), i.e. its quality, viability, fitting the certain targets, needs, demands and the like,
- external, i.e. such, that ensures the assessment of system as a part of a broader system (they take note of system and of its vicinity), i.e. viability, material and energy demands, sources, human aspects, environmental impacts, social impacts and the like,
- criteria tied up with a time trend, i.e. with possible changes of assessment in time or with changes of a system function in time (i.e. it is considered expected dynamic behaviour of system in time).

From the given facts, it follows that the assessment has several qualitative levels, namely:

- the simplest level is the comparison of real data value, quantitative or qualitative (e.g. data on the level of quality), with a certain strictly defined limit or model (that the following phenomena aroused or did not arise). The comparison with the limit is used when the surveillance is directed to the check-up of certain item quality or to the determination whether it is necessary or not to start a specified regulation or warning measures. The comparison with parameters of certain model is more typical for observation nets that have one of aims to identify phenomena in domains, which they cover,
- the impact assessment goes partly from data and partly from collected findings. It represents a tool for the complex and systematic investigation of disasters or planned actions. For this assessment type, there is important the reference level that may be represented by: original (present) conditions; conditions that will originate without any activity; some marginal or target (covetable) conditions; ideal conditions. There are systematically followed relations described as the chain of causes and impacts (disaster scenarios) and they are determined by impacts of the first order in cases in which it is possible to directly distinguish the cause. At data processing, they are used the predicative methods that are mostly based on: exact calculations; statistical formulas; experimental observation and mathematical modelling; expert approaches based on judgements, analogies and experiences; or quantities scoring, i.e. at incommensurable quantities, they are used methods of multi criteria analysis, i.e. e.g. the decision matrixes,
- the hazard assessment means the determination of disaster size on a certain level of credibility in a certain time interval and in a certain site (the time interval size and site dimension depend on the physical nature of followed disaster). For its determination, there are used the specific methods of mathematical statistics based on the great number theory,
- the risk assessment means to use the methods by which from hazard characteristics (size and occurrence probability) and site characteristics probable size of damages is determined.

At work with risks, it is necessary to consider that processes under way are not only characterised by one criterion, and therefore, it needs to be used the multi criteria approach.

The risk assessment is possible to carry out only on the basis of real, true and tried-and-true data sets on a given phenomenon that are valid for a correctly defined system and correctly defined time interval [4]. The target is to ensure the decision-making that supports the benefit for the human system. Therefore, it needs to be used the tested set of

criterions that guarantees the objectivity, the independence and the impartiality of assessment. With regard to these viewpoints we divide the criterions into:

- objective and subjective; in the objective ones, there are such criteria, the limit (comparative value) of which is created by current measurable units that are detectable by lab experiments, calculation or economic prudence,
- criterions of advantages and beneficial effect (the higher, the better) or the criterions of costs, losses and content of contaminations (the lower, the better),
- cumulative criterions that are characterised by the relation of mutual complementarities, i.e. they are mutually supplemented and supported. The higher performance of one is connected with the higher performance of the other and vice versa. The extreme cumulative criterions are such criterions, in which the performance of one is conditioned by the performance of the other; the criteria of such type warp the result and therefore, they need to be put out of the criterion set,
- alternative criterions are given by the relation of mutual competition perhaps, they are antagonistic. The higher performance of one indicator is connected with the reduced performance of the other and vice versa. The extreme alternative criterions are absolutely eliminated and therefore, they must be put out of criterion set,
- independent criterions are given by indifferent or variable relations.

The assessment methods from the viewpoint of approach to matter-of-fact problem we separate to: deterministic methods; probabilistic (stochastic) methods; engineering judgement; analogy; model; and aggregation of several criterions (multi criteria assessment).

The deterministic approach is based on a precondition that each phenomenon is the inevitable consequence of conditions and causes. The approach consists of fact that there is determined the vagueness of all input parameters and that from the safety reasons, there are considered marginal (usually most unfavourable) values in a given real case. Just the determination of marginal values is the critical activity of this approach. By use of different data sets and the application of different assumption sets, there are mostly obtained results that are substantially different; i.e. the output value from one procedure does not lay in the interval of deviations obtained by the other procedure. This approach is used in designing [3-4, 9].

The probabilistic approach is based on a precondition that the occurrence of each phenomenon has a certain random uncertainty, i.e. possibility of random phenomena occurrence is estimated with a certain value of probability. From the set of variants the creation of which is the critical activity of this approach, there are determined representative values as median or median + σ (σ – the standard deviation).

For the assessment of phenomena and processes that have random uncertainties and vagueness (i.e. the epistemic uncertainties) they are, at present, used the computations based on the fuzzy set theory or the possibility theory [9] that combines analytical approach with expert methods. In the case of experts´ use, it is necessary to solve the problem ***who is an expert***. With regard to discussion in world conference ESREL2011 in Troyes, the expert is a person who: has the knowledge; is neutral; has the competences; is capable to guess with the support of object matter and to reach the acceptable consensus. In some countries as the USA, there is the legal rule containing the requirements that the expert must fulfil.

At multi criteria assessment, it is possible to use the methods, tools and techniques supporting the creative thinking, e.g. Delphi method, SWOT analysis, brainstorming, panel discussion, decision supporting systems etc. [4]. Their use needs to be prudent and

careful, in order that the results bear confirmation of purpose in a value scale selected for criterions chosen for a given problem solution. For the selection of criterion sets (the order of criterions is usually important), for the establishment of scale characteristics and for the judgement of correctness or inaccuracy of outputs, it is necessary to use the empirical (experience) databases.

At risk assessment there is necessary to fulfil the following requirements:

- performance of assessment in the demanded depth and quality and in harmony with the accepted methodology,
- completeness,
- to include the recent knowledge of science,
- estimation of uncertainties and vagueness at an extrapolation use,
- united expression of risk characterization,
- transparency of the process performance of risk assessment.

If the risk assessment does not fulfil these requirements, it needs to be returned to re-processing. The involved situation arises when the risk assessment was done with the use of present scientific knowledge, but there is the lack of data for risk characterisation or the output is burdened by too big error. In this case, it is necessary to decide to postpone the decision with note that it will be performed again as far as additional data will be obtained [4].

For risk determination we use two basis approaches, namely:

1. Determination of hazard from disaster $\boldsymbol{H}$ and return period $\boldsymbol{\tau}$ (in years) is performed by methods based on the theory of large numbers, theory of extremes, theory of fuzzy sets, theory of chaos, theory of fractals etc. [4]. According to a site vulnerability in an investigated land (e.g. around a given site: square 10 x 10 km; circle with radius of 5 km) the whole damage on all assets is determined for the *H* denoted by $\boldsymbol{S}$, usually expressed in money. Risk $\boldsymbol{R}$ connected with the given disaster in a given site is determined by the relation

   $$\boldsymbol{R = S / \tau}$$

   The result is very clear: e.g. “the risk from a given disaster in a given site is X EURs and for town it is MX EURs”.
2. Determination of disaster scenario for the disaster with size corresponding to maximum expected disaster (it is possible with regard to demands of norms to use the probable size of expected disaster, or the value of standard size of determined disaster or at least unfavourable disaster) is performed; the exact scenario compilation methods [4] are used. According to data for a given land it is determined:
   - the value of whole damage on all assets in the area SS (the method for SS determination is described [4] usually expressed in money according to amount of assets and their vulnerability to the impacts of a followed disaster in the affected area, usually normalised to a certain land unit $\boldsymbol{S}$,
   - the occurrence frequency of maximum expected disaster, normalised to one year, $\boldsymbol{f}$ according to the professional data from databases or expert opinions. Risk $\boldsymbol{R}$ is given by relation

   $$\boldsymbol{R = S * f}.$$

The result is in the same form as in the foregoing case. This case is often used for technological and other disasters for which we have not good long-term catalogue (this shortage the EU want to remove by paying the special attention to the compilation of the MARS database.

4. Present risk management

If we want to manage risk, we need to identify, analyse, assess it and after this to decide what we can do, in dependence on our possibilities – knowledge, personnel, technical mean and finance sources. For this, we need to use a lot of different methods, tools and techniques and also principles of good practice (good engineering practice). According to [4] there are distinguished the management methods for:

- risk reduction in closed system considering only the technical causes of risks,
- risk reduction in closed system considering the technical and human factor causes of risks,
- ensuring the system security without respecting the system vicinity security,
- ensuring the system safety – system and its vicinity are safe,
- ensuring the system of systems (SoS) safety – overlapping systems and their vicinity are safe).

The present concept of risk management used in strategy management has been developed since 50s of the last century. As it was above mentioned, the risk partly depends on the hazard and partly on the vulnerability of assets in a given site. It expresses a possibility what it might happen. From this fact it follows that for each management it is important to know the risk, namely in a comprehensible formulation. It means that the quality of risk management depends on both the approach followed and the quality of decision.

From daily life experiences, data and knowledge summarised in professional publications mentioned in [3, 4, 9] it follows that situations, in which each human occurs and which each human solves in each moment represent to him / her the necessity of doing the decision. The deciding can relate to matters that are vitally important (the change of the way of life and that like), or to daily details (whether to go in an overfull metro / not to go in an overfull metro; cross a road when the lights are red / do not cross a road when the lights are red and that like).

Sometimes the decision takes a lot of time for deciding (e.g. while solving the working or other problems), sometimes it is necessary to decide immediately (in the situations with a direct threatening to life, real risk of a delay and that like). We adjudicate something either on our behalf (and on ourselves, what I do, what I do not do) or on behalf of our subordinate workers / persons (in harmony with their interests, but also against their interests). The decision can only be the result of arbitrament of one person, it can, however, be also the output of collective intellect. The decisions may be accurate but also false. The consequences of decisions can have the different rate of weight for both the arbitrary subject and its vicinity.

According to data in professional literature and experiences from practice concerning the human behaviour in different situations, the human reactions to external (also internal) inputs are very various. They can have the form of unconditioned reactions, as "automatic", inherent ways of reaction to inputs (e.g. the wince at an unpleasant input), facultative reactions (e.g. in the form of habits), or purposeful action controlled by will.

In psychological literature, we mostly meet with difficulties in the deciding connected with will and volitional processes, thinking, purpusefull behaviour, pertinetly in connection with the fight of incentives (while solving the internal conflicts). In the process of human manners purpuseful control, not only the deciding over a selection among the different incentives and targets is used but also over a selection between the alternatives to negotiate – not to negotiate. The person also adjudicates at selection of means and procedures in order to reach the aim, in situation requiring the interruption or the stop of activity. The capability to deal with problems correctly, prudently and in time, belongs to the basic conditions of a practical activity and creative thinking, and it is simultaneously the important component of a human personality.

At ensuring the complex safety with an accent to the protection of persons and properties, it is necessary to achive the right decision or at least such decision that will not lead sooner or later to destruction, namely_in case of a decision under the stress. The decision in this concept becomes the social process. In this process, there are the human intellect and certain inherent (natural, tacit) human knowledge and skills put forward. In the forefront, they manifest the human properties as:

- responsible approach to the problem and the results of its solution regarding the public or other assets,
- moral properties as a discernment, sense for commitment and consistency,
- the ability: to analyse the problem or situation; to take an attitude for creative approach to the problem solution; to know the art of the foreseen of the further development, to use analogy and the like,
- and also the capability to use experiences and social skills that enable to regulate the activity and his / her behaviour or the behaviour of the subordinate humans.

Just given facts form the characteristics of human factor and of well-conditioned managemental worker and it might be considered at the work with human sources. It means that the selection of managemental workers in all organisations might be performed with the aim of respecting the knowledge, capabilities, skills and experiences and not according to the political affiliation, colour of coat or other subsidiary features.

Regarding to all above, the human factor is the aggregation of human properties, capabilities, experiences that have in a given situation influence on the safety, productivity, effectivity and reliability of system, on which they act upon and they are evaluated from psychological, physiological and physical viewpoints.

The present cognition and proposition given above show that human factor cannot be considered only as a negative human manifestation. It is a present reality that positive manifestations of a human factor are currently seeked by the type of system management that is directed by knowledge – knowledge management; the human with his / her ideas is considered as an inestimable human capital. Given facts mean that human is the most critical and simultaneously the most capable part of each system.

The short description of procedure of risk management is shown in Figure 6. You can see basic important steps. Very important step is the decision if the risk is acceptable or unacceptable. Regarding the reality that the determination of the acceptability level is always very problematic and it depends on the situation in society, the risk management lean on two additional levels, namely: the insignificant one and the unacceptable one. Between these two levels, there is the domain of risk, which is acceptable with certain measures.

If risk is lower than the insignificant level, no measures and activities are required, in contrary, if risk is higher than the unacceptable level, it is immediately necessary to take

measures and activities for its reduction. The proposed measures and activities need to be further investigated from the viewpoint of their demands on economic, political and social domain; in particular, with the use of following analytical procedures: economic analysis - *"cost-benefit analysis";* legal analysis investigating the possibilities of the harmonisation of different variants with the legislation; political analysis investigating the possible political consequences following from the decision; and analysis of the public opinion.

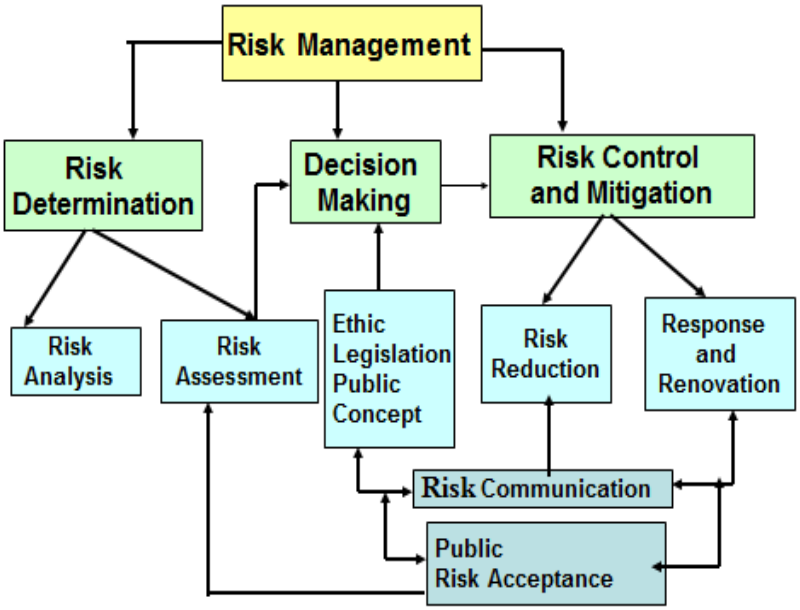


Fig. 6. Model of risk management in territory.

The analytical component of risk management is a scientific matter and its output is the proposal of several variants of a problem solution as groundwork. The part of all variants needs to be the proposal of mechanisms (Control Options) enabling the effective realisation of proposed measures. This step may be understood as the administrative one but it needs not to be underestimated or skipped because it is sufficiently known that each good mentioned executive measure without effective check-up and appropriate sanction has no effect.

The final step is the decision of the implementation of measures for risk reduction, eventually of the further following of the problem. It is necessary to accept the decision whenever, namely in case when it is evident that risk assessment will not give further results in sufficient time interval. It is necessary to accept the decision also in the case when the result of risk assessment is burden by great errors that follow from present scientific cognition and they cannot be reduced in a necessary time.

In practice two risk management models [4] are usually used:

- classical risk management (Figures 6 and 7),
- safety management, i.e. risk governance for security and sustainable development (Figure 8).

The Figures 6 and 7 are sufficiently expressive that we do not discuss them in details.

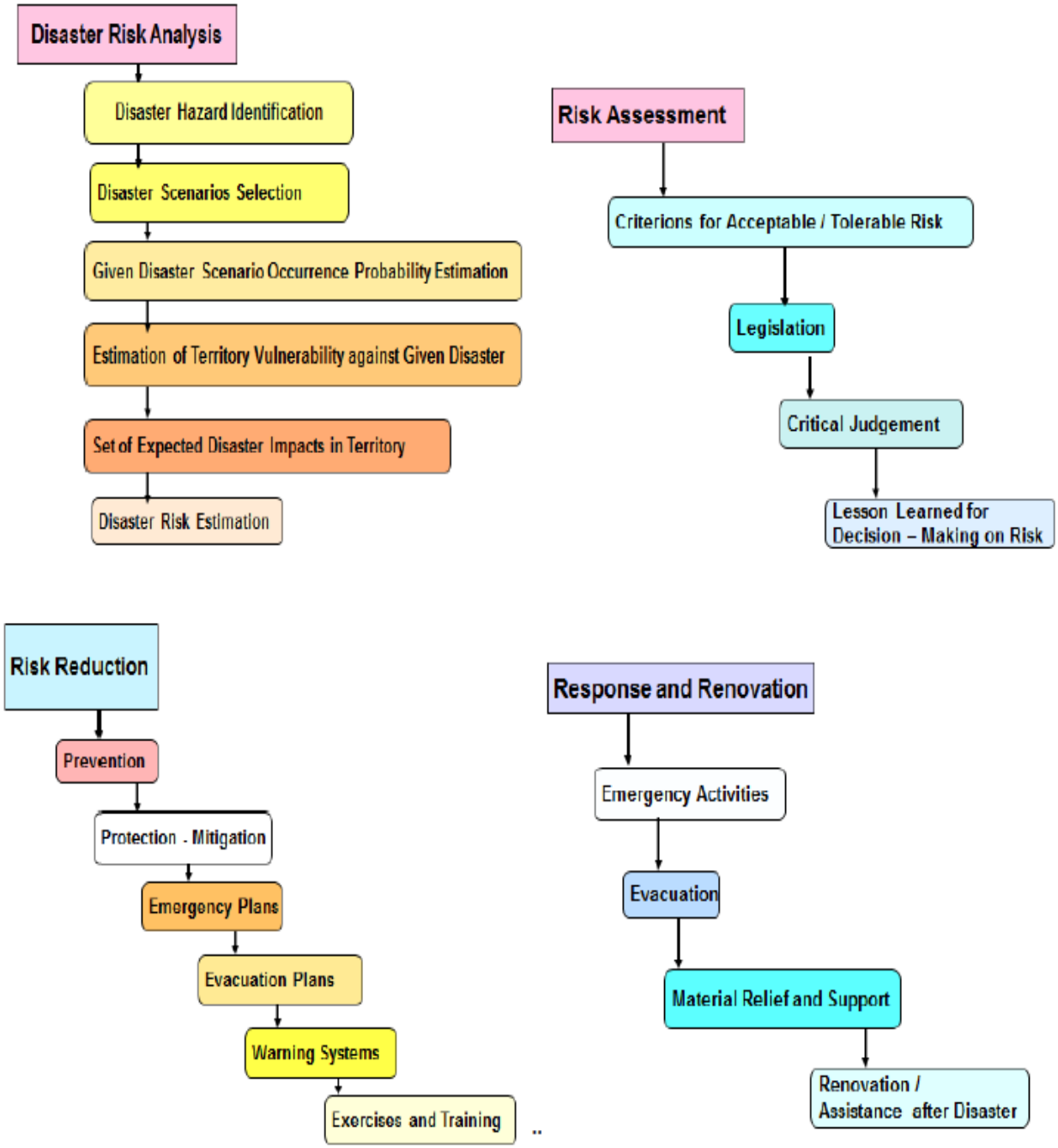


Fig. 7. Detail description of processes: disaster risk analysis; risk assessment; risk reduction; and response and renovation.

Figure 8 (part a) shows that the result of safety for followed system is a consensus for all considered disasters because each disaster type affects, owing to its nature, the system and its protected assets differently. Because the human factor failure, especially in risk management belongs to disasters, i.e. phenomena that damaged the human system from a certain size. With regard to the typical risk properties like uncertainties and vagueness, as was shown above, it is necessary at deciding on risk, to use more possible

variants of real human system behaviour and multi-criteria deciding by the help of experts with verified qualification [4].

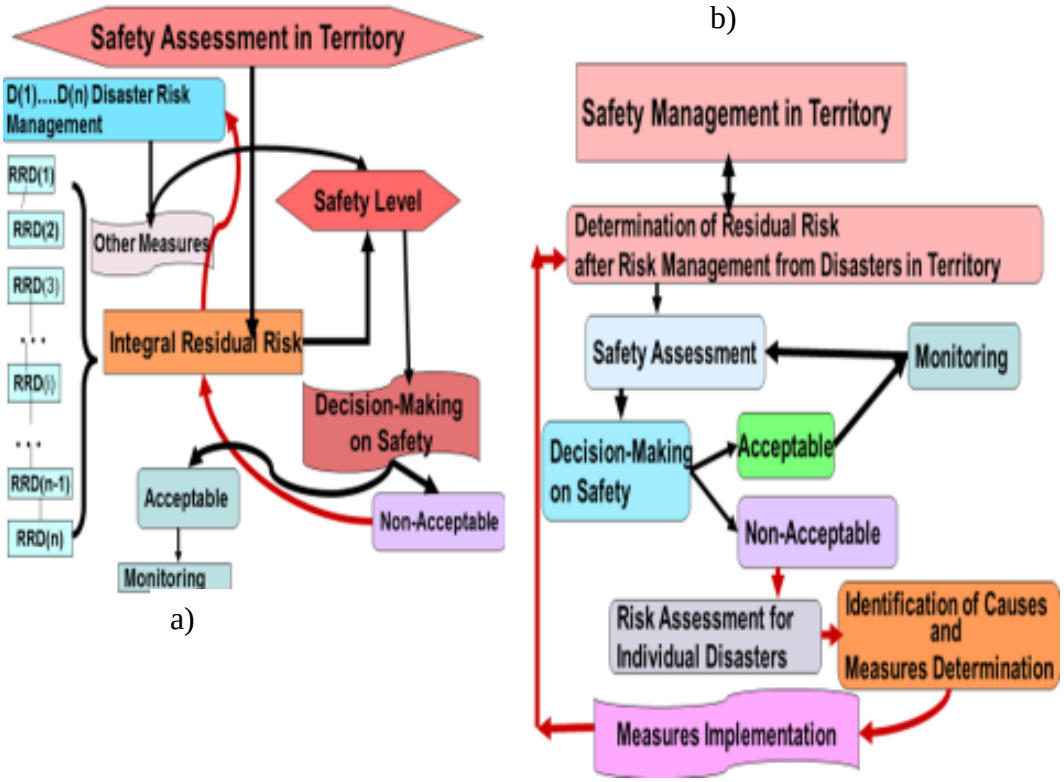


Fig. 8. a) - Model of safety assessment in territory (RRD(i) – risk from the i-th relevant disaster; b) – Model of safety management in territory.

From Figure 8 (both parts) it follows that the result safety for followed system is a consensus for all considered disasters because each disaster type affects, owing to its nature, the system and its protected assets differently.

For human safety and for human system safety (i.e. territory, organisation, plant) we need to manage the integral risk including the human factor, i.e. to find the way of cross-section risks management and to concentrate the investigation on interdependences and on critical spots with a potential to start the system cascade failures, domino effects, strange behaviour etc., and on the basis of such site knowledge to prepare measures and activities ensuring the continuity of limited infrastructure operation and of the human survival.

Evaluation of present knowledge shows that one of number of causes are interdependences inducing the cascade failures in the human system or in its part are the human errors (intentional or involuntary) in management and in deciding. Therefore, we need to do all measures in managerial and engineering activities to avert human failures, namely at decision-making. Because consequences of errors originating at decision are often huge, the great attention is concentrated to work with risks at present [6, 8].

5. Present trade-off with risks

In daily practice, the getting over the risks is the duty of all participants. The qualified activities are ensured by engineers who arrange co-ordinated implementation of measures for prevention, preparedness (directed to mitigation of severe impacts at risk realisation), response and renovation. The often used characteristic of engineering's work with the risks is:

- it considers multi-fields and cross-sectional disciplines that use both, the general and the specific methods, tools and techniques (specific ones are either simple or complex, complex ones represent well-ordered use of several general or simple methods, tools and techniques),
- it uses methods, tools and techniques logic, technological, financial, managerial and deciding because their integral part is a decision on technological problems, costs and time planning,
- it deals with tasks that connect the trade-off with risks for human system safety ensuring and the requirement of non-trivial solution of problems by use of multi-criteria methods, tools and techniques.

In all procedures it needs to be respected that assets and causes of risks have different natures that cause incommensurability of criterions and reasons, which only allows application of multi-criteria methods, tools and techniques that are suitable, i.e. correct and valid for a given problem target.

From the methodical viewpoint at selection of methods, tools and techniques they need to be respected: data quality; structure of problem that is solved and requirements on quality of results; which means specially to test both, the data quality (accuracy, completeness, homogeneity, bearing witness to a given problem [4]), and the qualification of experts if they are used (IAEA, OECD, World Bank etc. have strict criteria for judgement of expert qualification) [6].

Methods for determination of risk size need to respect both, the nature of phenomena that are their sources (i.e. characteristics and physical nature of disasters) and the parameters of medium in which phenomena affect. There are used methods based on the mathematical statistics, theory of extreme values respecting the random, sporadic and irregular great events occurrence, fuzzy sets theory, approaches of operational analysis etc., that inherently assume the certain model of phenomena occurrence, and methods based on scenarios that are simulated or empirically obtained [4].

For trade-off with a security risk, we use the safety management system (shortly SMS), concepts [9]. In the SMS we consider two cases, namely either the risk realisation is still substantially the same or it is significantly different. In the first case, we consider from safety reasons either the worst case (such approach is found in the standards based on a deterministic approach to safety provision) or we admit random uncertainties resulting from the momentary local and temporal conditions of assets and as a representative variable for risk management we use the mean value obtained by evaluating the possible alternatives (arithmetic mean, median, median + σ, where σ is the standard deviation, the probable mean value).

The other procedure is now commonly considered in the preparation of documents for strategic management (the alternative scenarios for the risk realisation and their occurrence probabilities are determined; and the mean and its dispersion are derived from them by a clear mathematical approach); we can find it in the norms and standards based on a probabilistic approach. In cases when we take into account the existence of

vagueness in data we need to use the combination of analytical and heuristic approaches that offers different theories; overview is in [6].

Strategy of management for negotiation with risks [4] is:

- part of risk is reduced, i.e. the risk realisation is averted by preventive measures,
- part of risk is mitigated, i.e. the non-acceptable impacts are reduced or averted by prepared measures and activities having the mitigating effects as warning systems and another measures of emergency and crisis management,
- part of risk is re-insured,
- part of risk for which there are prepared resources for response and renovation,
- part of risk for which there is prepared contingency plan, *i.e. it is used for part of risk that is low frequent and too difficult governable.*

At present work with risk, the risk is understood as the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). Now in practice there are used five types of risk management / engineering of systems [4, 5], i.e.:

- classical risk management and risk engineering,
- classical risk management and risk engineering including the human factor,
- security management and security engineering,
- safety management and safety engineering, i.e. risk governance / trade-off for security and sustainable development of system,
- safety management and safety engineering determined for system of systems (SoS).

Figure 9 shows the overview; the detail characterization is in [6].

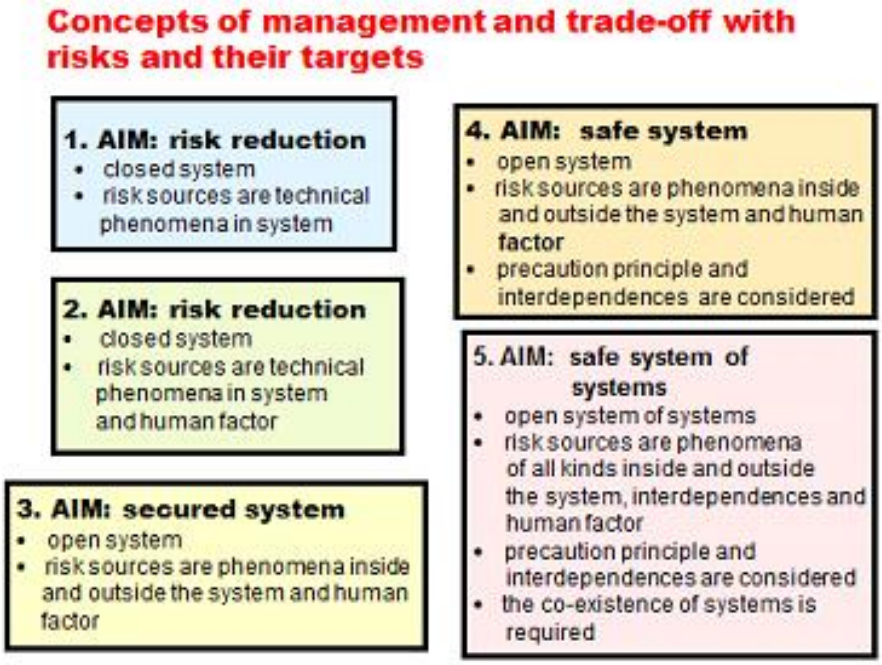


Fig. 9. Concepts of management and trade-off with risks and their targets arranged chronologically according to introduction in practice.

It is evident that each more advanced type keeps the higher demands on knowledge, tools, times, finance, personnel qualification etc. For each management and each engineering concept there has been developed a certain set of standards and norms for its

use in practice [5]. For different assumptions of concepts, the results of their applications in practice have not been the same; their capability to ensure human system safety, i.e. human security, existence and sustainable development, is different.

For each risk management and risk engineering type based on negotiation with risks there are standards and norms. Because the demands of various concepts are different, the standards and norms are different, the results are different and requirements on data, knowledge, material, technology, finances etc. are different.

Owing to provident handle with sources, forces and means, it is necessary in real cases to decide which concept is sufficient for a given problem solution. At deciding the role plays the risk size and the level of problem solution. The results of research [6, 9] show that at problem solution on:

- strategic level, it is necessary to use the system of systems safety management and system of systems safety engineering that fulfil demands of social engineers, technical engineers and environmental engineers,
- tactical and functional levels, it is necessary to respect the strategic concept recommendations and at site specific immediate problems´ solution it is possible to use the system safety management and system safety engineering because the character of solved problems is not so fundamental from the long term viewpoint,
- technical level it is necessary to respect the recommendations of all higher concepts, i.e. strategic, tactical and functional ones and for site specific immediate problems´ solution it is possible to use the system security management and security engineering if character of solved problems is not so fundamental from the time viewpoint,
- political level, it might be respected the strategic solutions, because politicians usually influence the strategic issues so public interests might be respected.

At solution of emergency situation there is lack of time, information and knowledge, and therefore, it is justified the reaction using the concept of management and engineering trade-off with risk directed to secured system and at critical cases only concept of management and engineering trade-off with risks directed to technical aspects.

The assessment of criticality of individual systems (sectors) of critical complex facility parts and the whole critical complex facility is not trivial matter because under different conditions the sectors and their whole have a different role - active, reactive, critical or damping (not additive); e.g. the existence of several variants of electricity supply to one site decreases the energy facility criticality but it increases expenses etc.

With regard to knowledge summarized in [9], the basic principles of safety technological complex facilities are:

- to apply the principles of inherent safety,
- to create a management system that has the basic control functions, alarms and responses of operator processed in the way, so that the system was maintained in normal (steady) state under normal conditions,
- to create a special control systems based on safety and protective barriers that keep the system in a safe state also at changing the operating conditions and prevent origin of undesirable phenomena, i.e. the system carries out the objectives as well as at abnormal conditions,
- to create special safety-oriented control systems that will keep the operation also at a greater change of operating conditions or they have the capability to ensure the operation after the application of corrective measures (clean-up, repair ...), i.e. there are measures for the inside emergency response, mitigation, and to return to normal operation, i.e. the system carries out the objectives as well as at critical conditions,

- to create special safety-oriented control systems which, in the case of loss of control of system and harmful impacts on the system and its surroundings, shall ensure the application of mitigation measures on the system and its surroundings, i.e. there are measures inserted in system to ensure that the system can be restored, and that the losses and damages caused in the area have been minimized, i.e. they provide measures for the off-side response. System supercritical conditions are the conditions for which the system was not designed, which can lead to situations that threaten the system itself and vicinity of the system.

It is necessary to apply the All-Hazard-Approach [10] and Defence-In-Depth concept [9]. In the professional area the layers mentioned above shall be regarded as protective barriers (so-called "protection in depth – defence in depth) and at the resolution of the facilities from the point of view of safety, it is used the security feature that the facility has a single stage or to a five-degree protection in depth. Individual safety management systems ensure the application of the technical, operational and organizational measures and activities that are designed to either prevent the initiation of chains of harmful phenomena, or stopped them [9].

6. Challenges for getting the control over risk

Recent FOCUS project outputs [5] show that the main EU problems, i.e. the EU vulnerabilities are the following:

- all hazard approach is not systemically applied – risk from some disasters is neglected,
- some disasters are underestimated – risk is lower than it is in reality,
- systemic, strategic and proactive management is not implemented into practice – it is only determined partial or integrated risk – omission of cross-sectional risks caused by linkages and couplings in system,
- gaps in risk management – list of criterions or targets of management are incorrect,
- errors in trade-off with risks – incorrect measures are used,
- research does not determine priority orientations, its targets are influenced by politicians or lobbies,
- application procedures and orientation of strategies are not regularly verified,
- reasonable strategy for disaster management is missing,
- the disaster management does not often respect disaster life cycle; accent to problem solving is missing, still only a lot of discussions on problems,
- lack of resources,
- lack of instrument for ensuring the EU finance stability; and lack of management supporting the public protection and sustainable development.

Mentioned gaps influence the level of control of risks in daily practice. The remove of these gaps or at least the mitigation of their criticality is the challenge in improvement of get over the risks.

The most serious challenge is connected with world dynamic changes in time. This reality very significantly influences the human capability for getting the risks under control, so acceptable conditions for human lives and existence of public assets might be preserved. Since 50s of last century, the data from all prognostic polygons in the world have been showing the relevant changes in processes, the products of which are the disasters. It means that we need to concentrate to the linkage between the process variabilities and the risks.

7. Target of publication

Regarding to above given facts, this publication summarizes the examples of dealing with the risks of processes being in existence in the human system, which are variable in space and time. On the basis of present knowledge and experiences, it proposes the super processes for management of risks that are connected with the human activities that can lead to organisational accidents.

References

[1] UN. *Human Development Report.* New York: UN 1994, www.un.org.

[2] EU. *Safe Community*. PASR projects. Brussels: EU 2004.

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

[4] PROCHÁZKOVÁ, D. *Analysis and Management of Risks* (In Czech). ISBN: 978-80-01-04841-2.Praha: ČVUT 2011, 405p.

[5] PROCHAZKOVA, D. *Critical Infrastructure Safety* (In Czech). ISBN: 978-80-01-05103-0 Praha: ČVUT 2013, 318p.

[6] PROCHAZKOVA, D. *Principles of Critical Infrastructure Safety Management* (In Czech). ISBN: 978-80-01-05245-7. Praha: ČVUT 2013, 225p.

[7] BOSSEL, H. 2004. *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*. ISBN 3-8334-0984-3.Norderstedt /Germany 2004, www.libri.de.

[8] AICHE, 1994. *Guidelines for Preventing Human Error in Process Safety.* New York: American Institute of Chemical Engineers 1994.

[9] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities*. ISBN: 978-3-659-74632-1. Saarbruecken: LAP 2015, 244p.

[10] FEMA, *Guide for All-hazard Emergency Operations Planning. State and Local Guide 101*. Washinton: FEMA 1996.

[11] EU. *The FOCUS Project Outputs.* EU grant No 261633, www.focus.eu.

Chapter 2

RISKS OF DRINKING WATER FAILURES*

1. Introduction

The significance of water for humans was emphasized with declaration of "European water chart" issued in Strasbourg on the May 6, 1968 [1]. The declaration contained twelve points:

1. There is no life without water. The water is a treasure indispensable to all human activity.
2. Fresh water resources are not inexhaustible. It is essential to conserve, control, and wherever possible, to increase them.
3. To pollute water is to harm man and other living creatures which are dependent on water.
4. The quality of water must be maintained at levels suitable for the use to be made of it and, in particular, must meet appropriate public health standards.
5. When used water is returned to a common source it must not impair the further uses, both public and private, to which the common source will be put.
6. The maintenance of an adequate vegetation cover, preferably forest land, is imperative for the conservation of water resources.
7. Water resources must be assessed.
8. The wise husbandry of water resources must be planned by the appropriate authorities.
9. Conservation of water calls for intensified scientific research, training of specialists and public information services.
10. Water is a common heritage, the value of which must be recognized by all. Everyone has the duty to use water carefully and economically.
11. The management of water resources should be based on their natural basins rather than on political and administrative boundaries.
12. Water knows no frontiers: as a common resource it demands international co-operation.

The human body consists of 70 % water, some flora even 90 %. The clear water at atmospheric pressure and room temperature is colourless and without smell. The prime physical properties of water are given in Table 1.

Because the life and health of humans strongly depend on water, the network of drinking water supply is one of basic infrastructures which belong to the critical infrastructure [2] in all developed countries [3-8].

The term "critical infrastructure" is introduced in the Czech legislation by the Law No. 240/2000 Coll., and described by the Government Ordinance No. 432/2010 Sb. Present paper deals with technical look, when we consider the critical infrastructure as a set of elements, links and flows, where the elements may be the liner and point structures, processes or management [3]. Set of all parts together and set of them

Authors: RNDr. Jan Procházka, Ph.D., Dipl. Ing. Linda Vašatová, Czech Technical University in Prague, Praha, Czech Republic, prochja31@fd.cvut.cz, vasatlin@fd.cvut.cz

interdependencies, then provides a certain service, necessary for the operation or survival of human system [2-4]. This problem has to be solved also for communities, which introduce the concept of "smart cities".

Table 1. Prime physical properties of water.

Molar mass	18.175 905 g/mol
Melting point	273.15 K (0 °C)
Boiling point	373.15 K (100 °C)
Density	0.99997 g/cm^3 (4 °C)
Refractive index	1.33
Surface tension	0.073 N/m (20 °C)

We have to especially recognize the close interconnectedness of individual systems in case of risk management [9], and safety management of critical infrastructure and individual infrastructures [4], which make up the critical infrastructure and which we describe by models "systems of systems". The put out of operation of one system, one infrastructure then sooner or later has a harmful effect on the functioning the other infrastructures that form the critical infrastructure [3, 4]. The criticality of certain infrastructure is then so high that their put out of operation means fast disruption and put out of operation of other services, namely even the most critical ones. At infrastructures with very high criticality it is required especially quick response in a sufficient scale [4].

From these reasons, the failures of certain infrastructures are included in the category of critical disasters, for which it is necessary to prepare the response on the level of crisis management [2]. As it was above mentioned, the supply of drinking water network is one of such infrastructures. We will deal with the causes of drinking water supply failure, the possible impacts and the conditions for cope with the emergency situations.

2. Critical infrastructure and its components

Critical infrastructure includes a series of infrastructures; and the supply of drinking water is one of elementary part of critical infrastructure [3]. We can explore properties of selected infrastructure from the perspective of external links on other protected interests of human system and on other infrastructures. For each infrastructure it is important internal topology of networks and processes.

The most of studies, which deal with critical infrastructure failure, describe blackout connected with electricity infrastructure. The comparison of drinking water supply failure and electricity infrastructures failure is shown in Figure 1. The failure of both mentioned infrastructure leads to the serious losses and damages to human health within a few days. In Figure 1 infrastructures are divided on hard elements (hardware), soft elements (software) and human resources.

The hardware is formed by physical construction, liner and point, necessary for the operation of given service provided from the source, through the transport up to the distribution. The hardware is mainly threatened by natural disasters, technological accidents or attacks. The hardware could potentially themselves provide the service, but not in the required form and functional range.

Services need software elements for working in the required range and quality. Software consists of processes, controls and monitoring. The processes are carried out

either cyber or human support staff. The disruption of software can be caused by a failure of other infrastructure (electric, cyber) or by a human error (routine in the execution of process, wrong management processes).

Even in the case that we would be technologically able to build an autonomous infrastructure just from hardware and software (cyber elements), the infrastructure could not without the human factor meet the requirements, which are imposed on it in the long term. The last part of the infrastructure, namely the human resources, has an influence at defining the structure of network (both, the physical and the procedural). Human resources are necessary for response to changes in progress of human system, new demands and new threats. Last but not least many routine processes we are not able to adequately automate. Human resources are vulnerable to all the disasters [9].

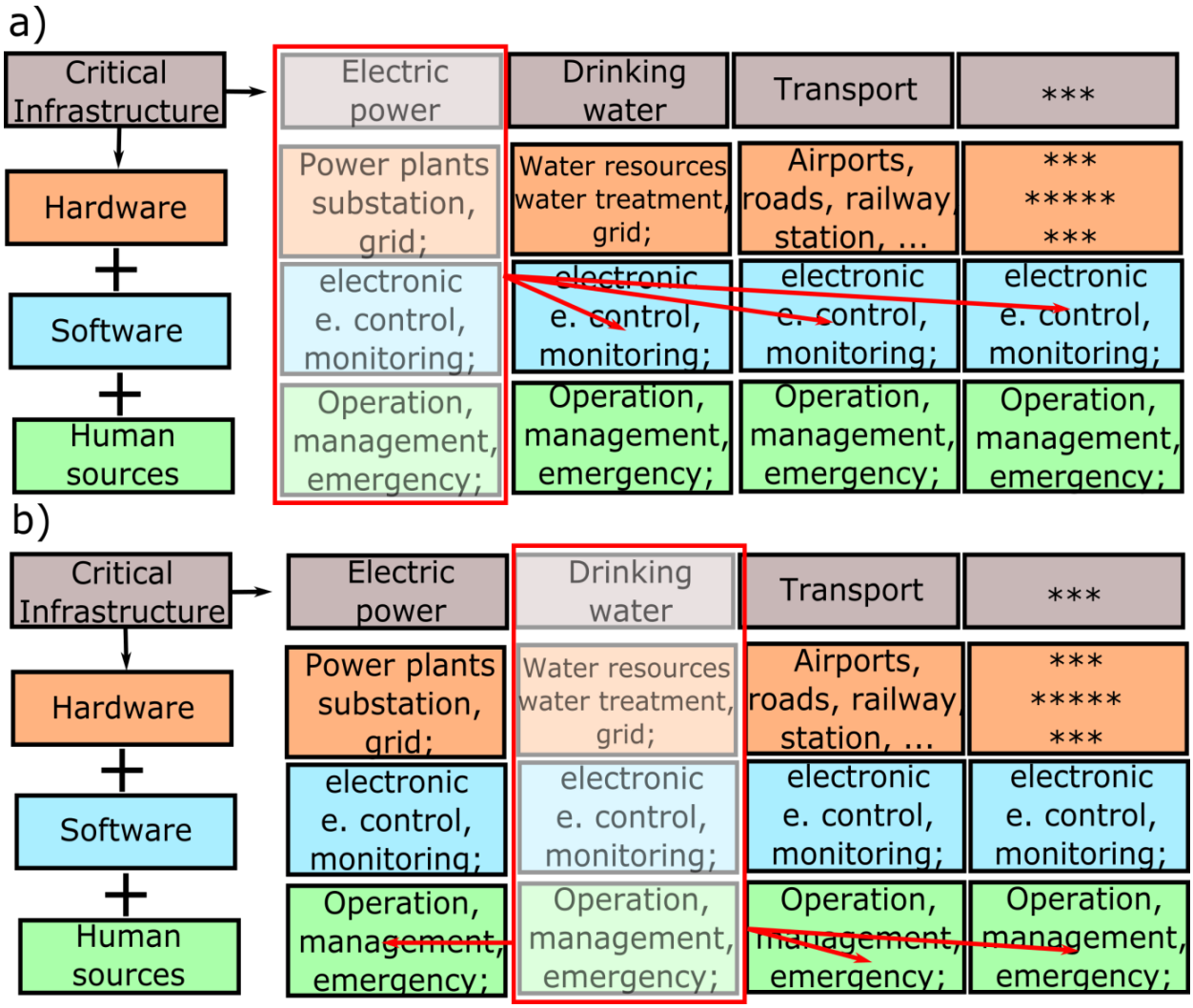


Fig. 1. Diagram of impacts of critical infrastructures failures on the elements of other critical infrastructures, a) electricity supply failures), b) drinking water supply failure.

When we return to Figure 1, we see a comparison of impacts of failure of electrical power supply and failure of drinking water supply. We can identify the impacts on the protected interests of all types in both cases, namely on all types of infrastructures. In the case of failure of electricity network, it goes on put out of operation of software elements

of all the other infrastructures, which will be out of operation immediately or within a few hours. The failure of drinking water supply has a slightly slower impact; however, it directly affects the people and it put out of operation the other infrastructure through human resources within a few days.

3. Topology of drinking water supply network

While the character of software elements and human resources can be completely different for different companies and different regions, the hardware part of infrastructure is similar everywhere in basic aspects. It has the resources, transport elements and distribution elements. Parameters, that define the properties of hardware of infrastructure of drinking water supply, are a lot. We will focus only on the main two parameters. The first parameter is located in domain of drinking water sources, the other in domain of transport – i.e. the network topology.

The basic sections of drinking water sources are on surface sources and underground sources, which can be further divided according to parameters like area, depth, volume, quality and so on. Each of two types of resources, ground and surface, has its advantages and disadvantages. The economic benefits of underground resources were recently preferred.

We can point at several differences from the perspective of risk analysis. Groundwater need less treatment then surface water. Groundwater sources have less probability of contamination, although due to very low protection occasionally smaller sources contamination occurs for example due to road traffic accidents [10, 11]. Cleaning of pollute groundwater resources is currently not technologically possible.

The main advantage of surface water sources is their renewability, that is associated purely with precipitation, and it is not dependent on the ratio of seeped and flow away water.

Transmission networks are composed mainly of pipeline in addition to the elements that ensure the water pressure in system. The network topology is fundamental feature of distribution network, where we know the three variants of topology, Figure 2 [12].

The cheapest option is to construct a branched network, where ever places of water distribution system are brought only by one pipeline [12, 13]. At the branched network it is the high probability of total collapse of network at simple faults. A loop network is an opposite of the branched network, and it supplies the water to all points of loop network from two directions. The costs for constructing the circuit network are high, but the disruption only its part requires the coincidence of many circumstances and the disruption of entire network can only be caused in reality by intent.

The best solution for practical use seems to be the combined network of loops and branches, which brings advantages of both networks at proper design and management; i.e., reasonable costs and high resistance at the level of main part of network. The ratio of combination of loops and branches depends on the objectives of network. The objective of drinking water distribution in the Czech Republic is the combined network. The risk of major failure is shifted to the domain of water resources in combined supply system. However, existed networks in the Czech Republic are mainly branched networks and change depends on finance.

4. Causes of drinking water supply failure

Vulnerability of infrastructures to damage is quite high. Many causes and processes can lead to the disruption of network [3, 4]. To some of causes, for example, to occurrence of natural disasters it is not possible to defeat. The main problem of many countries there are the causes which are entirely in the hands of public administration and owners of water supply network, namely construction, maintenance and monitoring of pipelines.

Causes of water supply failures can be separated by several ways; i.e. according to: elements that are disturbed; the size of impacts; region of origin of failure; characteristics of failure. The causes corresponding to last mentioned reasons are shown in Figure 3, that is constructed on data from [12] with the help of Ishikawa diagram [9]. The backbone of fish bone in Figure 3 is the drinking water supply network and the causes of water supply failures are demonstrated in six different branches.

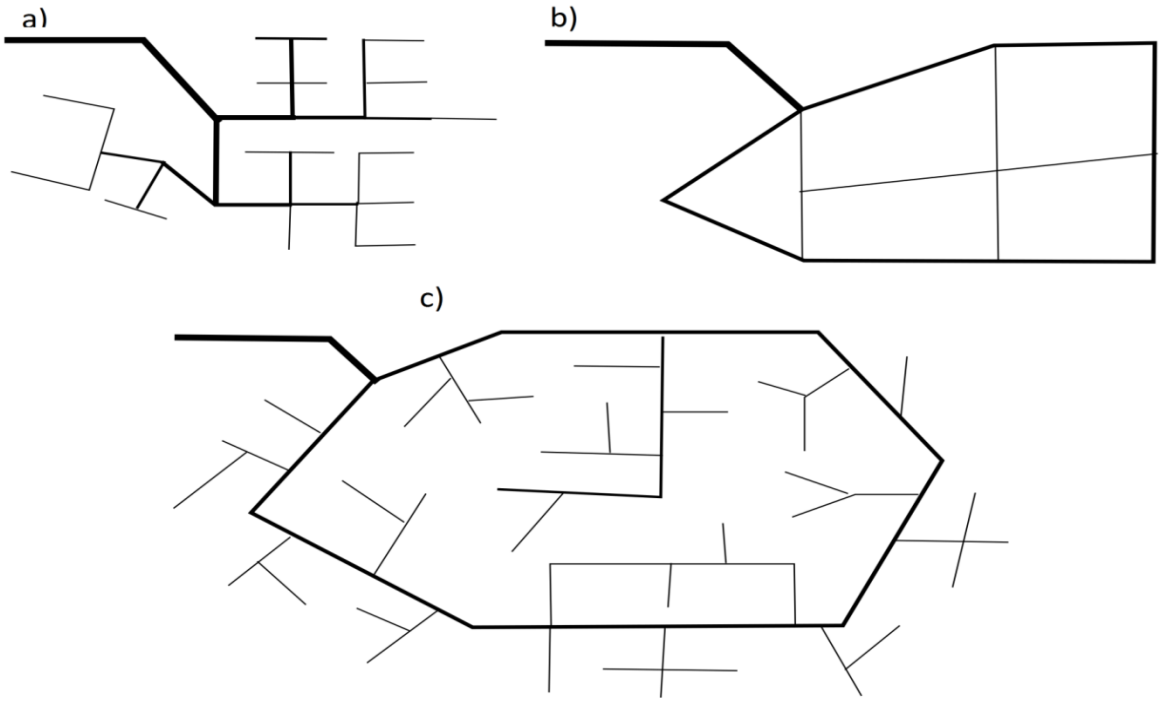


Fig. 2. Models of three variants of drinking water supply network topology: a) branch, b) loop and c) combined.

The wrong construction is a group of causes, which have origin in designing or in building phases of pipelines. Incompetent designer or attempt for the lowest costs on building and construction can lead to origin of many frequent breakdowns, high repair costs, or to the low efficiency of required services.

Surrounding subterranean environs affects permanently on network by its spreading and shrinking in dependence on various geomorphological conditions. The probability of disruption is then given by structure, material aging and the quality of maintenance of pipelines. Other problems there are natural disasters, which may reach different sizes and cause varied damages on infrastructure. Pipelines are resistant to smaller disasters, however, severe disasters damage seriously infrastructure, and therefore, it is necessary to have prepared in the frame of crisis plan the different variants of alternative sufficient water supply [2, 14]. Influences of environment cannot be prevented in any way.

Infrastructures interdependencies are discussed in paragraph 2. The failure of certain infrastructures may cause a critical situation, and similarly as at natural disasters it requires the sufficient high-quality crisis plan. Critical infrastructure protection is a necessary part of modern crisis management.

Human error has several dimensions. It includes errors at designing or at building the structure [9], which have their own branch in Figure 3. In mentioned Figure we can see the human errors during the operation of network. Human errors can also arise during the management, e.g. bad estimate of water consumption. The increase of drinking water demands is necessary to foresee, because building the new water resources is time consuming.

Human errors connected with routine operation are caused by violation of technical norms, standards and determined procedures. Technical problem is caused by routine human error, if ordered procedure is not kept. If the procedures have been kept, then it is a mistake of management at setting the operation regime. In the Czech Republic problems are primarily connected with organizational accidents [2, 4], i.e. the persons in management do not ensure his / her responsibility.

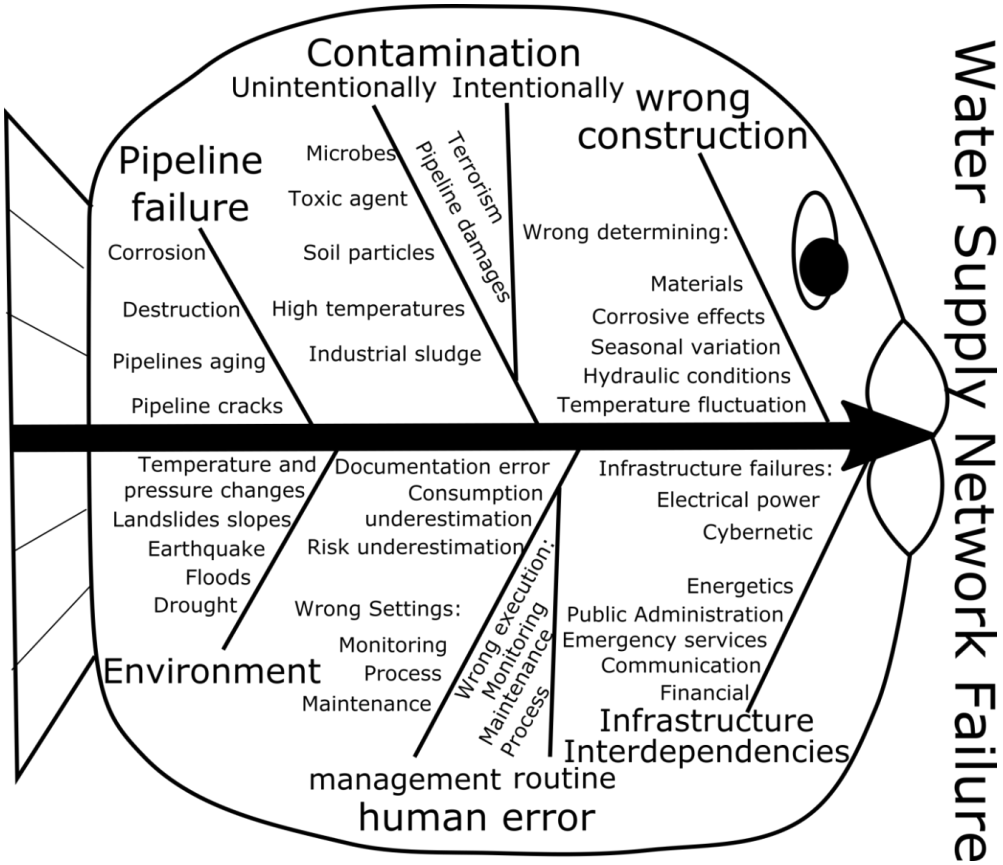


Fig. 3. Ishikawa diagram for the drinking water supply failure

The pipeline failure is the most common cause of drinking water supplies disruption. The main causes are incorrect structure, age and maintenance quality. If someone of these three factors is failing, the pipeline cracks and damages occur as consequence of common phenomena.

Contamination *c*an be divided into intentional and unintentional. Water resources are one of the possible targets of terrorist attacks, which can cause great damages. In the case of highly toxic substances it may also come to the pollution of entire network through small source of pollution. It is, therefore, important to protect the perimeter of resources and above all, to monitor the water quality supplied to the network [15].

Relatively common in recent years it has been the unintentional contamination. Its causes are drought and high temperatures, poor documentation, an accident during the transport of dangerous goods, storage of hazardous substances and harmful things near the water sources, which happened in recent years in the Czech Republic [11]. Contamination of water source may cause a critical situation also in the case of durable drinking water supply infrastructure.

5. Data and methods used in the research of drinking water supply failure

For monitoring the impact of drinking water supply failure it was selected the part of Central Bohemia. This region is divided into several districts with different area and different number of inhabitants. Districts can be described by several numbers in Table 2. Districts are named according to municipalities with district administration.

Table 2. Proportion of individual districts, number of municipalities, number of inhabitants and area.

District	**Municipalities**	**Inhabitants**	**Area (km^2)**
Kladno	48	122 000	351
Rakovnik	83	55 000	896
Slany	52	40 000	369
Melnik	39	43 000	457
Kralupy	18	31 000	131
Neratovice	12	31 000	113
All	252	322 000	2317

The number of drinking water supply system incidents in individual districts according to [16] is in Table 3; graphically shown in Figure 4.

Table 3. Statistics of water supply network incidents in individual districts.

Year	**Kladno**	**Rakovnik**	**Melnik**	**Slany**	**Kralupy**	**Neratovice**
2008	263	325	64	0	81	9
2009	192	95	77	3	54	7
2010	101	126	106	67	15	21
2011	107	111	69	4	23	21
2012	319	301	170	5	64	36
2013	139	223	68	3	14	3
All	1121	1181	554	82	251	97

For our research we use data on the layout of re-sources and on the network topology [16, 17]. From the safety reasons we only show the rough model of distribution network,

Figure 5, which we created from detail real data. The mentioned figure shows that we consider combined net-work with two water sources that has in internal part the branched networks. It means that there are all problems of network types, the combined and the branched, plus even more problems.

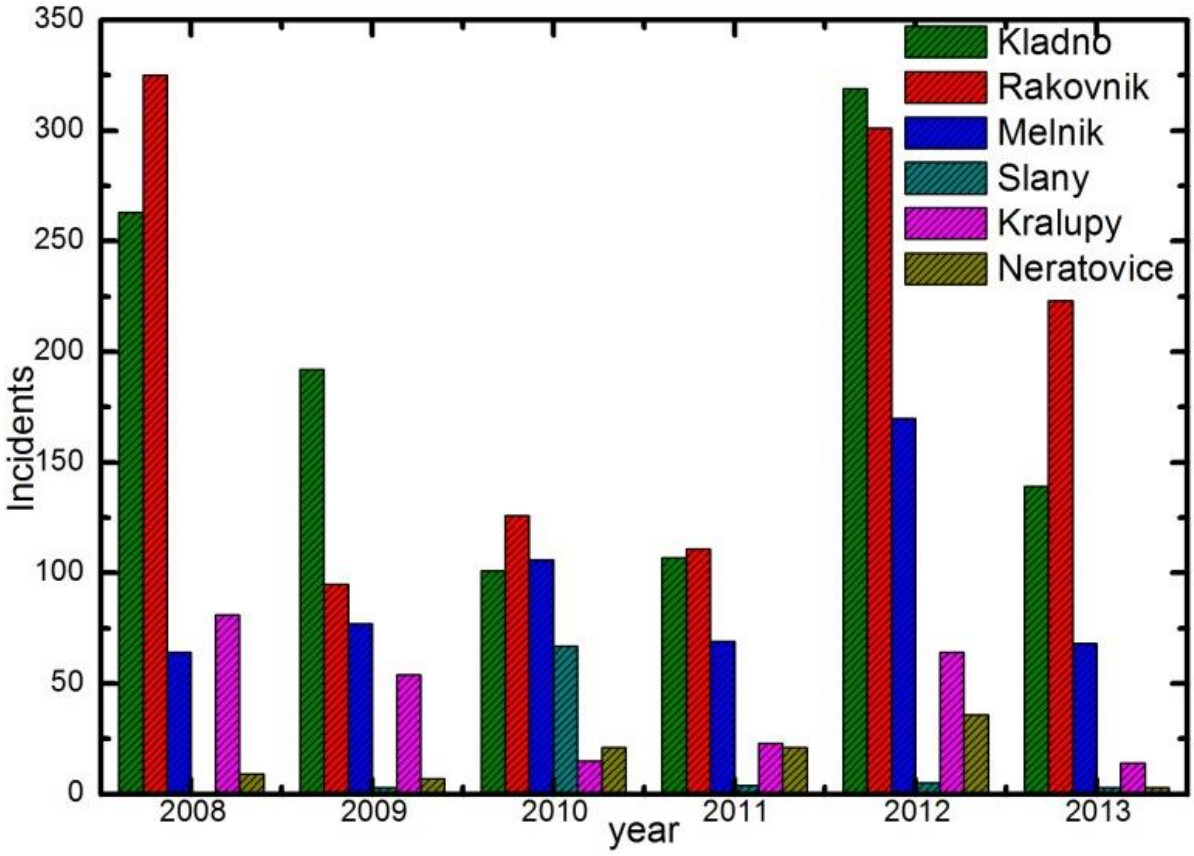


Fig. 4. Statistics of water supply network incidents in individual districts.

Our network includes two sources; the primary source A is a source of underground water, 80% all water. Source B is a surface water source and it provides 15% all water. The rest is covered with smaller resources. The predominance of underground resource corresponds to the situation, when the underground water is cheaper than surface water. New knowledge and experiences on hydrological changes and recent droughts supports returning to higher portion of surface water [16, 17].

The impacts of a critical failure of drinking water supply are locally specific and depend on the scenario, which led to the failure. At all critical failures, the citizens have lack of drinking water. At research of drinking water supply critical failure impacts we use the "What if" analysis modified for the needs of security problems in an integral and systemic conception of reality. We followed two possible cases, namely the large disruption of distribution network and the large contamination of source by highly dangerous substance.

Any contamination has several concentration levels, from which there are derived human health damages, or losses of human lives. In the case of highly toxic substances it may get to human life threat even at the dilution in the huge quantities of water, and therefore, to the danger of all consumers of water from contaminated infrastructure. It is

not essential, where the contamination occurred, if in main source, secondary sources, the water tank, the piping. It is also necessary to take into account that after the put out of operation of infrastructure it can be very problematic the decontamination of whole network.

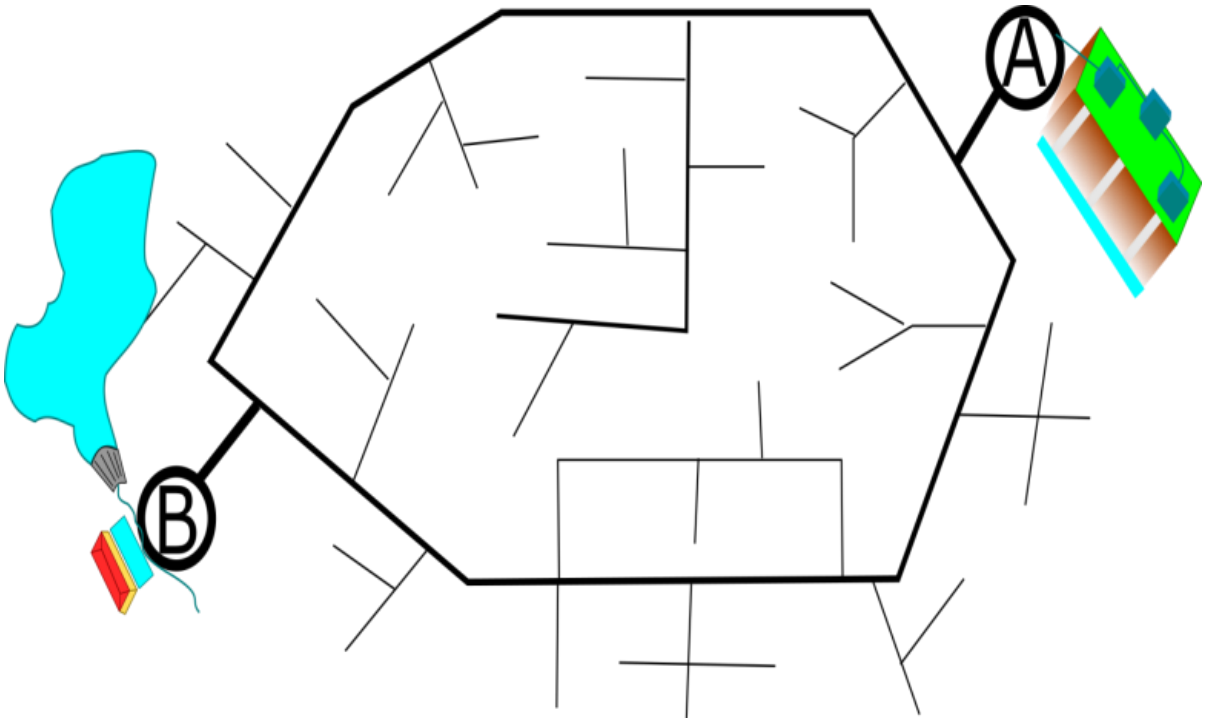


Fig. 5. Combined network of drinking water supply with two main water resources, A – underground 80% of all water and B - surface 15% of all water.

The network may be out of function in the case of insufficient response for several days, which is from the perspective of physiological needs of human too long.

6. Impacts of the selected scenarios of drinking water supply failure

We selected two scenarios, disruption of distribution network and contamination with toxic substance. Disruption of distribution network is presumed on connection of main source. Contamination describe situation, when substance with high toxicity get to water. Contamination does not be necessary in place of main sources.

6.1. Disruption of distribution network

Large water sources are always a critical part of the drinking water supply infrastructure. Criticality of the main pipelines is very high in the case of the branched network [12], but it is not so high for the combined network. Although our supposed network in Figure 4 is combined, we have only one line between the main source ***A*** (80%) and the rest of the network. Criticality of source connection is the same as criticality of source itself, if connections are not more than one. We assumed the disruption of such connections in the first scenario. It is necessary to note that pressure of water needs not to fall below a certain amount for the proper functioning of network. At outage of 80%

on input the pressure drops very quickly, water will not be available in all networks without the introduction of tough regulation on output, though not all sources would be knocked out [17]. The impacts of disruption of distribution network are in Table 4.

Table 4. The impacts of disruption of distribution network for drinking water supply; 0 - time of disruption, 12 h - 12 hours after disruption, 24 h – 24 hours after disruption, 3 days and 7 days - 3 or 7 days after disruption.

Public assets	**Impacts**
Lives and health of humans	0 h: 12 h: light dehydration of persons' dependent on the supply of drinking water from the water supply network (those who do not have access to the water packed), leading to damage of health and lives of people with a higher vulnerability on lack of drinking water, i.e., particularly persons for long time ill, patients in hospitals, older persons and children. 24 h: dehydration of all persons' dependent on supplies of drinking water from the water supply network (those who do not have access to the water packed). The lack of water affects headache and reducing the blood pressure. 3 days: increasing the dehydration. Persons with increased sensitivity to lack of fluid can died. Most of population suffers from dehydration symptoms, such as headache, pressure decrease, increase in heart rate and other physiological manifestations. Dehydration is already affecting the people who were frontloaded by bottled water. At all residents of affected area, it is starting to show the stress from emergency situation and it is also getting worse mental state. The deteriorating level of hygiene. 7 days: severe dehydration causing death of inhabitants.
Human security	0 h: 12 h: 24 h: the increase of tension in the society. 3 days: as a result of the decline in the quality of emergency services it goes to increase of possibility of origin of other disasters. 7 days: the loss of all internal security features, and it leads to big increase of possibility of further disasters origin.
Property	0 h: 12 h: property damage by fire. 24 h: disrupting the functionality of machines and equipment that are dependent on the supply of water. Damage of property caused by fire. 3 days: the origin of unrest within the society leading to the looting and destruction of property. Property damage caused by fire, the likelihood of which increases due to the degradation of society. 7 days: property damage by huge long-term fires.
Public good (welfare)	0 h: 12 h: interruption of work activities in the private and the public sphere. A forced holiday due to failure of compliance with the requirements in the labour code. The unavailability of restaurants and cultural facilities. 24 h:

	3 days: the deterioration of situation in human society. Negative effect on the perception of territory in the future. 7 days: as a result of disintegration of society due to mental and physical health of population the term public good loses its meaning.
Environment	0 h: 12 h: 24 h: 3 days: due to the affection of civic discordances and disruption of emergency services it increases the possibility of origin of further disasters affecting the environment, e.g. fires, waste water. 7 days: the increase of impacts of unresolved calamities on environment.
Water supply system	0 h: a significant worsening in the functioning of drinking water supply infrastructure. 12 h: the depletion of storage network systems, water towers. 24 h: 3 days: Out of function of all systems of drinking water supply infrastructure. 7 days: degradation of mechanical parts of system of drinking water supply network (the elements of system are not in conditions on which they have been designed).
Emergency services (police, fire-fighters, paramedics)	0 h: a sudden drop in pressure in the water line, the failure of some sources of water designed for extinguishing fires. 12 h: the worsening the conditions of patients in hospital devices. The worsening the availability of medical rescue services due to the transfer of patients outside of the affected area. 24 h: 3 days: the decline of physical possibility of emergency services workers caused by dehydration. The gradual attacks of staff of emergency services in the wake of deteriorating situation in the human society. 7 days: malfunction of internal components of infrastructure.
Transport network	0 h: 12 h: 24 h: possible formation of traffic jams as a result of migration of population from the affected area. 3 days ago: origin of traffic jams on road network as a result of evacuation of population. The failure of internal elements of territorial railway network. Disruption of pipeline elements of transport infrastructure as the result of social unrest. 7 days: malfunction of all elements of transport associated with human activities. Damage to the mechanical elements of transport infrastructure as the result of secondary disasters, e.g., traffic accidents, fires, riots, etc.
Other basic services and critical infrastructures (informational, financial,	0 h: 12 h: non-availability of basic services, e.g. educational institutions, governmental (public administration) and financial services. 24 h: loss of packaged liquids in stores and distribution centres. 3 days: malfunction of internal elements of the basic infrastructures and critical services. 7 days:

energy, social, State)	

6.2. Contamination with toxic substance

The second scenario deals with the contamination of smaller scale source ***B*** (15%) on Figure 4; i.e. surface source. If target of contamination it is not only source itself, but whole network, the contamination could be done almost everywhere (secondary sources, main pipelines). Quantity level of toxic substance to water volume determines the consequences in scenario. We presume the hazardous substance with very high toxicity, where small concentration can lead to high consequences. The impacts of contamination by toxic substance are in Table 5.

Table 5. The impacts of contamination by toxic substance; 0 - time of contamination occurrence; 12 h - after 12 h of contamination origin, 24 h – after 24 h of contamination origin, 3 days and 7 days - after 3 or 7 days of contamination origin.

Public assets	**Impacts**
Lives and health of humans	0 h: the first humans drinking the contaminated water, which started bad processes in the human body. 12 h: heavy damage to the health which is dependent on the character of used chemical, the first casualties. 24 h: number of casualties reaching a disastrous amount. The social tension starts. 3 days: stress and worsening of mental status of the survive humans in the affected area, and also in the extensive vicinity of affected area. Distrust in the central source of drinking water, which may cause panic and social unrest. Dehydration causing headaches and lower blood pressure. 7 days: at all the population it is seen the stress from emergency situations and it is also worsened its mental state. The deteriorating level of hygiene. Dehydration is already causing serious health complications.
Human security	0 h: poisoning by contaminated water in the vicinity. 12 h: poisoning by contaminated water from network in the whole area. 24 h: the increase in tension in the society. 3 days: 7 days: a decline in the quality of emergency services may lead to the origin of other disasters.

Property	0 h: contamination of property, the function of which is associated with the supply of water in the vicinity, e.g. household equipment, workplaces equipment, machines. 12 h: contamination of property, the function of which is associated with the supply of water in the area, e.g. stocked household equipment, workplaces equipment, and machines. 24 h: 3 days: the lack of water for fire-fighting as a consequence of disconnecting the water supply. 7 days: the danger of unrest within the human society which lead to the looting and destruction of property. Property damage caused by fire, the occurrence likelihood of which increases due to the degradation of society.
Public good (welfare)	0 h: 12 h: interruption of work activities in the private and the public sphere as the consequence of human deaths. 24 h: worsening the situation in the human society, the panic induced by the number of victims. Negative effect on the perception of territory in the future. 3 days ago: 7 days: to fears of poisoning the dangerous substance it adds the fear from a long-term interruption of drinking water supply.
Environment	0 h: contamination of water in the Klíčava water reservoir, the lower reaches of Klíčava stream, the Berounka River. 12 h: the contamination of further water streams (in the river basin of Vltava River and Elbe River), contamination of rivers banks. The death of aquatic fauna and possible necrosis of flora. 24 h: death of animals that use surface water sources in the affected area. 3 days: 7 days:
Water supply system	0 h: contamination of drinking water source in the Klíčava water reservoir, contamination of adjacent network for drinking water supply. 12 h: contamination of entire circuit of network for drinking water supply. 24 h: shut down of affected system of drinking water supply. 3 days ago: 7 days: degradation of mechanical parts of system of drinking water supply (the elements of the system are not in a status for which they have been designed).
Emergency services (police, fire-fighters, paramedics)	0 h: 12 h: the extreme load of health care by humans with symptoms of poisoning, and dying, e.g., hospitals, paramedics and medical rescue service. Increasing demands on the maintenance of public order. Affecting the human resources from the emergency services. 24 h: outage of some sources of water for firefighting. 3 days ago: 7 days: the decline of physical capabilities of emergency services workers caused by dehydration.

Transport network	0 h: 12 h: 24 h: huge panic is caused by the formation of traffic jams that originated on roads as a result of mass evacuation of population from affected area. The outage of internal elements of territorial railway network. Disruption of linear elements of transport infrastructure as result of social unrest. 3 days, 7 days
Other basic services and critical infrastructures (informational, financial, energy, social, State)	0 h: 12 h: non-availability of basic services, e.g. educational institutions, governmental (public administration) and financial services. 24 h: loss of packaged liquids in stores and distribution centres. 3 days ago: 7 days: malfunction of internal elements of basic infrastructures and critical services.

6.3. Discussion

The drinking water supply failure is one of possible critical disasters on the territory of the Czech Republic. Duty of ensuring the drinking water supply even in emergency situations is holding from the 80s of last century according to the law No. 274/2001 Sb., on water supplies and sewerages also in emergency situations, but it cannot be in the long term.

The failure of critical infrastructure, where the drinking water supply failure has a high criticality, threatens always a number of other protected assets. Possibilities, leading to drinking water supply failure are a number, and they have varied relevant impacts and have also different occurrence probabilities. This work presents the impacts for two different causes. Sources of drinking water are the key components of infrastructure, but further critical points can occur, when network topology is wrong or week.

The first scenario deals with the pipeline accident, which ensures the water distribution. The pipeline cracks are relatively common phenomena, which can be caused by various causes. The second scenario deals with the contamination of water source. The contamination of water source is one of terrorist attacks scenarios. But, the contamination may also occur in other ways, accident during the transport of dangerous substances, or bad management of hazardous substances, e.g. during the storage. Both phenomena have already occurred in the Czech Republic, fortunately without critical consequences.

When the impacts of both scenarios are compared, we see the differences mainly in the first hours, where the impacts of contamination are faster. The impacts of both scenarios become similar after exceeding one day. The prevention of serious impacts in the first hours of contamination requires the high quality monitoring (fish, physical parameters). Monitoring needs to be implemented in all critical sites, not only to the resources. The situation sharply changes after crossing one day in the case of both scenarios. The defeat of emergency situation in 24 hours is associated with relatively small impacts on the protected interests. Exceeding one day, however, leads to a critical situation. The next limit 5-7 days is then given by particular time during which the healthy human is able to endure without water [17].

7. Conclusion

The research was directed to identification of impacts of drinking water supply failure. We have identified two basic problems in managing the situation on the basis of carried out research. The first one is the issue of responsibilities [12]. Many top public administration workers do not know or does not admit all types of responsibilities associated with their position in public administration. This may lead to a delay in the response itself, which it is fatal especially in the case of contamination. The second problem is the robustness of response to the drinking water supply failure. As mentioned above, the drinking water infrastructure failure is identified as one of the possible disasters that may induce a critical situation, and therefore, it is processed contingency (type response) plan for it [2].

On the analysis of actual drinking water supply failures in the Czech Republic in recent years [12], some of response activities, e.g. informing the population, warning the population, emergency supply, rapid restoration of network, are not robust enough. Many of territorial units (communities) are able to solve the demands only in the case of small accidents of water series. Real response plans for the critical failures, however, have not been set up yet.

The concept of "smart cities" needs to take account the facts given above and it needs to include the plans for a high-quality and quick response to all life sustaining infrastructure failures, to which indisputably the infrastructure ensuring the drinking water supply belongs.

Acknowledgement

Authors thanks to the Czech Technical University in Prague for support (grant SGS2015-17).

References

[1] COUNCIL OF EUROPE. *European Water Charter.* Strasbourg (1968). http://iea.uoregon.edu/treaty-text/1968-EuropeanWaterCharterENtxt

[2] PROCHÁZKOVÁ, D. *Crisis Management for Technical Fields* (In Czech). ISBN: 978-80-01-05292-1. Praha: ČVUT 2013, 303p.

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

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

[5] EU. *ESRIF Final Report*. Brussels: EU 2009, 319p.

[6] US. *US Critical Infrastructure Conception*. Washington: US Government 2001.

[7] EMA. *Critical Infrastructure Emergency Risk Management and Assurance*. Handbook Emergency Management Australia, 2003, www.ema.gov.au

[8] VLÁDA ČR. *Domains of Critical Infrastructure in the Czech Republic* (In Czech). Usn. vlády ČR č. 1436 ze dne 19. prosince 2007 (usnesení BRS ze dne 3. července 2007 č. 30)

[9] PROCHÁZKOVÁ, D. *Analysis and Management of Risks* (In Czech). ISBN: 978-80-01-04841-2, Praha: ČVUT Praha 2011, 405p.

[10] PATÁKOVÁ, H., PROCHÁZKA, J. Analysis of Data on Traffic Incidents with Presence of Hazardous Substances. In: *Proceedings of the 11th European Transport Congress,* ISBN:978-80-01-05321-8. Praha: ČVUT 2013, 8p.

[11] PATÁKOVÁ, H. *Critical Sites at Transportation of Hazardous Substances on Highway D1* (In Czech). Diploma´ Thesis. Praha: ČVUT 2014, 124p.

[12] VAŠATOVÁ, L. *Risks Connected with Failure of Drinking Water* (In Czech). Diploma´ Thesis. Praha: ČVUT 2016, 74p.

[13] ASCE. *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters", Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards", Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters*".Washington: ASCE 2001, 3869p.

[14] TOMEK, M., SEIDL, M. Emergency Supply of Public by Drinking Water (In Slovak). In: *Ochrana obyvatelstva.* ISBN 80-86634-51-5. Ostrava: SPBI 2007, pp. 372-378.

[15] MONOŠI, M., ORINČÁK, M. Risks of Threat of Waterworks Reservoirs on the Slovak Republic Territory (In Slovak). In: *Ochrana obyvatelstva.* ISBN 80-86634 -51-5. Ostrava: SPBI 2007, pp. 218-224.

[16] KÚ Středočeského kraje. *Database of Water Network in Central Bohemia* (In Czech). Praha: Středočeský krajský úřad 2016.

[17] VÚV. *Technical Documentation of Ducts and Sewerage* (In Czech). Praha: Vodovody a kanalizace a.s. 2016.

Chapter 3

RISK MANAGEMENT DIRECTED TO SAFETY OF METRO CONTROL SYSTEMS*

1. Introduction

Transportation is created by huge network of traffic routes, facilities, support systems and traffic vehicles in various modes and kinds. The transportation infrastructure is one from the most important infrastructure that ensures the main functions of territories and States; it is very important for human survival at critical situations. Therefore, many parts of transportation system belong to the critical infrastructure. The transportation infrastructure criticality is determined according to its importance and vulnerability in selected entity and it is changed with the entity size; certain transportation infrastructure is important for municipality serviceability, but it is not important for the State and vice versa [1]. Therefore, the risk is comprehended in system concept, which means that the integral risk is considered.

From this reasons, the risk management targets consider both, the public assets and the transportation mode assets (traffic vehicle, building, traffic road, support systems, control systems including human factor, or even logistics services, transportation of goods and people). The present goal of risk management is the safety (or at least security) of human system (that represents our world); its assets and their interfaces. This goal has been reached by measures performed by humans; it goes on averting or reduction of losses and damages of public assets. For this aim, it is necessary to consider system interfaces, for example the impacts on transportation infrastructure consecutively damage the humans and disrupt the entity economy [2].

The research of urban guide transportation management system takes into accounts the recent advanced approaches and techniques of risk and safety engineering [1-19]. The metro system makes up one of important transportation infrastructure in bigger and capital cities. According to present knowledge, the metro system is a part of critical infrastructure, and therefore, it is need to pay attention to its safety and security [19, 20].

The target is the metro safe operation. From this viewpoint, the management and control system is important, because it determines the quality and performance of metro system [20]. It is characterized by interdependencies among systems of various natures which are monitored and managed by people or automata using the control system. The further given issues are the following:

- the list of technical and cyber assets of metro,
- the most important priority risks affecting the metro management system operation,
- critical spots of cyber infrastructure in the metro management and control system,
- vulnerabilities of selected public assets on the common cyber threats,
- the results evaluation and proposal on measures.

From the integral risk management point of view, the use case of risk management in

Authors: Dipl. Ing. Tomáš Kertis, Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc. Czech Technical University in Prague, Praha, Czech Republic, kertitom@fd.cvut.cz, prochazkova@fd.cvut.cz

the metro operation mainly deals with the phase of risk control, i.e. implementation of certain measures. It starts on the lower level - from the risk identification trough the risk analysis, assessment, evaluation, control, coping with risks up to monitoring in which there are prepared the corrective measures [12].

2. Safety management systems in transportation domain

The safety management systems are the systems of process and project management based on the TQM principles [5]. The safety management systems are possible to divide into three categories [4, 5]:

- vertical one – problem solution level: political; strategic; tactical; operative; and technical,
- horizontal one - problem solution domain: mode of transport; type of infrastructure; nature of the system under consideration; other domains,
- conditions of operation - criticality level: normal conditions (concentration to prevention); abnormal conditions (vigilance, readiness); critical conditions (response and recovery).

So the safety management system might be effective, it shall be introduced in all mentioned levels and domains. For illustration, we give an example of safety management system that considers three up to five levels of criticality of entity that is affected by disaster with different size.

In the model on Figure 1, it is shown the top level management on strategic level that on the outcomes from the risk management process establishes the requirements and criteria for the safety management at lower levels, i.e. in selected critical entities and areas.

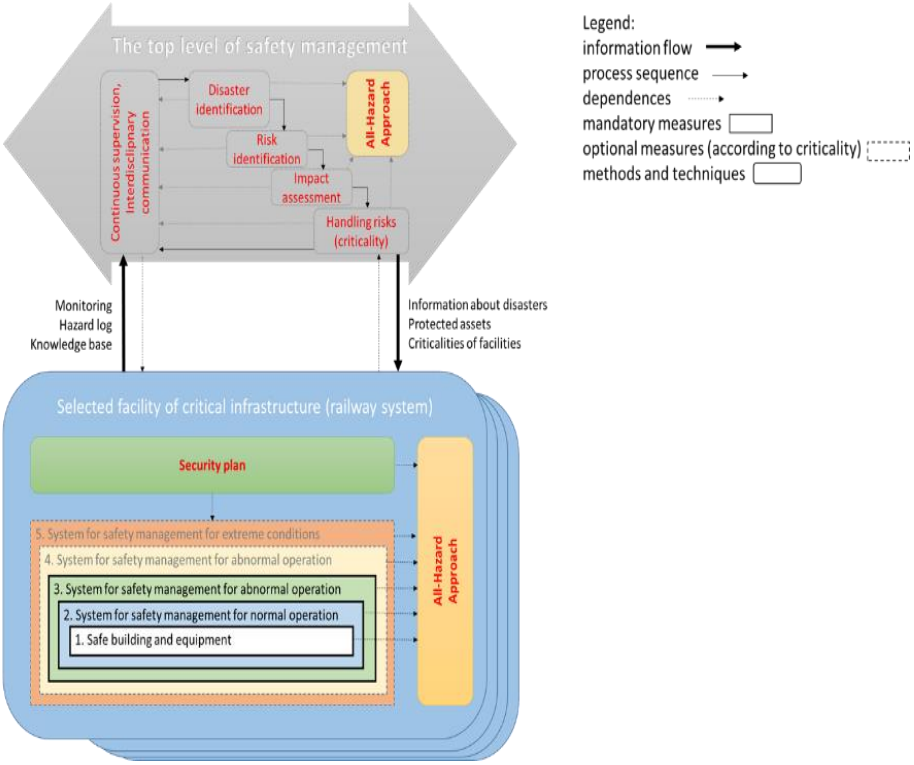


Fig. 1. General model of management of safety of facilities of critical infrastructure [3, 6].

On the entity level there are applied the safety management systems on the basis of knowledge from lower levels of problem solution, i.e. there are established the plans for management of safety with measures, which are implemented within the appropriate level of safety management system in the Defence-In-Depth approach [6]. The feedback to the top management is in the form of monitoring and continual assessment and improving the system operation, for which it is necessary inter sectoral communication through various fields [4, 7], is also shown there.

Present trends in the area of safety science and risk engineering are based on the above mentioned principles, namely with considering the system complexity that follows from the nature, properties and uncertainties of socio-technical and cyber-physical systems [2, 4, 7, 8].

Safety management systems in the transportation domain are particularly defined by European guidelines and then by appropriate national legislation. The legislation is divided for each mode of transportation domain and it is mostly brief or unclear, because it is too much generic or it only considers some of risks.

In industrial domains and in safety management terms of references, especially in quality management systems based on process and project management (TQM), it has been introduced the processes of risk analysis based on standard ISO 9001 [16] that were enhanced with requirements on quality and safety of products in the domain.

For electrical, electronic and programmable devices (E/E/PE) in industry domain, the international standard IEC 61508 [17] on functional safety has been introduced. Its approaches and mentioned standards for management systems are refined and enhanced with specific standards in each appropriate industrial domain. Their analysis shows that only very short group of items is assigned to critical infrastructure. In this case, the operator needs to introduce at least basic principles of crisis management; the operator has also duty to provide the appurtenant data to municipality for processing the off-site crisis plans.

The safety management system also includes the special part that is concentrated to tasks of cyber security. Process of ensuring the information security is based on protection of important assets of cyber (information) system by the way, that the required level of Confidentiality, Integrity and Availability (CIA) is ensured for important information [18]. In information technologies the CIA according to [18] means: information is not available or cannot be revealed by unauthorized individuals, entities or processes (Confidentiality); property describing the accuracy and completeness (Integrity); accessibility and usability of information on the request of authorized entities (Availability) [19]. Therefore, some subjects, such as owners or operators of critical informational infrastructures or operators of critical infrastructures, have duty to introduce the information security management system. These subjects may also require such system according to [18] from their suppliers.

Above mentioned facts imply the claim that current transportation systems are mainly secured in terms of functional safety. However, it is the fact that inconvenient events with sizes greater than design ones can occur, i.e. cyber-attack or other disasters can lead to system abnormal up to critical conditions, which severe endanger its surrounding, Figure 2.

In rail transportation, the Directive 2004/49/EC of the European Parliament and of the Council [20] introduces both, the CST – Common Safety Targets and the CSM – Common Safety Methods [21]. Each technical, operational or organizational change is subjected to strict documentation, assessment and justification it terms of factors

influencing the safety according to the CSM; the risk management methods are used. Any rail operator is obliged to introduce the safety management system with considering the normal and abnormal conditions. Indeed, it does not consider the critical conditions. The railway accidents shall be announced to national The Rail Safety Inspection that investigates accidents and proposes safety measures.

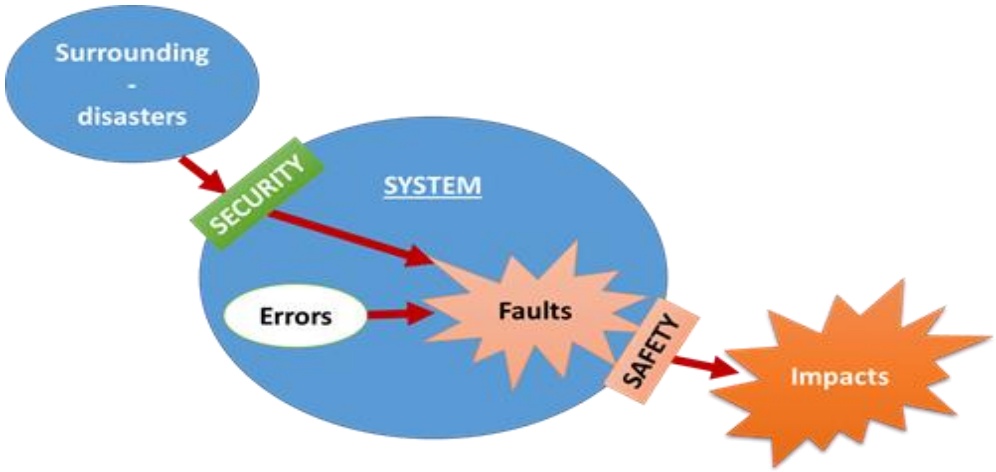


Fig. 2. Relation among safety and security of system [10].

The safety management system in the railway industry domain is based on high rate of quality assurance in the IRIS standard (International Rail Industrial Standard by UNIFE) and it applies the requirements on the system life cycle in accordance with EN 50126 [22]. Each change (technical, organizational and in management system) in the railway system is, therefore, subjected to risk evaluation with target, whether the change affects the safety or not. According to result of evaluation, the proposal of appropriate measures is performed. The standard EN 50126 [22] defines the railway system life cycle including the determination and demonstration RAMS (Reliability, Availability, Maintainability and Safety) properties and the life cycle costs (LCC) that take into consideration also the system operation, maintenance, renewal up to disposal.

The RAMS properties apply the system approach that divides the system into several layers. Each of such layer contains own functional subsystems, and on the basis of risk analysis it assigns the functions and safety functions. In terms of railway domain, the risk is expressed by relationship:

Risk = frequency x consequence.

The risk mitigation is performed by ALARP / ALARA approaches [22]. Functions, the malfunctions of which have severe impacts, or functions that mitigate the analysed risks are called the safety related functions. The safety related functions have assigned the safety integrity levels (SIL) from 1 up to 4 that are determined according to the tolerable hazard rate (THR), Table 1.

For the safety related functions, the protection measures are applied, which are similar to measures recommended by the industrial standard EN 61508 [17]. The protection measures are expressed by requirements focused on HW (hardware) according to EN 50129 [23] or SW (software) according to EN 50128 [24]. There are also requirements for the safety case elaboration. The 0 safety integrity level is used for the SW (software)

in the rail domain that is not related to safety, but it establishes minimal requirements for quality assurance.

Table 1. Relationship of THR to safety integrity level according to EN 50129 [23].

Tolerable Hazard Rate (THR) per hour, related to system function	**Safety Integrity Level (SIL)**
$10^{-9} \leq$ THR $< 10^{-8}$	4
$10^{-8} \leq$ THR $< 10^{-7}$	3
$10^{-7} \leq$ THR $< 10^{-6}$	2
$10^{-6} \leq$ THR $< 10^{-5}$	1

3. Data on technical and cyber assets of metro

We step by step describe the technical and cyber assets; we do not discuss the human sources that are also very important, but they create other separated issue. We pay the special attention to Urban Guided Transportation Management and Control System (UGTMS) and to safety related legislative requirements.

3.1. Technical assets

Beside the public assets (human lives and healthy, property and places including construction, well fare) which are interconnected with the metro system, the metro system has following groups of technical assets [26].

Technological parts and some support subsystems of controlled system include the assets:

- energy devices (transformer substations and distribution transformers),
- communication equipment (communication cables, VHF connection with trains; passengers' information systems including automatic check-in; communication systems for passengers and staff; CCTV, telephone, public address; clocks and fire alarms; protection systems and signalling),
- machinery (escalators; pump stations in nodes in stations and between them; elevators; workshops and warehouses maintenance stations),
- air-conditioning,
- mobile machines and devices (rolling-stock; devices and substances for cleaning, including the containers, cleaning machines, ladders, scaffolding for cleaning the lighting systems; fire protection equipment),
- next important equipment (security keys and alarm buttons; equipment for fire alarm start; traction devices and lighting; track devices, the main water shut; moving stairs, plates, signal panel for machinery devices; closing equipment (shutters)).

The control system involves the following assets:

- train dispatcher (surveillance and control of trains); and operation control centre (OCC) nodes, station nodes, nodes for automatic route setting system,
- energy dispatcher,
- technology dispatcher,
- lighting system dispatcher,
- communication and protection systems dispatching,

- fire dispatching,
- depot dispatching for train services and maintenance.

For a model metro station, the control system involves station, which has also assets as:

- station nodes of control system,
- station node for automatic route setting,
- station nodes for connection of energetic and technological dispatching,
- station nodes for central lighting control system,
- station interacting with dispatchers (communication, protection, operation, fire men).

In the railway practice context, the protection system is primary understood as system that is needed to mitigation of risks connected with the train operation. It has following main assets:

- station protection systems,
- wayside protection systems,
- train protection systems.

The metro stations´ assets are also:

- energy flow,
- information flow,
- central dispatching and station nodes of control system,
- central dispatching and station communication units,
- station nodes of control system and protection systems,
- station nodes of control system and communication system,
- protection systems and technologies (on the track and on-board)
- telephone connection between central dispatching (OCC) and station,
- telephone connection between central dispatching and trains.

3.2. Cyber assets

The metro management and control system depends on information technologies. The information systems show the observed features of metro using the linguistic communication language and it can serve to the making up the information about the observed object. Process of information origination, origination of information system, new object or modification of original object is assembled from following sub-processes, respectively sets and their relations [27], which are described in Table 2.

Table 2. Information origination process according to [27].

No.	**Process / set**	**Affected items / nodes**	**Used information technologies**	**Process inputs**	**Process outputs**
1	Object identification	object, observer	physical receptors (sensors)	observed condition (physical) quantities of object	signals
2	Observation statement	observer, language (syntax)	sampling, quantization, coding / encoding	signals	data

3	Communication between the source and receiver of message	language (of observer resp. system of data acquisition), message receiver	telecommunication, transmission and communication systems	data	data
4	Interpretation set, information origination	language (of observer resp. system of data acquisition, message receiver), information set (see item 6)	ontology, language	data	information
5	Relations hips of functions and structural arrangement of object, integrity verification	information (see item6), the object	actuator of system, action information system	object, information	information correctness, change of object
6	Information set in set of information systems	information systems	information systems	information	information
7	Interpretation process	information (see item 6), the object	signalizing and representation technology, artificial intelligence	information	image of object, new object

Regarding the nature of our task connected with the distributed transportation system with geographically distributed remote system nodes in the city, it is appropriate to give relations, which describe the quality of information transmission in the transmission medium (see item No. 3 in Table 2). Thus, we consider the control system with feedback that is expressed in Figure 3 in accordance with [19, 28, and 29].

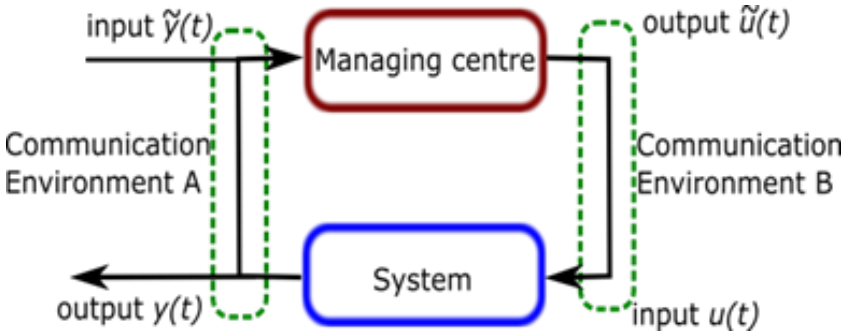


Fig. 3. Relationships of control system in the cyber-system [19].

The cyber-system represented in Figure 3 exhibits the specific qualitative properties, such as the information power and the information security, i.e. to their confidentialities, availabilities and integrities. Both of them, the information power and the information security, are described in detail in [19]. Information technologies, with connection of hardware and software, serve to performing certain functions that are further described.

3.3. UGTMS

The description of metro system general function follows from the description of Praha metro management and control system (ASDR) [28, 30] and the European standards on functions and parameters of Urban Guided Transportation Management and Control System (UGTMS) [31]. From the technical viewpoint, the metro system can be divided into three main parts: control; controlled; and protection systems. They have mutual interconnections and some common inputs and outputs. Information from planning the operation process (as timetables, duty rosters etc.) is the input into the system. The system output is the ensuring the transport performance in required quality and in given transportation mode, and the mitigating the disasters´ impacts in protection mode [19].

According to executed functions given in [31], the management system (UGTMS) is divided into several levels regarding to the problem solution level (operation planning, operation management, supervision, trains´ control) and the degree of automation (from GOA 0 up to GOA 5; from manual train operation up to fully automation operation - Unattended Train Operation ATO) [31].

Table 3 contains the general description of metro system according to [14, 30] and also assigned technical and functional blocks and interfaces according to UGTMS [31].

Table 3. General model of metro system [14, 30, 31].

Parts	**Assignment of blocks and interfaces of UGTMS**	**Inputs**	**Outputs**
Management and control system	Core of UGTMS (operation control system, wayside devices, on-board systems, data communication system), Management (central human-machine interface (HMI), local human-machine interface, wayside devices, interlocking, operation planning), Information and telecommunication systems (audio communication, communication with staff, passenger communication), Stations (CCTV surveillance, passenger information systems, audio communication), Train (HMI with train staff, rolling stock diagnostics (for maintenance), train condition (in terms of operational capability), fare collection (location	vicinity, operation planning, controlled system METRO	protection systems, controlled systems METRO

	information), CCTV surveillance, audio communication), Maintenance (maintenance depot systems), Traction power supply (traction power supply management).		
Protection system	Stations (fire detection/react to detected fire, platform-to-track intrusion detection system (passenger on the track), platform doors and/or platform end doors, interfaces with other equipment (emergency handles, emergency call devices, equipment for detection/closing of unprotected areas, the check button “the train is ready to depart”), Train (equipment for detection of obstacles, derailment, fire or smoke, equipment for detection/closing of unprotected areas, emergency handle, release of doors / emergency button), Infrastructure (detection of broken rail, detection of fire or smoke, intrusion detection system).	vicinity, management and control system	controlled system
Controlled system METRO	Information systems, Stations (supporting equipment (elevators/escalators)), Train (doors, traction, brakes, equipment that connects the train (electrical inter-vehicle jumpers), interfaces with other systems (lighting, heating, ventilation, air-conditioning (HVAC), batteries), passenger information system), Infrastructure (tracks, tunnel ventilation, interface with other equipment (pressure doors)), Traction power supply (high-voltage switch)	vicinity, protection system, management and control system	management and control system, quality of operation and transport performance, mitigating impacts of disasters.

Specific features of Praha metro system are described in detail in [14]. Functions, functional relations and general requirements on function execution of UGTMS are defined in the standard [31]. Requirements are appropriately marked for each degree of automation as mandatory, conditioned or optional.

Above mentioned functions and divisions we use for definition of high level requirements on the system in terms of references. They do not provide the detail description of affiliations of functions, parameters of individual subsystems, demands on safety of partial systems and whole system (integral safety - quality). Mentioned properties need to be specified according to local demands and conditions of related and superordinate systems, including the connections to surface transportation, geological and climatic conditions, and hazard rate from all relevant disasters, etc.

Because we also deal with issues of cyber safety, we focus on demands and features of UGTMS core, which is the most critical part of management system and its interfaces; it is on: operation control system; wayside devices (it includes point transmission between the track and train); on-board systems (it includes localization, speedometers, time measurement); data communication system (it includes data transmission between the wayside devices and operation control system, and communication between wayside devices and trains).

Figure 4 shows the relation between the cyber security management of system, compiled according to EN 62290 [31] and real scheme of information infrastructure in metro [19, 28, 30]. The UGTMS system segmentation shown on the left site is according to management level (operation planning, operation management and supervision, train control).

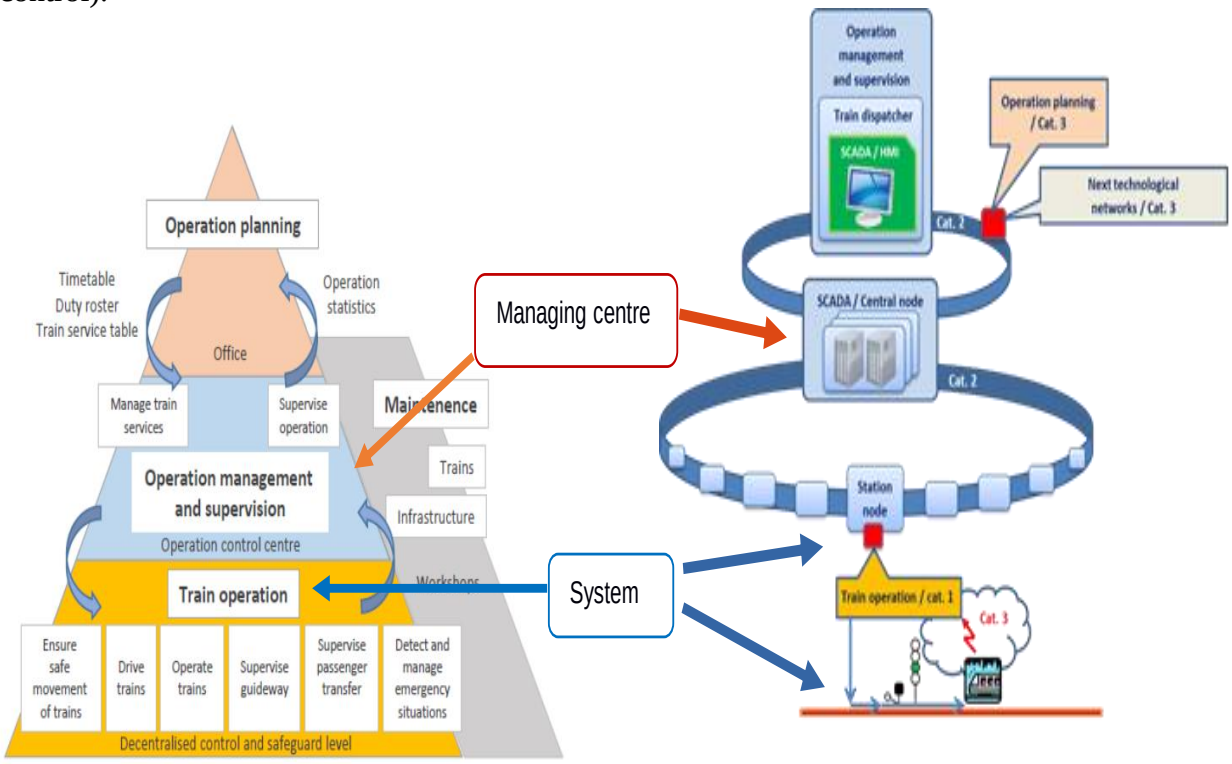


Fig. 4. Model for cyber security management of the system according to EN 62290 and real scheme of information infrastructure in metro [19, 28, 30, 31].

Real organization of system for the Praha metro traffic management, the dispatcher workstations are connected with central system nodes (in this level they are shown also other interfaces with other technological or facility systems). The central nodes are interconnected together to proper communication infrastructure with station and way side subsystems. Red points on the figure right side mark the critical communication interfaces and transmission medium according to data in [19, 28]. The designation Cat. 1-3 means the category of transmission system according to the railway standard EN 50159 [32].

At certain rate of abstraction, according to Figure 4 it is possible to enhance the classification of cyber-physical system with blocks of UGTMS and parts of ASDR management system for transportation operation of metro Praha:

1. Managing centre – operation management and supervision – central nodes of ASDR (resp. control nodes in stations).
2. System – train operation – station systems, interfaces and communication access points on the track, on-board communication units, on-board computers.
3. Communication environment A, B according to Figure 3 – system of data communication – network of dispatcher centre, network of station and wayside nodes, wireless transmission system.

The metro functions shall be also performed and supported by other interconnected systems of technological, physical and human nature. Any part of metro system has fittings and flows, the disruption of which could lead to malfunction and an accident. Therefore, we are looking for important part criticality, it means for assets, which have certain rate of importance and vulnerability. Due to system complexity we have created model of metro station based on data on real metro operation in Praha capital [19, 28, 30].

3.4. Safety related legislative requirements

The ground for ensuring the safe metro and its safe operation is the correct technical background that includes the sitting, technical implementation design, building, construction and operation [5]. The greater requirements, the greater demands on knowledge, material, construction and operation are. Therefore, it is necessary to codify all relevant requirements. The Czech Republic legislative takes over the European Union technical demands on product, the Act No. 90/2016 Coll., on conformity assessment of product when it is made available on the market [33] or the Act No. 22/1997 Coll., on technical requirements on products [34]. From the legislative it follows that each product before introduction on the market needs to take the conformity assessment with the legislative regulations, stipulated and selected harmonized standards.

The legal rules assign the duties on work with information, thus the information systems need to carry out the specific legislative demands and to ensure the security demands of domain for which the information system is designed. The example is the Act No. 101/2000 Coll., on personal data protection [35], the Act No. 365/2000 Coll., on information systems for public administration [36], the Act No. 412/2005 Coll., on the protection of classified information and security capability [37] etc.

The standards specified by legislative include the real requirements for given product purpose, resp. system, and all subjects participated on the given system life cycle need to respect these standards. Other harmonized standards (mainly taken on from foreign wording) or other specific standards are not mandatory, but by their using the certain system parameters systems are improved.

The technical standards establish both, the requirements on management systems (i. e. standards introducing the process and the project principles of TQM [4, 14]) and the real technical requirements on products. The examples are the standards on management systems belonging to set ISO 9000 [16], on quality management systems, ISO/IEC 20000 [38], on IT service management (that implements parts of ITIL concept), ISO/IEC 27000 [18], on information security management systems, or EN 50126 [22] on case of railway systems for the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). The standards stipulating the requirements on products, resp. systems are EN 62290 [31] or EN 50159 [32].

Systems for management of urban tracked transportation in the Czech Republic are governed by Act No. 266/1994 Coll., on rail system [39] and also by related notices and

executive regulations. In these legal rules, it is the list of determined standards, namely including the EN 50126 [22] standard and other ones, as EN 50129 [23], EN 50128 [24].

Due to reality that the metro system in Praha belongs to critical infrastructure, it needs to fulfil the demands of other acts, Act No. 240 Coll., on crisis management [40], Act No. 181 Coll., on cyber security [41] from the viewpoint of cyber-physical systems. From last one it follows that the operator of such system needs to use such tools, which ensure:

- limitation of physical access to network and equipment of industrial and control systems,
- abatement of interconnections and remote access to network of industrial and control systems,
- protection of individual technological assets of industrial and control systems against to use of known vulnerabilities,
- renewal of operation of industrial and control systems after the cyber security incident.

On the basis of present knowledge, the first two requirements can be resolved by technical measures. The other two are ensured at current practice by existing railway methods; by fulfilment of determined railway standards.

It is the fact that the present railway standards are oriented to technical and functional safety (except several specific areas given in standard EN 50159 [32]). It means that they consider neither the critical conditions of systems, nor the extreme disasters, which can cause them the serious losses and damages. To such disasters, the possible cyber-attacks belong. It is indeed the truth that it has been designated many standardization commissions which have been dealt with the cyber security in the railway domain, but applicable and proven methodologies are still not available, everything is generated by method trial and error.

With regard to described situation, the railway practice follows the standards on ensuring the cyber security from other sectors. They, however, need to be implemented by specific parameters of railway domain [1]. The examples are standards: ISO/IEC 27000 [18], EN 15408 [42] or ISA/IEC 62443 [43].

Respecting the legislative and standards in force, the railway operators ensure the certain level of safety (quality of whole safety) and security of products appointed for specific needs and areas. If we consider the complex cyber-physical system as system of systems with many linkages and couplings, and primarily with subsystems at interfaces of various sectoral mediums, the mentioned requirements of legislative and standards are insufficient. Therefore, in practice, it is necessary to look for solutions that exceed the legislative requirements [3, 44].

4. Methods used for data processing

Considering the principle Defence-In-Depth, described for complex technological facilities [6], we shall mostly concentrate to the management units that keep the sufficient level of safety at normal, abnormal and critical conditions. Safety management system of metro (SMS) has the central control system and controlled systems, Table 3. It is very complex distributed system that involves controlled, control and protection subsystems, their interdependences, operation states and conditions.

In previous works, we have crated the model metro station and its security plan that is based on integral safety [14]. On basis of model and using methods of risk engineering, we have identified common protected assets and elaborated the risk management plan on priority risks. The priority risks have been determined by comparison of: normative

requirements that respect the principles of All-Hazard-Approach and Defence-In-Depth that have been created for complex technological systems [14, 20], with the real state in the Praha metro that corresponds with legislative requirements – described above.

Although we consider the integral safety, this part deals with safety of cyber-physical system, the metro management and control system that is categorized as the processes information system according to [19] and which is affected by all information technologies from Table 2 and. We deal with the real system that was not built according to the current law and standards. Due to the risks connected with the change of complex system, it is not simple to change the present cyber-physical systems and socio-technological systems; within some system we can improve one from critical parameters but it leads to decrease of safety for other one. On the other side the system is changing, day to day, from the view of system, and also from the view of super ordinary side, like the whole transportation infrastructure, government, city, the State etc. We need to react on the new technological, organizational, and legal demands [28]. The issue is to trade-off with the priority risks in terms of control system and information flow.

In management and engineering disciplines, there are special tools by which we identify, analyse, assess, manage and trade of with risks of various kinds including the cross-sectional ones. On the basis of present knowledge and experience on behaviour of advanced complex technological facilities [5, 28, 30], we need to take into account that there might be occurred sooner or later some disruptions of management and control system cyber safety. Of course, according to present knowledge and experience, there are several disasters that can disturb the system safety [44, 28, 30], and therefore, the complex solution is very wide-ranging [28].

Due to the complex structure of followed system we need to consider the non-structure problems. Therefore, for their research we choose the case study method and the What-If method modified for solution of security problems [12, 16]. The What-If method is in our work divided into pars of evaluated assets and impacts of possible common incidents. On the basis of: critical judgement of What-If results; results obtained in the SESAMO project [45]; experiences from practice; and respecting the demands of cyber act (law No. 181/2014 Col.) in force, which is based on standard ISO/IEC 27001 [18], we propose the improvement for both, the safety and the security of metro supervision and management system [28]. The case studies deal with the disruption of cyber safety of metro supervision and management system, the model of which is shown in Figure 4. They are focused on the most priority sites of system [28, 30].

On the basis of critical judgement of data in documentation [28, 30], there are identified three vulnerable sites, explored in the case studies. The vulnerable sites make up the interface with the surrounding, between the close system, in which there is ensured multiple physical protections and security, and a vicinity of system that is accessible for several stakeholders.

5. Priority risks and measures for their mitigation

The most important findings of the previous research related to the present work are that humans are secured very little; control, energy and information flows, air conditioning, machinery, communication and next equipment have higher security; and the mobile machines and devices, next important equipment, construction (property) and places are more secured [20, 26]. According to [20], following items are danger, they have high or very high probability and high severity:

- failures in processes and human errors in all levels of safety management system (according to Defence-in-depth),
- execution of mutually influencing functions in term of mutual links and flows between secondary and superordinate systems,
- faults in dependences between levels of safety management system (SMS): flawed methodology for hazard identification and risk analysis within the higher levels of SMS; misunderstanding of requirements and information from other level of SMS; missing input information,
- other unpredictable events and human factors (internal, external factors or malicious attacks).

The generic recommended measures are [25]:

- to introduce quality / safe and monitored processes of maintenance and operation, which are introduced in the station operation rules,
- to apply the security, plan at the design, construction and management of changes, which is targeted to elimination of system failures and to have a plan for the cope with system failures in the operation,
- to introduce periodic training, examination and exercises of staff; the confirmation function of E/E/PE from [17] and feedbacks,
- to ensure the safety by the high quality of the installed systems according to the requirements of [16, 22],
- to carry out regular audits, evaluation of competences and to ensure the independence of solved teams, etc.

6. Selected cyber risks and countermeasures for their mitigation

We concentrate only on three originators of cyber risks that we revealed on the basis of data in the operation documentation [28, 30]. For these phenomena we construct impacts by the What, If method. It goes on:

- the impacts of penetration through the interface, denoted in Figure 4 as “Operation planning”,
- the impacts of penetration through the interface denoted in Figure 4 as “Train operation”,
- the impacts of penetration through the air transmission information between train driver or on-board systems and station controller, Figure 4 [28].

Each of cases has specific features. In first case, it is the interface with opened network from the view of the supervision and control system. The second case deals with problem of different safety integrity levels (SIL) in the view of functional safety, and moreover it could be exploit after disruption in first case, it means, more sophisticated attack that is not usually considered in the context of the functional safety domain. The third case study considers the open environment, there attacker can handle with transmitted messages or he can penetrate closed system.

From the safety reasons, it is necessary to ensure the high quality of protection, which means to understand the severity of least unfavourable security incidents, and therefore we take into account the boundary issues. The results of What-If method application are in Table 4; it contains the security incidents impacts on public assets and on the metro assets obtained by assessment of the most critical unfavourable cyber security incidents. It was used the scale with the four degrees: insignificant; marginal; critical; and

catastrophic, which is in detail characterised in documentation [28] and that goes from the standard EN 50126 [22].

Table 4. Impacts of disruption of the system cyber safety on public and metro assets [28].

Assets	**Impacts**
Case study 1 – (threats: system disruption, loss of system integrity, loss or even taking control)	
Human lives, health and security	Employee: marginal; only indirect impacts caused by confusing the dispatcher and his wrong decision. Passengers: marginal; only indirect impacts caused by confusing the dispatcher and his wrong decision. Humans outside the metro: insignificant; catastrophic only in the case of more sophisticated terrorist attack, series of commands (improbable).
Property	Metro: marginal. Public: marginal; it follows from panic and size of danger of minor thefts.
Environment	Insignificant.
Welfare	Marginal; panic and possible discredit.
Metro transport	Significant; direct impacts on train movement, worsening the transport and delay.
Finance and other losses	Metro: significant; loss of profit due metro operation stoppage, harm on goodwill. Public: critical; loss of transport possibilities
Case study 2 (threats: system disruption, loss or even taking control)	
Human lives, health and security	Employee: critical; single fatality or severe injury. Passengers: catastrophic; fatalities or multiple severe injuries. Humans outside the metro: critical; it follows from panic and movement of many people.
Property	Metro: Critical – loss of major system. Public: Marginal; it follows from public and size of danger of looting.
Environment	Insignificant.
Welfare	Marginal; panic and discredit in the high range.
Metro transport	Significant – direct impacts on train movement, worsening the transport and delay.
Finance and other losses	Metro: significant; loss of profit due metro operation stoppage, harm on goodwill. Public: critical; loss of transport possibilities
Case study 3 – (threats: system disruption, loss of system integrity, loss or even taking control)	
Human lives, health and security	Employee: marginal; only indirect impacts caused by confusing the dispatcher and his wrong decision. Passengers: marginal; only indirect impacts caused by confusing the dispatcher and his wrong decision. Humans outside the metro: insignificant; catastrophic in the case of more sophisticated terrorist attack,
Property	Metro: marginal. Public: marginal; it follows from panic and risk of minor thefts.

Environment	Insignificant.
Welfare	Marginal; panic and possible discredit.
Metro transport	Significant; direct impacts on train movement, worsening the transport and delay.
Finance and other losses	Metro: significant; loss of profit due metro operation stoppage, harm on goodwill. Public: critical; loss of transport possibilities.

Because the entire control and controlled system in metro is formed by distributed structure with number of system nodes, and most commands or dispatcher actions are conditioned by correct information and set of acknowledgement messages sent in various ways, we considered the Bayesian theory described in chapter [19, 28] based on the cyber system given by Figure 3. The theory points to information availability and integrity, which are in the case of such real-time systems more important than confidentiality. For understanding the problem, we give three case studies. On their base we propose the optimum improvement the system from the viewpoint of safety and security [28].

The critical evaluation of the results in [19, 28] shows the vulnerable sites at metro cyber safety. For reduction of revealed vulnerabilities and cyber safety improvement we use the provisions in legislation. The measures enforced by the legislative need to be mainly implemented in the interfaces of metro supervision and management system with other parties. Because the legislation, norms and standards in force only involve the common organization and technical measures, it is necessary to improve them. It means to establish the sufficient and effective risk management – at all levels of a problem solution, monitoring and measures for improving safety [19, 28]. Beyond the scope of given measures, it is also necessary to introduce in the top level safety management the united terminology and correctly defined scales for assessment of assets criticalities, interdependences criticalities and risks in system concept.

Therefore, the owners and operators of system such as metro and metro management and control system shall at least ensure following tasks:

- manage public assets with interdependences, it means to establish risk management in terms of integral safety (top level safety management based on All-Hazard-Approach and with consideration of Defence-In-Depth), to evaluate assets criticalities and protect the most critical assets (active and passive safety, security plan of system),
- manage and supervise other stakeholders (subcontractors, vendors etc.) due to ensuring high level of availability, it includes well assigned requirements and responsibilities to next subjects in terms of dependability and safety parameters, organizational demands (well implementation of IT standards on information power and safety / security, the TQM principles such as COBIT, ITIL, ISMS, ICS security etc. with clear communication matrix) [19],
- define the most important functions, their CIA parameters and manage them (including reliability, availability, maintainability and safety and/or security; RAMS), analyse vulnerabilities mainly at interfaces with systems of different nature; the matter also includes to establish not only technical parameters, but also well-established common criteria and scales for risk management through all stakeholders (requirements and responsibilities for these parameters on all subjects),
- check all important monitoring activities, whether they are sufficient, take into consideration the time correct and valid report to users on system faults, be aware different meanings of some terms in different industrial fields,

- supervise the information power mainly under construction of the system, because changes during operation are time consuming, expensive, it subjects to change management and safety assessment, it could bring new vulnerabilities and errors due to interdependences,
- audit system accuracy in defined range, because all activities consumes certain resources, the system is facing trade-offs between benefit, costs and safety; the cost benefit analysis shall be performed.

The mentioned points above exceed legislative requirements, because they are multidisciplinary and they oblige more subjects.

7. Conclusion

Real world is full of uncertainties and diverse events, which may occur either by graduated way or imminently with severe diverse impacts. Human capabilities are limited to certain set of knowledge. Thus it appears that regarding the real world uncertainties, people are not able to prepare on all events which endanger human security. Human intervention into real world at development of new technologies, its installation and interconnecting, changes the world and makes it more complex – difficult. It means that the human being introduces new uncertainties and endangers. We are not able to protect against all hazards, but we can effort to introduce new hazards as least as possible, and also to prepare people on unexpected events with the only aim – to ensure human security and survival.

For ensuring the certain rate of safety, we introduce safety management systems with (SMS). The main assumption for well performance of the SMS is that it is applied at all management levels in both, horizontal and vertical dimension and where the effective communication and propagation of common management targets to lower levels is ensured. Particular SMS areas shall bind on requirements and targets of higher layers (political at the State level or whole continent or world), so that it might react on context of surrounding systems in the best way. It needs to ensure the management system at the highest level (top level), propagate them into lower levels, to keep interdisciplinary communication, to establish monitoring and to enforce appropriate measures. The mentioned system with considering of different risk management and perceiving the risk in various transportation domains is described above.

The work provides comprehensive overview of safety management and risk management issues from both, general layer and with focusing on the railway system. The approach of proactive SMS with consideration of integral risks is introduced into the use case present in the work. The use case builds on ongoing research of the safe metro operation and at this paper it focuses on cyber safety of urban guided transportation management and control system. Unfortunately, neither there is available nor tool or standard, which would specify the procedure for security practices in this specific field of cyber systems. The IT method [19, 28] or method from the field of industrial control systems [43] can only be used provided that they complied with the railway specifics, resulting from the requirements to ensure the functional safety of all interfaced equipment; availability, cyber security, interoperability and scalability of the data communications infrastructure are attributes that need to be maintained during the system life cycle.

Acknowledgement

Authors thank to the Czech Technical University in Prague for support (grant SGS2015-17).

References

[1] PROCHAZKOVA, D. *Critical Infrastructure Safety* (In Czech). ISBN: 978-80-01-05103-0. Praha: ČVUT 2012, 318p.
[2] PROCHAZKOVA, D. *Strategic Management of Safety in Territory and Organization* (In Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT, 2011, 483p.
[3] UN. *Human Security in Theory and Practice*. New York: United Nations 2009.
[4] KERTIS, T. Comparison of approaches for safety management in transportation (In Czech). In: *Business process and territorial risks and knowledge for crisis management.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 34-59.
[5] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.
[6] PROCHAZKOVA, D. *Safety of Complex Technological Facilities*. ISBN: 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing, 2015, 244p.
[7] KERTIS, T. Introduction of modern approaches of ensuring safety into business processes in railway industry. In: *Selected risks of business processes*. ISBN 978-80-01-05831-2. Praha: ČVUT 2015, pp. 26-38.
[8] GLENDON, I. A. et al. *Human Safety and Risk Management.* ISBN 0-8493-3090-4. Boca Raton: CRC Press 2006.
[9] NOVAK, M. et al. *Dependability of hybrid system* (In Czech). In: Issues of system dependability, service life and safety. ISBN 80-903298-2-9. Praha: Neural Network World, 2005, pp. 23-24.
[10] KERTIS, T., PROCHAZKOVA, D. Tools for Risk Management of Model Metro Station. In: *Smart Cities Symposium Proceedings in Prague*. ISBN: 978-1-5090-1116-2. Praha: CVUT 2016, 8p.
[11] PROCHAZKOVA, D., PROCHAZKA, J., KERTIS, T. Safety of Complex Critical Technological Systems (In Czech). In: *Proceeding of international conference on security technologies, systems and management 2015*. Zlin: UTB 2015,11p.
[12] PROCHAZKOVA, D. *Analysis and Risk Management* (In Czech). ISBN:978-80-01-04841-2. Praha: ČVUT 2011, 405p.
[13] KORECKY, M. & TRKOVSKY, V. *Project Risk Management* (In Czech). ISBN 978-80-247-3221-3. Praha: Grada 2011, 578p.
[14] KERTIS, T. *Security Plan of Selected Station in Praha Metro* (In Czech). Diploma´ Thesis, Praha: CTU 2015.
[15] PROCHAZKOVA, D. *Principles of Management of Critical Infrastructure Safety* (In Czech). ISBN 978-80-01-05245-7. Praha: CVUT 2013, 223p.)
[16] ISO. *EN ISO 9000:2005 Quality Management Systems. Fundamentals and Vocabulary*. Geneva: ISO 2005
[17] IEC. *IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related System*. Geneva: International Electrotechnical Commission 2011.
[18] ISO. *ISO/IEC 27001: Information Technology – Security Techniques - Information Security Management Systems – Requirements*. Geneva: ISO 2013.

[19] KERTIS, T. PROCHAZKOVA, D. Cyber Security of Underground Railway System Operation. In: *Smart Cities Symposium in Prague*. Praha: ČVUT 2017; in print.
[20] EU. *Directive 2002/49/EC of the European Parliament and of the Council of 25 June 2002 Relating to the Assessment and Management of Environmental Noise - Declaration by the Commission in the Conciliation Committee on the Directive Relating to the Assessment and Management of Environmental Noise*. Brussels: EC, 2002.
[21] EU. *Regulation 402/2013 on the CSM for Risk Assessment and Repealing. Regulation 352/2009*. EC, 2013.
[22] CENELEC. *EN 50126-1: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety*. Brussels: EC for standardization 1999.
[23] CENELEC. *EN 50129: Railway Applications - Communication, Signalling and Processing Systems – Safety-Related Electronic Systems for Signalling*. Brussels: EC for standardization 2003.
[24] CENELEC. *EN 50128-ed.2: Railway Applications - Communications, Signalling and Processing Systems – Software for Railway Control and Protection Systems.* Brussels: EC for standardization 2011.
[25] KERTIS, T., PROCHAZKOVA, D. Risk Management Plan for Metro Station Safe Operation. In: *Risk, Reliability and Safety: Innovating Theory and Practices*. ISBN: 978-1-315-37498-7. London: Taylor & Francis Group 2017, pp. 1306-1314.
[26] KERTIS, T. PROCHAZKOVA, D. Assets of Model Metro Station and Their Criticality. In: *IRICoN 2016*. ISBN: 978-80-01-06022-3. Acta Polytechnica CTU Proceedings. ISSN 2336-5382. 5 (2016), pp. 29-37.
[27] MOOS, P. MALINOVSKY, V. *Information Systems and Technologies*. ISBN: 978-80-01-04064-5. Praha: CVUT 2008, 210p.
[28] NOVOBILSKY, P. et al. Cyber Security of Metropolitan Railway Communication Infrastructure. In: *Risk of business and territorial processes.* Usti nad Labem: FVTM UJEP 2016.
[29] SVOBODA, V. SVITEK, M. *Telematics over Transportation Networks* (In Czech). ISBN 80-01-03087-3. Praha: CVUT 2013, 86p.
[30] DOPRAVNÍ PODNIK PRAHA. DP Kontakt. *Journal of Employees of Public Transportation Company in Praha Capital* (In Czech). ISSN 1212-6349. Praha: DPP, 1999-2016.
[31] ISO. *EN 62290-1:2006: Railway Applications. Urban Guided Transport Management and Command/Control Systems. System Principles and Fundamental Concepts*. Geneva: International Organization for Standardization 2006.
[32] CENELEC. *EN 50159: Railway Applications. Communication, Signaling and Processing Systems. Safety-Related Communication in Transmission Systems.* Brussels: EC for Electrotechnical Standardization 2010.
[33] CR. *Act No. 90/2016 Coll., on Conformity Assessment of Product When It Is Made Available on the Market* (In Czech).
[34] CR. *Act No. 22/1997 Coll., on Technical Requirements on Products* (In Czech).
[35] CR. *Act No. 101/2000 Coll., on Personal Data Protection* (In Czech).
[36] CR. *Act No. 365/2000 Coll., On Information Systems for Public Administration* (In Czech).
[37] CR. *Act No. 412/2005 Coll., on the Protection of Classified Information and Security Capability* (In Czech).

[38] ISO. *ISO/IEC 20000-1:2011 Information Technology. Service Management. Part 1: Service Management System Requirements.* Geneva: IEC 2011.
[39] CR. *Act No. 266/1994 Coll., on Rail System* (In Czech).
[40] CR. *Act No. 240 Coll., on Crisis Management* (In Czech).
[41] CR. *Act No. 181 Coll., on Cyber Security* (In Czech).
[42] ISO. *ISO/IEC 15408-1:2009 Information Technology-Security Techniques-Evaluation Criteria for IT Security -- Part 1: Introduction and General Model.* Geneva: IEC 2009
[43] ISA. *ISA/IEC 62443-1-1. Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*. Geneva: IEC 2007.
[44] PROCHAZKOVA, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing, 2014, 218p.
[45] ARTEMIS Joint Undertaking. *D2.1 Specification of Safety and Security Mechanisms, v01. SESAMO.* Brussels: ARTEMIS JU 2013.

Chapter 4

EVALUATION OF RISKS IN TRANSPORTATION OF ITEMS

1. Introduction

It is very important to compare the risks in transportation of goods in multimodal transport. Today, multimodal transport is preferred because by combining a number of separate transportation modes, one can transport goods at great distances, even at a global scale. Multimodal transport is defined as transport using two or more transportation means. This means that trans-loading of goods occurs, and can occur several times. And it is at these times when risk is higher, both of damage and theft.

In order to simplify trans-loading, containers are used which can be used on all transportation types. This eliminates the risk of damage to the goods while handling during the trans-loading. At the same time, however, demands on securing the container grow, as this security must meet the conditions of all transportation means which will be used during the course of transportation. Damage to the transported goods can be a highly risky affair, such as when carrying hazardous goods and in this case protection must be secured to prevent any danger to human health or life, damage to the environment, or theft of the goods. It is necessary to mention the importance of the human factor as a risk during the transportation of goods. It is necessary to evaluate it together with the other risk factors that occur during transport.

It is essential to compare and assess the system of checks and identify weak points in the safety and security of goods in the multimodal transportation process [1].

2. Background research and solution concept

When resolving problems, it is necessary to identify risks for certain types of transported goods and determine the types of danger during transportation.

2.1 Types of transported goods

In order to ensure an optimal transportation method, one must differentiate between various types of transported goods due to weight, size and shape [2]. There are four types of transported cargo:

1. Container - the optimal method for transporting goods. In containers, goods are protected from the weather and a number of other factors by steel walls. The standardised container size is convenient for multimodal transport, since its dimensions correspond to requirements for sea vessels, lorries and railway carriages (e.g. electronics, food, consumer good, etc.).
2. Liquid bulk (no packaging) - transportation is secured using large tankers or through pipelines (e.g.: crude oil, petrol, light fuel oil, vegetable oils, etc.).

Authors: Assoc. Prof., Dipl. Ing. Helena Bínová, Ph.D., Dipl. Ing. Daniela Heralová, Czech Technical University in Prague, Praha, Czech Republic, binova@fd.cvut.cz, heraldan@fd.cvut.cz

3. Dry bulk (no packaging) transportation is secured within the hold of ships, train carriages or lorries (e.g.: grain, coal, iron ore, cement, sugar, salt, sand, etc.).
4. Breakbulk - transportation can occur in containers or within the cargo hold of the transportation means. The goods are often packaged on pallets or in crates (e.g. paper, wood, sacks of cocoa, bulky and oversized objects, etc.).

2.2 Types of transport modes and related risks

During transportation, goods are subject to various dangers and they must be secured against damage and against endangering third persons if necessary (e.g. release of the cargo, etc.).

Newton's First Law applies in transporting goods, and this reads: 'An object that is at rest relative to an appropriately selected frame of reference will remain at rest. 'In an inertial reference frame, an object either remains at rest or continues to move at a constant velocity, unless acted upon by a force' [3]. We can distinguish five basic modes of transport: road, rail, see, inland waterway and air.

Road transport

During movement of the transportation means, vertical movements caused by impacts and vibrations from the road reduce the force of friction to as low as zero. When using road transport, the following risks can appear:

1. Securing cargo – it is a good idea to use immobilising methods. Frictional forces depend on the joint properties of the cargo and the trailer cargo space with which it is in contact [4]. Additional immobilisation methods are used to prevent tilting and tipping. Attention must be paid to the location of the centre of mass.
2. Load distribution – if the transportation means is partially loaded or unloaded during the course of the journey, a change in the load distribution occurs.
3. Dangerous goods, i.e. items which have the properties of being flammable, corrosive, explosive and others – during transportation, the safety of people, property and the environment may be put at risk.
4. Cargo with limited shelf-life – special conditions must be observed to ensure that no changes to the goods' properties occur. Temperature, humidity and other values must be checked.
5. Theft of cargo or cargo including transportation means – this applies to road, rail and sea transportation. Theft can also be undertaken using GPS signal interferences, followed by the lorry being stopped and the goods being stolen [5].

Rail transport

When using the railway transport, the following risks [6] can appear:

1. Impacts as a result of train composition - during this activity, individual carriages or groups of carriages are pushed together and coupled. Carriages going down from the humps are stopped by buffers and if there is an error impacts may occur, which represent a marked deceleration. Containers are not designed for this kind of stress, and should not be subjected to this kind of acceleration.
2. Dangerous goods – in rail transport, the carriage of dangerous goods must be undertaken in accordance with RID - Reglement concernant le transport international ferroviaire marchandises dangeroeuses.

3. Cargo with limited lifespan – railway transport is more danger than road and air because it is significantly slower.
4. Theft of cargo - theft can occur when a train is stopped, or even when it is moving. Compared to road transport, the risk of this is very low.

Sea transport

A key factor here is the values of acceleration which can be anticipated in sea transport, dependent on the shape of the ship, its support, centre of mass and its ability to stay afloat and similar parameters which determine the behaviour of the ship on the sea [6].

When using maritime transport, the following risks can appear:

1. Heaving – i.e. the upwards and downwards acceleration of the boat along its vertical axis. If the troughs of waves predominate, the ability to remain at sea level goes down and the boat falls; if the crests of wave predominate then the boat rises. This constant oscillation has a marked impact on containers and their contents.
2. Surging and swaying – if the bow of the vessel is on one side of the crest of waves, and the stern is on the other side, then the ship's hull can be subjected to marked torsion.
3. Rolling – the movement of the ship from side to side. Roll angles can reach up to 45° or more. If containers are insufficiently secured, this situation is very dangerous.
4. Vibration – goods are subjected to pressures from the extreme low-frequency vibrations caused by sea conditions and high-frequency technology and vibrations of propellers. This risk can and must be eliminated by the use of packaging adapted for sea transport.
5. Dangerous goods – carriage is undertaken in accordance with IMDG - International Maritime Dangerous Goods Code.
6. Cargo with limited lifespan – the carriage of perishable goods is danger due to the longer duration of sea transportation.
7. Theft of cargo; pirates are the main danger here. According to the International Maritime Bureau, most ships are attacked in the waters of Nigeria [5].

Inland waterway transport

In terms of acceleration, inland waterways are considered a very safe transportation means. Nevertheless, also here the following risks can appear:

1. Cargo is usually subjected to lower forces than during road transport. Boats' diesel engines may cause low-frequency vibration, higher frequency vibrations which could cause damage to cargo can be eliminated using packaging, i.e. appropriate dampening materials [6].
2. Dangerous goods - during inland waterway transport, dangerous goods are carried in accordance with the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways of 2000.

Air transport

A very particular method for transporting goods, mainly small consignments [7]:

1. Scratched and damaged packaging – especially when handling material during sorting and other operations during transportation.

2. Crushing - if external forces act on the sides, walls or corner of the package. Stacking, impacts, vibration, equipment for handling material create compressive forces which may result in damage to goods.
3. Climatic conditions - high and low atmospheric pressure can have fatal consequences for cargo. High and low humidity can cause condensation or corrosion. Temperature differences ranging from -62°C to 71°C, which may affect the properties of the goods packaging.
4. Handling consignments - using cushioning materials, damage caused by impacts during handling of parcels can be eliminated.
5. Impacts - during handling and carriage. Many kinds of goods require a certain level of protection against impacts.
6. Vibration - occurs in all types of transportation means. Suitable cushioning materials can be used to eliminate the negative impact of vibrations on goods.
7. Dangerous goods – carried in accordance with the Convention on International Civil Aviation of 1945. The International Air Transport Association (IATA) uses the Dangerous Goods Regulations (DGR).
8. Theft of cargo – this may occur during loading into the aircraft or during storage. Most cases involve minor theft. The most danger time is when the cargo is loaded onto a lorry.

3. Data description and methods

3.1 Protecting transported goods from damage and theft

The below detailed information on securing goods is applicable to all kinds of transport as a result of the use of multimodal transport [3, 8].

Table 1 shows the methods of protecting goods against damage, including possible elements that can be used for this purpose. This is the basis for the selection of a suitable method of securing. More detailed information is presented below.

1. Use of the following elements implies from the Table 1:
2. Interlocking or bracing - wooden beams, strips and other elements are fitted in to fill any gaps between cargos.
3. Lashing - steel straps, chains, steel rope, textile straps, rope and other securing materials.
4. Gap filling - wooden strips, cardboard which can be used for very small gaps, boards and single wooden beams for small gaps and pallets for larger gaps.
5. Locking - locks should be regularly checked for wear, damage and operational defects.

Table 1. Protecting transported goods from damage.

	Method for securing goods	**Description**
1	interlocking or bracing	the cargo is located so it is at one level against solid structures, bracing is undertaken between the cargo and container and between individual parts of the cargo
2	lashing	lashing parcels prevents them from moving in a longitudinal or transverse direction or rising out of the cargo space or

		turning over; tension in the ropes reduces safety force, depending on circumstances friction forces can be increased.
3	gap filling	gaps can be longitudinal or transverse and should be filled in an appropriate manner if there is no better way to secure the goods.
4	locking	cargo containers such as ISO containers, swap bodies etc. with weight greater than 5.5 tons should only be carried on transport means equipped with locks

Protection from theft varies according to specific transport type. It is also necessary to identify risks of theft of goods during the use of various modes of transport, and proposals for measures are also specified in the comments in this Table. These data are very important in proposing a combination of modes of transport – the types risks are specified in Table 2.

Table 2. Protecting transported goods from theft; data in [9] were adapted by authors.

	Transport type	**Danger**
1	road transport	theft of part of goods or whole lorry
2	rail transport	theft of part of goods or whole carriage
3	sea transport	theft of containers in port
4	air transport	minor theft, trespassing

Use of following measures to prevent theft implies from the Table 2:

1. Road transport - irregular departure time from warehouse, closed goods hold, protective escort for valuable goods, electronic monitoring systems tracing and quick turnaround.
2. Rail transport - security company/inspector at tranship points and shunting yards, areas or empty containers in different sections to goods, areas for transhipment or train shunting closed without open access.
3. Sea transport - containers are equipped with a BIC - Bureau International des Containers - serial number.
4. Air transport - camera systems, guarded docks, guarded warehouses, security services.

Figure 1 shows a diagram of data transfer when using smart containers. RFID - smart containers - are used in multimodal transport. This type of container is equipped with sensors and systems for data monitoring and reporting. One of the systems used is RDIF - Radio frequency identification. Chips can be tuned to various frequencies, e.g. 125 kHz, 134 kHz and 13.56 MHz. Authorised persons can acquire information on movement of goods in the container, condition of goods, any unauthorised intrusion by a third party. Temperature can be controlled remotely according to need and in real time for containers equipped with satellite reception [10].

One of the possibilities for eliminating the risk of theft or monitoring damage to containers is to use a container that is equipped with sensors and a system for monitoring and reporting data.

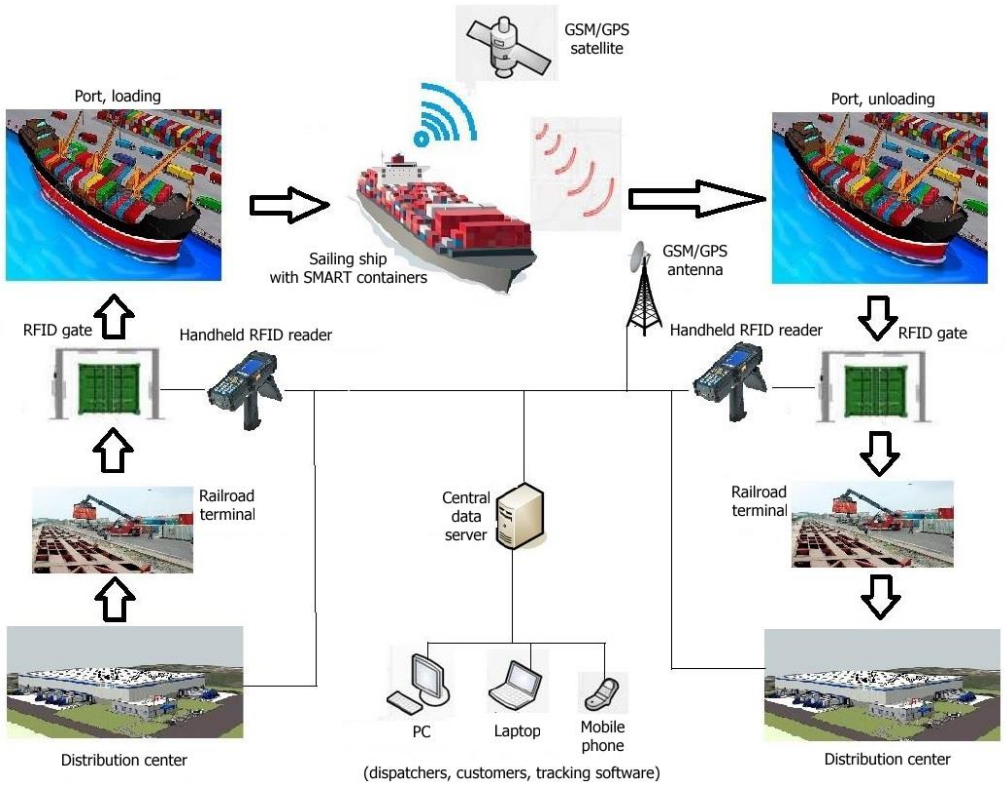


Fig. 1. Information transmission diagram when using SMART containers [11].

3.2 Securing the quality of transported goods

Securing the quality of transported goods is one of the key requirements – if a change in the required parameters of the goods were to occur, they would be spoilt and thus their transportation would also become redundant. Due to the large number of types of goods and many risks, only selected information is detailed here, thus partial risks [6].

In Table 3 there are specified the types of goods divided according to the type of sensitivity, including identification of impacts that are determining for the given type of goods. This is an important requirement that the transporter must ensure. Additional information is specified in the comments to this Table.

Additional information regarding Table 3 on measures to mitigate the risks for selected type of goods is:

1. Items sensitive to temperature (temperature-sensitive goods).
2. Transport and carriage temperature - optimal product storage temperature which when observed will ensure maximum lifespan 5 - 20°C.
3. Carriage with controlled temperature – heating -_solidification range 24 - 19°C, temperature during travel > 24°C.
4. Carriage with controlled temperature – cooling and/or freezing -_required temperatures during loading, travel and unloading; refrigerated containers.
5. Items sensitive to humidity (hygroscope and sensitivity of materials of humidity).
6. Hygroscope - relative humidity 60 to 70 % - optimal storage conditions for most hygroscopic goods.
7. Materials sensitive to humidity - slight adsorption of water vapour quickly causes major changes at low relative humidity.

8. Items sensitive to biotic activity.
9. Biotic changes and their consequences - changes caused by microorganisms, biochemical conditions, pests.
10. Items sensitive to contamination.
11. Dust contamination - gaps filling with dust, abrasive dust, chemically active dust, infectious dust.
12. Dirt contamination - moisture is a vehicle/means for contamination with dirt, goods in canvas bags are sensitive.
13. Contamination by fats/oils - leaves stains on fabrics, penetrates the surface or surface layers of goods, oil impregnation may result in spontaneous heating and combustion.

Table 3. Selected types of goods and possible risks.

	Type of goods	**Risk**	**Identification**
1	items sensitive to temperature (temperature-sensitive goods)	damage or deterioration in quality	transport and carriage temperature
			carriage with controlled temperature – heating
			carriage with controlled temperature – cooling and/or freezing
2	items sensitive to humidity (hygroscope and sensitivity of materials of humidity)		hygroscope
			materials sensitive to humidity
3	items sensitive to biotic activity		biotic changes and their consequences
4	items sensitive to contamination		dust contamination
			dirt contamination
			contamination by fats/oils

3.3. Control processes

For procedure of control processes, it is necessary to identify risks during transport of items, and to evaluate protection methods. Protecting transported goods is divided into protection from damage (‘safety’) and protection from theft (‘security’).

When planning security measures, so-called weak points must be eliminated. One hundred percent protection cannot be guaranteed because it would be excessively expensive. As such, it is more efficient to secure a security system so that the weak points of different types of security are always at different points (eliminating a domino effect).

In order to propose an optimal combination of modes of transport for transporting goods, it is necessary to assess and compare flexibility, speed, reliability and other properties of individual modes of transport – they are specified in Table 4. It is also necessary to assess the advantages and disadvantages of using individual modes of transport - they are specified in Tab. 5. When processing this data, it is appropriate to use risk analyses and expert methods.

Data from the practice obtained during visits of logistic centres, ports, transhipments and container terminals, afterwards processed by expert methods were used for processing the Table 4 and Table 5.

Table 4. Selected properties of modes of transport; data from [11] were adapted by authors.

	Type	Flexibility	Speed	Reliability	Other properties
1	road	high	average	average	very dense network of highways and roads; almost any place is accessible; transportation for short, medium and long distances
2	rail	average	average	average	dense network in the Czech Republic, but partially technically inadequate; freight trains; possibility of transportation of large cargo at a time; need for reloading;
3	sea	low	low	average	limited network of sea routes; large capacity of ships – possibility of transportation of large quantity of cargo at a time, even different cargo; transportation of goods with lower priority
4	air	low	high	high	limited network of air routes; transportation of goods with high added value; quick to spoil or fragile; rescuing of human lives; low risk of damage; dimensionally smaller shipments; large distances

Table 5. Advantages and disadvantages of the use of modes of transport; data from [11] were adapted by authors.

	Type	Advantages	Disadvantages
1	road	"door to door" transportation; reloading only exceptionally; flexibility	high rate of transport externalities; congestion, high accident rate; increasing truck traffic problems
2	rail	speed over long distances; economically advantageous; possibility of transporting large quantities of cargo at a time	limited time possibilities of transport; breaks during transport caused by the necessity to free up the route; difficulties in tracking goods
3	sea	low transportation cost; possibility to transport large quantities of goods;	long transport times; necessity of reloading in ports; waiting in front of ports; risk of theft at a port; climatic effects; danger of pirate raids; risk of corrosion; inability to land at any port – shallow depths in some ports;
4	air	speed; reliability; minimization of losses; minimization of damage; tracking goods without problems	high transport costs; time-consuming inspections at airports during customs clearance; limited cargo capacity for dangerous goods; limited cargo capacity for heavy loads; limited cargo capacity for oversized loads

3.4. Protection from damage

Since applied forces have different values for different types of transportation, there are also different requirements for securing loads. In designing a method for securing

goods from damage, all types of transportation which will be used during the course of the journey must be considered, and the goods must be secured in such a manner as to meet the highest demands. The Table 6 gives values for forces in different types of transportation. Knowledge of this data is important for making a decision on the type of the method of securing transported goods. The highest demands are seen in railway transport, which arises from the value specified in Table 6.

Table 6. Forces acting in different types of transport [12].

	Transport type	**Forwards**	**Backwards**	**Sideways**
1	railway transport	7 kN	7 kN	2.9 kN
2	road transport	7 kN	2 kN	2 kN
3	sea transport	1.5 kN	1.5 kN	2 kN

Tying ropes using loops is not permitted for transport by rail (in accordance with Directive UIC[9]), and it is therefore not possible to use this securing method throughout the duration of the transport. All the elements by which tying and strengthening is secured must be regularly checked due to their depreciation, and their replacement and elimination must be secured.

Containers are exposed to impacts, and therefore deformations. During impacts, abrasions on their walls occur, and thus not only a breach of the anti-corrosion protection, but also to loss of strength and stiffness of container walls. If a container or its walls are damaged by corrosion deformations and thus it does not meet safety conditions in terms of handling and protection of goods, it must be eliminated.

From this perspective, it is suitable to use "smart containers" disk protection against damage, which has a built-in warning system that informs about a change in the environment inside the container, thus preventing damage to the transported goods. An operator who monitors the conditions in individual containers can remotely change the conditions for goods (temperature, humidity, etc.) if they are unfavourable, thus preventing damage to the transported goods in the shortest possible time. However, the question of economic cost remains, as equipping all of the containers with "container safety equipment (CSU)" would be costly, and they are therefore only used in justified cases.

3.5. Protection from theft and external attack (security)

Protection measures are important in terms of protection from theft and also in terms of the possibility of a terrorist bomb or biological attack. Another reason is to prevent human smuggling, and possibly limiting the spread of disease. After unloading, the container must be fumigated, i.e. to destroy pests.

When transportation begins, the container is loaded with goods, sealed and locked, although during transportation it may be opened a number of times, mainly at customs where there is a suspicion the consignment is not in order.

Containers are inspected using scanners which can display an image of the goods like an X-ray image. If there is any suspicion, the container must be opened and unloaded.

If there is a suspicion that the container contains electronic equipment which could be a part of an explosive device, the area must be evacuated and a police pyrotechnics unit must be called in. The use of mobile telephones and other electronic devices must also be

restricted. Table 7 gives risks and preventative measures for different types of transport [13].

If damage or theft of goods, or another attack occurs, this means that all the inspection elements set up in the system have failed. Most inspections at control points are undertaken visually by an authorised worker or customs agent. It follows that the human factor is very significant [14, 15].

For using the risk analysis, it is necessary to identify possible risks for individual modes of transport in the largest scope possible. Selected partial risks are specified in Table 7, including the proposed measures for prevention or reducing the consequences.

Table 7. Selected risks for different transport types; data from [11] were adapted by authors.

	Transport	**Risk type**	**Proposed measures**
1	road transport	traffic accident	observe breaks, electronic safety systems (adaptive cruise control, automatic braking, lane support systems, micro sleep detection)
		theft of goods	parking at frequented rest sites, passenger, GPS system, sealed cargo
		robbery	passenger, automated assistance call system
2	railway transport	theft at shunting yard	use an electronic seal with GSM/GPS for valuable consignments, seals
3	sea transport	weather conditions	propose new routes, extended transportation duration
		theft at port	use an electronic seal with GSM/GPS for valuable consignments, camera system at port
		pirates	propose new routes, eliminate risky waters
4	air transport	terrorist attack	scanner, thorough inspection of people and luggage
		bad weather	flight delay, delay of hours
		minor theft	Seals

3.6. Risk analysis

The risk analysis determines the critical points in the process of inspecting goods as protection against damage and theft. A risk is defined as any factor that may negatively affect the protection of transported items. This means any event that may affect, with a certain probability, the inspection process at the time when goods are loaded. They can be divided into essential (significantly influencing process) and less significant or negligible. The risk factor is more significant the higher the probability of its occurrence, and the higher the intensity of its negative impact on the given process. The basic procedures of the risk analysis are - determination of risk factors and assessment of the significance of their impact, risk assessment and risk management (proposal of measures to reduce risks). The evaluation consists of evaluating a partial risk, i.e. one asset; Table 8.

Table 8. Evaluation of risk factor.

Probability of occurrence of risk factor (P)		**Intensity of impact of risk factor occurrence (D)**	
1	unlikely	1	negligible
2	improbable	2	small
3	very likely	8	large
4	almost certain	16	critical

Risk = probability x impact (P x D): risk is acceptable for P x D = 1 to 8, risk is conditionally acceptable for P x D = 16 to 24 and risk is unacceptable for P x D = 32 to 64.

It is necessary to include factors whose occurrence is certain with a critical impact upon its occurrence, and whose negative impact may even be critical, although the probability of occurrence is low. For these reasons, a linear scale is chosen for probability of occurrence of a risk and a non-linear scale for evaluating the negative impact of a risk.

It is necessary to emphasize the fact of very risky situation which can occur in unlikely occurrence, but with critical impact. Although the probability of occurrence is very low, it is necessary to evaluate this case carefully.

3.7. Waiting Time

The waiting time in the queue is an important indicator for truck operators. While the truck with a container waits in a queue, it is usually idling. That leads to wasting of fuel and economic loss for the operators, not to mention unnecessary engine emissions.
Average Checkpoint Waiting Time - let us consider the total waiting time in the queues for the whole checkpoint. According to the simulation output, there is typically negligible waiting time for Case 1 (not even reaching 1 second) and Case 3 (range 1.76 – 5.08 seconds). However, for the case of 100% container screening (Case 2), the average waiting time increases rapidly with increasing arrival rate, ranging from 0.5 minute to 6.76 minutes [16]. Figure 2 shows graphs for all cases; the results for Case 1 are the same as for Case 3.

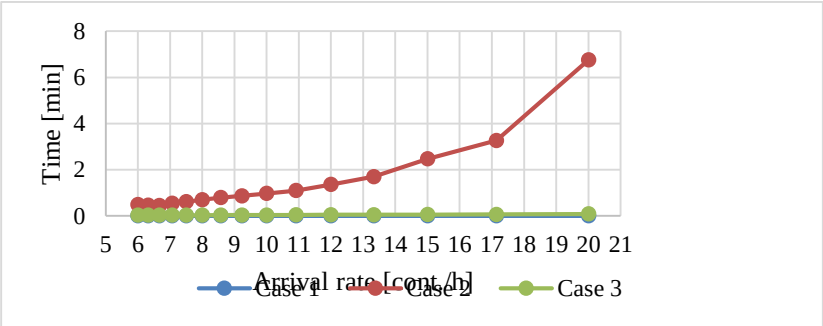


Fig. 2. Average waiting time in the queue [16]; Case 1 = Case 3.

Maximum Average Checkpoint Waiting Time - however, we should also focus on the values of maximal average waiting time in the queue. In Arena, this was the highest average waiting time among the 100 replications in a simulation run, for a certain container arrival rate. Figure 3 shows graphs for all cases; the results for Case 1 are the

same as for Case 3. As it can be seen from plots at Figure 3, the maximum average waiting time in Case 2 starts increasing rapidly at the arrival rate of 12 containers per hour (2.4 minutes), eventually reaching 25.28 min. This is already quite significant. Should such case apply, the container terminal operators ought to analyse their traffic statistics to determine whether such arrival rate is occurring frequently or not. If the answer is yes, adding a checkpoint lane for NII station should be considered. For comparison, a simulation with the same setting for 20 containers per hour but with 2 NII lanes was conducted, which led to decrease of maximum waiting time to 0.7061 seconds, effectively eliminating the queue (reduction by 97.21%). Other measured parameters showed a similar trend [16].

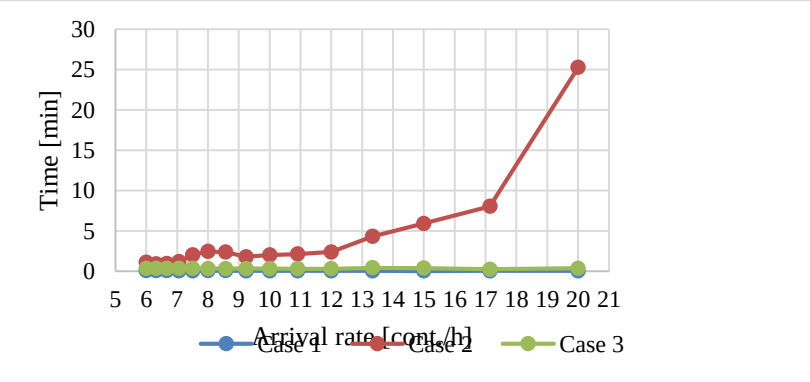


Fig. 3. Maximal average waiting time in the queue [16]; Case 1 = Case 3.

3.8. Procedure of control processes

The procedure during control processes is shown in the following images: Figure 4 – for export and Figure 5 for import alternatives. These diagrams show a clearly evident procedure that must be adhered to in checking processes in order to minimize risks.

4. Results

Workers in the logistics chain play a key role, but it must be noted that in the modern world, where there is a large volume of transported goods, inspection of containers involves random spot checks. Figures 6 and 7 shows a so-called Swiss Cheese Diagram, where every hole in each slice of cheese represents a minor failure, or negligence in carrying out duties at a specific inspection point. An important point here is that an individual failure in and of itself should not impact on the security of the goods in the container. Where these ‘minor failures’ align, however, a serious situation can occur. As such, it is essential to set up the inspection system to ensure the holes in the cheese do not overlap.

In practice, often certain elements of the inspection are left out if there is not a specific suspicion about the goods transported in the container. It is in these situations where the risk of theft/smuggling may be higher.

If the system is not continuously monitored and if any weakness (weak points) is not found on time, a critical situation will arrive very likely. Therefore, it is necessary to set up the system in a way that any weaknesses are not linearly arranged. This method is suitable for application at the input and output controls of transported goods.

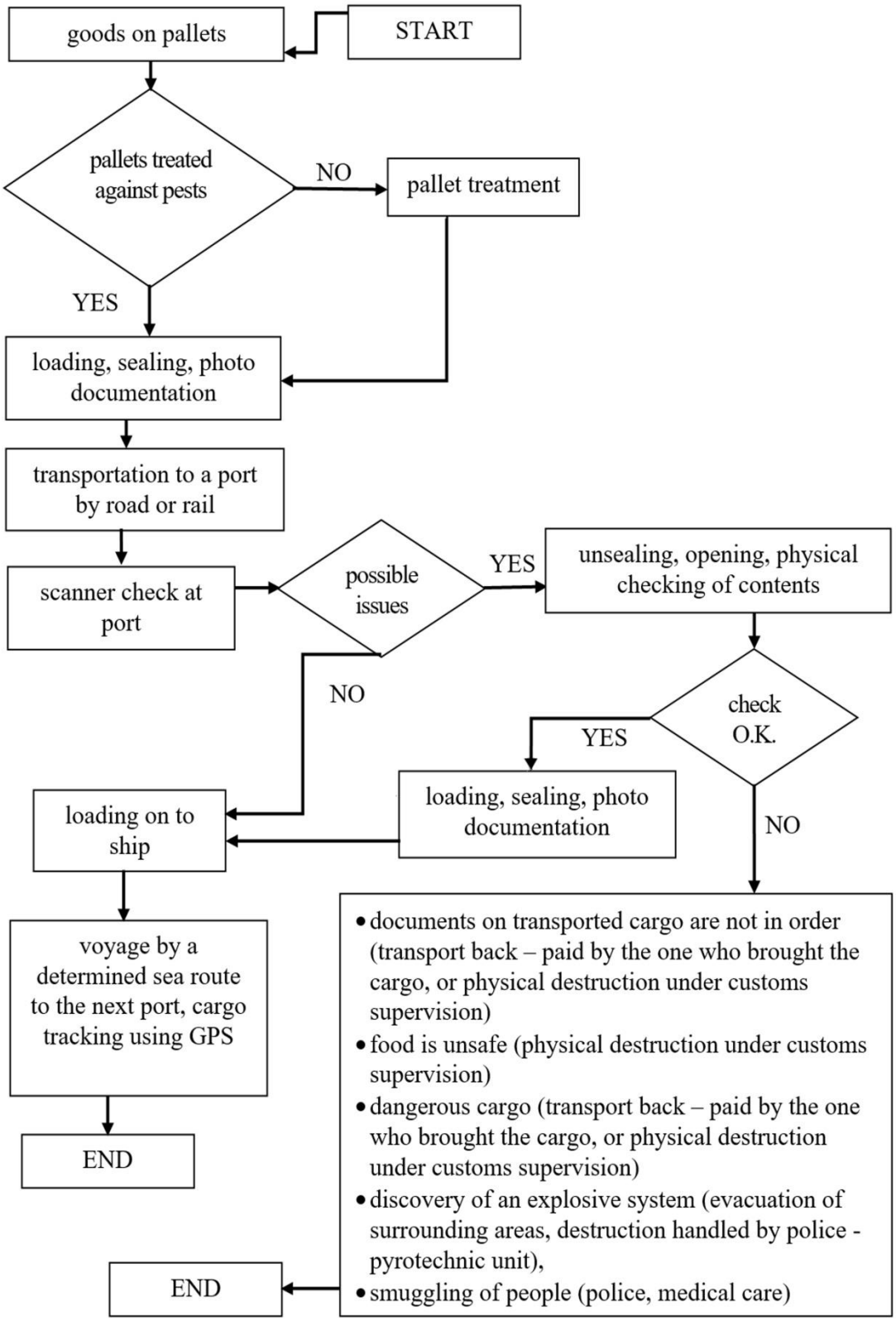


Fig. 4. Scheme of control processes – export.

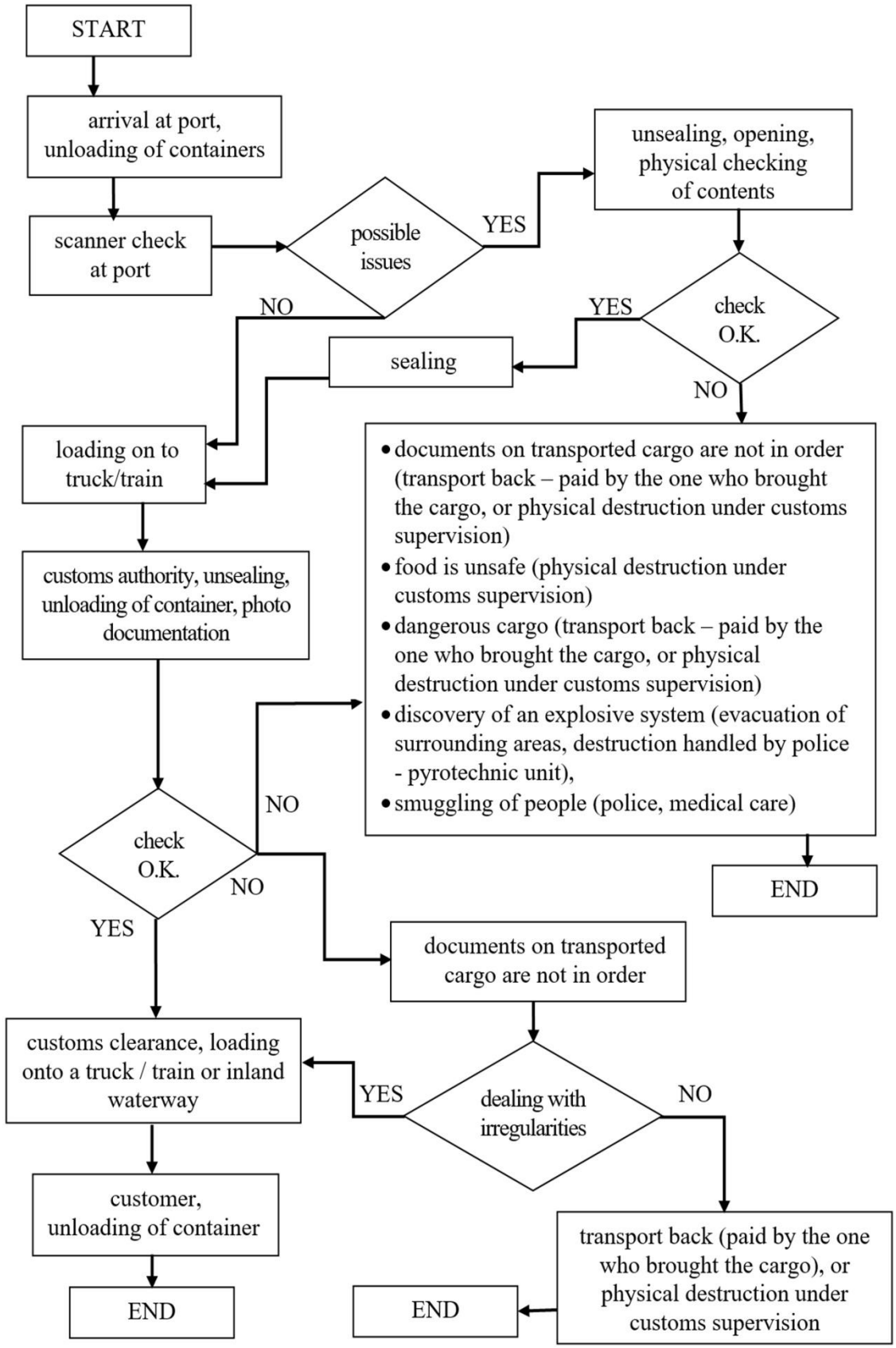


Fig. 5. Scheme of control processes - import.

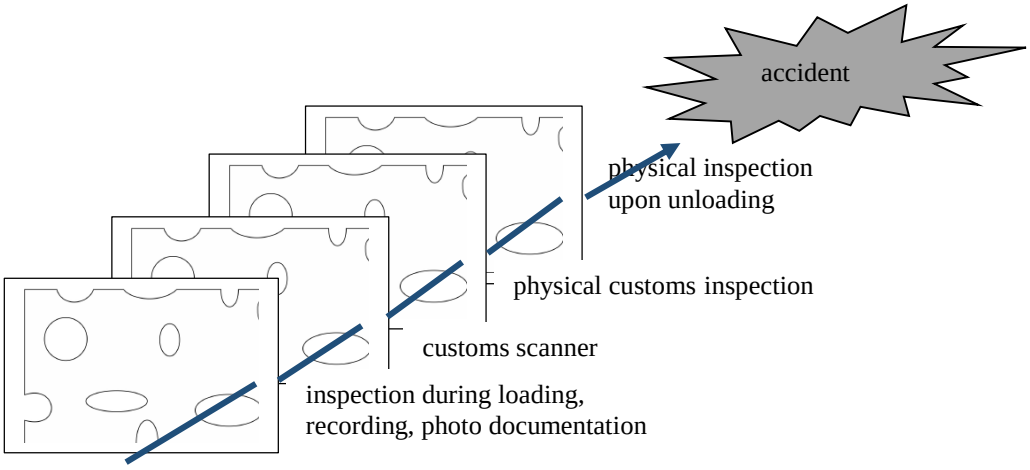


Fig. 6. Swiss cheese model – increased risk; data from [16] were adapted by authors.

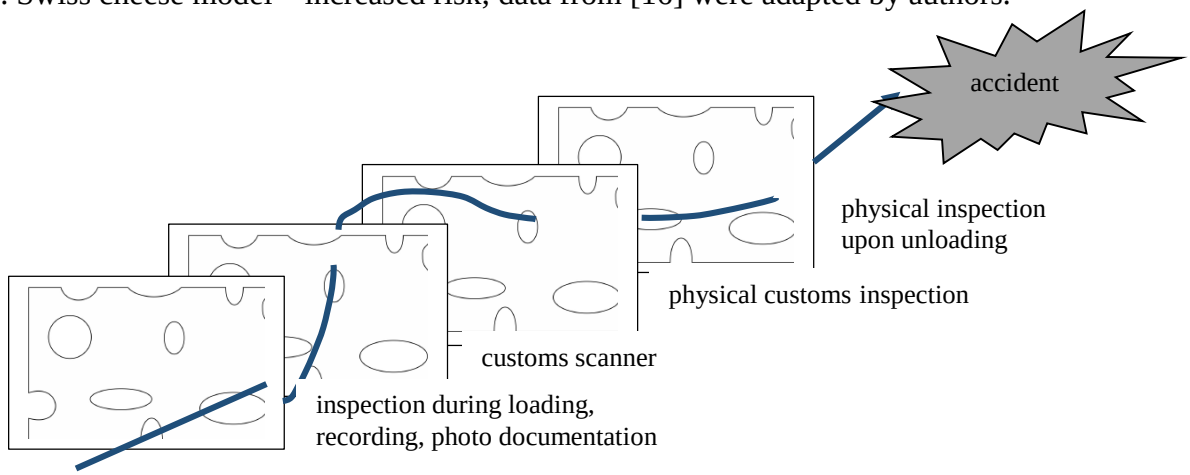


Fig. 7. Swiss cheese model – decreased risk.

5. Conclusions

When determining the transport routes and logistics systems, the danger of damage and theft to the carried goods must be considered with partial risks as an integral part of doing so of the transportation process.

One-hundred percent security against damage and theft cannot be guaranteed due to the high financial costs and the necessity to secure technical and technological resources

Security is, however, ever more important and due to the ever greater use of multimodal transport, risk and safety assurance is a very topical issue. The aim is to achieve optimum securing so that risk factors cannot exist in succession.

Safety and transport, “safety” and “security”, is an increasingly important factor in deciding on modes of transport in the transport system.

It is important to note that every transport means places different demands on security measures, and as such the security and protection of consignments must meet the highest of these demands.

In protecting goods from theft and damage, the following are important packaging (sufficient packaging), insurance (for damages that the shipment can cause, or for damage to shipment), seals (can be characterized as identification of whether the shipment was

handled, but in no way can they prevent direct damage or attack by a third party) and loading into the container (ensuring that the cargo does not move or get damaged).

The human factor should not be underestimated; it must be considered a high risk factor. People can fail because of errors or negligence, or if they have an indifferent approach to goods being damaged. Not all cargo is checked, and it is therefore not possible to check every container.

The use of RFID technology provides great opportunities. Some of the safety devices can be installed in a container and it can be monitored in real time. In combination with various other sensors, the container acquires the "Smart Container" statute. However, the price of this equipment will always be the decisive factor – even considering the nature of the transported goods.

When designing security measures, security costs must always be included in the transportation price, and optimum cost-effectiveness must be achieved.

Acknowledgment

The authors acknowledge support from the project "Rozšiřování kapacit pro nasazování aplikací využívajících GNSS navigační signál v oblasti civilního letectví "H20 641627.

References

[1] ČOREJOVÁ, T., ROSTASOVA, M. Regional Development, Innovation and Creativity. *IX. International conference on applied business research* (ICABR 2014). ISBN: 978-80-7509-223-6. Talca 2015, pp. 114-127.

[2] PORT OF ANTWERP. *Type of Goods.* www.portofantwerp.com

[3] HALLIDAY, D., RESNICK R., WALKER, J. *Fyzika* (In Czech). Brno: Vutium Brno 2000.

[4] EC. *European Best Practice Guidelines on Cargo Securing for Road Transport.* http://ec.europa.eu/

[5] www.inboundlogistics.com

[6] CONTAINER HANDBOOK. *Cargo Loss Prevention Information from German Marine Insurers,* 2002-2006, Record Nr. 1807292. www.containerhandbuch.de

[7] PROJECT LOG4GREEN. www.log4green.eu

[8] HOSPODKA, J., SZABO, S., NOVÁK, M. Influence of Autonomous Vehicles on Logistics. *International Review of Aerospace Engineering,* ISSN:1973-7459, 8 (2015), 5, pp. 179-184.

[9] FUCHS, P., NĚMEC, V., SOUŠEK, R., SZABO, S., ŠUSTR, M., VISKUP, P. The Assessment of Critical Infrastructure in the Czech Republic. *Transport Means 2015.* ISSN: 2351-7034. Kaunas: Kaunas University of Technology, pp. 418-424.

[10] GIERMANSKI, J. *RFID vs. Satellite in Smart Container Cargo Security.* www. securityinfowatch.com

[11] VALENTA, Z. *Bezpečnost přepravovaných věcí v multimodální dopravě* (In Czech). Diploma´ Thesis. Praha: ČVUT 2014, 86p.

[12] ANDERSSON N. a P. et al. *Equipment for Rational Securing of Cargo on Railway Wagons.* ISBN: 91-85084-07-7, ISSN:1650-3104. Stockholm 2004. http://www. vinnova.se/upload/epistorepdf/vr-04-05.pdf

[13] VITTEKOVÁ, M., STOJIČ, S., VITTEK, P. Introduction of the Barrier – Based Approach to the Supply chain Security. Drive your knowledge be a scientist. *Conference proceedings.* ISBN:978-80-7454-475-0. Zlín 2015, pp. 321-330.

[14] REGULA, M., SOCHA, V., KUTÍLEK, P., SOCHA, L., HÁNA, K., HANÁKOVÁ, L., SZABO, S. Study of Heart Rate as the Main Stress Indicator in Aircraft Pilots. *The 16th International Conference on Mechatronics.* ISBN:978-80-214-4817-9. Brno 2014, pp. 639-643.

[15] ROZENBERG, R., SZABO, S., VAJDOVÁ, I. Comparison of FSC and LCC and Their Market Share in Aviation. *International Review of Aerospace Engineering* (IREASE). ISSN: 1973-7459. 7 (2014), 1, pp. 149-154.

[16] JIZBA, M. *Safety & Security of Transatlantic Container Logistic Chains.* Diploma´ Thesis. Praha: ČVUT 2015, 89p.

Chapter 5

ECONOMICAL AND TECHNICAL EVALUATION OF MACHINERY ENTERPRISE AND SYSTEM RISKS CONNECTED*

1. Introduction

Economic progress and growing competition place great demands on technical and economical standards of engineering enterprises. High-efficiency efforts and optimal use on the market requires vast co-operation and business relationships between supplier and customer subjects. To expand business while starting it and in many cases also when investing into its upgrade calls for somebody else´s capital.

For many enterprises and financial institutions, it is necessary to have an objective instrument for economic and technical evaluation (rating) in such a situation [1]. To fulfil this goal there was an initial prerequisite: to gather and upgrade optimal list of specialized literature and references or their parts which would correspond with the topic of the thesis. Practical layout of the topic represented the creation of functional and easily presentable enterprise rating model for the SME including the methodology for domestic and international comparison.

The evaluation of the SME, which brings academic and practical aspect of solving this issue, is not available as a whole at this point. This has become intent for the scientific research.

In connection to the above, there were defined the goals as following:

1. To suggest and evaluate an easily usable and functional rating model for the SME for this country while using academically well-known methods, statistically valid financial data of anonymous engineering enterprises and their ratings during an observed period of time.
2. To suggest and evaluate an easily usable and functional model for the abroad SME while using the domestic rating model of the SME and international rating for the countries during an observed period of time.

The hypothesis, which would correspond with the above mentioned intention and which would measure the results of the thesis against the respected Rating of SME validated by the Czech National Bank, was as following:

***„It is possible to create a new, simpler model of the SME evaluation with less input data than it is typical for the SME Rating. The ability of the new model will be close to the SME Rating in its quality.* "**

Following the research and technical findings that the professional literature focused on the evaluation rating models of the SME (including the methodology of domestic and international comparison), contained the solution of this issue only partially, the authors tried to fill in this gap in the present condition of the economical evaluation of the SME.

Authors: Dipl. Ing. Petr Kocour, Ph.D., Assoc. Prof., Dipl. Ing. Karel Sellner, PhD., University of J. E. Purkyně, Ústí nad Labem, Czech Republic. petr.phk@email.cz, sellner@fvtm.ujep.cz

2. Background research and solution concept

Procedure schedule of tasks and targets to be solved was as following, Figure 1.

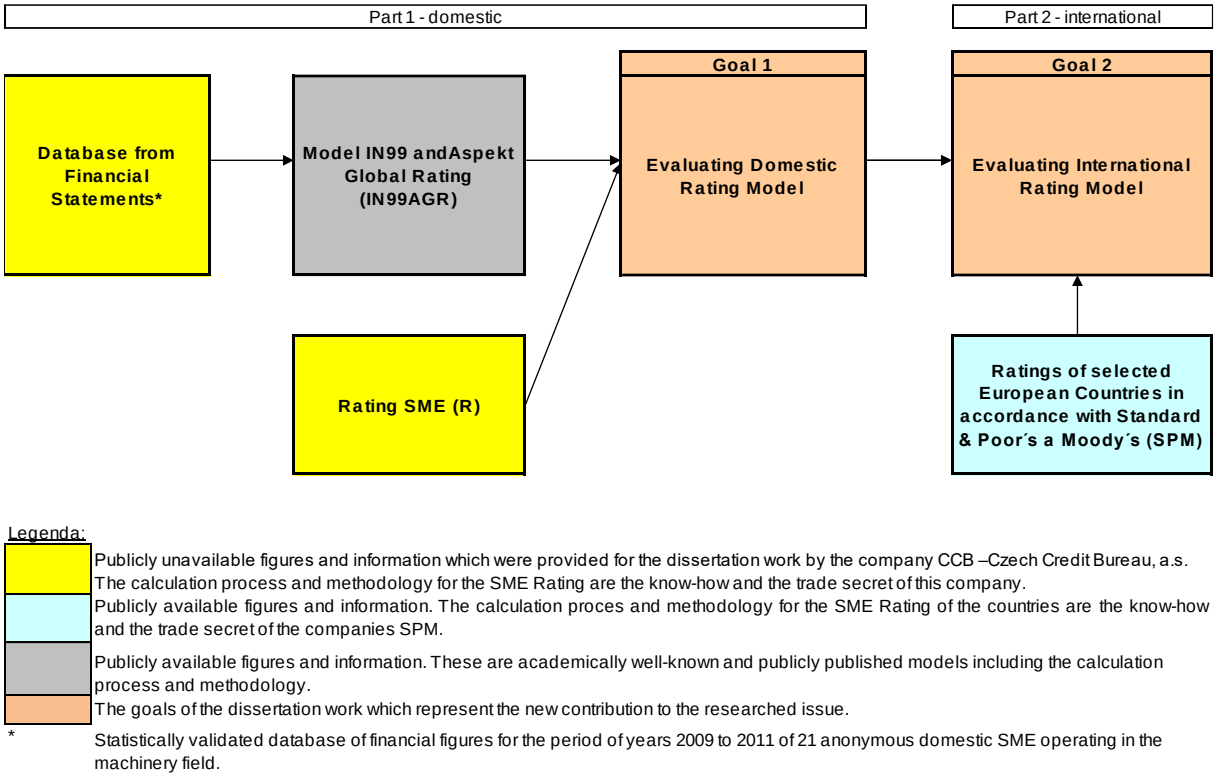


Fig. 1. Procedure schedule of tasks and targets to be solved.

In compliance with the procedure schedule there came the solving of tasks and targets in those steps:

- calculation on the basis of models IN99 by the Neumeiers and the AspektGlobalRating,
- meeting of the goal 1 – creating and evaluating domestic rating model for the SME,
- ratings of selected European countries following the Standard & Poors´s and Moody´s,
- meeting of the goal 2 – creating and evaluating international rating model for the SME.

3. Data description

3.1 Calculation on the basis of models IN99 by the Neumeiers and AspektGlobalating

The company CCB – Czech Credit Bureau, a.s. provided the authors with the statistically validated database of figures from the financial statements covering the periods of 2009 to 2011 showing 21 anonymous domestic SME which do their business

in the machinery field (they are labelled as 28 and 33 following the first two positions of economic activities classification CZ-NACE, which has been used in the Czech Republic since 2008 and which replaced the branch classification of economic activities called OKEČ). The number of financial data (variables) which are the input figures for calculation of the Domestic Rating KMEP as per the section 2.2 was in total 15 [4]. More detailed information for the variables is in the Annex 1.

The obtained results were very good [11]. It is possible to say that with the IN99 there was a practical result gained each time (i.e. in the single years 2009 to 2011 in 21 cases out of 21 cases) and with the AspektGlobalRating almost each time (i.e. in 2009 in 20 cases out of 21, in the years 2010 and 2011 in 21 cases out of 21).

The results were then matched (harmonized) within the intervals into seven rating levels, following the same principle as with the SME Rating [4]. Then it was possible to carry out their comparison with the SME Rating, which could be graphically represented in the single years 2009 to 2011, see graphs in Figure 1.

The authors worked with the figures using the mathematical and statistic apparatus. It is possible to say that during the period of the years 2009 and 2001 the rating of the SME oscillated within the interval of figures of the IN99 and the AspektGlobalRating with the probability of 85 to 85.71 %. This provided a proper space for generalization and creation of pattern for domestic rating of the SME. Here originated a simple and practically usable formula.

3.2. Meeting of the goal 1 – Domestic rating model for the SME

Within the framework of meeting the goal 1 there was a rating model (see the Pic. 1) formulated, which the authors named as the ***Domestic Rating KMEP*** (KMEP is the abbreviation of the Management and Economics Department of his faculty in Ústí nad Labem), and which they wrote as a mathematical formula:

$$DomesticRatingKMEP = 0.9\frac{IN99 + AspektGlobalRating}{2} \quad (1)$$

It is necessary to round the formula results according to the rules to whole numbers, unless there is a level of default in the evaluated enterprise and the use of the criteria O.K. or K.O.

The validity and accuracy of the formula results has been verified on the figures used from the financial data database of 21 anonymous SMEs from the machinery field (i.e. on the qualitative data set). For the single years of 2009 to 2011 there is the graphical illustration of the results against the validated SME Rating, enabling the comparison with the use of the benchmarking method. For further details, see also the Annex 1.

The validated sets of qualitative (non-financial) data of SME from the machinery field, nor from any other field, are not publicly accessible. Selected figures are systematically gathered and handled only by banks and financial institutions for their own use as they offer the leasing, factoring, forfaiting, credit insurance, etc. [5]. The same thing is true also for the benchmarking, and this is why the authors could only process the initial and basic methodology in this field.

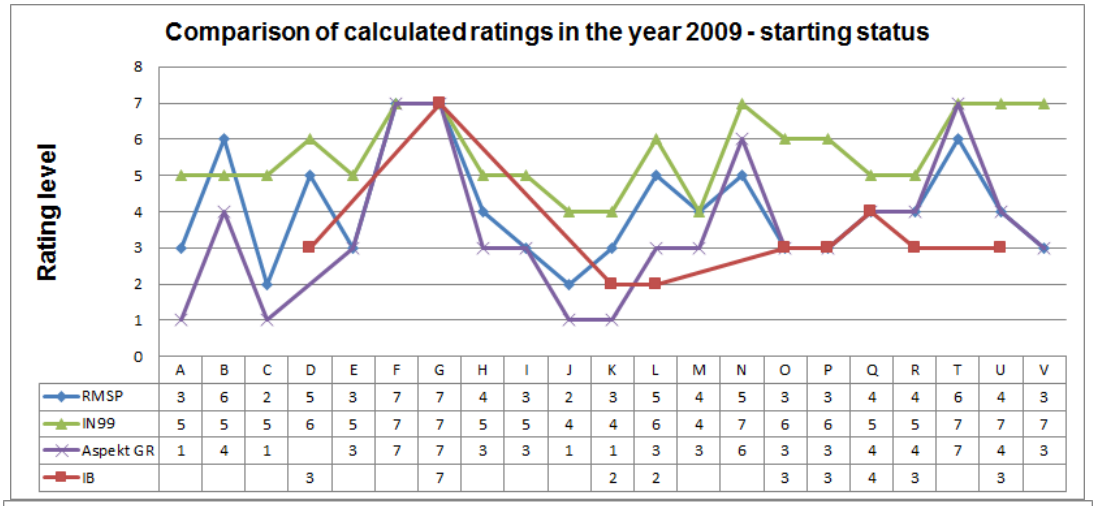
The evaluation of technical standard of an enterprise is basically completely dependent on the willingness and trust of particular partners, next also on the voluntary providing

and publishing of relevant figures which are (same as the financial data) very sensitive in any competitive settings.

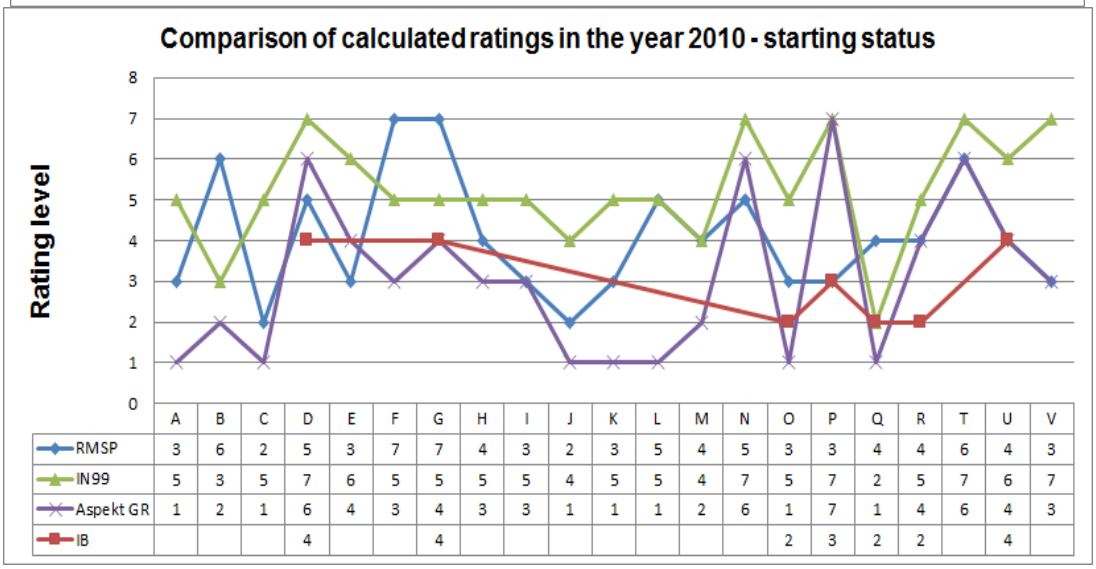
While the evaluation of economical standards of an enterprise comes out of the figures from the financial statements and it is possible to work with them directly using the mathematical and statistic apparatus, the evaluation of technical standards is primarily necessary to be done by an expert or by a group of experts, i.e. by qualitative description which would be to a certain degree subjective. Next is usually used a point system which evaluates the single factors (criteria).

The developed methodology (instruction) of calculation for Domestic Rating KMEP and the rating methodology of non-financial (qualitative) criteria of the SME from the machinery field based on the benchmarking, with the evaluation suggestion of the five factors described into particular criteria using the point system of evaluation, are following [8]:

1. Factors of economic and branch setting.
2. Factors of business activity and management.
3. Factors of sale and purchase.
4. Factors of production.
5. Other factors.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	T	U	V
RMSP	3	6	2	5	3	7	7	4	3	2	3	5	4	5	3	3	4	4	6	4	3
IN99	5	5	5	6	5	7	7	5	5	4	4	6	4	7	6	6	5	5	7	7	7
Aspekt GR	1	4	1		3	7	7	3	3	1	1	3	3	6	3	3	4	4	7	4	3
IB				3			7				2	2			3	3	4	3		3	



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	T	U	V
RMSP	3	6	2	5	3	7	7	4	3	2	3	5	4	5	3	3	4	4	6	4	3
IN99	5	3	5	7	6	5	5	5	5	4	5	5	4	7	5	7	2	5	7	6	7
Aspekt GR	1	2	1	6	4	3	4	3	3	1	1	1	2	6	1	7	1	4	6	4	3
IB				4			4								2	3	2	2		4	

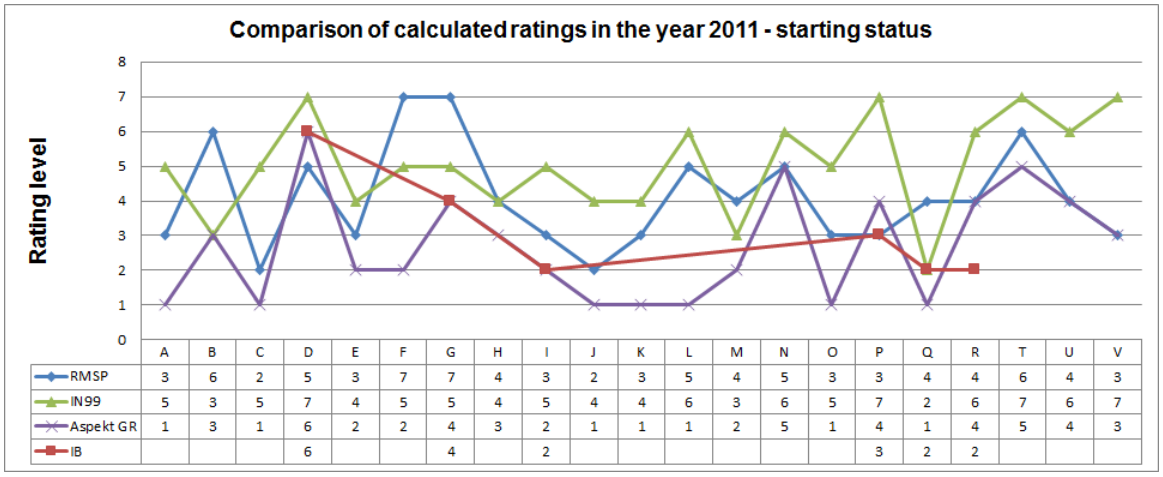


Fig. 1. Comparison of ratings based on IN99 and AspektGlobalRating with the SME Rating.

The goal 1 was met in the domestic evaluation of financial and non-financial figures of the SME, or rather the machinery enterprise. Compared with the Rating of SME, the new methodology is less time consuming and simpler for the programmers because it works with a lower number of the input data. Practical benefit of this new rating model is its methodology and the fact that the model shows a high accuracy of 95% against the reputable product – the SME Rating.

3.3. Ratings of selected European Countries

The ratings of world countries including the Czech Republic are published on the ČNB´s web page. These ratings were determined by the international rating agencies Standard & Poors´s and Moody´s [10] (Tables 1 and 2). Based on this information there was a chart of selected European countries ratings created.

Table 1. Rating evaluation of selected European countries as of 25th March 2015.

Moody´s		**Standard & Poor´s**	
Investment Levels			
Aaa	Denmark, Finland, Luxembourg, Germany, Netherlands, Austria, Sweden	AAA	Denmark, Luxembourg, Germany, Great Britain, Sweden
Aa	France, Great Britain	AA	Finland, Netherlands, Austria, Belgium, France, the CR, Estonia
A	The CR, Estonia, Poland, Slovakia, Malta	A	Ireland, Slovakia, Poland, Slovenia
Baa	Lithuania, Slovenia, Bulgaria, Ireland, Latvia, Romania, Spain	BBB	Malta, Latvia, Bulgaria, Lithuania, Spain, Italy
Speculative Levels			

Ba	Croatia, Hungary, Portugal	BB	Romania, Croatia, Hungary, Portugal
B		B	Greece
Caa	Greece, Cyprus	CCC	Cyprus

Table 2. Ratio of country ratings.

Moody´s and Standard & Poor´s	Harmonized into 7 Rating Levels		Country Index Rating in %
Aaa	1	Top Level	100
Aa	2		85
A	3	Average Level	70
Baa	4		55
Ba	5	Speculative Level	40
B	6		30
Caa	7	Delayed Level	20
Ca	8		10
C	9		5
D	default		0

3.4. Meeting of the goal 2 – international rating model for the SME

Within the Framework of meeting the goal 2 there was a rating model (Figure 1) formulated which the authors named as the ***International Rating KMEP*** and which they wrote as a mathematical formula:

$$InternationalRatingKMEP = DomesticRatingKMEP.\frac{1+(100-CountryRatingIndex)}{100}, \quad (2)$$

The results of the formula 2 are necessary to round according to the rules to whole numbers unless there is a level of default, the use of the criteria O.K. or K.O.

The Rating Index of a country is expressed by the index in %, from which the SME comes and in which the Domestic Rating KMEP was calculated. See the following table with examples which were used for the formulation of general formula version. This formula was next harmonized by intervals into the 7 rating levels.

It was not possible to verify the results of the formula 2 because the data file of 21 anonymous SME contains only domestic data about the enterprises, but it doesn´t contains the international figures and comparisons. It is possible to state that there has not been developed any publicly available validated database of needed figures in order to verify the results with the mathematical and statistical apparatus. We can see a similar result in the basic evaluation methodology of quantitative (non-financial) criteria of machinery enterprises. The same situation is also with the benchmarking and that is why the authors could only develop the initial basic methodology.

Following the two input figures, i.e. from the formula 1, the Domestic Rating KMEP and the rating evaluation of the selected European countries, the authors created a matrix

of total resulting figures with a brief recommendation – the legend for its use with the International Rating KMEP (Figure 2).

Domestic Rating KMEP \ Country Rating after the Harmonization into 7 Rating Levels	1	2	3	4	5	6	7
1	1	⟨1; 2⟩	2	⟨2; 3⟩	3	⟨3;4⟩	4
2	⟨1; 2⟩	2	⟨2; 3⟩	3	⟨3;4⟩	4	⟨4; 5⟩
3	2	⟨2; 3⟩	3	⟨3; 4⟩	4	⟨4; 5⟩	5
4	⟨2; 3⟩	3	⟨3; 4⟩	4	⟨4; 5⟩	5	⟨5; 6⟩
5	3	⟨3;4⟩	4	⟨4; 5⟩	5	⟨5; 6⟩	6
6	⟨3;4⟩	4	⟨4; 5⟩	5	⟨5; 6⟩	6	⟨6; 7⟩
7	4	⟨4; 5⟩	5	⟨5; 6⟩	6	⟨6; 7⟩	7

Legend for the grey area: Area with the double evaluation 7 has 100% probability of the usage of criteria K.O.
Area with the one evaluation 7 has ≥ 50% probability of the usage of criteria K.O.

Fig. 2. Matrix of final figures for International Rating KMEP in total.

For the Matrix of final figures on Figure 2 it is possible to recommend the following:

1. If the SME or a country from which the SME comes from are evaluated by one or double rating level 7 (see the grey colour), it is desirable for the evaluator to pay caution because it is very probable to certain that there will be the criteria O.K. or K.O. applied within the risk speculative level.
2. It is also recommended to pay caution with higher probability to apply the O.K. or K.O. criteria if the evaluated SME or the country it comes from, is evaluated by double rating level 6.

The goal number 2 was fulfilled by the proposal of evaluating methodology for the international comparison of the SME. Although it was not possible to verify the result´s accuracy by the comparison of International Rating KMEP with the SME Rating, because the SME Rating is used only within the domestic scale but it is possible to assume that this new evaluating methodology will be beneficial for the corporate and academic institutions. There is also an indication in which possible direction the scientific research and the follow-up practical application in the company practice might go.

4. Method

For the processing and comparison (evaluation) of this work results there was used a validated database of financial (quantitative) figures from 21 anonymous domestic small and medium enterprises (SMEs) observed for the time period of years 2009 - 2011 which was provided by the reputable company CCB – Czech Credit Bureau, a.s.

Next there were used the following methods of scientific work to solve the given goals and hypothesis [9]:

- comparison of index and ratings in the economic and financial calculations,
- analysis and synthesis of the above mentioned, including the mathematical and statistical methods of processing, where the result of the work was the formation of a problem to be solved, i.e. the creation of a domestic and an international evaluation model of SME with an accent on its performance activity in the machinery industry.

In total the procedure of given issues in the work included also the use of a scientific method of induction and deduction, i.e. deduction of a general conclusion based on much knowledge about single items and vice versa, because these two approaches are closely linked together.

4.1. Risks of economic and technical evaluation of enterprises

It is necessary to allow for some risks in any human activity. This of course applies also for the machinery enterprises. The basic areas of risk are most of all the operational risks, economic risks, quality risks, the human resource risks, IT risks, legal and legislative risks. The risks usually involve the damage, the fact that the expected result is not coming or that the result is not reflecting the objective reality. The last mentioned aspect is usually taken into consideration while evaluating the machinery enterprises rating [5]. It then becomes the system risk, the consequence of which could be the lowering of accuracy and credibility in the economic and technical evaluation, incidentally also obtaining an incorrect result. Single components of this integral risk are subsequently analysed and there are taken measures to eliminate the risk.

Before we talk about the causes for the risks in this area, let´s mention reasons and the importance of the machinery enterprise rating evaluation. Assessment of the company rating is usually required because of internal reasons or it is needed because of the external conditions [6].

The internal reason is mainly the need to know the company´s position on the market in comparison with the similar companies in the given or in analogous segment. It is possible to use the positive results in marketing and in economic and contractual dealings [8].

The external reasons to define the company rating are usually the market subject's requirements for the knowledge about the company position, its economic health and its business vitality (perspective). This often corresponds with the requirements of the financial institutions when they deal with granting or restructuring the credits or the bank guarantees [8]. Next to the risk investigation, the risk of the bank guarantee, etc. the financial institutions require also the knowledge of creditworthiness and rating of a given company. Also the state institutions that provide in the well-founded cases the grants require the knowledge of the company position on the market and of its economic results. A similar situation is also in the field of the grant applications for the projects using the EU structural funds. Next reason can be the requirement of the customer within the

supplier-customer relations. Especially significant enterprises require an evaluation and selection of their suppliers during a time line and this periodic monitoring is included into the contractual documentation. Reaching of the required rating is necessary but not sufficient condition for making a contractual agreement. In some cases, there is a sanction for provable stating of incorrect or incomplete data for the enterprise rating determination.

The risks during the enterprise rating determination and their usage within the domestic and international scale are mainly the following [12]:

- inappropriate and non-objective methodology of the enterprise quality determination,
- non-objective or incomplete input data,
- evasion of the processed evaluation results to the third subjects.

4.2. Inappropriate or non-objective methodology

As there was already given the evidence in the previous text, the method suggestion in the domestic scale was checked and with the objective validated input figures it showed the results with the 95% accuracy against the reputable product – the SME Rating. One of the risks while determining the enterprise rating could be the usage of non-verified methodology or usage of subjective evaluation which operates on the assumption of randomly or improperly chosen resource materials.

4.3. Non-objective or incomplete input data

Non-objective or incomplete data represent the greatest risk while determining the enterprise rating. It is caused mainly by two facts. The first is that according to the Accounting law no. 563/1991, which is up-to-date in force, is the enterprises divided into four groups: the micro enterprises, small enterprises, medium enterprises and big enterprises. Legally obliged to have audited financial statements containing the balance sheet, profit and loss account, and next the cash flow, are only the medium and big enterprises. These enterprises also have to publish the annual report in the given extent. The micro and the small enterprises are legally obliged to audit the financial statements only in the case that they exceed two of the required criteria set by the law in the given year, i.e. total assets, net total turnover and the number of employees. The quantification of values for these criteria is specified in the law.

It is obvious that a higher objectivity of the input data while determining the enterprise rating is guaranteed with the medium and big companies while with the micro and the small enterprises there is a risk of non-objective and incomplete figures which will affect the total evaluation result.

Even more difficult situation is with the non-financial (qualitative) criteria. The resource materials are not defined by the law at all. That is why there is a great risk that the data for the determination are going to be incomplete or less non-objective. Another risk is the fact that the mutual interconnections of financial and non-financial criteria for the total evaluation have not been firmly set and verified yet.

A similar situation has been so far also with the suggestion of methodology for the international enterprise rating determination. Within the given framework and following the actual scientific and research condition there has been processed a scheme of Complex KMEP Rating. There are more detailed figures in the Annex 2.

4.4. Evasion of the processed evaluation results to the third subjects

Taking into consideration the risk of the evasion of the evaluation results of machinery enterprises functioning in a market setting there is a possibility of considerable economic loss with long-term consequences. With reputable institutions, organizations and rating agencies this risk is greatly minimalized though.

4.5. Measures for the risk minimization

The measures for the risk minimization of rating evaluation in machinery enterprises are possible to summarize into the following points:

- to use only the reputable organizations and agencies with verified methodology of evaluation for determination of machinery enterprise rating,
- to pay attention to the completeness and truthfulness of the resource materials and put this requirement into the evaluation determination contract,
- to finish and verify the evaluation methodology according to the non-financial criteria,
- to consider the possibility of legislative adjustment to the effect that there will be a legal obligation to audit determinative economic figures also for the micro and the small enterprises,
- to enshrine the obligation of confidentiality in the evaluation results used in contracts.

5. Results

The authors worked with the figures using the mathematical and statistic apparatus. It is possible to say that during the period of the years 2009 and 2001 the rating of the SME oscillated within the interval of figures of the IN99 and the AspektGlobalRating with the probability of 85 to 85.71 %. This provided a proper space for generalization and creation of pattern for domestic and international ratings of the SME, which are simple and practically usable formulas.

6. Conclusions

Economic and technical evaluation of enterprises involves also risks. Therefore, the risks have to be mentioned, specified as well as processed based on their priority, probability and importance to occur.

The new evaluating methods (The Domestic Rating KMEP and The International Rating KMEP) are based on the company financial data (quantitative figures) and they are structured the way so they allow also for the quantitative aspect of companies on the non-financial factors base (economic setting and branches; business activities and management; sale and purchase; technical and technological production facilities; others).

The hypothesis which was as following ***„It is possible to create a new, simpler model of the SME evaluation with less input data than it is typical for the SME Rating. The ability of the new model will be close to the SME Rating in its quality.*** **“**, was in the goal number 1 proved.

Compared with the SME Rating, The Domestic Rating KMEP provides the verified results with an average accuracy of 95 %. This discovered accuracy was verified by the

mathematical and statistical apparatus on the validated database of financial figures from 21 SMEs for the period of years 2009 to 2011.

With the non-financial data (qualitative part) it was not possible to verify and find out the accuracy of this new method aspect due to the absence of needed non-financial data. The qualitative part of the enterprise evaluation has been academically proposed within the framework of the thesis based on the 5 evaluating criteria from which 4 are evaluated by points and they have assigned the balance of 0.25 and in one criteria it is possible to use the O.K. or K.O. rule. With the qualitative part of the enterprise evaluation it is supposed that the evaluation is primarily done in the expert way. In order this evaluation to be more objective, it is recommended to be done by a group at least 2 to 3 expert specialists.

The aim of this work was also to make accessible the method which would enable the practical usage, quality improvement and also increased the enterprise transparency and comprehensibility of the complexity in the enterprise evaluation process.

The scientific and research activity within the framework of this work was also the identification of the next continuing course of the research. It possible to see it in the area of continuous collecting of enterprise data, i.e. respective time lines of domestic enterprise data as well as the international data.

Acknowledgment

The authors thank the company CCB – Czech Credit Bureau, a.s. for the validated data of the 21 anonymous domestic machinery SMEs. Big appreciation also belongs to the families for their long-term support.

References

[1] BARTÁK K. *Průvodce Evropskou unií* (In Czech). ISBN:80-85864-92-4. Praha: MZV ČR 2005.

[2] BREALEY R. A., MYERS, S. C. *Teorie a praxe firemních finance* (In Czech). ISBN: 80-85605-24-4. Praha: Victoria Publishing 1992.

[3] FINGER P. Neinformovanost ohrožuje zdravé podnikání (In Czech). *Zpravodaj Hospodářské komory.* (2013), 1, pp. 6-8.

[4] FINGER P. CRIBIS informace o firmách (In Czech). *Prezentace předsedy sekce malých a středních podniků na Hospodářské komoře Praha*. Praha 2013.

[5] HNILICA J., FOTR J. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování* (In Czech). ISBN:978-80-247-2560-4. Praha: Grada 2009.

[6] HORVÁTH G., SELLNER K., MÁDLOVÁ D., LACKO B., KOCOUR P. Rizika vybraných podnikových procesů (In Czech). ISBN: 978-80-7414-522-3. In: *Rizika podnikových procesů.* Ústí nad Labem: UJEP 2012, pp. 73-129.

[7] KANTOREK P. Benfordův zákon (In Czech). *VESMÍR,* ISSN: 1214-4029, 77 (1998), pp. 583-584.

[8] KORECKÝ M., TRKOVSKÝ V. *Management rizik projektů se zaměřením na projekty v průmyslových podnicích* (In Czech). ISBN: 978-80-247-3221-3. Praha: Grada 2011.

[9] MAŘÍK M. *Metody oceňování podniku – proces ocenění, základní metody a postupy* (In Czech). ISBN:978-80-86929-32-3. Praha: Ekopress 2007.

[10] MAŘÍK M. *Metody oceňování podniku pro pokročilé – hlubší pohled na vybrané problémy* (In Czech). ISBN:978-80-86929-80-4. Praha: Ekopress 2011.
[11] MAŘÍK M., MAŘÍK, P. *Moderní metody hodnocení výkonnosti a oceňování podniku* (In Czech). ISBN:80-86119-61-0. Praha: Ekopress 2005.
[12] SMEJKAL V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích* (In Czech). ISBN:978-80-247-3051-6. Praha: Grada 2010.

Annexes

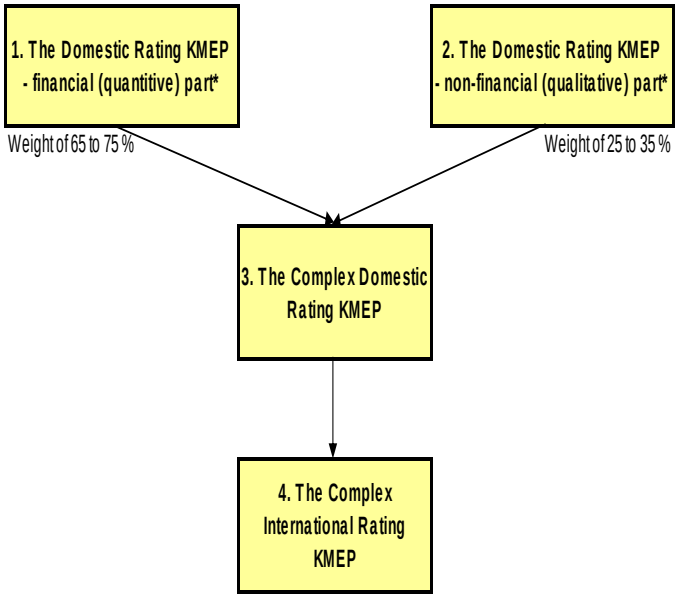
Annex 1 -Financial data (variables) which are the input figures for The Domestic Rating KMEP calculation

Financial data (variables), which are the starting figures for calculation of the Domestic SME Rating

Data Order Number	Name of data
1	TOTAL ASSETS
2	Current Assets
3	Short-term Debt
4	Short-term Financial Assets
5	Equity
6	Debts
7	Short-term Debts
8	Bank Loans and Credits
9	Turnover
10	Sales of own Products and Servises
11	Depreciation of Long-term Tangible and Intangible Assets
12	Operating Profit/Loss
13	Cost Interests
14	Income Tax
15	Profit/Loss of the Accounting Period
Note for the column name "Data Order Numer", which marks in colour the figure according to the Financial Statement:	
	Figure from the Line enters the Calculation of the Domestic Rating KMEP in part 1 (calculation IN99).
	Figure from the Line enters the Calculation of the Domestic Rating KMEP in part 2 (calculation AspektGlobalRating).
	Figure from the Line enters the Calculation of the Domestic Rating KMEP in parts 1 a 2 (calculation IN99 and AspektGlobalRating).

Annex 2 – The Scheme of Complex Rating KMEP

Scheme of the Complex Rating KMEP



The Notes for the Above Mentioned Scheme:

1. It is possible to work with the mathematical and statistic apparatus directly. There is a validated database of financial figures and their time lines for the SME available.

2. It is possible to describe it in the qualitative expert way and only later within the framework of e.g. benchmarking work with the mathematical and statistic apparatus. There is not a validated database of the non-financial figures and their time lines for the SME available.

1 and 2 are processed in the MS EXCEL 97 in the dissertation work attachment which is not publicly available.

1 is processed in the dissertation work as a proposal of methodology of the SME and the accuracy of its result was compared against the reputable SME Rating, which expert guarantor is the CCB - Czech Credit Bureau, a.s. from the multinational group seated in Bologna, Italy.

For 3 a 4 are not available the validated databases of figures and their time lines for the SME.

For 4 there are available the ratings of the sovereign countries and their time lines from the reputable agencies e.g. Moody´s and Standard & Poor´s from the USA.

*) Financial (quantitative) part and non-financial (qualitative) part, i.e. economic and technical aspects are the integral part of the complex evaluation of the SME where there is necessary to bear this fact in mind and fully abide it in order to gain the maximum objective result of the domestic or/ and the international SME evaluation.

Chapter 6

RISK ASSESMENT OF PROJECT OF IMPLEMENTATION OF VIDEO TOLLING FOR FEE COLLECTION SYSTEM WITHIN ROADS NETWORK OF CZECH REPUBLIC AS PART OF REGULATORY IMPACT ASSESSMENT*

1. Introduction

The aim of this article is to present the results of the risk analysis, which is an obligatory part of the RIA in the case of legislative acts in the Czech Republic. The process, which is the subject of the risk analysis, is the implementation of the video tolling for the fee collection system within the roads network in the Czech Republic. The risk in the context of this article is understood as a possible unacceptable impact on the interests of any subject affected by the regulation and any chance or probability that a person or something will be harmed or experience an adverse effect if exposed to a hazard.

2. Background research and solution concept

Initially, the RIA process need is explained and then the application of RIA in the Czech Republic is summarized. The risk analysis as a part of RIA is described and justified.

2.1. The need of RIA justification

Governments need to work systematically to ensure that the regulation they develop and implement is of high quality, since the costs to society of poor quality regulation are substantial. Poor quality regulation increases compliance costs for business and other groups, leads to unnecessary complexity and associated uncertainty as to regulatory obligations and reduces the ability of government to achieve its objectives.
RIA is a process of systematically identifying and assessing the expected effects of regulatory proposals, using a consistent analytical method, such as benefit/cost analysis. RIA is a comparative process: it is based on determining the underlying regulatory objectives sought and identifying all the policy interventions that are capable of achieving them. These "feasible alternatives" must all be assessed, using the same method, to inform decision-makers about the effectiveness and efficiency of different options and enable the most effective and efficient options to be systematically chosen. According to the OECD [1]: "...RIA's most important contribution to the quality of decisions is not the precision of the calculations used, but the action of analysing – questioning, understanding real-world impacts and exploring assumptions".

Authors: Dipl. Ing. Olga Mertlová, Dipl. Ing. Milan Dont, Czech Technical University in Prague, Praha, Czech Republic, olga.mertlova@fd.cvut.cz, milan.dont@sfdi.cz

RIA should be integrated with a public consultation process, as this provides better information to underpin the analysis and gives affected parties the opportunity to identify and correct faulty assumptions and reasoning. RIA is now used in virtually all OECD countries and in many developing countries.

Regulations usually have widespread effects: they affect many different groups in society and the effects may be of many different types. Many of the effects are "hidden", or at least are difficult to identify when a regulation is being considered. RIA can help to ensure you have a good understanding of who will be affected by a regulation and how.

By using RIA, you can help to improve the decision-making process that shapes the final regulation. In particular, RIA helps to promote systematic decision making and a comparative approach to policy decisions. RIA requires you to ask:

1. What, in general terms, is the problem to be addressed?
2. What is the specific policy objective to be achieved? and
3. What are the different ways of achieving it?

The authorities should ask these questions before proposing to make a regulation. Starting with these questions, it can be ensured that as many different practical ways of achieving the objective as possible is identified. Then the authorities can get closer to the identification of the best option.

According to work [1] "RIA has developed quickly, and an increasing proportion of laws and other regulations affecting citizens are being shaped by various forms of RIA. Although only two or three OECD countries were using RIA in 1980, by 1996, more than half of OECD countries had adopted RIA programmes. By end-2000, 14 out of 28 OECD countries had adopted universal RIA programmes, and another 6 were using RIA for at least some regulations. As well, RIA is increasingly being applied to primary legislation, where in the past it has principally been used in relation to lower level rules. This will necessarily have a major positive impact on its potential contribution to regulatory quality. "

2.2. The RIA in the Czech Republic

In the Czech Republic RIA has been applied since 2007 in case of all the generally binding legal regulations prepared by the ministries and other state central administration authorities pursuant to the Government's Legislative Rules, including implementation of the EC/EU legislation, which accounts for a major portion of the prepared legal regulations [2]. There are only few exceptions from the obligation such as the state budget, and final state account, special cases (Government's Legislative Rules [9], Part Four, Articles 17 through 19), emergency legislation, crisis situations, general procedural rules, etc. Whenever any of the above-mentioned exceptions are applied, this must be expressly mentioned in an explanatory report to the draft legal regulation.

The RIA rules [3] are given by the Government of the Czech Republic and the rules determine the process and the methodology undertaken by the ministries and the other central government authorities.

Existence of a problem does not necessarily mean that measures have to be taken, particularly so at the level of state administration. Some problems may be of a more or less theoretical nature, marked by low probability of their occurrence. That is why it must be immediately explained in this opening section of the RIA why state intervention is crucial for problem solution, if that problem is real. The most cogent reasons for state intervention are the threat to health or security of the population or the threat of damage

to the environment. State intervention may also be justified by a long-standing *"market failure "*, caused, for instance, by insufficient or unbalanced approach taken by some market actors towards information, lack of competition on the market or side effects/externalities. State intervention may also be justified by the need to ensure "public welfare/public assets „that cannot be safeguarded by individuals themselves. The risks assessment part of the RIA should deal with the justification.

2.3. Risk analysis as a part of RIA

A quantitative risk assessment is an obligatory part of the RIA and it has a specific set of definitions set out in the respective rules. These are affected by the specific features of the risk analysis in the context of the regulatory process assessment.

2.3.1. Risk definition in the context of RIA

According to [4] we should any source of potential damage, harm or adverse effects on something (e.g. the environment) or someone. The same source gives that risk is the chance or probability that a person or something will be harmed or experience an adverse effect if exposed to a hazard. Hazard is a function of the inherent properties of the agent/event in question whereas risk is a function of both the hazard and of the potential likelihood and extent of being exposed to the hazard. In other words, while hazard represents an abstract danger, risk expresses the combination of the level of hazard and the likelihood of its occurrence. In today's society, where potential risks are numerous and inter-related, risk can be identified on the basis of a wide range of evidence including past experience, monitoring data, expert opinions, etc. Note that risk may not be related exclusively to the problem itself but also to the alternative measure(s) to reduce the initial risk.

2.3.2. Risks treatment and the regulation

The public response, often encouraged by the media, to a perceived risk (be that a risk emerging over time or a specific incident) is usually to call for regulation. The process can be characterized as a "regulatory spiral", summarized as follows [5]:

1. The perception of a risk emerges. This can be progressive over time, such as the risks following a specific incident (such as a terrorist attacks).
2. A public debate follows, often based around headlines and incomplete or biased information, resulting in a call for 'something to be done', which is amplified by the media.
3. Instinctively, the public looks to the authorities to manage the risk. Responding to this public pressure, the authorities or politics make ambitious claims that they can solve the problem and steps in with a regulatory response, rarely considering the trade-offs involved.
4. As a result, the role of the authorities as risk manager is reinforced.
5. When the regulations are implemented, they may fail to solve all the problems and also, bring with them unintended consequences.
6. With good implementation, some hazards are prevented, but other hazards are not prevented and problems persist, leading to calls for more government action.
7. Because of more regulation, people complain that liberties and enterprise are diminished and criticize the 'nanny state'.

8. Governments are blamed for interfering and acting unreasonably and, as a result, the national level of frustration grows.

(If we are not careful), authorities may seek to address issues of frustration and disengagement through more regulation.

The conclusion we can make is that each regulation should be carefully assessed not only from the view of effectiveness and efficiency, but also with the consideration of the "regulatory spiral" and the respective risks.

The process of the RIA application is designed to eliminate the drafting of such new regulation, which is not immediately needed.

2.3.3. Risks evaluation as a part of RIA

According to [6]: „An analytical method that is gaining ground in OECD countries is quantitative risk assessment, which allows regulators to understand more clearly the risks for humans or the environment from a particular factor, and the contributions of a regulation in reducing the risk. Quantitative risk assessment improves the capacity of a government to focus on the most important risks and reduce them at lowest cost, while identifying those risks that fall below a threshold justifying government action. Risk assessment has rapidly become among the most high-profile and controversial regulatory issues in the OECD area, and has become one of the most frequent sources of trade and investment disputes."

Evaluation of risks associated with failure to resolve the problem is an obligatory part of bot the so called small RIA and the big RIA (connected with higher volumes in the field of the quantitative or qualitative impacts). In the case of the big RIA, an evaluation of costs and benefits should be performed and the risk analysis should be included.

The RIA should describe the problem concerned not only by the goals attained, but also by the risks posed by the inactivity.

As the RIA Methodology says, that always at least 2 options must be determined, each of the options must be described not only according to the overall goals, but also according to the risks connected with the implementation and enforcement, and the compliance costs of the regulation on the part of the stakeholders. It is likewise necessary to assess risks posed by the implementation of proposed options.

As a part of the costs and benefits analysis, the RIA should weigh the risks connected with the implementation and ascertain how they affect the actual amount of costs and benefits.

The RIA should assess the risks posed in case of failure to solve the given problem.

It is likewise possible to employ techniques for the evaluation of changes in the risks posed by the emergence of an event. This is enormously useful and truly necessary when evaluating many impacts on the environment or health. Many policies will, for instance, seek to reduce risks of diseases and death. It is hardly possible to ascribe monetary values to life as such or to lives of other people. Due to this reason, change in risks is used, since nobody would exchange one's life for a specific amount of money; most people will be willing to choose between different safety precautions and devices sold for different prices offering different levels or security or different modes of crossing the street as compared with saving time. That is why you can fix a value, which people ascribe to small changes in risks.

As part of the procedures for evaluating risks, the risk of the emergence of an undesirable event and its potential repercussions for the individual and society, should such an event really occur, are also assessed. Risk evaluation may later be used for the

specification of options available for reducing or eliminating that particular risk and/or its consequences.

In order to perform a risk analysis, you need:

- to identify the risk,
- to evaluate the likelihood of its emergence,
- to assess potential impact on the proposed solution, if a specific risk does occur.

Scientific evaluation of risks makes a decisive contribution to regulatory decisions, especially in the field of public health and security, environmental protection, use of resources, creation of wealth, innovation and national security, while signalling whether a specific policy is likely to rationalize the process of limiting risks in a significant manner.

The RIA risk analysis can bring severe negative aspects:

1. Impacts of risks may be different and need not be mutually proportionate (i.e. need not be projected into a single draft),
2. Usually, it does not estimate costs that are likely to arise, if an undesirable event occurs,
3. It does not take into account profits and impacts, save for the risks associated with proposed measures for the solution of risks and/or their consequences,
4. This method should not be employed as the only starting point when deciding whether to accept a specific measure or when determining the type of measure to be adopted.

3. Data description

The data used for the RIA performance consist of full description of current state of roads fees in the Czech Republic including the regulatory and legislative framework, the scope of the tolled roads, and description of the target state and the goals of the new charging system.

3.1. The fees charged for motorways and selected class 1 roads in the Czech Republic

In the Czech Republic using of the motorways and selected class 1 roads by the motor vehicles with the highest permissible weight till 3.5 tones has been charged by fees since 1995. The regulation is given by the Act No. 13/1997 Coll., On the Road Network, as amended [7]. The obtained money becomes an income of the State Fund of Transport Infrastructure [8], which is responsible for issue and distribution of the so-called coupons. Motorways, which are marked with a road sign as a motorway, determined by an Implementation Regulation, can only be used by a motor vehicle with at least four wheels, upon the payment of a fee for the use of a motorway.

The fee can be paid for a whole calendar year, one month, or ten days. The fee is paid prior to the use of a motorway by a motor vehicle. The payment of the fee is documented by a valid two-part coupon, one part of which is completely attached to the interior side of the clear glass of the windshield of a motor vehicle, in the lower right hand corner (from the driver's perspective), so that the driver's view is obstructed as little as possible and the coupon is visible from outside of the vehicle.

The Ministry of Transport and the State Fund of Transport Infrastructure have concluded recently that the way of payment of the fee should be changed. As a suitable option of the time-based fee collection is an implementation of an electronic charging system (so called video tolling), which would enable to collect the fee in a reliable and

continuous way with high efficiency. The automatic control system would bring a preventive effect and a repressive effect of the fine enforcement. The roads users would be provided by a modern, user friendly tool including environment for payments realization.

The vehicle would be identified by its unique identification mark. The video detection of the registration marks of the passing vehicles would enable many times more effective permanent automatic control of the payments for the individual vehicles. The system would be able to accept on-line payments of the time-based charges.

3.2. Scope of the time-based fees

The list of the roads and motorways, which are subject to fees as to January the 1st, 2016 is in the Annex 2 of the regulation of the Ministry of Transport No. 383/2016 Coll. [9]. The list represents the following 1015 km of roads (Table 1).

Table 1. The list of the charged road sections as applicable from the January 1st, 2016.

Road No.	**Section**	**Length (km)**
D0	Modletice – Praha, Slivenec (exits 76–16)	23.0
D1	Praha, Chodov – Kývalka (exits 2–182)	180.0
D1	Holubice – Kroměříž, west (exits 210–258)	48.0
D1	Kroměříž, east – Říkovice (exits 260–272)	12.0
D1	Lipník nad Bečvou – Ostrava, Rudná (exits 298–354)	58.0
D2	Brno, Chrlice – state border (exit 3 to km 61) (in opposite direction from Lanžhot, odpočívka)	58.0
D3	Mezno – Čekanice (km 62 to exit 76)	14.0
D3	Měšice – Bošilec (exits 79–109)	33.0
D4	Jíloviště – Háje (exits 9–45)	36.0
D5	Praha, Třebonice – Beroun, east (exits 1–14)	14.0
D5	Beroun, west – Ejpovice (exits 22–67)	45.0
D5	Sulkov – state border (exit 89 to km 151) (in opposite direction from Rozvadov, odpočívka)	62.0
D6	Jeneč – Nové Strašecí (exits 7–32)	25.0
D6	Jenišov – Jesenice (exits 131–162)	31.0
D7	Kněževes – Knovíz (exits 3–18)	15.0
D8	Zdiby – Řehlovice (exits 1–65)	65.0
D8	Knínice – state border (exit 80 to km 92) (in opposite direction no fee)	12.0
D10	Stará Boleslav – Bezděčín (exits 14–39)	25.0
D10	Kosmonosy – Ohrazenice (exits 46–71)	25.0
D11	Jirny – Hradec Králové, Kukleny (exits 8–90)	82.0
D35	Sedlice – Opatovice (exits 126–129)	4.0
D35	Mohelnice, jih – Křelov (exits 235–261)	26.0
D35	Holice – Lipník nad Bečvou (exits 276–296)	20.0
D46	Vyškov, východ – Prostějov, jih (exits 1–21)	21.0
D46	Držovice – Olomouc, Slavonín (exit 26 to km 39)	13.0
D48	Bělotín – Bělotín, east (exits 1–3)	4.0

D48	Frýdek-Místek – Žukov (km 47 to exit 70)	19.0
D52	Rajhrad – Pohořelice, south (exits 10–26)	17.0
D55	Hulín – Otrokovice (exits 16–32)	16.0
D56	Ostrava, Hrabová – industry zone – Frýdek-Místek (exits 40–51)	12.0

3.3. Description of target

The proposed change aims to replace the contemporary paper motorway coupons by the electronic version, which would be linked up with the unique vehicle ID. There will be no paper or physical form of the electronic coupon.

The vehicles will be equipped neither by any technical device nor label proving the payment of the time-based fee. The fee will be paid at a retailer or via electronic ways and the payment will be registered in a central database. The vehicles exempted from the payments will be registered in the central database too.

The goal of the regulation change is to offer an on-line tool for payments of the fee to the users (internet sale, mobile applications, etc.). These accesses can reduce costs needed for the temporary system of payments, printing and distribution of the coupons. The users' comfort would be improved, especially for the occasional and foreign user of the charged roads. Also, the number of the violations of the duty to pay the fee should be reduced (including mitigation of the risk of falsification of the coupons).

3.4. Goals of the new charging system

Implementation of the electronic coupons in the time charging system should achieve the following goals:

1. Reliable and continuous way of toll collection.
2. High efficiency of the toll collection.
3. Preventive effects of the continuous automatic system of vehicle control on the tolled roads.
4. Repressive effects of the automatic system of enforcement of the fines for the violations of the duty to pay the fee.
5. Modern and user friendly tools and environment for the payments of fee.
6. Reduction of the current costs of the toll collection.

The goals cannot be achieved in the temporary toll collection system, which uses the paper coupons.

Achievement of the listed goals can bring following benefits:

1. Higher comfort for the tolled roads users:
   - expansion of the possibilities of buying the electronic coupon – electronic way,
   - no need to glue the coupons, fill in the registration marks, removal of old coupons,
   - immediate possibility to buy a new coupon via a mobile phone (just before the toll road is used),
   - no risk of buying two coupons for one vehicle and one period – protection of the user,
   - no need to keep the receipt of payment.
2. For the recipient of the revenues:
   - higher income from the distribution,

- effective way of collection of the fee, reduction of the share of non-paying users of the tolled roads,
- reduction of complaints and claim for replacement of coupons,
- on-line information on the progress of the sale,
- swift payments on the income accounts,
- no need of prints of reserve coupons, no need for logistics and distribution to the retailers, no need of disposal of the old coupons,
- variability of the system.

3.5. Explanation of the need for regulation change

The regulation given by the law no. 13/1997 Coll. [7] brings a complex rule concerning the time charging of the vehicles including the roles of individual subjects. The current wording of the legislation stipulates that the coupons are used in a paper version.

To achieve the goals described above the change of the legislation is inevitable. An alternative solution in this case is only the "zero" option, which means the conservation of the current state.

The proposed change of legislation would not bring any new obligation for the users of the tolled roads; only the current obligations would be transformed technically and procedurally.

4. Methods

The methods used to pursue the risk analysis are chosen and performed according to the regulatory environment in the RIA sector.

4.1. The methods given by the government methodology

The risk analysis is an obligatory part of RIA and the way of assessment is undertaken by the "Methodology of the risk evaluation within the Regulatory Impact Assessment (RIA)" [10]. The document defines the risk and the relation between the risk, the event and the negative impact. It describes the way the probability and the impact of the risk and event and the sources of risks are identified.

The methodology states that within the RIA the evaluation is performed in order to assess the risks of preservation of the status quo (without the regulation) and the risks of the possible options. These two evaluations are performed separately within the RIA report.

The risks of the status quo are assessed within the justification of the regulation. The risks of the possible options are assessed within the evaluation of the costs and benefits.

4.2. The risks of status que preservation

This part of the RIA should describe the risk, which would result from the inactivity and the preservation of the status quo. These risks are specific, because they are closely bound to the reasons of the proposed regulation. Usually these risks become part of the discussion about the need for the change and the need for the regulation.

4.3. The risks of possible options

The individual options of the proposed regulation can bring uncertainty concerning their possible negative impacts (risks). These risks stem mainly from the evaluation of the individual options' impact.

Since the individual proposed options usually have not been tested in real life, the consultation phase is very important as a part of these risks identification.

4.4. The risk assessment process

The process of risks evaluation is recommended to be undertaken as follows and is shown in detail in Figure 1:

1. Risk identification.
2. Assessment of the degree of risk using the determination of the risk parameters - the probability of the negative impact and the degree of the impact.
3. The analysis of the possibility of reduction or elimination of the risks.

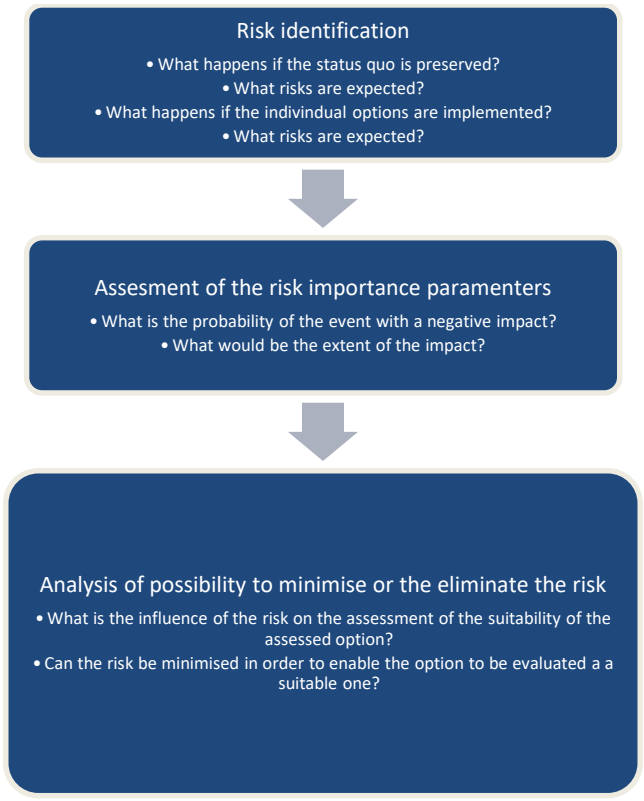


Fig. 1. The risk assessment process

4.4.1. The risk identification

The risk identification is a crucial step of the process. The RIA usually presents a complex problem and the omission of risky facts is prevented by maximization of consultation with all the participating stakeholders and specialists.

The methods of risks identifications are:

1. Consultations – the parties, which are best qualified to identify the risks, should be questioned and consulted.

2. Evaluation of impacts of possible options – the method of progress analysis can be used. The evaluator designs sequence of individual events and the possible progress. If an uncertain impact is identified it is assessed as a risk.
3. Lists of typical risks review – the checklists are used in this method for the individual options. The best practice is used as a part of this method.

Numerous complementary methods (e.g. SWOT analysis) can be used for the RIA, if it helps to identify the relevant risks.

4.4.2. The risk classification

For the RIA purposes the risks can be classified as follows:

1. Legal risks – usually inconsistency of the legal status with other legislative acts (national vs. European),
2. Material risks,
   - economical risks – financial impact on individual subjects,
   - ecological risks – negative environment impacts,
   - social risks – impact on different social groups and increase of inequality in society,
   - safety risks – safety of the stakeholders influenced by the regulation,
3. Political risks – can be prevented by wide consultations and negotiations.

4.4.3. The risk evaluation

The identified risks are evaluated from the view of their occurrence probability, scope and the scale of the impact and the time horizon of the occurrence of the event. The result of this analysis determines which risks are important enough to be treated further.

Probability of the event says the possibility of its occurrence. The probability is expressed in percent from 0 % to 100 %. If a probability of an event is higher than 0 there is a risk. In some cases, the exact numeric evaluation is not possible. We can only assess whether the probability is low or high.

Apart from the probability we have to assess the intensity of the impact of the event. If it is possible the impacts are evaluated as a quantity (e.g. financial amount in CZK). In other cases, we assess the scope via qualitative methods. Since there is the uncertainty factor, the respective methods can be used (e.g. sensitivity analysis or intervals assessment).

The evaluation scale for assessment of the level of probability and impact is shown in Table 2.

Table 2. Evaluation scale.

Probability		**Impact**	
Very low	1	Very low impact	1
Low	2	Low impact	2
Middle	3	Middle impact	3
High	4	High impact	4
Very high	5	Very high impact	5

As a result of the probability and impact assessment we can determine the risk degree, which results in the strategy of the risk treatment. The risk matrix is used as a tool of the risk classification (Table 3).

Table 3. Caption – risk classification.

	Very low impact	**Low impact**	**Middle impact**	**High impact**	**Very high impact**
Very high probability	5 low risk	10 middle risk	15 high risk	20 high risk	25 high risk
High probability	4 low risk	8 middle risk	12 middle risk	16 high risk	20 high risk
Middle probability	3 low risk	6 low risk	9 middle risk	12 middle risk	15 high risk
Low probability	2 low risk	4 low risk	6 low risk	8 middle risk	10 middle risk
Very low probability	1 low risk	2 low risk	3 low risk	4 low risk	5 middle risk

If the risk assessment results in the "low" degree, the RIA does not require undertaking further steps. The risk and the respective evaluation steps must be described only. In the case of the "middle" and "high" risks, the risk has to be treated further by the RIA.

The RIA requires determining the risks, which are serious enough to decline the respective option and to find possibilities to minimize or eliminate risks in order to find a suitable option.

5. Results

The "zero" option, which assumes the conservation of status quo, is assessed according to risks, which are identified and evaluated. The performance of this part of the risk analysis expects a comprehensive description of current state and its comparison to the projected system.

5.1. Identification of risks of the status quo

The following risks were identified for the "zero" option:

- risk of falsification of the paper coupons,
- risk of high transaction costs connected with the paper coupons handling,
- risk of non-using of the modern tools for sale and payments,
- risk of unavailability of the paper coupons,
- risk of destroying, losing or theft of the paper coupon,
- risk of double buying the coupon on the side of users,
- risk of burdening of the environment by the disposal of the paper coupons,
- risk of low effectiveness of the fee collection.

5.1.1. Risk of falsification of the paper coupons

The actual system shows many cases of the falsification of the paper coupons. The risk of this fact is a reduction of income, which is higher when higher number of fake coupons.

The future losses could be hundreds of millions CZK, since the newly discovered fake coupons are characterized by a high quality.

5.1.2. Risk of high transaction costs connected with the paper coupons handling

Another aspect of the current state is the need of the physical production, storage, distribution, exchanges, further production and disposal of the paper coupons. These costs could be eliminated by the implementation of the modern technologies.

The risk of the current state is a conservation of costs connected with the physical existence of the coupons and missing the opportunities of the new technologies, which could eliminate these costs.

5.1.3. Risk of non-using of the modern tools for sale and payments

The current state brings a user-unfriendly environment, which cannot benefit from the modern tools for sale and payments.

5.1.4. Risk of unavailability of the paper coupons

A parallel impact of the current state is a risk of unavailability of the coupons in the case of selling out, limitation of the distribution network by the opening hours, limitation for the foreign users, who cannot buy the coupons abroad.

5.1.5. Risk of destroying, losing or theft of paper coupon

The existence of the paper coupon brings a risk of destroying or losing the coupon (for instance a theft or a broken front glass of the vehicle).

5.1.6. Risk of double buying the coupon on the side of users

The current system does not prevent the users from buying two coupons for one car (by accident, wrong coordination of users, etc.).

5.1.7. Risk of burdening of environment by the disposal of paper coupons

An ecological aspect of the physical existence of the coupons is a need to dispose the expired coupons. Each period (year) requires the distributor to hold a reserve volume of coupons in the distribution system, which has to be disposed after the period, is over.

5.1.8. Risk of low effectiveness of fee collection

The current state brings a risk of a low effectiveness of the fee collection. There is no technical possibility to implement an automatic vehicle control system in the current state. There is only a random control of the vehicles realized by watching the vehicles, which has only low preventive impact on the discipline of users.

5.2. Evaluation of identified risks of status quo

The above identified risks are evaluated according to the RIA methodology consisting of the Evaluation scale (Table 2) and the Risk classification (Table 3).
The individual risks are identified according to the methodology processes and each risk is evaluated in the terms of occurrence probability and impact size (Table 4).

Table 4. Evaluation of individual risks.

	Probability	**Impact**	**Total**
Risk of falsification of paper coupons	4	4	16
Risk of high transaction costs connected with the paper coupons handling	4	5	20
Risk of non-using of modern tools for sale and payments	5	3	15
Risk of unavailability of paper coupons	4	4	16
Risk of destroying, losing or theft of paper coupon	3	3	9
Risk of double buying the coupon on the side of users	2	2	4
Risk of burdening of environment by the disposal of the paper coupons	5	5	25
Risk of low effectiveness of fee collection	5	5	25

The results of the risk analysis were presented as a matrix (Table 5).

Table 5. Matrix of evaluated risks.

	Very low impact	Low impact	Middle impact	High impact	Very high impact
Very high probability					- risk of low effectiveness of the fee collection - risk of burdening of the environment by the disposal of the paper coupons
High probability				- risk of falsification - risk of unavailability of the paper coupons	- risk of high transaction costs connected with the paper coupons handling

Middle probability			risk of destroying, losing or theft of the paper coupon		risk of non-using of the modern tools for sale and payments
Low probability		risk of double buying the coupon on the side of users			
Very low probability					

The conclusion of evaluation is that some of listed risks are evaluated (Table 4) with the result "high" or "middle". The aim of selection of the best option (which was the stage following the evaluation) is to eliminate the most serious risks.

The RIA process does not require a plan of processing of the identified risks nor a proposal of actions to be taken. Only the identification, analysis and evaluation of risks of the "zero" option were subject of the process.

6. Order of options

When dealing with the question of the future system of the time charging of the roads in the Czech Republic, the order of options obtained by the Feasibility study [11] is:

1. OPTION 0: current solution via „paper „coupons.
2. OPTION 1: technical solution based on the identification of vehicles via video identification of the registration mark.
3. OPTION 2: technical solution based on the identification of vehicles via microwave DRSC on-board unit.
4. OPTION 3: technical solution based on the control of the payment of the time charging via the satellite on-board unit.
5. OPTION 4: technical solution based on the identification of the vehicles via the coupons with RFID chip.

6.1. Brief description of analysed options

The Feasibility study [11] provides a detailed evaluation of each option. The option 0 represents conservation of the current state for the future. This option was used as a comparison basis for evaluation of the other options. The option 1 provides a new technical solution to detect and control the time charging for the use of toll roads by vehicles weighing less than 3.5 tones. The vehicle will be registered in a central database with its unique the registration mark and the state of registration. The control will be carried out by automatic camera system recognizing the registration marks of the vehicles and the subsequent comparison with the records time charges in the central database.

The option 2 provides a new technical solution to detect and control the time charging of the fee for the use of toll roads by vehicles weighing up to 3.5 tones. Vehicles in the system of charging time will be fitted with an electronic on-board unit (OBU). It is

proposed to use the units, using short-range microwave communications at a frequency of 5.8 GHz, dedicated to telematics applications in transport.

The option 3provides a new technical solution to detect and control the time charging for the use of toll roads by vehicles weighing less than 3.5 tones. Vehicles in the system of time charging will be fitted with an electronic on-board unit (OBU). It is proposed to use units employing satellite GNSS positioning and mobile telephony GSM / CN.

The option 4 provides a completion of the technical solution of time charging based on coupons with the possibility of electronic control without having to stop the vehicle, reduce speed or use a dedicated lane. The motorway coupons in the paper form will contain the security features on RFID identification chip that enables electronic checking.

6.2. Estimating the order of options and a selection of recommended option

The Feasibility study [11] recommends the following order of proposed options:

1. Option 1 – Video tolling.
2. Option 0 – Paper coupons.
3. Option 4 – RFID.
4. Option 2 – Microwave.
5. Option 3 – Satellite.

The option of using video detection was evaluated from the view costs of operation, technical solutions, requirements of users and system implementation. In the used methodology, the video technology was evaluated as the most suitable.

6.3. The affected entities

During the RIA elaboration, there were consultations performed in order to detect the most suitable option, which will be acceptable for all respective stakeholders.

The affected stakeholders are the following authorities and entities:

1. State Fund of Transport Infrastructure and Ministry of Transport.
2. Ministry of Finance and Customs Administration.
3. Ministry of Interior.
4. Police of the Czech Republic.
5. Roads and Motorways Directorate of the Czech Republic.
6. Citizens, entrepreneurs.
7. Disabled persons.

The most affected groups are the citizens and entrepreneurs. The other authorities will be affected by technical or procedural changes of the current processes.

A benefit of selected option falls primarily on citizens and businesses, which can use an electronic method of payment, without having to purchase, posting or removal of a paper coupon as it is currently. With the ability to pay the fee using electronic sales channels the distribution network can expand.

For entrepreneurs, the change brings simplification of the process of payment for the entire fleet of vehicles of the entity without requiring physical posting coupons.

In terms of state revenues is the positive impact of a much better opportunity to control and enforcement of the obligation to pay time fee. At the same time the very existence of a more robust monitoring system works preventively against violations of the obligation to pay the fee and time can bring increased revenue.

The new obligation may be negatively perceived by the persons exempted from the payment. Regular registration in the database of exempted people (and their specific vehicle) will be required. Without the registration of exempt vehicles into the system it cannot be operated in the charged network until the fee is paid. Unregistered vehicle would be recorded as a vehicle committing a breach duty to pay the fee.

7. Conclusion

The risk evaluation is an obligatory part of the RIA to the new legislation or legislative change. The methodology of RIA risk assessment was used in the case of the proposal of the law no 13/1997 Coll., which is proposed to be changed in order to implement new system of the time fee collection on the charged roads and motorways in the Czech Republic. The selected option of the fee collection should answer to the highest risks identified by the risk analysis of the "zero" option. The performed RIA resulted into the recommendation of the video detection system for the purpose of the operation of the tolled roads in the Czech Republic.

References

[1] OECD. *Introductory Handbook for Undertaking Regulatory Impact Analysis (RIA).* Version 1. Paris: OECD 2008. https://www.oecd.org/gov/regulatory-policy/447 89472.pdf

[2] ÚŘAD VLÁDY ČESKÉ REPUBLIKY. General Principles for Regulatory Impact Assessment (RIA). Praha: UV ČR 2007. www.mvcr.cz/soubor/ria-guidelines-czech-republic.aspx

[3] ČR. *Obecné zásady pro hodnocení dopadů regulace, schválené usnesením vlády ČR* č. 922/2011 (In Czech). https://www.vlada.cz/cz/ppov/lrv/ria/metodiky/ obecne-zasady-pro-hodnoceni-dopadu-regulace-90556/

[4] EC. *Better Regulation "Toolbox".* 2015. http://ec.europa.eu/smart-regulation/ guidelines /docs/brtoolboxen.pdf

[5] BETTER REGULATION COMMISSION. *Risk, Responsibility and Regulation – Whose Risk Is It Anyway?* London, 2006.

[6] OECD. *Regulatory Policies in OECD Countries: from Interventionism to Regulatory Governance.* ISBN:978-92641-7743-7. Paris: OECD 2002.

[7] SBÍRKA ZÁKONŮ ČESKÉ REPUBLIKY. *Zákon č. 13/1997 Sb.* (In Czech). ISSN:1211-1244. 3 (1997), pp. 47-31.

[8] SBÍRKA ZÁKONŮ ČESKÉ REPUBLIKY. *Zákon č. 104/2000 Sb.* (In Czech). ISSN:1211-1244. 32 (2004), pp. 1549-1552.

[9] SBÍRKA ZÁKONŮ ČESKÉ REPUBLIKY. *Vyhláška č. 383/2016 Sb.* (In Czech). ISSN:1211-1244. 154 (2016), pp. 6122-6125.

[10] ČR. *Metodika hodnocení rizik v rámci hodnocení dopadů regulace (RIA)* (In Czech). Praha: Vláda 2015. https://www.vlada.cz/assets/ppov/lrv/ria/databaze/ Metodika-hodnocen i-rizik.pdf

[11] STÁTNÍ FOND DOPRAVNÍ INFRASTRUKTURY. *Studie proveditelnosti zavedení elektronických kupónů sloužících k úhradě časových poplatků za užití pozemních komunikací vozidly do 3,5 tun v ČR* (In Czech). Praha: SFDI 2013

[12] ČR. Legislativní pravidla vlády schválená usnesením vlády č. 188/1998 ve znění pozdějších úprav (In Czech). Vláda ČR: Praha 1998. https://www.vlada.cz/cz/ppov/lrv/dokumenty/legislativni-pravidla-vlady-91209/

Chapter 7

EMPLOYEES FLUCTUATION RISKS AND HOW TO MEASURE THEM*

1. Introduction

Risk can be seen from different points of view and can affect different systems [1]. Long-time existing company can face many problems and risks. From minor ones like bankruptcy of one of many possible suppliers to major one like technological shift in current industry and with this connected decline of quantity of sold product and decreasing of companies' revenue. This paper aims on soft part of the system (a company) risks and also benefits connected with process of selecting employees with probable intention to leave the company.

In case a key employees leave the company this could result in threat to an organization's operations, development of new products or services and innovations of introduced ones. Also know-how, important business contact and information can be lost. The organization's survival depends upon their readiness and supporting tools in the face of these threats.

European economy is still in good condition [2]. Unemployment rates are quite low and companies suffer from understaffed professions like programmers, general practitioners, dentists and medical staff in general but also qualified labour force. In this situation could loose of one or group of key leading employees result in existential problems of the company. Companies must be ready to this inevitable development. Getting to know own employees, their value and values, their importance for the company is one way how to improve quality of decisions made about these employees.

Research [3] showed that more that 20% of respondents plan to expand their business in 2017. This means that additional employees will be needed and as shown previously Czech Republic has quite small supply of qualified unemployed workforce.

Solution of this situation can be requalification of unemployed applicants but this could be costly and also takes time to successfully receive necessary skills. Opposite side of this approach is that the success rate of requalification could be lower than estimated and costs of this activity were totally unacceptable.

On the other hand, making contact with unsatisfied employees of different company (or competitor) and offer them to change employer is easier but ethically discountable. One could say that this approach can start or escalate competition between these companies as the result of headhunting of scares employees not available on the job market.

2. Background research and solution concept

Social Network Analysis (SNA) goals are to reveal, describe and analyse the relations among e.g. individuals or organizations. Different tools (e.g. social network

Author: Dipl. Ing. Libor Měsíček, Ph.D., Jan Evangelista Purkyně University in Ústí nad Labem, Ústí nad Labem, l.mesicek@ujep.cz

metric, sociogram, matrix) can be used to represent social network structure e.g. the nodes and connections between them and compare different networks.

Moreno laid foundations of Social Network Analysis when he observed the interactions within small social groups and he has developed a system of communication and interaction records which were published in his work in 1934 [4]. He is also one of the first researchers who introduced a graphical representation of social networks and who has created a sociogram.

If we separate the form and the content of the communication it is possible to identify and to compare the structure of various social groups, and to create the models of their relations based on mathematical analysis of the networks [5].

Figure 1 shows example of a social network within a company. Every point represents an employee, colour represents that this point belongs to a group and line shows that these two employees are connected and they exchange information. Detail description of these connections is possible by using different metrics and values (e.g. number of interactions, duration, etc.).

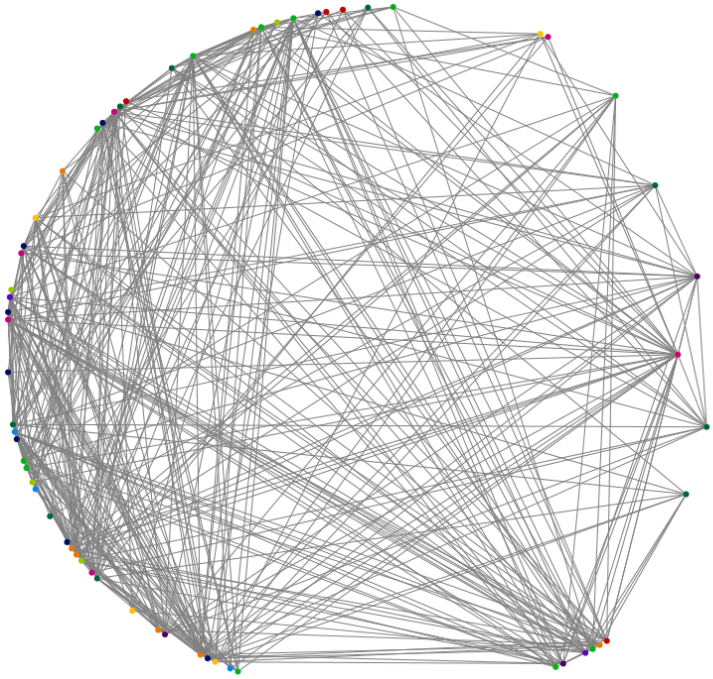


Fig. 1. Example of one possible layouts of sociogram. Where points represent employees and their colour represents group, in which they belong. Line represents connection between two employees (this sociogram shows that every connection works both ways).

For every node and network, a number of parameters can be observed, e.g. closeness centrality, clustering coefficient, degree, durability, eigenvector centrality, intensity, etc. [6].

Graph level measures express the structure and characteristics of the network. Every node has sets of metrics too (e.g. centrality express position of a node within the network, degree is number of nodes directly connected to concrete node, etc.).

Degree centralization indicates if there is big difference between nodes degrees. If every node in the network has the same number of connections to other nodes degree centrality is 0.

The density of a network describes how many connections are within the network and how much nodes we have. If the network is well connected (e.g. every node is directly connected to 50% of other nodes within the network) information spreads quickly, on the other hand low density makes it hard for information to be communicated.

Average centrality in combination with other metrics values can describe and reveal additional information about structure of the network (e.g. there is a few well connected nodes and rest of them is with low degree).

To gather, process, measure, calculate and evaluate there is number of tools. Some of them offer free or low cost use for scientific purposes (e.g. NodeXL, Gephi). Also much more expensive tools are available with specialized functions (e.g. ONASurveys).

List of software for social network analysis could be found for example in [7].

Study of Carboni and Ehrlich shows that individuals close to the core of a team outperformed more peripheral individuals, but only to the extent that teams were high-performing or had been together longer as a team [8]. The research results also coincide with a general discussion on the implications for human resources theory and practices targeted at improving individual performance outcomes.

To be able to map the social network easily we need sufficient source of data. The work of Kazienko et al. lists main data sources [9]. There are several cheap and fast sources of information about structure of the social network within the company. Mainly e-mail communication, instant messaging records, information about meetings and phone calls could be used to get brief image about how the social network of the company could look like.

Additional tools could be used to get more accurate Figure of actual social network structure. Questioners for employees about their contacts and frequency of the contact could be also used. Connections like meeting at lunch, smoking room or out of work activities could be discovered when we use a questionnaire.

Newer statistical approach how to reconstruct the network when e.g. detailed information (e.g. exact time) is not available in the log files of the tracked events are mentioned in the work of Corallo et al. [10]. Some files might not include time range when a given user participated to a given activity. Set of matrix and heuristic methods can use to reason probable structure of the network. Agent-based simulation could be also used to predict structure of a group [11] showed that it is possible to use CLUS-SOCI (an agent-based and CLUStering tool for simulating SOCIograms) to train the program to be able to predict actual structure of groups based on set of training data.

3. Data description

Data used to validate the research were acquired from different systems. E-mail network was used as a background, mainly information about who is writing to whom and what is the subject of the message (form: Sender, Receiver or Receivers, Subject). Blind carbon copies were also included. As additional data are used exports form logs of company's instant messaging system and also data from attendance at meetings. Company managers selected 15 employees for parallel questionnaire information harvesting. The questionnaire was focussed on work satisfaction, revenue and desired benefits. Last phase consisted of structured interviews with highlighted employees by the initial analysis.

4. Method of research

Set of processes using social network analysis to identify important employees within social network of the company was prepared. These important persons, together with key employees connected with research and development and also with unique skills or know-how should be focused, periodically gathered information about their attitude towards the company and current work position.

4.1. Creation of social network map

Figure 2 shows process of social network map creation.

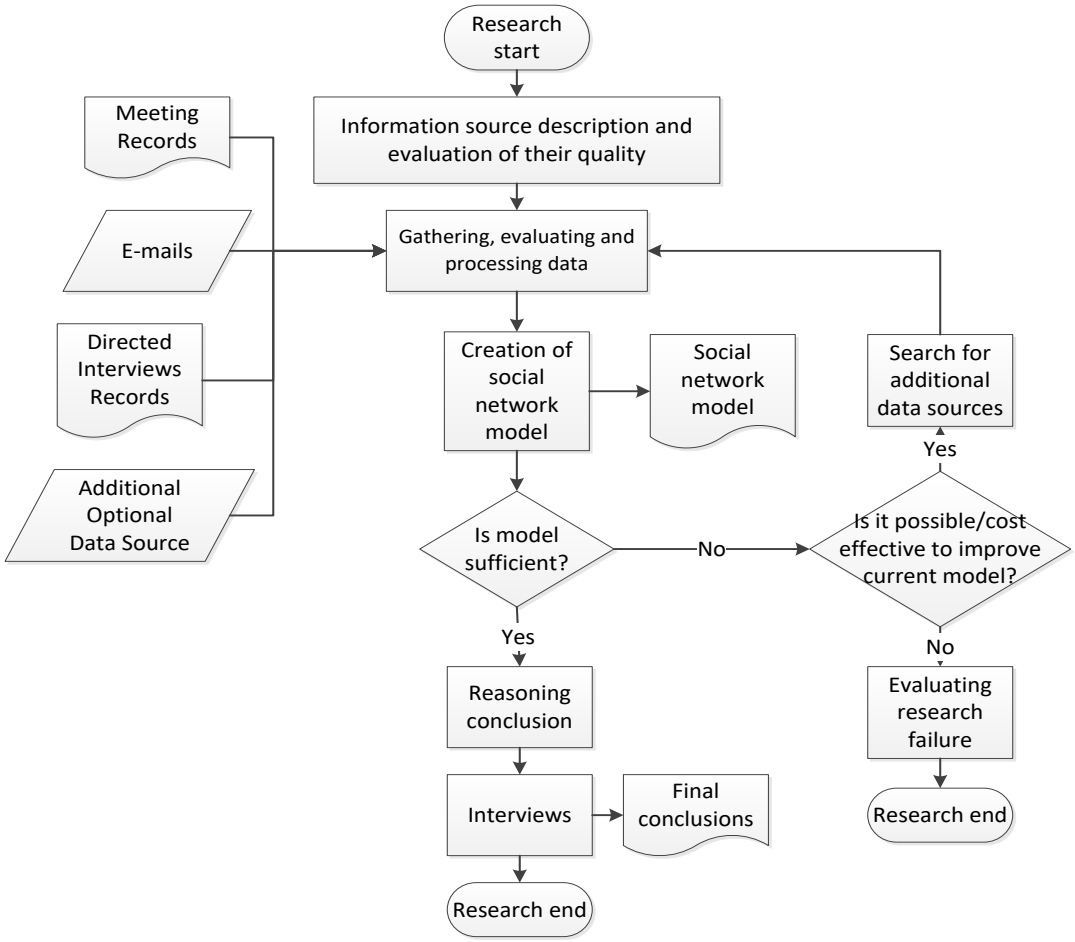


Fig. 2. Process of creation of a social network map.

The process starts with information sources description and evaluation of their quality. This process and evaluation is feasible only if certain level of quality of information sources has been met. Otherwise additional costs to prepare, distribute and evaluate large volume of questioners with possible inaccuracy of responses must be expanded. Selected sources are mined to receive information about who is communicating with whom. Based on these records, we can create social network model. To evaluate if the model is covering real structure of the network we can ask a sample of employees if recognized connections are all they have within the company or we missed some of them. To validate the model

of the network it is possible to perform interviews with sample of employees. If we discover that our model missed more that small amount of connections (depends on structure of the company, number of employees, etc.), there should we a meeting with responsible project team and they should search for the reasons why the model is not sufficient. Most common reasons are company culture and unofficial meetings which are not covered by electronic devices (e.g. smoking room). This is necessary for decision, if it is possible to effectively improve the model and if so, which data sources and methods should we use.

4.2. Evaluation of social network map and additional data sources

Figure 3 shows process of Social network evaluation. We can use the social network map as input for social network analysis methods. After structural analysis we can choose appropriate additional methods of analysis to improve results reasoned from the input data. There is group of classical method describing network, nodes and groups within social network based on mathematical analysis; another approach is based on heuristic analysis of the network.

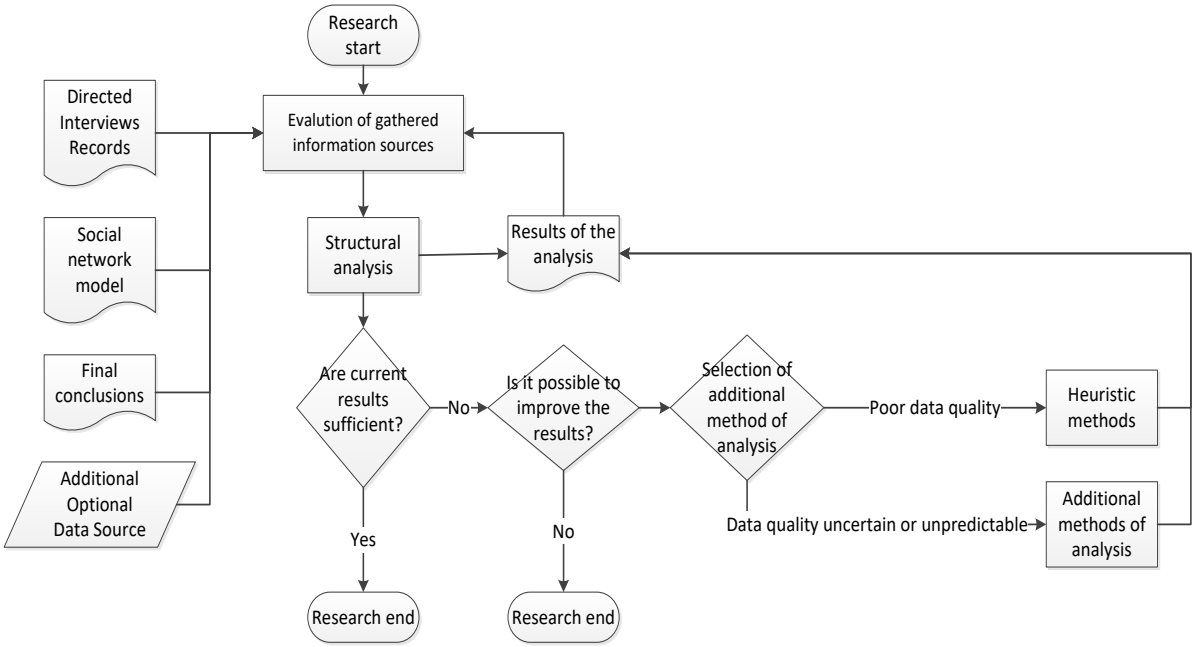


Fig. 3. Selection and performance of selected method or methods.

The heuristic analysis will be preferred in case, that the source data are not complete (e.g. are not describing whole networks or we have incomplete records of communication) and it is necessary to predict probable structure of missing nodes or nodes which are described insufficiently. Results of the analysis should include information about social network position of each evaluated employee (e.g. his or hers Eigen vector, degree, centralities, etc.), results of evaluation by his or hers superior, colleagues and subordinates. Also job description and job history should be included. As additional sources of date could be used overview of available job positions at advertisement servers (in Czech e.g. www.prace.cz, www.jobs.cz, etc.).

4.3 Process of evaluation, group distinction by probable risk of leaving a company

Result of this evaluation should be an index from 0 to 1 where employee with low (approximately from 0 to 0.2) is likely ready to leave the company. Employee who scores from 0.2 to 0.8 (boarders not included) might leave but he or she will probably need bigger incentive and employee with index near 1 has probably no intentions to accept offer from another employer. Part of equation is weight of each factor (sum of these four weights must be 1).

First part of index is social network position. Because every company's social network is more or less unique and due constant changes of environment major changes over time can occur we should compare an employee to his or her kind (same work position or same department, etc.). We can calculate social network position of each employee and order them by result of clustering coefficient or different metrics within the network. The group of employees with highest values will score 1 to 0.8.

Second part of index is internal evaluation of the employee. Based on his or her evaluation by co-workers and also background like education, job history, etc. Again, employees with highest overall score (qualified, with great score from colleagues, etc.) will receive 1. Employees not meeting the criteria will score less. Another factor is that employee who commutes every day for two hours is more likely to accept a good job offer near his or hers home than employee living nears his work place. Important part is self-evaluation of the employee, connected with job satisfaction, career options and promotion.

Third part of index is connected with job positions available for this employee by other companies. This evaluation goal is to find out how easy it is for the employee to find another job with same or better position.

Last part of index is reserved for special and additional points reserved for factors not included in three previous parts of the index like unique skills not included in internal part of the evaluation.

The index is possible to calculate as:

$$I_n = A \times Soc + B \times Inter + C \times Out + D \times Special$$

where: I_n is the index of employee' stability, *Soc* is the social network position, *Inter* is the result of internal evaluation of an employee, *Out* is the result of overview of available work positions outside of the company, *Special* is additional points (unique skills, know-how, etc.), A, *B, C, D* are weights of each factor, sum of weights is 1.

This index combined with other methods of human resource management should highlight employees which are important to the company stability (e.g. those who provide important information to the rest of the cluster or group, with unique skills or important knowledge) and also could easily leave the company.

The management of company should make decision to offer seminars, training or study break to these employees who score high index score and also during interviews/self-evaluation express desire to improve their skills, receive new certification related to their position or express concern that they lack new skills which could help them to work more efficiently.

5. Demonstration of the index

Presented index was tested since late 2016 on data from a middle size company operating mainly in Prague and Brno, Czech Republic.

Based on presented processes social network model of employees' interactions was assembled. The model was successfully tested after 10% of randomly chosen employees and two key employees (with highest Eigen vector) within the company were interviewed to confirm conclusions made based on the model. Only minor deviations were discovered (e.g. assumed connection between two employees was stronger than was expected because of recent events).

Second part was calculation of additional relevant metrics of social network and every node. Additional data were linked to every employee (e.g. work position and its description, qualification (level of education, education classification), distance from home address to his or hers work place and duration by car, public transportation and on foot (in case they live less than 4 km from work place, etc.)).

Portal www.jobs.cz and one private head hunting company was used to find number and quality of job offers for every group of employees (from less qualified employees to top managers and data architects of the company). Available LinkedIn profiles of the company employees were also checked for changes and possible signs that the employee is possibly looking for a new job (function of hidden availability for possible employers was intentionally not tested).

For every employee of company, a set of more than four hundred criteria was created. Tens of thousands values in total were in the final version of tables for the whole company, most of them generated by scripts, imported and transformed from a company' system or public system. Some of the values (e.g. results of employee evaluation from their superior etc.) had to be done manually. Some of the values (e.g. there wasn't found any LinkedIn profile, the employee was in the company just a few months and no previous evaluation was available, etc.). Last part of the index (Special) was inserted by direct superior of evaluated employee in first week of December 2016 based on prepared manual (e.g. recent actions of the employee which are not included in the previous reviews).

Last part of the calculations consisted of final check of values for extreme values and possible errors and then the score for every employee was calculated for every part and the final value of the index has been calculated (weights of A, B, C, D were set after discussion of top managers to 0.2, 0.5, 0.2 and 0.1).

Several red flags raised and marked 6 employees with score 0.2 and less at the end of the research.

These employees could be or even might be open to accept an offer from another employer and it will be probably difficult to replace them with sufficient replacement in weeks or even months.

One of them commuted 1 hour and 48 minutes every day had history of changing employers and is at non-crucial position. Hers direct supervisor refused to take any action to prevent her from leaving the company.

Another discovered employee already left the company before the research result was delivered.

Result showed that rest of them were from same crucial department of the company. In case these four employees decide to leave, the company will be in existential troubles because the department will lose two thirds of the employees with specialised skills and knowledge. This information let the managers to update crisis scenarios to reduce

possible vulnerability and impact (to find possible supplier in case they need to replace their function) and also prepared a package of incentives to improve the department loyalty.

6. Discussion

Presented sets of processes and the index could help with discovering which employee could be both important to the company and ready to leave it. In case the company wants to prevent that or postpone this certification or additional education could be offered as well as partial work from home or other benefits.

Framework to estimate returns in training of an employee is presented at [12]. They found that an increase in training investments is significantly linked to an increase in revenue per employee. Also, those large firms benefit more from training.

Research by [13] showed that the provision of company training is largely determined by firm-specific factors, such as human resource management practices.

Survey of HAYS Company at 2016 showed that 69% of employees in Czech Republic are expecting salary increase after they change their employer and 62% further career advancement [14]. From employers' point of view 73% of companies is offering language courses and 64% offer further education of their employees (certification, etc.).

On the other hand, there is real risk that new skills could improve value of the employee at job market and there will be stronger pressure from him or her to increase his or her salary and work conditions.

Problem of migration of labour force to Germany and Austria is also one of the concerns of the employers. This risk of loose qualified labour force is probably higher in the border regions. Several larger cities (e.g. Brno, Plzeň, Most or Ústí nad Labem) are within every day or work week commute range with much more interesting work positions, with better work condition and financial perspectives. The employee can get self-confidence to try working abroad after receiving language courses. This could result in undesired situation which could end up in higher salary.

Focussing right employees for additional language or specific training could enforce their loyalty to the employer and sign that the employee is important to the company. Also the process of learning could bring change of environment for the employee and break the day to day routine.

Another possible risk of this process of choosing the right employees is that unhappy employee is skipped and this will trigger his or her process of leaving the company without suitable replacement.

7. Conclusions

Problem of evaluating employees and risk of leaving their company without having proper replacement is quite serious when we consider current situation at the job market. Crucial employees must be discovered and the company should offer them several benefits like additional training, benefits or special care. The prepared set of processes, which should help to evaluate and choose employees with high risk of leaving their current company, has been demonstrated. These processes use among other things methods of social network analysis to identify attributes of employees describing their social network position, internal and external sources of data and information as well. Main benefits of selecting employees for direct offers to improve their work satisfaction

could enforce loyalty of the employee, improving his or her skills and thru this work performance. Additional benefit of a future trainings could be chance to meet other people from the company and improve social network position within the company.

Main part of this chapter could be seen in results of the applied research in a company. The research took almost two months and successfully identified employees with high risk of leaving the company. Based on the results management of the company took contra measures like additional packages of benefits for selected employees. Also human resources and how the company is working with them started to be an issue.

Risks of not only further education but also flexible working hours or home office could be seen in the fact, that some employees could be missed during the selection process, also investments to the employees could not return to the company in case the new skills are not practiced and not related to his or her work or new freedoms are misused. One of the major concerns these days is also migration of work force to different company of even to different country due higher standard of living and career opportunities.

Every company must consider this delicate topic with caution. Like every decision in human resources management this could start chain reaction with massive consequences.

In 2017 there are already signs that European economy has reached peak and in years to come there is growing concerns of economic decline. This will almost certainly change job market situation and importance of employee migration as well.

References

[1] PROCHAZKOVA, D. Validity of Use of Various Concepts of Risk Management and Risk Engineering in Practice. *International Journal of Computer and Information Technology*. 03 (2014), 1, pp. 21-30.

[2] THE WORLD BANK. *A World Bank Group Flagship Report: June 2016 Global Economic Prospects, Divergences and Risks*. http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf

[3] Československá obchodní banka, a. s. *Podnikatelé zůstávají optimističtí. Index očekávání firem byl ve třetím kvartále zatím druhý nejvyšší* (In Czech). https://www. csob.cz/portal/o-csob/o-csob-a-kbc/servis-pro-media/tiskove-zpravy/-/asset_publisher/5FasXY5AUiLR/content/id/2994616

[4] MORENO, J. L. *Who Shall Survive?* ISBN: 978-1446601853. Nervous and Mental Disease Publishing Co.: New York 1934, 466p.

[5] NADEL, S. F. *The Theory of Social Structure.* ISBN: 041-5866685. Cohen & West: London 1957, 180p.

[6] SCOTT, J. *Social Network Analysis*. ISBN: 978-1446209042. SAGE: London 2013, 201p.

[7] HUISMAN, M. *Software for Social Network Analysis.* https://www.gmw.rug.nl/~huisman/sna/software.html

[8] CARBONI, I., EHRLICH, K. The Effect of Relational and Team Characteristics on Individual Performance: A Social Network Perspective. *Human Resource Management*. 52 (2013), 4, pp. 511-535.

[9] KAZIENKO, P., MICHALSKI, R., PALUS, S. *Social Network Analysis as a Tool for Improving Enterprise Architecture.* IN: 5th KES International Conference, KES-AMSTA 2011, 29 June – 1 July, Manchester.

[10] CORALLO, A., BISCONTI, C., FORTUNATO, L., GENTILE, A.A., PELLE, P. *An Approach from Statistical Mechanics for Collaborative Business Social Network Reconstruction*. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 25-28 August, Paris 2015.

[11] GARCIA-MAGARINO, I., MEDRANO, C., LOMBAS, AS., BARRASA, A. A Hybrid Approach with Agent-Based Simulation and Clustering for Sociograms. *Information Sciences*. 201 (2016), 345, pp. 81-95.

[12] MEHRA, A., LANGER, N., BAPNA, R., GOPAL, R. D. Estimating Returns to Training in the Knowledge Economy: A Firm Level Analysis of Small and Medium Enterprises. *MIS Quarterly* 38 (2014), 3, pp. 757-771.

[13] HANSSON, B. Company-Based Determinants of Training and the Impact of Training on Company Performance. Results from an International HRM Survey. *Personnel Review*. 36 (2007), 2, pp. 311-331.

[14] HAYS, *Platový průzkum Hays: Pracovní trh v roce 2016* (In Czech). https://www.hays.cz/cs/groups/hays_common/@cz/@content/documents/digitalasset/hays_1602 080.pdf.

Chapter 8

ASSESMENT OF ECONOMIC SECURITY IN ENTERPRISES

1. Introduction

The current economic environment bringing permanent fears of the globalisation effects emphasises more and more the need to change the understanding of the security. The traditional perception of security as a state linked with the ability to ensure forces and means for defending the country's territory against armed conflicts is retreating. The security is becoming a system phenomenon which enlarges understanding the national security in relation to preserving the quality of life as well as the economic stability of the state [1]. The stability should not be perceived solely from the point of view of the need to protect the country's sovereignty but also from preserving adequate life conditions. Not only the state but also other economic subjects that operate inside of it perceive the security more and more from the economic point of view and it is of primary importance for them to ensure the resources (monetary, material and personal ones) which would give them a feeling of security [2]. This is also the reason why it is necessary to perceive the security as a complex consisting of components which overlap and affect each other. This paper will characterise one of the components, namely the economic security which can be perceived as [2]:

- the security of the economic subjects, processes and relations between them,
- the sustainability of the given processes and relations between the economic subjects in terms of fulfilling the requirements of economy.

The object of the economic security can be – an individual or a small social group, an enterprise, the regional self-government and the state. The international perception of the economic security adds here also the economic and integration groups but also the global economics.

This chapter deals with the economic security of an enterprise. Based on the available information about a selected group of companies we will state the boundary values of the economic security in four basic areas characterising the financial situation of the companies from the selected line of business.

2. Background research and solution concept

The economic security of an enterprise is influenced by a complex of factors affecting the enterprise in the same time. These factors result in risks. Risk can be defined as: "Risk is a condition in which there is a possibility of an adverse deviation from a desired outcome that is expected or hoped for [3]".

Risks can be classified as internal and external ones. The internal risks result from activity of the enterprise itself and consist of items such as an unsuitable structure of

Authors: Assoc. Prof., Dipl. Ing. Stanislava Strelcova, Ph.D., Dipl. Ing. Veronika Bobanova, Dipl. Ing. Denisa Janasova. University of Žilina, Žilina, Slovak Republic, stanislava.strelcova@ fbi.uniza.sk, veronika.boban ova @fbi.uniza.sk, denisa. janasova@fbi.uniza.sk

capital and assets, insolvency, inability to maintain the ownership structure, of capital and assets, insolvency, inability to maintain the ownership structure, the character and development of the transformation process, intentional or unintentional errors caused by employees, process and management failures, shortages and errors in the area of concluding contracts, information explosion, etc. [4, 5] The external risks impact the enterprise from its surroundings. Here, they belong to competition, disruption of confidentiality, accessibility and integrity of information, corruption, situation on the financial market, exchange rate risk, act of sabotage, espionage [6], demographic and educational structure, industrial accidents, geophysical and climatological phenomena, etc. [5]. All of mentioned risks affect the enterprise goals.

The majority of the known definitions of the enterprise [7, 8, 9, and 10] show directly or indirectly that one of the main goals of the enterprise is to achieve profit. This requires from the enterprise to have a sufficient amount of financial means for performing the entrepreneurial activities and to utilise the means in such a way that its return will be ensured, i.e. the adequate profitability.

However, under the means for performing the entrepreneurial activities we do not think solely the monetary means in cash or other financial assets but also the work and physical capital. The task of the enterprise is to select and utilise the employees and manufacturing equipment in such a way that will ensure the highest productivity of work. But here we have to take into account the fact the excessive utilisation of these manufacturing factors can cause their failure and losses of property, health or even people's lives.

The resources the enterprise utilises for performing its activities are at the same time the resources of its economic security [11]. They can have both tangible and intangible form.

The intangible resources of the enterprise economic security are created by the human abilities, information, utilising the technologies, patents, licences, know-how but also the enterprise's reputation. From the point of view of the economic security the human abilities and information are considered to be the most important resources. Due to their character and because it is impossible to assess them financially, it is a very complicated thing to state criteria for assessing the enterprise economic security. The enterprise can determine e.g. the optimal number of employees but is not able to enumerate what financial resources are to be invested to e.g. the development of technologies for the economic security not to be threatened.

The financial tangible resources of the economic security arise inside the enterprise or the enterprise achieves them from the external environment. For the economic security it is important for the enterprise to be able to ensure a sufficient amount of the financial resources in such a way it will be able to perform the entrepreneurial activities, to pay its liabilities to the business partners, banks, insurance companies, the state and in the case of emergencies to be able to ensure putting the enterprise to the original state.

The typical natural tangible resources of the enterprise economic security are – the buildings, manufacturing and other equipment, transport means, estates and inventories, in other words the tangible components of the long-term and short-term property utilised in the framework of the entrepreneurial activities or which ensure the premises for their operation. From the point of view of the economic security it is important for the natural resources to be deployed in the enterprise in such a way they will enable to achieve the highest possible savings and their utilisation will be as high as possible.

The natural tangible resources of the enterprise economic security represent (from the balance point of view) the capital and property of the enterprise and their values are reflected in the financial statements. Therefore, the financial and economic indicators [12] – we will be dealing with them also in the analytical part of this paper – are the most important means which enables revealing the symptoms of a negative development in the area of the enterprise economic security. However, enterprises have to manage all partial risks resulting from corporate assets (tangible or intangible) in the terms of economic security.

3. Data description

The Slovak Republic is an export-oriented country and the automotive industry is its key line of business covering more than 40 % of Slovakia's industrial production. Due to this fact we chose companies ranked according to the classification of the economic activity SK NACE to the sub-group 29.10.0 – Production of Motor Vehicles. 175 companies performed this activity in Slovakia by 1st August 2016 and 77 of them published their financial statements and number of employees in the Register of Financial Statements.

The analysis was carried out for the financial year 2015, i.e. from 1st January 2015 to 31st December 2015 based on the financial statements published on the web site of the Register of Financial Statements established by the Ministry of Finance of the Slovak Republic [13]. Through determining the time span we reduced the number of the analysed companies to 62 and it represents more than 35 % of all enterprises dealing with production of motor vehicles. We removed one enterprise from this group of enterprises – it was declared bankrupt and its economic results would have distorted the values of the indicators achieved. It was also necessary to exclude 20 enterprises, the economic results of which did not enable calculating all financial and economic indicators.

4. Method

One of the criteria which can be implemented for determining the general criteria of the enterprise economic security is the comparison method. The comparisons can be as follows:

- with the plan when the really achieved results are compared with the planned ones,
- in time when we monitor the development of the selected indicators for a certain time period,
- in space when the results of certain selected enterprise are compared with others.

The third method, the so called intercompany comparison which states the values typical e.g. for a certain line of business and subsequently they can be modified regarding other characteristics of the observed object of the economic security, e.g. the time period or it is possible to make the planned values more accurate is the most suitable one for stating the criteria of economic security.

The intercompany comparison enables revealing reserves in the companies´ activities in such a way they show the differences of the companies´ activities and shows those enterprises whose resoles are worse or better.

One of the methods enabling to realise the intercompany comparison is the method of the indicators´ variability. Its basis is the symptom of a certain state of the enterprise. A symptom can be a certain system of indicators and on the basis of their

changeability/variability it is possible to identify the strengths or weaknesses of the enterprise [14] and also the areas threatening the enterprise economic security.

For us to be able to realise the comparison procedure, it is necessary to set a system of indicators which characterise the activities of the compared enterprises as comprehensively as possible. A determinative criterion for their selection is the possibility to compare them with other companies of the same line of business. Therefore, it is necessary to choose such indicators which can provide the same information of all conditions being compared. Usually they are the value indicators (absolute or proportional ones) but we can also use the natural indicators (e.g. the number of employees in operation per one manager or a manufacturing device, etc.). It is also important for the compared companies to have the quantitative characteristics (e.g. the achieved turnover, the number of employees, the total assets, etc.).

Due to the fact that we have available only the financial statements, we decided solely for identification of financial risks affecting enterprise economic security. They conduct the system of eleven indicators which contains the proportional indicators characterising the liquidity (the equations 1and 2), the activity (the equations 3 – 5), the indebtedness and the financial structure (equations 6 – 7) and profitability (the equations 8 – 11) of the companies in the group. The following equations were used for their calculation [15]:

$$Current\ Ratio = \frac{Current\ Assets - Inventories}{Current\ Liabilities} \quad [-] \tag{1}$$

$$Cash\ Ratio = \frac{Cash + Cash\ Equivalents + Invested\ Funds}{Current\ Liabilities} \quad [-] \tag{2}$$

$$Inventory\ Conversion\ Period = \frac{Average\ Inventory}{Net\ Sales} \cdot 360 \quad [\text{days}] \tag{3}$$

$$Receivables\ Conversion\ Period = \frac{Average\ Receivables}{Net\ Sales} \cdot 360 \quad [\text{days}] \tag{4}$$

$$Liabilities\ Conversion\ Period = \frac{Liabilities}{Net\ Sales} \cdot 360 \quad [\text{days}] \tag{5}$$

$$Financial\ Leverage\ Ratio = \frac{Total\ Debt}{Total\ Equity} \quad [-] \tag{6}$$

$$Self-financing\ Ratio = \frac{Shareholder\ Equity}{Total\ Equity} \quad [-] \tag{7}$$

$$Cash\ Flow\ in\ \%\ of\ \ Sales = \frac{Cash\ Flow}{Sales} \cdot 100\ [\%] \tag{8}$$

$$Return\ on\ Equity = \frac{Net\ Profit}{Shareholder\ Equity} \cdot 100 \quad [\%] \tag{9}$$

$$Return\ on\ Assets = \frac{Net\ Profit}{Total\ Assets} \cdot 100 \quad [\%] \tag{10}$$

$$Return\ on\ Investment = \frac{Net\ Profit + Interests}{Total\ Equity} \cdot 100 \quad [\%] \tag{11}$$

The maximal and minimal value achieved in the group of the compared companies is detected for each chosen enterprise. The minimal and maximal value of the indicator defines the variation range of the companies included in the group.

Subsequently the values of each indicator are ranked from the minimum to maximum and the median is determined.

In the next phase we determine the quartiles. The value of the upper quartile is determined by the value of the indicator in the enterprise which determines those enterprises whose indicators move between the median and maximum. We achieve the value of the bottom quartile in a similar way. It corresponds with the value of the enterprise indicator which determines the place of the companies achieving lower values of the indicator than the median. The range between the upper and bottom quartile is called the quartile range or also the standard zone. In a very simplified way we can say that the value of the upper and bottom quartile represents the boundary values of the enterprise economic security on the base of financial risks. But, it is necessary to consider system relationships with other partial risks, which could affect determined boundaries.

It is suitable to depict this method graphically for a complex comparison of the particular enterprise's position in the investigated group of enterprises. The maximal and minimal values (variation range), the median and the values of the bottom and upper quartile are marked in the diagram for all selected indicators. Subsequently the values of indicators achieved by the particular enterprise are depicted and they are connected for a better illustration – in this way we create a line of the enterprise's position. If the enterprise's position line bypasses the standard zone, it can show disruptions of the enterprise economic security but also a situation when the enterprise achieves higher economic security than other companies. Thus, correct understanding of the meaning of deviations from the standard depends on a specific asset or indicator.

5. Results

The investigated statistic group consists of 41 enterprises carrying out a similar activity classified as production of motor vehicles. However, their quantitative characteristics are different. The number of employees according to which the companies are divided into micro-enterprises, small enterprises, medium enterprises and large enterprises was taken into account. The Figure 1 shows the structure of the companies from the point of view of employees´ numbers.

Fig. 1. Structure of the enterprises according to their size [13].

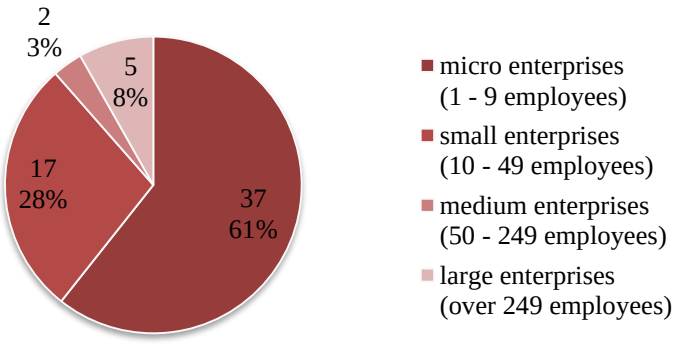


Fig. 1. Structure of the enterprises according to their size [13].

In the first step we acquired information from the financial statements which were used for calculating the financial and economic indicators according to the equation 1 – 11. Subsequently we determined the values of minimum, bottom quartile, median, upper

quartile and maximum for each indicator. The real values were transformed to the percentage ones due to the median which was assigned the value of 100 %. The Table 1shows the transformed values of the variation range for the whole sub-category of the 29.10.0 companies.

Table 1. Variation range.

Indicator	**Designation**	**Variation Range**	
		Minimal Value in %	**Maximal Value in %**
Current Ratio	I1	2.23	16 135.96
Cash Ratio	I2	13.78	11 643.63
Inventory Conversion Period	I3	0.00	41 188.62
Receivables Conversion Period	I4	0.00	1 724.73
Liabilities Conversion Period	I5	0.74	9 240.91
Financial Leverage Ratio	I6	1.10	316.55
Self-financing Ratio	I7	-296.28	297.30
Cash Flow in% of Sales	I8	-3 256.74	822.11
Return on Equity	I9	-6 110.60	31 457.16
Return on Assets	I10	-9 475.51	1 745.87
Return on Investment	I11	-9 369.06	1 726.26

The Table 1 clearly shows the group of enterprises is remarkably heterogeneous. It is demonstrated by the wide variation range. The biggest dispersion of values is recorded in the indicator profitability of the shareholders' equity whose values move from – 6.110.60 % to 31.457.16 %. Due to this fact we used also the classification of the enterprises from the point of view of their size for calculating the boundaries of the economic security (quartile range). The Table 2 depicts the boundaries of the economic security of the enterprise sub-class SK NACE 29.10.0 – the micro-enterprises, small enterprises, medium enterprises and large enterprises.

Table 2. Boundaries of economic security. Q1= Bottom Quartile, Q3 = Upper Quartile.

Indicator	**Boundaries of economic security**									
	29.10.0		**micro-enterprises**		**small enterprises**		**medium enterprises**		**large enterprises**	
	Q1	Q3	Q1	Q3	Q1	Q3	Q1	Q3	Q1	Q3
I1	41.64	266.50	31.75	169.61	56.29	763.63	97.41	102.59	80.36	111.10
I2	60.30	192.31	73.24	176.99	55.97	479.83	94.35	105.65	73.66	110.02
I3	0.00	452.04	0.00	599.07	0.00	305 247.67	93.34	106.66	42.34	168.33
I4	40.27	243.83	27.86	292.22	20.02	149.96	96.39	103.61	79.44	238.41
I5	56.96	314.80	63.29	362.12	56.18	351.79	87.80	112.20	90.14	533.72
I6	52.85	141.89	58.17	151.92	19.20	130.36	86.16	113.84	88.71	107.00
I7	24.10	199.92	35.66	179.78	-103.50	641.53	7.10	192.90	74.88	119.94
I8	1.25	338.04	0.98	266.86	-170.51	403.09	84.03	115.97	33.45	167.59
I9	39.85	294.72	18.99	385.61	41.48	370.70	169.37	30.63	90.32	123.86

I10	-9.82	256.42	-9.82	383.15	-419.73	530.33	85.08	114.92	72.02	133.02
I11	1.42	253.54	1.13	301.54	-419.73	530.33	90.31	109.69	72.50	132.85

The next step compares the economic security of a particular enterprise with the determined boundaries. When we assess the chosen enterprise economic security we compare its values of achieved indicators with the standard (quartile) zone. If the value of indicators is in this zone, the economic security of the X enterprise is maintained. If the values are outside of this zone it is necessary to consider the character of the particular indicator. If it is, e.g. the activity ratios, it is good if the value is as low as possible. On the other hand, the profitability ratios should achieve the highest values. The character of some indicators does not allow assessing directly their influence on the enterprise economic security and then we need a deeper analysis.

One enterprise was chosen from virtually every group (the micro-enterprises, small enterprises and large enterprises). The number of medium-sized enterprises was too small to be able to carry out intercompany comparison.

Firstly, this paper assesses the economic security of ***micro-enterprise*** operating in the region of Zilina. It was founded by one person and was registered in the Trade Register on 11th March 2014. The legal form is a Ltd. Company. Furthermore, it will be designated as X1 enterprise. The graphical depiction of the X1 enterprise's position in the group of indicators, the so called line of the enterprise's position is depicted in red colour – see the Figure 2.

Due to the fact the selected indicators have absolutely different values we completed the results of the situation in the area of the X1 enterprise economic security by a table. The Table 3 shows the real values of the indicators in difference to the Table 2 where the percentage values regarding the median are depicted.

Out of the selected group of indicators five are in the standard zone therefore we can say their values do not disrupt the X1 enterprise economic security. The value of the Current Ratio is moderately over the standard zone. The X1 enterprise is able to pay its short-term liabilities more reliably than other micro-enterprises. However, if the liquidity ratios were too high, it could inform about an inappropriate utilisation of the short-term assets.

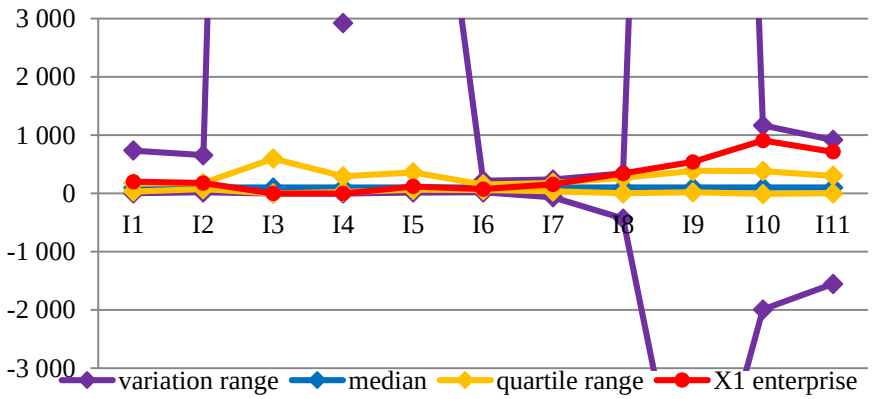


Fig. 2. Line of the enterprise's X1 position.

Table 3. Comparison of X1 enterprise with the boundaries of economic security.

Indicator	**Standard Zone**	**X1 Enterprise**	**State of Economic Security**
Current Ratio	0.38 – 2.03	2.39	Non-Disrupted, Above-Standard
Cash Ratio	0.99 – 2.39	2.39	Non-Disrupted, Upper Quartile
Inventory Conversion Period	0.00 – 107.37	0.00	Non-Disrupted, Bottom Quartile
Receivables Conversion Period	7.60 – 79.75	0.00	Non-Disrupted, Above-Standard
Liabilities Conversion Period	64.66 – 369.92	121.97	Non-Disrupted
Financial Leverage Ratio	33.22 – 86.75	41.82	Non-Disrupted
Self-financing Ratio	0.13 – 0.67	0.58	Non-Disrupted
Cash Flow in% of Sales	0.10 – 26.34	33.71	Non-Disrupted, Above-Standard
Return on Equity	2.51 – 51.07	71.52	Non-Disrupted, Above-Standard
Return on Assets	-0.45 – 17.55	41.61	Non-Disrupted, Above-Standard
Return on Investment	0.07 – 17.55	41.61	Non-Disrupted, Above-Standard

The value of the indicator Inventory Conversion Period at the minimal level and at the same at the level of the bottom quartile does not enable any direct assessment of the X1 enterprise economic security. We need additional information which can be acquired from the financial statements. It shows the X1 enterprise does not create any inventories and therefore this value can be considered safe from the economic point of view.

When we assess the Receivables Conversion Period and Liabilities Conversion Period it is suitable to proceed parallel. As a matter of fact, they also express the payment discipline of the business partners and the X1 enterprise itself. It is suitable for each enterprise when the Receivables Conversion Period is shorter than the Liabilities Conversion Period. We can also say that from the point of view of the Receivables Conversion Period the X1 enterprise achieves above-standard values of the economic security compared with other enterprises.

The indicators of profitability show the return of invested funds. If the values are positive, it means the enterprise achieves a profit, in an opposite case a loss. In all of these indicators the X1 enterprise achieves better values than other micro-companies; its economic security is of an above-standard level. However, it is also inevitable to take into account the fact that the standard zone is affected by a situation when more than one quarter of the micro-enterprises (6 out of 22) achieves loss. Therefore, in practice it would be necessary to check these results by another analysis which would be aimed e.g. at prognosis the future development or a deeper analysis of the cash flows.

Secondly, the economic security of ***small enterprise*** was assessed. It was founded on 21st February 2014 and is operating in the region of Bratislava. The legal form is a Ltd. Company. Furthermore, it will be designated as X2 enterprise.

Economic situation of this enterprise is in red numbers. It achieved losses in both years of its existence even its equity is negative. Due to this fact we can assume, that economic security of enterprise X2 is disrupted. The Figure 3 points up our assumption – the most of the X2 enterprise's line position is situated outside the boundaries of economic security.

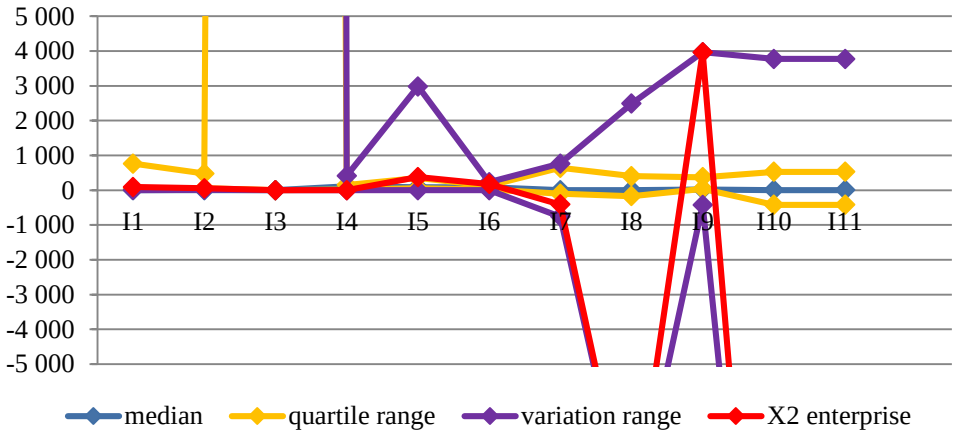


Fig. 3. Line of the enterprise's X2 position.

The Table 4 shows the real values of the indicators in difference to the figure 3 where the percentage values regarding the median are depicted.

Table 4. Comparison of X2 enterprise with the boundaries of economic security.

Indicator	**Standard Zone**	**X2 Enterprise**	**State of Economic Security**
Current Ratio	0.41 – 5.59	0.65	Non-Disrupted
Cash Ratio	0.65 – 5.59	0.65	Non-Disrupted, Bottom Quartile
Inventory Conversion Period	0.00 – 47.17	0.00	Non-Disrupted, Bottom Quartile
Receivables Conversion Period	21.73 – 162.73	0.00	Non-Disrupted, Above-Standard
Liabilities Conversion Period	48.38 – 302.95	323.04	Non-Disrupted, Substandard
Financial Leverage Ratio	16.71 – 113.44	153.44	Disrupted, Substandard
Self-financing Ratio	-0.13 – 0.83	-0.53	Disrupted, Substandard
Cash Flow in% of Sales	-4.39 – 10.38	-253.79	Disrupted. Substandard
Return on Equity	8.49 – 75.89	812.14	Disrupted, Above-Standard
Return on Assets	-8.89 – 11.24	-433.97	Disrupted, Substandard
Return on Investment	-8.89 – 11.24	-433.97	Disrupted, Substandard

Out of selected group of indicators solely tree is in the standard zone therefore we can say their values do not disrupt the X2 enterprise economic security. The value of two of them – Cash Ratio and Inventory Conversion Period – is at the same level of the bottom

quartile. For this reason, we can say that economic security of X2 enterprise is non-disrupted but threatened.

When we assess the indicators of activity we can observe that from the point of view of the Liabilities Conversion Period the X2 enterprise achieves substandard values of the economic security compared with other enterprises.

The indicators of profitability demonstrate significant differences. We need additional information from the financial statements to assuming them. It shows the enterprise X2 achieves a negative economic outcome. In this case, the indicators of profitability should have negative value. Actually, value of Return on Equity is above-standard. This value is misleading. It does not mean the economic security is non-disrupted, it solely shows that both net profit and shareholder equity are negative.

In the third, the economic security of ***large enterprise*** was assessed. It was founded on 3rd March 2011 and is operating in the region of Presov. The legal form is a Ltd. Company. Furthermore, it will be designated as X3 enterprise.

The graphical depiction of the X3 enterprise's position in the group of indicators is depicted in red colour, Figure 4.

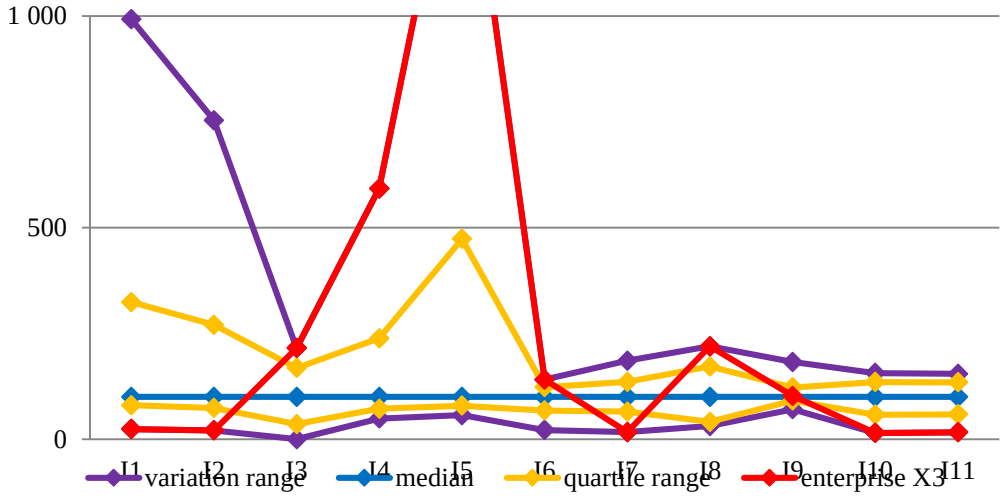


Fig. 4. Line of the enterprise's X3 position.

However, the group consists of solely four large enterprises, their quantitative characteristics are different. The Figure 5 presents structure of large enterprises according to number of employees.

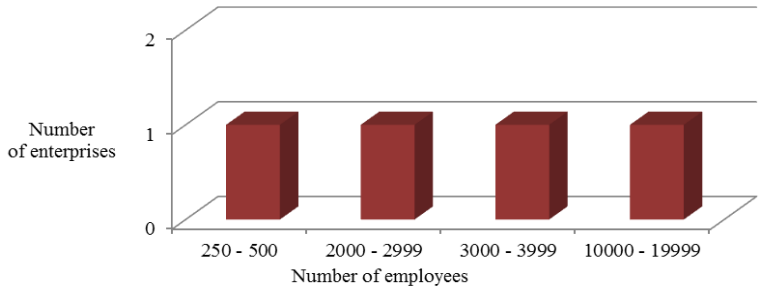


Fig. 5. Structure of the large enterprises according to number of employees [13].

The X3 enterprise is the smallest one. This is the main reason why their results are mostly marginal (10 from 11 indicators).

The Table 5 shows the real values of the indicators and state of X3 enterprise's economic security.

Table 5. Comparison of X3 enterprise with the boundaries of economic security.

Indicator	**Standard Zone**	**X2 Enterprise**	**State of Economic Security**
Current Ratio	0.71 – 2.88	0.21	Disrupted, Substandard
Cash Ratio	0.86 – 3.16	0.25	Disrupted, Substandard
Inventory Conversion Period	4.94 – 23.44	29.98	Disrupted, Above-Standard
Receivables Conversion Period	27.59 – 91.58	227.53	Disrupted, Substandard
Liabilities Conversion Period	54.53 – 325.50	1 068.09	Disrupted, Substandard
Financial Leverage Ratio	35.27 – 64.21	73.50	Non-Disrupted, Substandard
Self-financing Ratio	0.31 – 0.65	0.08	Disrupted, Substandard
Cash Flow in% of Sales	5.92 – 24.75	31.63	Non-Disrupted. Above-Standard
Return on Equity	12.32 – 16.52	13.80	Non-Disrupted
Return on Assets	4.35 – 10.13	1.11	Disrupted, Substandard
Return on Investment	4.46 – 10.21	1.25	Disrupted, Substandard

We can observe that economic security is disrupted almost in every area of enterprise activity. Liquidity and Self-financing Ratio are low. Inventory Conversion Period is long. Although Receivables Conversion Period is shorter than Liabilities Conversion Period they are too long. Financial Leverage Ratio is high, but acceptable. Indicators of profitability are low, even it can be stated that the X3 enterprise does not use credit efficiently (Return on Investment is lower than Return on Equity).

6. Conclusions

The intercompany comparison by the method of the indicators´ variability can be utilised as one of the supporting tools of the risk management. It is possible to reveal the critical points which can disrupt the enterprise economic security by detecting the quartile range of the indicators typical for a certain economic activity and comparing the really achieved values in a certain enterprise.

Due to a limited access to information about indicators characterising the activities of the companies in the selected sub-class, this paper has no ambition to carry out any comprehensive comparison of the companies by the method of the variability of indicators. Its aim is solely to draw attention to a relatively fast and cheap method how the companies are able to compare their economic strength with their competitors and to detect the state of their economic security.

On the base of carried out assessment we can state that:

- the criteria of enterprise`s economic security based on financial risks are significantly influenced by the economic results (profit or loss) of enterprises included into statistic group,
- informative ability of criteria is influenced by the amount of enterprises included into the statistic group,
- it is very important to analyse the financial statements and other reports providing information about enterprise activities in assessing the status of a particular enterprise. Only this way it could be captured the relationship with other partial risks.

If the enterprise wanted to carry out a complete analysis, it can use the services of those companies that deal with providing information for managing the business and entrepreneurial risks. However, there is a condition – to purchase the licence which can represent a high cost item for companies with a small number of employees and a low turnover. And just for such companies there is a solution – there is publicly available information in the Register of Financial Statements established by the Ministry of Finance of the Slovak Republic (as mentioned in this paper).

Acknowledgment

This paper was created with the support of the project „Solving Economic Risks in Small and Medium Enterprises.

References

[15] KELÍŠEK, A., KLUČKA, J., ONDRUŠEK, M., STRELCOVÁ, S. Economic Security – a Principal Component of Multilevel Security Concept in Global Economy. *Communications: scientific letters of the University of Žilina.* ISSN: 1335-4205, 13 (2011), 2, pp. 44 – 48.

[16] STRELCOVÁ, S. *Ekonomická bezpečnosť* (In Slovak). ISBN: 978-80-554-1061-6. Žilina: Žilinská univerzita 2015.

[17] VAUGHAN E. J., VAUGHAN T. M. *Fundamentals of Risk and Insurance*. ISBN: 13 978-0-47008753-4. New York: John Viley & Sons 2008.

[18] CHOD, J., ZHOU, J. Resource Flexibility and Capital Structure. *Management Science*, ISSN: 0025-1909, 860 (2014), 3, pp. 708-729.

[19] STRELCOVA, S., REHAK, D., JOHNSON, D. E. A. Influence of Critical Infrastructure on Enterprise Economic Security. *Communications: scientific letters of the University of Žilina.* ISSN: 1335-4205, 17 (2015), 1, pp. 105-110.

[20] SINHA, S. Understanding Industrial Espionage for Greater Technological and Economic Security. *IEEE Potentials.* ISSN: 0278-6648, 31 (2012), 3. pp. 37-41,

[21] SEDLÁK, M. et al. *Podnikové hospodárstvo* (In Slovak). ISBN: 978-808-8078-317-4 Bratislava: Iura Edition 2010.

[22] ŠÍBL. D. a kol. 2002. *Veľká ekonomická encyklopédia. Výkladový slovník.* ISBN: 80-89085-04-0. Bratislava: Sprint, 2002.

[23] SR. Zákon 513/1991, obchodný zákonník. *Zbierka zákonov č. 98/1991*, pp. 2474. https://www.slovlex.sk/static/pdf/1991/513/ZZ_1991_513_20160701.pdf

[24] KUPKOVIČ, M. et al. *Podnikové hospodárstvo* (In Slovak). ISBN: 80-88848-71-7., Bratislava: Sprint vfra, 2003.

[25] STRELCOVÁ, S. Ekonomická bezpečnosť podniku (In Slovak). *Security Revue*. ISSN: 1336-9717.http://www.securityrevue.com/article/2012/10/ekonomicka-bez pecnost-podniku/
[26] ŠIMÁK, L., KLUČKA, J., STRELCOVÁ, S. Modulácia hraničných hodnôt ekonomickej bezpečnosti podnikov (In Slovak). *Ekonomika poľnohospodárstva*. ISSN: 1335-6186, 14 (2014), 2, pp. 89-104.
[27] SR. Register účtovných závierok (In Slovak). Bratislava: Ministerstvo financií Slovenskej republiky. http://www.registeruz.sk/cruz-public/domain/accounting enti yy/simple search
[28] ŠINDELÁŘ, J., EISLER, J. *Rozbor hospodárské činnosti dopravy* (In Slovak). Praha: VŠE 1986.
[29] KUBÍČKOVÁ, D., JINDŘICHOVSKÁ, I. *Finanční analýza a hodnocení výkonnosti firmy* (In Czech). ISBN:978-80-7400-538-1. Praha: Nakladatelství C. H. Beck 2015.

Chapter 9

MARKETING COMMUNICATION RELATED TO CARRIER – CUSTOMER RELATIONSHIP IN EMERGENCY SITUATIONS

1. Introduction

Communication with customers is an essential marketing process. By nature, it runs continuously, the content and form of communication are determined by its goal. In terms of marketing, communication with customers during emergencies comes under crisis communication and as such is a part of public relations (PR). It all implies its goals as described e. g. in Jozef Ftorek´s definition: *"Crisis communication is specific communication of a company or institution in emergency situations where the stability, security and/or reputation are compromised by emergencies or negative publicity. The goal of crisis communication is to prepare and release effective information or eliminate negative publicity in order to minimize the damage caused by the newly-emerged communication situation – crisis."* [1].

The process of communication with customers has its risks that can be defined as presumable amount of loss, damage and injury on protected assets upon the occurrence of a harmful effect [2]. We focus on partial risk of injury on protected asset - the good reputation of a carrier company in case of harmful effect occurrence - emergency situation. Protected asset in this case has specific characteristics of an intangible nature and its value cannot often be properly quantified. To calculate the goodwill of a company is quite difficult and several possible approaches can be used in regard to this matter. Purely economic/accounting approach is widely but not always used in the Czech Republic. Its display can be seen, for example, in reporting goodwill of the company among long-term assets on the balance sheet. As it is difficult to calculate business goodwill, so is the calculation of loss or injury and therefore the risk itself. Nevertheless, this issue should not be overlooked.

Companies operating in transportation services may be affected by the same type of crisis as any other businesses. Emergency situations play a specific role among a wide range of possible communication situations. This includes both incidents as defined by Act no. 239/2000 Coll., on the Integrated Rescue System, as well as accidents and threats defined e.g. by Act no. 266/1994 Coll., on Railways or Act no. 361/2000 Coll., on Road Traffic. Nowadays, carriers have prepared contingency plans for such situations. Within their framework or follow-up operational rules, the communication with customers (participants of emergency situations) is treated with care. The basic objective of such a communication is to transfer all the information needed to minimize damage to the health and lives of people and property. In such situations the objective of crisis communication in the concept of PR, thus minimizing damage to the reputation of the company and negative publicity, recedes into the background.

***Author:** Dipl. Ing. Alexandra Dvořáčková. Czech Technical University in Prague. Děčín. Czech Republic. dvorackova@fd.cvut.cz.

However, in less serious cases, the above described objective of communicating with customers should have priority. In cases of poor communication with passengers' companies of public transportation are more vulnerable to the negative impact on the reputation of the company regardless of the severity of property damage. These negative impacts are often underestimated.

Typical situations with potentially high reputation risks are often related to limited or delayed operation due to imminent emergencies or situations that have just occurred, such as road accidents, infrastructure disruptions by natural disasters or technical failure. Such primary incidents give rise to temporary traffic restrictions which, in terms of marketing, can be seen as just other situations requiring emergency communication. Passengers often do not know the original cause of service restrictions and can assess their discomfort as unsatisfactory customer care on carrier´s part. Early and open communication with customers may have a major impact on long-term perception of the quality of services and the quality of the carrier itself.

Communication with customers is also subject to measurement and evaluation as well as other business processes. Marketing uses many tools to measure the effectiveness of communication, both quantitative and qualitative. The predominant criterion for communication efficiency is the degree of achievement of expected communication objectives. Tools based on qualitative methods are becoming increasingly important in cases of communication with customers during emergencies. However, it is necessary to take into account psychological and ethical aspects when used and when results are interpreted.

2. Background research

2.1. Measurement and evaluation of communication

Measuring the effectiveness of communication is one of the major problems of marketing. Measuring communication with customers as part of CRM (Customer Relationship Management) faces the same problems as the measurement and evaluation of PR activities.

Especially in those cases where specialized PR companies and media agencies provide measuring services, their efficiency used to be evaluated in combination of several indicators that quantified provided services. Those included in implemented media outputs can be mentioned:

1. Clipping: evaluation by number of articles or view posts; other indicators such as circulation, readership or article positon on the site may be also taken into account.
2. AVE (Advertising Value Equivalent) compares the value of 'editorial space' with the price of the same amount of space in advertising. Basic information that this indicator reveals is how much less was needed to pay in comparison with paid advertising. It does not take into account either the tone of the message, not the media focus on the target group or other important aspects. However, it is easily measurable indicator and thanks to its financial character it can be conducted as an indicator measuring the effectiveness of communication.

In cases where the communication takes place via electronic media (typically a website, Facebook, or Twitter), such measuring criteria are used which can be tracked very easily via electronic media. There are web analysis tools, even social networks

analysis tools. According to the portal w3techs.com that provides information on the usage of various types of technologies on the web and is updated daily, on January 14, 2017 34.4% of the websites used none of the traffic analysis tools that are monitored there. The most famous tool is Google Analytics. It was used by 54.7% of all the websites, which is a traffic analysis tool market share of 83.4% [3].

Following indicators are observed most frequently, even though there can be set much more sophisticated indicators when using web analytics tools:

1. Number of community members.
2. Number of subscribers of RSS channel.
3. Number of registrations in application or subscriptions to newsletter.
4. Number of article views (Page view statistics).
5. Number of comments.
6. Number of links.
7. Number of visits coming from links.
8. Percentage of new and returning customers.
9. Percentage of visitors in a particular segment.
10. Percentage of visits that lasted long, medium and short period of time.
11. Ratio vote on comments and information; "I like it" and "I do not like" (like / dislike rate).

Relatively easy availability and cost efficiency of this type of indicator monitoring, results in their widespread use. In many cases, such monitoring is considered a measurement of the communication effectiveness.

However, PR professionals point out that quantitative evaluation of communication output does not correspond with measuring the effectiveness of communication. This issue has long been dedicated to the International Association for Measurement and Evaluation of Communication (AMEC). On its website AMEC presents itself as the world's largest media intelligence and insights professional organisation, representing organisations and practitioners who provide media evaluation and communication research. AMEC currently has more than 150 members in 86 countries worldwide. AMEC's pioneering work in the field has included the development of the Barcelona Principles; Barcelona Principles 2.0 and bridge most recently the launch of the AMEC Integrated Evaluation Framework [4]. After a broad discussion AMEC has formulated the basic principles that should be followed when measuring PR activities. These so-called Barcelona Principles were published in 2010 and in 2015 have been updated. Briefly, they can be summarized as follows by AMEC [5]:

1. ***Principle 1:***
   2010: Importance of Goal Setting and Measurement
   2015: Goal Setting and Measurement are Fundamental to Communication and PR
2. ***Principle 2:***
   2010: Measuring the Effect on Outcomes is Preferred to Measuring Outputs
   2015: Measuring Communication Outcomes is Recommended Versus Only Measuring Outputs
3. ***Principle 3:***
   2010: The Effect on Business Results Can and Should Be Measured Where Possible
   2015: The Effect on Organizational Performance Can and Should Be Measured Where Possible
4. ***Principle 4:***

2010: Media Measurement Requires Quantity and Quality
2015: Measurement and Evaluation Require Both Qualitative and Quantitative Methods

5. ***Principle 5:***
   2010: AVEs are not the Value of Public Relations
   2015: AVEs are not the Value of Communications
6. ***Principle 6:***
   2010: Social Media Can and Should Be Measured
   2015: Social Media Can and Should Be Measured Consistently with Other Media Channels
7. ***Principle 7:***
   2010: Transparency and Replicability are Paramount to Sound Measurement
   2015: Measurement and Evaluation Should Be Transparent, Consistent and Valid

In their supporting material 'The PR Professionals Guide to Measurement' the authors mention other examples of indicators that could be used meaningfully, such as:

1. KPI (Key Performance Indicators): a company sets these indicators itself so they can depict specific situation of the company, if possible, in relation to economic indicators. According to AMEC Glossary KPIs must be defined to reflect objectives and strategy, and will be sufficiently robust for the measurement to be repeatable. Quantitative KPIs can be presented as a number, ratio or percentage. KPI's tend to be:
   a. Quantitative indicators which can be presented as a number.
   b. Practical indicators that interface with existing company processes.
   c. Directional indicators specifying whether organisational performance is improving or not.
   d. Actionable indicators sufficiently in an organisation's control to effect change.
   e. Financial indicators used in performance measurement and when looking at an operating index [7].
2. ROI (Return on Investment) measures the amount of return on an investment relative to the investment's cost. It is a simple and clear indicator but in PR it faces a fundamental problem - it does not reflect those types of non-financial benefits such as increasing brand awareness and improved company's reputation with the public.
3. Comparison of the values of selected indicators before and after the assessment of events / campaigns: It is obvious that these indicators are closer to the effectiveness of communication in terms of achievement of the objectives. Their practical application, however, is knowledge-intensive and time-consuming.

This may also be the reason why, according to the results of some research studies, 65% of small firms and 60% of advertising agencies in the Czech Republic do not deal with measurement of efficiency. The vast majority of cases where the efficiency measurement is used and is related to advertising campaigns [8].

2.2 Emergency situations in transport

According to the Act no. 239/2000 Coll., on the Integrated Rescue System, an emergency is viewed as *"harmful effects of forces and phenomena caused by human activity, natural effects and also accidents that threaten life, health, property or the environment and require rescue and relief work"* [9]. When a crisis situation occurs, authorities may declare a correspondent state of emergency, i.e. during a time of natural

or human-made disaster, during a period of civil unrest, or following a declaration of war. It is important to realize that the term 'crisis situation' is often, even in the media, used incorrectly. In terms of crisis management, a road accident is not considered to be a crisis situation. Emergency situations arise in connection with impending situations or the ones which have already occurred.

Emergency situations, for example in rail transport, are defined in § 49 of Act no. 266/1994 Coll. on Railways. We differentiate serious accidents, accidents and emergency situations:

1. Serious accidents in rail transport are collisions or derailments of rail vehicles which occurred during rail transport operations, causing death or injury of at least five individuals or extensive damage (within the meaning of the Penal Code).
2. Accidents in rail transport are situations which occurred during rail transport operations, causing death, injury or significant damage (within the meaning of the Penal Code).
3. Emergency is different situation that endangers or impairs safety, regularity and smoothness of rail transport, the safety of people and the safe operation of buildings and facilities or endangers the environment [10].

Railway transport covers not only rail transport as perceived by common passengers; it also includes metro, tram, trolleybus and cable car operations. Therefore, emergency situation in rail transport becomes a traffic accident in road traffic, if there is an accident on a level crossing or in case of an accident of a trolleybus or tram.

Emergency situations in road transport are represented by serious accidents with consequent restriction of traffic on roads or disruption of infrastructure and traffic on it as a result of natural disasters, climatic phenomena or human action. Such diverse situations starting from traffic accidents with the need for time-consuming extrication work or with damage to infrastructure due to hazardous substance spill, landslide or floods and ending with dangerous but common black ice are included in the list.

In terms of marketing communication with customers/passengers, emergency can be described as a situation when the range of transport and shipping services is temporarily limited. In a narrow sense, it is limitation due to unexpected events, which means that this approach would not include e.g. planned track closures.

2.3 Communication with customers throughout emergency situations

As mentioned above, efficiency is considered to be a level of achieving (or facilitation of achieving) a stated objective when it comes to communication with a customer. In the case of communication between a carrier and its customer (i.e. a passenger) during emergency situations, the objective is basically determined by the seriousness of the given emergency and the passenger's involvement.

1. The passenger is a direct participant in the emergency in the form of a mass accident: the basic objective of the communication is to transmit all information necessary to minimize damage to health and lives of people and damage to property. A secondary objective with a much lower priority may represent the target state when the passenger is convinced that the carrier took care of its passengers in the best way possible given the situation, and that the benefit of passengers was the key objective for the carrier.
2. The passenger is influenced by consequences of an emergency without being a direct participant therein: in transportation, these include situations when the emergency led to temporary limitations of transportation and provided services (delays of trains on a

track afflicted by a traffic accident, diversion of the journey, or stoppage of metro or trolleybus operation due to disruption in electricity). In such cases, the communication objective is to limit any negative impact on reputation of the carrier by providing the passengers with information about the cause of the situation, about activities which the carrier performs in order to remedy the situation, and possible compensation for passengers.

In these situations, the achievement of the above specified objectives of communication is measurable only to a certain limit. It is clear that even with these established objectives of communication, the utilized methods are not always based on quantitative data. It is the communication with passengers during emergencies itself that is the best evidence of the fact that purely quantitative data fail to hold sufficient explanatory power. The values of indicators, such as number of articles or views, are significantly increasing during emergencies, both in the case of articles in standard media or numbers of reactions and comments on social networks.

The same applies to share ratios, such as the ratio of new and returning visitors, ratios of inquiries and complaints, etc. In analogy, also the value of AVE is increasing in an extreme manner during such situations, since it is influenced by the volume of media space given to the emergency and the representatives of the carrier. The examples of emergencies described in chapter 5 (number of contacts with customers during a black ice calamity or during the accident in Studenka) clearly show that these extremely high values during emergencies do not imply neither impact on reputation in any way, nor the customers' opinion regarding the carrier's company.

As for the abovementioned indicators, we can use, for example, the number of viewing an article or a post, the number of comments, like/dislike rate and similar indicators. However, when interpreting the results, we have to bear in mind that these indicators only quantitatively characterize the reach of the carrier's communication towards the customers, not its effect. In order to be able to assess, at least in an indicative manner, the impact on the good name of a company, also other indicators have to be taken into consideration – the tone of the messages, posts, comments and their sharing, e.g. by following the like/dislike rate while dividing the posts to positive and negative ones, etc. Such assessment is hard to automate, and it is therefore more expensive and time consuming.

Another option for measuring negative impact of an emergency on the good name of a company is to compare the values of indicators such as 'brand perception' or 'loyalty of customers' before and after the given emergency. However, this option requires implementation of rather extensive marketing surveys. Especially in cases when the carrier wants to distinguish between the impact on its reputation caused by the emergency itself and the impact caused by unsuitable or insufficient communication, it is desirable to hire specialized companies to carry out these surveys.

In such cases, the most suitable methods in view of their informative value are methods using focus groups or in-depth interviews. Yet these are methods which demand proper execution (it is essential that a professional – a psychologist performs them) and their subsequent evaluation. Besides these, especially in cases of serious emergencies, such survey focusing on customers' attitudes towards the brand (carrier) may encounter ethical limitations right after the person experienced such traumatic situation.

3. Data description and methods

This article includes the findings of preliminary surveys done in January 2017 as a precursor to anticipated research on the theme of end-user communication in transportation. The survey took the form of a loosely structured interview with representatives of selected public passenger transport companies in the Czech Republic. The respondents were organizations that provide nationwide railway transport, coach lines at the national and regional level, and, through the Czech Association of Transport Companies, municipal public transport companies as well. Of those solicited for participation, a total of 14 carriers agreed to take part in the survey, including 13 municipal public transport companies and Czech Railways (České drahy, a.s.). Other railway carriers and coach transport agencies waved participation in the preliminary survey, but expressed interest in participating in the anticipated research.

The interview consisted of 11 questions addressing issues of the use of social media for communication with end-users as well as measurement and evaluation of communications. Interviewees were competent representatives of the companies in question, primarily supervisors in the public relations, communications, or marketing departments, or, in some cases, top-level managers. Answers were recorded on a separate report page for each company and then collected into a comprehensive report. The answers were then supplemented with a content analysis of publicly available information for each of the respondent companies, e.g. web sites, social media profiles, annual reports, and relevant press releases.

4. Results

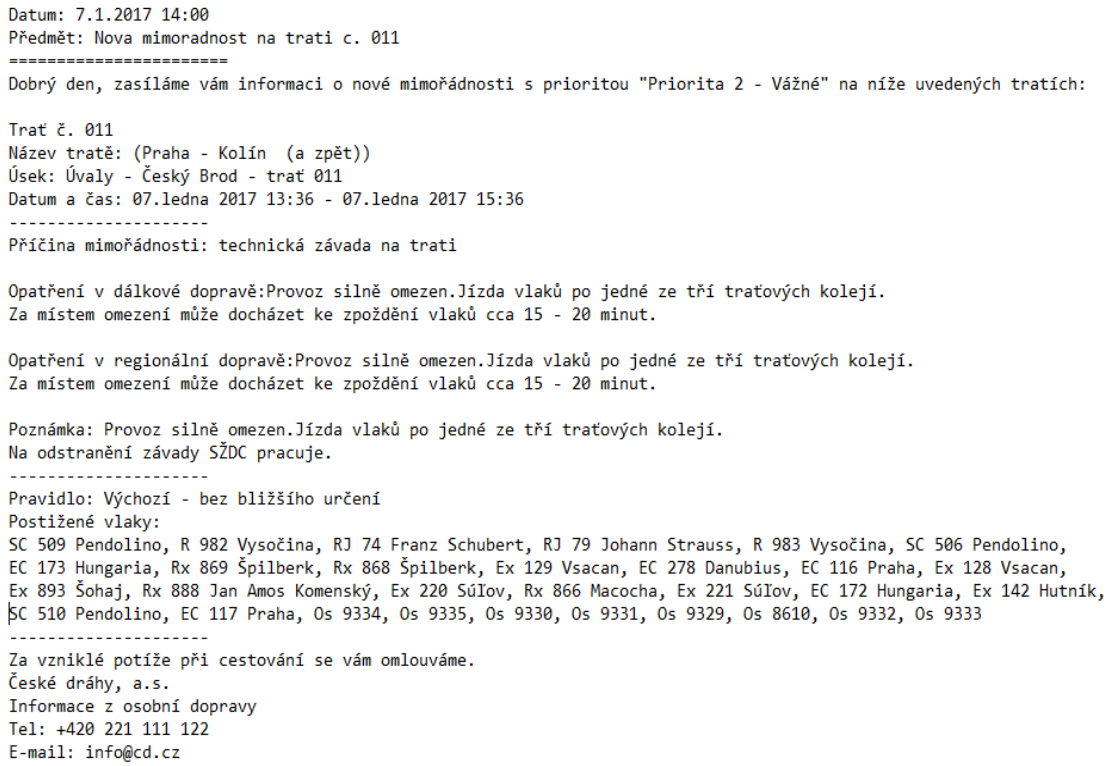
4.1. Carrier communication channels – case study Czech Railways (ČD)

The keystone of the public passenger information system used in special situations is the MIMO system, into which dispatchers enter information about closures (planned operational restrictions) and disruptions (unplanned operational restrictions) [11]. This information originates primarily from the rail transport infrastructure administrator (SŽDC) but processing and distribution is the responsibility of Czech Railways. The following inputs are entered into the system: the segment affected, cause, duration, affected trains, and comments. Each event is rated at a level of seriousness from the lowest (e.g. cases where just one track is open, resulting in delays) to the highest (complete cessation of operations on main lines). MIMO is an internal system, serving the dispatching administration, and is not primarily meant for public consumption. It is, however, a system that collects, in real time, all relevant data about anomalous events. Information from MIMO finds its way to passengers by three main routes:

1. ***Directly.***

   A fundamental role in direct communication is played by the electronic media. Information may be provided in whole or in part. The most comprehensive portal for travellers is the web site http://www.cd.cz/omezeniprovozu/, and a selection of the major situations appears in an orange box on the carrier's main web site www.cd.cz and its mobile page m.cd.cz. Information may be provided selectively, in which case only travellers who are likely to be affected receive the information. In this case the information is filtered to users searching the web-based route planner IDOS, the route planner at cd.cz, or the Czech Railways mobile application, or is sent by email to users

who have registered for updates on certain segments. An example of an email announcing a disruption for a client who has registered for updates is shown in Figure 1 (translated in annex).



```
Datum: 7.1.2017 14:00
Předmět: Nova mimoradnost na trati c. 011
=======================
Dobrý den, zasíláme vám informaci o nové mimořádnosti s prioritou "Priorita 2 - Vážné" na níže uvedených tratích:

Trať č. 011
Název tratě: (Praha - Kolín  (a zpět))
Úsek: Úvaly - Český Brod - trať 011
Datum a čas: 07.ledna 2017 13:36 - 07.ledna 2017 15:36
---------------------
Příčina mimořádnosti: technická závada na trati

Opatření v dálkové dopravě:Provoz silně omezen.Jízda vlaků po jedné ze tří traťových kolejí.
Za místem omezení může docházet ke zpoždění vlaků cca 15 - 20 minut.

Opatření v regionální dopravě:Provoz silně omezen.Jízda vlaků po jedné ze tří traťových kolejí.
Za místem omezení může docházet ke zpoždění vlaků cca 15 - 20 minut.

Poznámka: Provoz silně omezen.Jízda vlaků po jedné ze tří traťových kolejí.
Na odstranění závady SŽDC pracuje.
---------------------
Pravidlo: Výchozí - bez bližšího určení
Postižené vlaky:
SC 509 Pendolino, R 982 Vysočina, RJ 74 Franz Schubert, RJ 79 Johann Strauss, R 983 Vysočina, SC 506 Pendolino,
EC 173 Hungaria, Rx 869 Špilberk, Rx 868 Špilberk, Ex 129 Vsacan, EC 278 Danubius, EC 116 Praha, Ex 128 Vsacan,
Ex 893 Šohaj, Rx 888 Jan Amos Komenský, Ex 220 SúĽov, Rx 866 Macocha, Ex 221 SúĽov, EC 172 Hungaria, Ex 142 Hutník,
SC 510 Pendolino, EC 117 Praha, Os 9334, Os 9335, Os 9330, Os 9331, Os 9329, Os 8610, Os 9332, Os 9333
---------------------
Za vzniklé potíže při cestování se vám omlouváme.
České dráhy, a.s.
Informace z osobní dopravy
Tel: +420 221 111 122
E-mail: info@cd.cz
```

Fig. 1. Example or report (translation in Annex 1).

Another on-line method for informing about disruptions in operations is the official Czech Railways Twitter account, which is automatically fed information from the MIMO system – https://twitter.com/cdmimoradnosti/.

A benefit of the use of electronic media is that the transfer of information is often automated, so it presents an effortless communications channel. The fundamental condition, however, is the willingness and ability of travellers to use these channels at a given moment. This potential drawback may be partially eliminated by the proper selection of technologies. For example, with the mobile application *Můj Vlak*, travellers can set their own notification options. If a traveller does so, he will receive updates throughout the journey about delays, closures, and disruption (as they happen) including measures taken (detours, alternative coach transport, etc.). Examples of disruption and closure alerts in real time via notification through the mobile application are shown in Figure 2.

It should also be born in mind that this is a channel intended primarily for one-way communication from carrier to rider. In comparison to classic communication channels, however, electronic media is better suited to handle a situation when there are tens of thousands of people on trains at any given moment who need the fastest possible information.

An example of the marketing tool of *advocacy*, where loyal customers and fans promote a company, might be found in the Facebook profile *@ceskedrahy01*, the home of "Czech Railways – operational disruptions," which bears the notice "This is an unofficial page of Czech Railways dedicated especially to updates in operations" (https://cs-cz.facebook.com/ceskedrahy01/#) [11]. An example of information for riders about a disruption in service is shown in Figure 3.

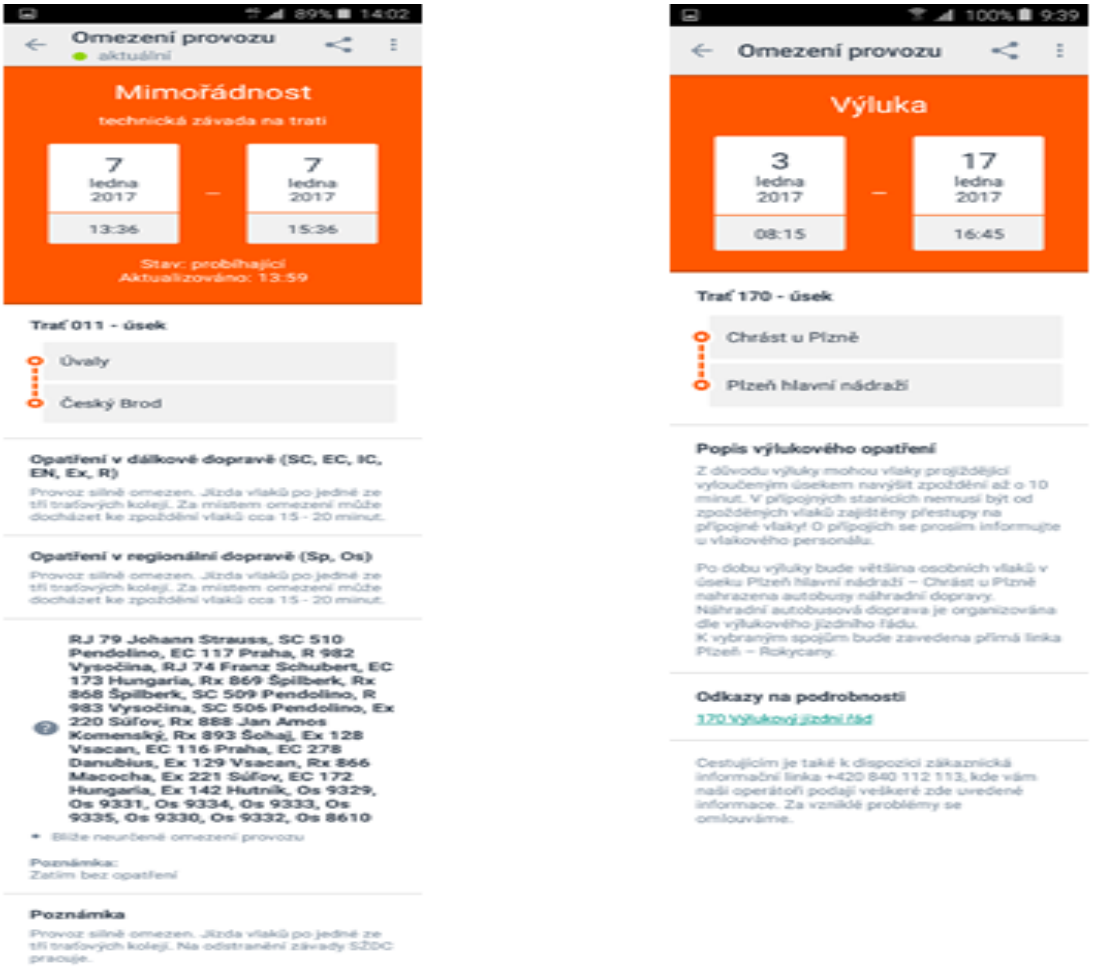


Fig. 2. Disruption and closure information as displayed on the application *Můj Vlak* (source Czech Railways 2017, www.ceskedrahy.cz)

2. Through train personnel.

This is the primary informational channel for travellers who are already on their way when a disruption occurs and are not momentarily using electronic communications channels. Train personnel obtain information in various ways:

- mobile individual registers (POP), with which all conductors are equipped, receive automatic updates about disruptions [13],
- mobile telephones, with which train personnel are also equipped. Notice of important disruptions is sent by text message (SMS) as shown in Figure 4. Train personnel can also get information through the mobile application *Můj Vlak* or the web site. Above all, a call can be made with the dispatcher directly.

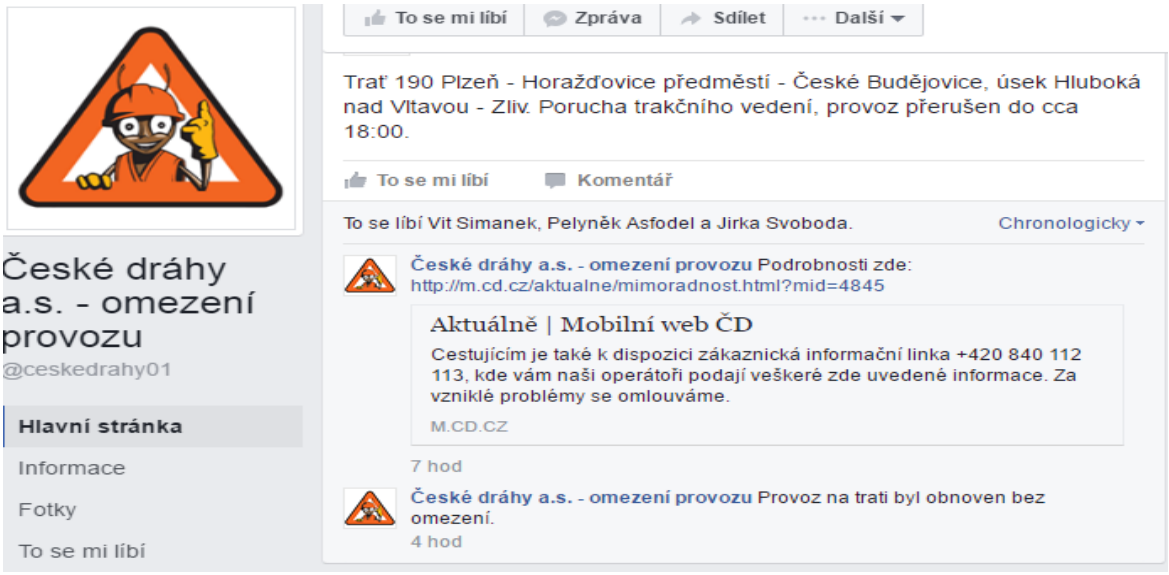


Fig. 3. Announcement of a disruption in service via an unofficial profile on social media [12] (translation in Annex 2).

Fig. 4. Informational text message about a disruption sent to train personnel (source: Czech Railways 2017, www.ceskedrahy.cz); translation in Annex 3.

At the current time, Czech Railways is testing its own chat application for its operational staff. After tests conducted in August 2016 it appears that the system works on data networks dependably; if the signal is weak, the application can translate information into the form of SMS messages and send that way, which means that information about events on the line reach train crews and dispatchers within seconds [14].

In wagons equipped with intercom service, the crew announces available information about journey disruptions. Where an intercom is not available, the conductor walks through to make the announcement. Yet, even this information channel is subject to the limits of its human actors. It must be kept in mind that, in a disruption situation, train personnel may have other responsibilities related to

ensuring safety and minimalizing unwanted outcomes; informing riders in tense situations is often not the main priority.

3. Through station personnel.

The main actors in this scenario are staff at ticket windows and information booths in the railway station. When selling a ticket for a given segment, the agent will see adisruptions displayed in an orange box on his monitor. The ticket agent should open the warning and relay the information to the traveller. The information booth clerk would proceed in a similar fashion. This information channel is also susceptible to human limitations (e.g., the hurried pace at rush hour). Furthermore, it can only reach those riders who are at the start of their journey and are interacting with station personnel when a disruption takes place. It is of no use to riders who do not need to purchase a ticket (e.g., regular riders with some form of pass) and does not serve those who are already aboard.

The primary channel for two-way communication is the Czech Railways contact center. In the event of a disruption, it serves as the front line for providing information to customers and is driven by their specific needs. In such cases, the most common form of communication is by telephone, although email communication is also used in connection with such events. It goes without saying that the contact center also provides information about transfers, fares, e-shop transactions, and so on.

Some examples and quantitative date related to the activity of the contact center will serve to demonstrate the various types of disruptions and the reactions they evoke in riders:

1. Long-term disruptions in quality of service:

   In 2015, major construction was being done on the railway network in the Czech Republic to maintain and modernize transport routes. This resulted in extensive re-routing of traffic for all rail carriers. According to Czech Railways data [15] the contact center recorded more than 100 thousand calls in June 2015, roughly a 100% increase in volume from the same period the previous year. The daily average volume of telephone calls for this period was roughly 3,000 whereas at the end of 2014 it averaged 1,500 [16]. The contact center supervisor, Mr. Gregor, reports that a decisive impact was made by the long-term disruptions at that time. Riders asked primarily about transfers, delays, and replacement coach service.

   This sort of disruption has a high potential to damage the reputation and good name of a carrier. The comfort of the rider is affected, but from his perspective the causes are not so serious as to excuse the reduction in quality of service as it would be in the case of a fatality-inducing accident on the lines, for example. The willingness of the rider to tolerate a reduced quality of service also naturally decreases with the length of time that the disruption continues and the risk of customer dissatisfaction is perceptibly higher than in the case of isolated disruption events. In such situations, proper communication with riders is the deciding factor and represents the only way that a carrier can alleviate customer displeasure and possibly even prevent his flight to the competition with all of the risks of negative impact on the carrier's reputation therein.

2. Short-term disruptions caused by acts of God:

   A typical cause of such disruptions is a natural disaster, which often intrudes into other areas of a rider's life beyond the carrier's services. The ice storm of December 2014 is one example. Unfavorable meteorological conditions on December 1–3 caused a collapse in public transportation across the country. Ice on the trolley lines

made electrical traction impossible, affecting roughly 100,000 commuters, according to data from the Ministry of Transport and Czech Railways [16]. There were roughly 20,000 passengers stranded on 120 trains. The flow of information to these passengers was limited by overloaded telephone lines between train personnel and dispatchers, so even the train crews themselves often lacked information about measures to be taken or how long the situation was expected to last. The contact centre, as the information channel for direct communication with customers was able to test its capacity for immediate communication (by telephone conversation) and delayed communication (e-mail). At a time when the average daily calls were around 1,500, the call centre logged 4,000 calls on the first day of the calamity and 8,000 on day two; it received roughly 800 emails through info.cd and another 400 through emails addressed to the management of Czech Railways. A later evaluation of Czech Railways response to the calamity resulted in the hire of additional dispatch staff and the decision to adopt measures related to crisis communications. In 2015 the contact centre was moved to new, better equipped quarters and its staff was significantly increased.

From a marketing perspective, such situations present a high risk of reputation damage. The impact on customer perceptions depends on a number of factors – because the problem was caused by an act of God, riders may have a greater understanding for necessary restrictions or reduced services. This potential good will can be entirely expended, however, in cases where the rider has the impression that the carrier did not pay enough attention to his needs. This impression can be entirely subjective and can be influenced by appropriate communications. The ice storm demonstrated how vastly different riders 'reactions were depending upon how well informed they were of the situation. Thus, the Czech Railways decision concerning its communication strategy can be assessed positively, both as to strengthening direct communication with customers (e.g. by expanding the contact centre capacity or utilizing social media) and as to strengthening technical means of transferring information from dispatchers to station and train personnel.

3. Isolated short-term disruptions:

In transportation, such disruptions are most often caused by serious traffic accidents. A typical example might be the incident in Studenka on 22 July 2015, when a Pendolino train hit a lorry that had violated the right of way at a railway crossing. The accident left three dead and 17 injured some permanently. Material damages came to over 150 million Czech crowns. All rail traffic on the Suchdol nad Odrou – Jistebník segment was immediately stopped for roughly 13 hours, with 20 coaches providing alternative transport. According to Czech Railways data [15], [17] the event caused the delay of 126 trains for a total of 5,127 minutes. The Brno region dispatch office fed information to impacted staff in 1,500 calls totalling over 1,000 minutes, which is three or four times the usual load. The contact centre logged 5,300 customer calls relating to this incident (a daily average of 1,500 calls), of which 20 calls were with passengers sitting on the train involved in the incident. In addition, Czech Railways and the Moravian-Silesian Regional Fire Department set up a crisis hotline, through which they offered help and psychological support. Immediately following the accident, the carrier also set up a special hotline for those who had suffered injuries or damage, to enable damage claims to be made. On the very day of the accident the carrier also made public its terms for payment of damages, stating that it would honour damage deposit levels set by European legislation whether the payments correspond

to the injuries or damage caused by the accident or not and that Czech Railways would then collect any difference from the person who had caused the accident.

This sort of incident does not present a great risk to the carrier's reputation so long as the carrier is not clearly at fault and so long as it adheres to general rules of communication in crisis situations. Of prime importance is the release of timely, brief, and constructive statements in cooperation with the emergency services and the elimination of concrete measures to repair damages and mitigate consequences. In cases where the company is not as clearly free of fault as in the case above, there should be a timely, public attempt made to clarify matters through investigative bodies such as the Rail Safety Inspection.

4.2. Issues arising from preliminary research poll

In order to hold semi-structured interviews with 14 representatives of companies providing public passenger transport in the Czech Republic, 11 questions were prepared, which were thematically focused on using social networks for communication with customers and measurement and evaluation of the communication.

It was found that all of the companies except one have their own profiles on some of the social networks that are used to communicate with customers. By far the highest proportion of the used social networks has Facebook. A Facebook profile is used by 13 companies, one company is examining the possibility and appropriateness of setting up their own profile. Other represented social networks are Twitter, Instagram, YouTube and Google +. Four businesses have an Instagram profile, three carriers run an official company YouTube channel. Three companies have a Twitter profile and one carrier manages their own Google+ profile.

Six carriers, who have their profiles on more than one social network, differentiate their content. An example might be the company Czech Railways. Their Facebook profile is used as a classic marketing tool that is content-oriented on entertainment, advertising and PR. The profile functions as a two-way channel; the carrier takes into account posts of users and replies to their inquiries. In case of complex queries, users are referred to the Contact Centre. Information about extraordinary events in traffic are not communicated on this profile; the carrier in this way reflects the existence of an unofficial Facebook profile called 'Omezení provozu' (Restricted traffic), which is run by the colleagues and fans of the company. The official Instagram profile of Czech Railways functions as a one-way communication channel that is content-oriented on the company's image. In contrast, the official Twitter profile is designated exclusively for extraordinary events in traffic; information from the dispatcher system MIMO is automatically routed here.

Twelve participating carriers said that they used social networks to inform passengers about extraordinary events such as traffic restrictions, traffic closures, substitute connections and the like. One of the carriers even has two official profiles on Facebook, Twitter and Instagram, one of which is intended for marketing and PR content and the other profile passes current traffic information. Apart from this way, all of the carriers also give information about extraordinary events via their websites. The dominant method of announcing such events on the websites is in the News section, or in the section entitled directly Extraordinary events or Traffic restrictions. However, it is always on the homepage. Nine carriers also provide RSS feed on their websites. Two carriers said that customers interested to receive news through RSS can choose; RSS can be divided into

news, traffic information and commercial offers, or more precisely complete information or news, changes in traffic and extraordinary events.

The management of social network profiles is predominately the responsibility of the marketing, communications or PR departments or the spokesperson. Information about extraordinary events is announced by staff from these departments in cooperation with operational divisions, such as operating control or a public transport department. In two cases, the information from the operating control are given automatically, in three cases, announcements also involve an IT department.

These findings can be summarized so that social networks are currently considered by carriers a standard and commonly used communication channel. Carriers are aware of the undeniable advantage of social networks, which presents the possibility of quick and forthright announcement of important information. This is a positive finding as official profiles were not so widely spread on social networks recently. Some mentioned profiles were set up in 2016. Czech Railways, as the dominant railway carrier with a nationwide scope, established their official Facebook channel only in the second half of 2015. Until then, the sufficient form of electronic communication was considered the official website. Among others, the interviews also showed that a one-way nature of communication through a website was perceived as a kind of advantage. A fairly widespread reason for not promoting establishment of official profiles on social networks with a possibility of two-way communication sooner were concerns of the management about abuse (so called trolling) or at least about excess of complaints and hostile comments, which was seen as a risk to reputation and good name of the company. This attitude of the management was in some cases overcome only in the situation, where the absence of official profiles on social networks was perceived and presented by the public and media as a deficiency, so the risk of damage to the company's image by this fact was subjectively assessed as higher than in the case of hostile or unpleasant comments and posts.

Regarding the latter topic of the research, i.e. the measurement and evaluation of communication with customers, the situation is not so positive. Only 9 carriers reported that they were evaluating communication with customers, four of which stated that it involved only evaluation of the communication concerning complaints and comments.

Evaluation of communication by various information channels is carried in a minority of the participating companies. One carrier said that they evaluated communication only through conventional channels (personal involvement, telephone, email and complaints); one distinguishes communication between social networks and conventional channels during evaluation, three carriers use separate assessment for personal communication, call centres and hotlines, web and social networks without much distinction.

Regarding the indicators used for the evaluation of communication, seven carriers mentioned the ratio of complaints and inquiries as the monitored indicator, and for three of the carriers, it was the only monitored indicator. Only two carriers stated that they were pursuing quantitative indicators such as the number of hits/views or the number of shares. One of them uses the like/dislike rate. Only one carrier said that they used web analytics tools (specifically Google Analytics). The relative ease of collection of this information on social networks apparently does not present an advantage for carriers, which would lead to their widespread use.

The fact that measuring and assessing of customer communication do not mean a priority for managements of carriers is evidenced by the response to the question whether and how often the management receives information about the assessment of communication. The responsible departments in five companies present these data to their

management once a year, one carrier does so twice a year, and only in two cases does this happens once a month. The management of other carriers does not require this information.

In neither case was it noted that communication with customers would have been systematically measured and then evaluated in case of extraordinary events in terms of impact on the reputation of the company. Collection of data quantifying communication with customers in the event of a crisis takes place in rare severe cases; see the example given in section 4.1 – black ice calamity in December 2014. There was an evaluation of these data at least at the level of sufficient/insufficient communication capacity, and based on this evaluation, measures to remedy the situation were taken. However, it cannot be evaluated as a continuous activity.

One can assume that the risk of damaging the reputation of the carrier due to an extraordinary event is perceived rather intuitively by businesses. There is a total consensus on the fact that in cases of extraordinary events in traffic, which could consequently reduce the quality and scope of provided services, the customers – passengers must be informed about them. Setting of the passenger information system in these situations is, however, not usually perceived as a risk management tool of damage to the reputation of the carrier. It can be assumed that this risk is not generally considered to be serious. Its assessment and settlement occurs once in cases of large-scale extraordinary events with serious damage to health and property. During extraordinary events with less negative impact, which "only" make the journey unpleasant for passengers and reduce their comfort, a sufficient measure is considered one-way communication in terms of a plain timely transmission of information with an excuse and, if possible, via all designated channels. Two-way communication accompanied by systematic evaluation could, in fact, become at least a tool for monitoring, if not elimination, of the risk of damaging the reputation of the carrier.

The question is, whether, at higher time, professional and hence financial demand of measurement of the effectiveness of communication with sufficient information value, the management of the carrier would even be interested in such measurement. Especially in the area of public passenger transport, the funding of which is not only based purely on market principles, companies must carefully consider the effectiveness of spent funds. Willingness to finance such measurements may then paradoxically increase in situations of prolonged decline in the number of passengers, which is reflected in the decline in sales. The management of the carrier then understands such measurements as one of the tools of analysis of causes, which is a prerequisite to a decision on how to remedy an unfavourable situation.

An example might be Public Transport Company of Usti nad Labem, which has long been struggling with a decline in passenger numbers, as shown in the Table 1.

In the last few years this company is trying to analyse the situation and propose possible solutions. There have been several passenger satisfaction surveys which included also questions whether passengers are satisfied with the awareness for changes in traffic and how much weight they attach to this matter when assessing their satisfaction with the carrier. In addition, the carrier has collaborated with universities in the processing the final reports that are focused on analysis of transport-performance and economic indicators of the company. It also had the economic and personnel audit handled. Among other changes it led to the need of establishing a new position of a spokesperson. These days the carrier is considering an appropriate way of measurement and evaluation of communication with customers both in normal operation and in emergency situations.

Table 1. Number of passengers of Public Transport Company of Usti nad Labem according to the methodology of the SDP (Czech Association of Transport Companies) [18].

	Passengers in thousands per year		
Year	**Trolleybus**	**Bus**	**Total**
2001	31 063	23 226	54 289
2002	30 545	24 331	54 876
2003	28 945	22 725	51 670
2004	28 470	22 205	50 675
2005	28 092	21 874	49 967
2006	27 441	22 871	50 312
2007	29 238	23 080	52 318
2008	31 768	20 000	51 768
2009	32 075	19 318	51 393
2010	31 392	19 873	51 265
2011	30 935	20 151	51 087
2012	28 260	18 831	47 091
2013	26 499	19 308	45 190
2014	25 196	17 965	43 162
2015	24 457	16 413	40 869

5. Conclusion

The risk of damaging the reputation of the carrier due to emergency situations in traffic and their consequences in the form of limiting or reducing services is reflected by carriers. It is not, however, usually attributed too much priority, so as businesses would systematically work with it in terms of identifying, analysing, monitoring and managing risks. One of the causes of this approach of carrier managements is difficult calculability of the protected asset, i.e. a good company reputation. This also implies a difficult quantification of risks.

One of the tools for monitoring and analysis of this risk could be the systematic measurement and evaluation of customer communications. With the growing use of electronic communication channels, including social networks, possibilities to measure and evaluate the effectiveness of communication extend for businesses. There are more and more accessible methods of an almost automated monitoring of quantitative indicators of communication, including web analytics tools. The meaningful evaluation of customer communications during the emergency situations, however, needs more than quantitative data. It is necessary to supplement them in terms of assessing the impact of communication on the thinking and behaviour of customers. But this is time consuming and costly, and companies in the segment of public passenger transport currently does not consider the evaluation of the effectiveness of communication during extraordinary events a sufficiently effective action with immediate benefits. Determination of the

applicable metrics, which would not mean excessive staffing and financial burden, then represents a major challenge for the future.

Annex 1 – translation of text in Figure 1.

Date: 2017-01-07 14:00
Subject: New disruption on track 011
==========
Track 011
Track name: (Praha – Kolin (both directions))
Segment: Uvaly – Cesky Brod – track 011
Date and time: 7 January 2017 13:36 – 7 January 2017 15:36

Cause of situation: Technical defect on track
Steps taken for long-distance transport: Operations severely restricted. Trains running on one of three tracks. Below this segment trains may be delayed 15 – 20 minutes.
Steps taken for regional transport: Operations severely restricted. Trains running on one of three tracks. Below this segment trains may be delayed 15 – 20 minutes.
Note: Operations severely restricted. Trains running on one of three tracks. SZDC is working on removing the problem.

Rule: Default – without further specification
Affected trains:
SC 509 Pendolino, R 982 Vysocina, RJ 74 Franz Schubert, RJ 79 Johann Strauss, R 983 Vysocina, SC 506 Pendolino, EC 173 Hungaria, Rx 869 Spilberk, Rx 868 Spilberk, Ex 129 Vsacan, EC 278 Dubius, EC 116 Praha, Ex 128 Vsacan, Ex 893 Sohaj, Rx 888 Jan Amos komensky, Ex 220 sulov, Rx 866 Macocha, Ex 221 sulov, EC 172 Hungaria, Ex 142 Hutnik, SC 510 Pendolino, EC 117 Praha, Os 9334, Os 9335, Os 9330, Os 9331, Os 9329, Os 8610, Os 9332, Os 9333

We apologize for any inconvenience in your travels.
Czech Railways
Passenger Transport Information
Tel: +420 221 111 122
E-mail: info@cd.cz

Annex 2 – translation of text in Figure 3.

Czech Railways – operational disruptions
Track 190 Plzen-Horazdovice predmesti – Ceske Budejovice, segment Hluboka nad Vltavou – Sliv. Defect in traction line, transport disrupted until roughly 18:00.
(like) (comment)
Liked by Vit Simanek, Pelynek Asfodel and Jirka Svoboda
Czech Railways – operational disruptions wrote:
New | CD mobile web
Riders can use the customer information hotline +420 840 112 113, where our operators will provide any information shown here. We apologize for any problems arising from the situation.

Czech Railways – operational disruptions wrote:
Operations on the track were renewed without disruption.

Annex 3 – translation of text in Figure 4.

Disruption: Track 011 segment Uvaly – Cesky Brod, start 13:36, technical defect on the track, end 15:36
SMS 14:00

References

[1] FTOREK, J. *Public relations jako ovlivňování mínění* (In Czech). ISBN: 978-80-247-2678-6. Praha: Grada 2009.

[2] PROCHÁZKOVÁ, D. *Analýza a řízení rizik* (In Czech). ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, p. 405.

[3] WWW. Usage of Traffic Analysis Tools for Websites. *W3Techs: World Wide Web Technology Surveys.* https://w3techs.com/technologies/overview/traffic _analysis/all

[4] AMEC. Who We Are. *International association for the measurement and evaluation of communication*. London: AMEC 2016. http://amecorg.com/about-amec/ who-we-are/

[5] AMEC. How the Barcelona Principles Have Been Updated. *International association for the measurement and evaluation of communication*. London: AMEC, 2016. http://amecorg.com/how-the-barcelona-principles-have-been-updated/

[6] AMEC. The PR Professionals Guide to Measurement. *International association for the measurement and evaluation of communication*. London: AMEC 2016. http:// prguidetomeasurement.org/portfolio/pdf-downloads/

[7] AMEC. Glossary – Plain Speaking. *International association for the measurement and evaluation of communication*. London: AMEC 2012. http://amecorg.com /2012/06/glossary_plain_speaking/

[8] STAŇKOVÁ, P. Měření efektivnosti reklamy (In Czech). *E + M Ekonomie a management,* 3 (2011), pp. 117-128.

[9] ČR. Zákon č. 239/2000 Sb. o integrovaném záchranném systému (In Czech). Praha: *Sbírka zákonů ČR*. http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio= 49556& nr=239~2F2000&rpp=15#local-content

[10] ČR. Zákon č. 266/1994 Sb. o drahách (In Czech). Praha: *Sbírka zákonů ČR*. ny/zakonPar.jsp?idBiblio=42341&nr=266~2F1994&rpp=15#local - content

[11] REDAKCE ČD, MIMO. unikátní systém mimořádností Českých drah (In Czech). *YouTube.cz* https://www.youtube.com/watch?v=uB4yVrnlCcg

[12] ČD. *České dráhy a.s. - omezení provozu* (In Czech). https://cs-cz.facebook.com/ ceskedrahy01/

[13] ČD. Vlakové čety podávají zprávy v přímém přenosu (In Czech). Praha: České dráhy a.s. 2008. http://www.ceskedrahy.cz/tiskove-centrum/aktualni-tema/-16477/

[14] HOLEK, J. ČD Komunikátor uspěl v zátěžovém testu (In Czech). *Železničář*. ISSN:0322-8002, 16 (2016). https://zeleznicar.cd.cz/zeleznicar/zpravodajstvi/cd-komunikator-uspel-v-zatezovem-testu/-12075/

[15] RUBEŠ, V., NAVRÁTIL, M. Dispečink a kontaktní centrum obstály v zatěžkávací zkoušce (In Czech). *Železničář*. ISSN:0322-8002. 16 (2015).

https://zeleznicar.cd.cz/zeleznicar/hlavni-zpravy/dispecink-a-kontaktni-centrum-obstaly-v-zatezka vaci-zkousce/-8701/
[16] NAVRÁTIL, M. Ledovka sevřela troleje (In Czech). *Železničář.* ISSN:0322-8002. 25 (2014), https://zeleznicar.cd.cz/zeleznicar/hlavni-zpravy/ledovka-sevrela-troleje-/-6148/
[17] HARÁK, M. Zkáza Pendolina ve Studénce: krev, slzy a otazníky (In Czech). *Železničář.* ISSN:322-8002, 15 (2015), https://zeleznicar.cd.cz/zeleznicar/ zpravodajstvi/zkaza-pendolina- ve-studence--krev--slzy-a-otazniky/-8610/
[18] DP. Výroční zpráva 2015. *Dopravní podnik města Ústí nad Labem* 2016 (In Czech). http:// www.dpmul.cz/download.php?idx=7582

Chapter 10

RISK CONNECTED WITH COMMUNICATION IN CRITICAL SITUATION

1. Introduction

Crisis communication ensures the information of people about dangers. It manages potential problems, helps to reduce panic and protect the reputation of company. Mistakes in crisis communication mean the risk because they can cause panic, increase of damages on assets etc. The article deals with communication in the company before, during after crisis. It gives proposals how to improve communication skill and techniques to process crisis situations.

2. Crisis communication

Each company goes through several critical situations during its development. This equally regards private enterprises as well as public institutions. The size of an enterprise, or the period of existence of an enterprise, has no decisive influence on the presence of a crisis. Small enterprises can sometimes survive the crisis and sometimes the crisis destroys large companies with long-time presence in the market. There are a large number of reasons for the crisis onset and they will change alongside the development of the environment, but there is one thing they have in common: maximum time pressure that is brought about in case of the burdened company.

Demands on tackling and averting the crisis are enormous. They require high level of professionalism, disproportional effort of people, many times they affect financial, material and innovative base of the company, and they verify good management practices as well as completely new practices. The final outcome is often unequal with the inputs expended.

According to the survey of the Institute for Crisis Management in USA [1], most of all crises in the world, namely 33.47%, are caused by the management of respective companies, which is an alarming observation. Human factor cannot be underestimated and it is necessary to pay more attention to the stakeholders, even before the crisis onset, in the form of preparation of a quality crisis scenario. The imminent crisis can be pointed out well in advance by attentive employees who are experienced in the area of running their own business, or have experience from other similar companies. If the management is willing to listen and respond to the warnings, it can take effective corrective actions in order to attenuate or even avert the crisis. However, if the management underestimates these warnings, if it does not communicate with employees, or even imposes sanctions against them, then it responds to the crisis with delay, or it does not respond at all. It is exactly the incorrect communication of management in the workplace while dealing with a crisis situation that can escalate

Author: Dipl. Ing. Iveta Sedláková, PhD. College ISM Slovakia in Prešov, Slovak Republic, sedlakova@ismpo. sk

tension and contribute to further damages. Acquiring communication techniques with internal and external stakeholder can mitigate the negative impact of the crisis and eliminate the impact of the crisis on the enterprise or the company.

2.1. Communication in the organization

Communication represents social interaction during which information is transmitted wittingly or unwittingly. The Latin origin of the word as such - communis - means common, this later derived into communicare, i.e. joining, making common and transmitting information. A significant share of working time of managers is represented by communicating. According to Sedlák [2], it is up to 75% of their working time that is dedicated to communication with other people. In order for the organization to function effectively, it is necessary to communicate properly on all levels of internal or external communication. Information that managers get or share comes from different sources and is destined for different stakeholders, whereas each group of stakeholders pursues fulfilment of its expectations.

Kunz [3] claims that individual groups of stakeholders have very specific claims and requirements, whereas it is exactly the crisis in the company that can preclude them and make them complicated. Customers mainly expect the enterprise to deliver high quality of products and services, fast and correct clearance of potential complaints and warranty claims, observance of standards, no threats to their health or safety.

Employees expect appropriate job titles, fair remuneration for their work as well as creation of such working conditions that will protect their health and safety. Similarly, they anticipate the respect for dignity of each employee. Owners as well as investors mostly put emphasis on their capital appreciation and the enterprise value growth, they also expect such management in the enterprise that will act professionally, transparently and will be fully engaged in their interest.

The interest of suppliers is an early settlement of payments under agreed terms and conditions, a stable possibility of sales and supplies, honesty. A local community has its interests in relation to the enterprise as well; they mostly expect engagement and support of development of local communities. Their effort is to respect, dialogue and mutually favourable cooperation as well as provision and creation of more jobs, tax contribution and local economic impact.

Incorrect communication of the management during the crisis can make the stated groups uncertain and they will rightfully feel threatened with regard to their legitimate interests. If the communication gets out of control, it becomes uncontrolled, causes damages, contribute to spreading false information, half-truths, defamation and panic increase. It often represents a pass on competition which can benefit from the situation. Incorrect communication during the crisis is then another component that contributes to termination of the company activities, or to the loss of the company reputation. Goodwill of the enterprise is created over many years, it helps its competitiveness, and it influences decision-making of customers. However, it can be irrecoverably destroyed over a short period of time.

2.2. Necessity of crisis communication

Not to leave things to chance is a very important step that the enterprise can take in peaceful time when the enterprise is doing well and problems classify as common, easily

manageable. Risk management includes also preparation of communication with each group of stakeholders, including communication with the public. As stated by Hvizdová et al. [4], the principle of public relations dwells in building good relationships of the enterprise with the public. It is based on creating a positive image in a defence against adverse information about the company. Public relations and crisis communication have the common base which is to protect the company goodwill before the crisis, but also during the crisis, to limit the impact of the crisis and to speed up the enterprise reputation recovery.

Targeted activities of the reputation management, as stated by Zuzák and Königová [5], cannot be just passive activities, but must also include the following set of activities:

- targeted formation and creation of reputation as part of the overall or marketing strategy,
- identification of reputation and its changes,
- corrections in reputation (influencing opinion) if there is a shift in the reputation development or a violation of the development due to a sudden negative event.

Each crisis specifically influences and changes behaviour and reactions of people affected by it. Therefore, the company management that deals with common, routine situations in the enterprise does not have to be prepared for the increased demands in communication during the crisis. That is why the company management should have experts ready - crisis managers who will take control during the crisis in order to eliminate a negative impact of the crisis on the enterprise. This represents a usual part of risk management.

Mika [6] points out the demanding character of the work and factors influencing crisis managers´ decision-making that need to be taken into account. A crisis situation can, for example, cause that communication between managers and other members of the enterprise which is usually without any problems can be marked by many disruptive and undesirable influential factors impeding the effective decision-making process.

When communicating, it is important to consider the following facts:

- increasing stress makes people less alert, underestimation or omission of important information can occur,
- lack of clarity of information and pressure on their fast processing often leads to its incorrect interpretation,
- emotional pressure imposed on crisis managers leads to limitation of their ability to accept new, adequate information, mainly information that is in contradiction with their or general expectation,
- biological rhythms in conditions of long-term activities in demanding situations restrict flexible thinking of people,
- a crisis situation requires a temporary limitation of certain needs of people taking part in the crisis solution as well as of those who are directly affected by the crisis,
- there is a need to suppress or cancel currently less important tasks and activities and to focus on key issues,
- long-term responsible work under physical and mental strain, under the influence of strong emotions, increases fatigue and decrease the ability to think reasonably and to decide.

The stated factors point out that crises communication needs to be included as part of risk management. The aforesaid area is developing and is bringing new findings.

3. Phases of crisis communication

Elaboration of individual steps of crisis communication, authorization of persons selected to communicate with internal and external groups, represent a part of risk management. It is best to divide communication into phases of pre-crisis communications, crisis communication and post-crisis communication.

3.1 Preparation of pre-crisis communication

Experience of many crisis managers suggests that it is necessary to have a communication strategy ready before the crisis onset. Its basic items prepared before the crisis consist of what follows:

1. Emergency plan which will consist of several crisis scenarios depended on possible sources of the crisis onset. Crisis scenarios need to be updated on at least yearly basis. It is recommended to have a list of current contacts in case of danger.
2. Appointment of a spokesperson. Enterprises must have their spokespersons, so called communicators, who will inform stakeholders, mainly the media, in case of a crisis. Well-prepared spokespersons can acquire, by means of their appearance, a positive influence on individual groups of stakeholders, be it employees, customers, business partners, media or experts. Crisis communication manual of the company should include a description of powers and responsibilities of spokespersons. It is not necessary that the company chief executive is its spokesperson, it is important for a spokesperson to be available and interviews he or she gives must convince the media that he or she is a reliable and competent source of information. He or she should keep the media attention so the media will not try to obtain information from other sources. His or her appearance towards the media must be professional at all times and must harmonize strategic aspects of the enterprise with interests of the journalists. Several authors recommend that the company can have even more spokespersons available, if necessary and for the purposes of their turn-taking. It is then important to give uniform, coordinated information. Training of spokespersons should be often focused on unpleasant questions from individual stakeholders via conferences simulations and crisis tests.
3. Establishment of a press and communication department. Communication department in the company should have staff trained for the work with the media and other stakeholders, both internal and external. From the view of technical equipment, it is important to have available phone lines, e-mail, and basic information about the company available on the internet, current contacts for representatives of local or international media, and a room where a briefing might be held if necessary.
4. Communicate with individual stakeholders including the media on a regular basis. This rule has proved successful as help while building the company reputation in the course of several years. It belongs to the policy of honesty and transparency, it is built in good and bad times and it strengthens credibility during the crisis. One of the best ways how to send out positive signals with regard to the current affairs of the enterprise is behaviour in terms of corporate social responsibility. As mentioned by Kislingerová [7], loyal employees are often the most secure capital that is left to the enterprise in difficult times.
5. Pay attention to the local media. Local regional TV news, local radio stations or local newspaper are often the source of information for national or foreign media. Even if

the objective of the company management is, for example, foreign media, it is not recommended to underestimate, ignore local media. Even if the interest of international media is later focused on different issues, the interest of local media in the latest news from the enterprise affected by the crisis will remain.

6. Have questions regarding safety and protection elaborated. Provide enough information.

It is easier to respond in stressful times extremely burdening the entire company management when pre-crisis communication is addressed correctly. Crisis communication follows from pre-crisis communication.

3.2. Crisis communication

Mikušová [8] defines the crisis as a basic unforeseen event that bears potential negative impacts that are dangerous for the organization, employees, products, services, financial conditions and reputation. Its solution lasts for a longer period of time and it is often necessary to invite external consultants. The crisis disrupts the ability of the enterprise to continue in its everyday operations. During the crisis, the organization must deal with the crisis as such and simultaneously respond stakeholders in its area. However, it is able to satisfy only certain groups in its area. If we observe successful organizations, we can see that they mostly satisfy the main groups of stakeholders that have a decisive influence on their operations. Requests for the crisis solution differ depending on whether it concerns customers, employees, owners, investors, banks, suppliers, local communities, state institutions or non-profit organizations. It is the interest of each group of stakeholders to make logical effort to cover their own risks. Their efforts depending also on the source of the crisis have different priorities. If the crisis initiator was, for example, a fraudulent conduct, the most significant groups in crisis will be employees and investors. If there is leakage of hazardous substance into the environment, non-profit organizations of activists protecting the environment, the local community and other groups will be interested in the company. If there is a breach of laws, the media, state authorities or competition, which benefits from the given situation, are interested in the enterprise.

Enterprises sometimes underestimate stakeholders that, on the contrary, show little interest in the company and have little influence, thus those not involved or not directly informed. However, in the course of a certain phase of the crisis, such a group can mobilize and change dynamically. Groups of stakeholders' exchange information about the enterprise that is dealing with the crisis, they form their opinions, and they draft their requirements. For crisis management it is therefore important to have individual steps approved by stakeholders with decisive influence. It is not necessary that a complete agreement is reached with regard to expectations of stakeholders and actions of a crisis team, a threshold approval will do. At the moment of the crisis onset, it must answer the following questions:

- when the enterprise learnt about the crisis for the first time,
- what steps it took,
- how and who noticed / did not notice the first signals,
- whether the crisis is a mistake of the organization, and other questions.

Even though it is quite difficult to answer the aforesaid questions, there is a moral and economic obligation of the management to answer them. The public can often critically respond to the organization that found itself in crisis. A successful organization can involve its stakeholders in the process of revitalisation by getting an approval of inevitable

steps leading to its rescue, it communicates actively, presents a uniform version of events and a solution strategy. To detriment of enterprises, the management is not always able to anticipate and respond to the crisis onset.

3.2.1. Crisis communication strategies

The crisis disrupts the ability of the enterprise to continue in its everyday operations. Unlike the crisis, a problem is defined by a limited period of duration, without the interest of the public, without a threat to employees. According to Mikušová [8], the enterprise can adopt one of the four basic strategic approaches in relation to its stakeholders during the crisis:

- stagnation (do nothing),
- refusing approach to the crisis,
- respond and defend itself at the same time,
- transition to attack.

Stagnation at the time the company should act, as every kind of passivity, will take its toll. Managers try to convince themselves and the others that there is no crisis in their enterprise and that only usual problems are concerned. They do nothing to solve the crisis. Zuzák and Königová [5] explain responses of the company management to the crisis by way of an example of a research carried out in 2002 by the German advisory company Ronald Berger in 130 large German, Austrian and Swiss enterprises. At first, it was the crisis suppression, later thorough execution of measures to eliminate it. Sometimes it is problematic for the inexperienced management to distinguish between problems and the crisis, mainly in its first phase.

Refusing the opinion that the organization is undergoing the crisis is an approach of "apparent death". Silence of the management during the crisis is perceived by stakeholders as confessing one´s guilt for the crisis onset, or as manifesting one´s arrogance. According to some authors, in cases of confidential nature or, for example, if a judicial follow-up is expected, the silence is the right strategy. Lawyers in the organization want to talk least in order to minimize legal liability. On the contrary, marketing managers want to regain the trust of consumers via provided information. If the media learns classified information from other sources, a strong breach of trustworthiness of the enterprise occurs. Mihok and Kádárová [9] hold the opinion that there is no confidential information during the company crisis that the company should be concealing. Those organizations that initiatively try to solve the crisis have higher success rate.

In case the company decides to adopt the third strategy, i.e. to respond and to defend itself at the same time, the company spokesperson can attack the one who blamed the company for the crisis. The enterprise can blame an individual or an organization. The enterprise can take legal actions against "the plaintiff", can disparage the amount of damages, can remind the public of previous successes of the organization, can downplay the organization liability for the crisis or it can also apologize. The following statements belong to the defence part: the crisis is a result of somebody else´s conduct and the management did not have enough information and that is why it did not take control over the matter as fast as desired. Everything the organization later does will be presented by the company spokesperson as a good intention of the organization.

If the organization decides to adopt the fourth strategy, it does not leave the crisis onset to chance. This is a proactive behaviour. The organization is prepared for the crisis onset

in the future, it has the crisis scenario elaborated, the crisis team established as well as the spokesperson prepared as part of the pre-crisis phase.

3.2.2. Phases of crisis communication

At the time of the crisis onset, communication related to safety should be more sensitive than proactive. Provide enough information without putting too much emphasis on safety issues. Respond and communicate well based on honesty and transparency is the key to the crisis solution. On the contrary, a sign of professional incompetence is aggression and attacks on employees, journalists´ or competitors´ questions. According to opinions mentioned by Mihok and Paška [10], functions, tools, communication environment and other phenomena of communication process change significantly in crisis situations. Special rules based on flexibility and speed of a respond in everyday contact with customers and the media apply and become one of the decisive success factors in the time of the crisis. The enterprise that does not respond quickly in the time of the crisis and is not able to communicate will get to the point that there will be communication about the enterprise without the enterprise. This can deepen the crisis significantly. The crisis in the enterprise attracts the attention of the general public. Unpreparedness of the enterprise for such a situation will provoke criticism and difficult questions. The company management takes a chance of increasing potential damages by inappropriate measures instead of preserving them. The enterprise thus gets on the defensive. As stated by Remišová [11], the company representatives should not act arrogantly, should not devolve responsibility to unspecified subjects, or search for alibi for its unethical conduct. It is imprudent to, for example, hide the incident that gave rise to the crisis in the enterprise because true facts will be discovered after certain time and new lies or camouflage manoeuvres will cause more harm to the enterprise than the crisis as such. The organization management should be ready even for a potential apology to its clients.

Problematic issues that the spokesperson needs to deal with while communicating with the media are pointed out by Vymětal [12]. These are efforts to find an absolute answer, to pretend compactness with the public opinion, sometimes questions regarding the spokesperson´s personal opinion, or to look for discrepancies. The spokesperson must often encounter searching for various constructions, speculations and contradictory and emotional information for headlines of front pages of newspaper. Effective communication with the media during the crisis should therefore consist of the following seven steps:

- assessment of needs and limits of the media and own possibilities for the media relations,
- creation of targets, plans and strategies for the media communication,
- training of communicators, spokespersons for the media communication and direct communication with citizens,
- preparation of clear, brief, targeted announcements and of a list of key persons, groups, enterprises and interests,
- identification of the media activities and their target groups, provision of clear, early, visible, targeted announcements,
- evaluation of announcements and procedures, reactions of the public, feedback and improvement.

If the company decides to remain silent, it will make further development of the crisis situation more complicated. Not providing information to the media does not give the

company an opportunity to express its own opinion important for its stakeholders and subsequently the media is forced to look for alternative sources of news which will be less careful when considering their words than it would be useful for the enterprise. Often, room is left for other sources of information such as police, emergency services, false and inaccurate information may occur. It is this forethoughtful to be well prepared for communication during the crisis. As stated by Bednář [13], it is very important to pay attention to so called "toxic media" in the course of crisis communication. There is certain media that are unacceptable for majority of enterprises, commercial subject and politicians. This means it would not be suitable if references to the enterprise appeared there. It is necessary to be aware of such media and try to avoid it. Certain tabloid press belongs to this group, as well as publications focused on a very small group of readers, or publications focused on problems that do not correspond to the company approach.

3.2.3. Post-crisis communication

If the company manages to cope with the crisis, it is important not to forget and to maintain communication with stakeholders. The following should apply as a rule:

1. To be proactive in communication that means to provide enough news on the recovery process of the company. To focus mostly on positive news, return of the company back to its normal operation.
2. To organize a meeting with the media representatives. To call attention to new things that the company started to do, to get a positive response of the media on the company affairs.
3. Not to forget the anniversary. To anticipate the interest of local, or national, media in termination of the big crisis and to communicate after its termination what was achieved, what target there was set for the company, how the company developed, etc., for example, after a period of 100 days, 6 months, one year, etc. To have ready materials, stories, everything that will be interested for target groups focused on the company.
4. To be prepared for legal proceedings, judicial follow-ups after the crisis. Each entity that was somehow affected by the crisis of the enterprise can press for investigation, file complaints, and deal with its affairs seeking judicial remedies. It is therefore very important not to overlook, already during the crisis, inaccurate news spread by the media in the effort to achieve sensations regarding the affected enterprise and to write a letter to its editor with a request to correct inaccurate, misleading issues. According to Stanová [14], it is important to correct mistakes and faults immediately. It is necessary to announce that the enterprise did not provide an adequate answer and want to do it again in order to avoid confusion. It is important to call journalists as soon as it is discovered that an article is inaccurate. The enterprise has a right to kindly notify of inaccuracies and give reasons why the information is inaccurate. In the court proceedings, the enterprise often needs evidence that it was not silent and responded to inaccurate news immediately.
5. To create own web newspaper where the company proactively responds to new issues in its surroundings. This represents an alternative to the news of the media which will be later spread. To provide more detailed information with as of the current date.
6. As pointed out by Chalupa [15], to choose appropriate arguments for stakeholders in order to calm the situation after the crisis, i.e. to convince employees that the most difficult part is over and the enterprise remains a perspective employer, to provide

reasons to customers for restoring their confidence in products and services of the enterprise. This also applies to banks, suppliers and clients.

4. Data

The subject of the research was a specific part of risk management that deals with elaboration of crisis scenarios with the view of the area of crisis communication. Secondary data was gathered from the best practices of domestic and foreign crisis managers working in various industries. The data are from companies: Johnson & Johnson, Texaco, Porsche, Slovnaft SpA., ZSE, SpA., Slovak Telecom, SpA [16-18]. All these companies have successfully managed the public relations and the communication with staff during a crisis situation.

The aim was to comprehensively describe individual steps of pre-crisis communication, during the crisis and after the crisis and this way to provide instructions for the crisis management on responding during the crisis. Procedures of how to work with information and stakeholders mainly during the crisis are very similar, without distinct particulars with regard to various industries. Crisis communication has enormous strength that can help sustain and save values such as a functioning enterprise when applied appropriately during a demanding period of the crisis.

5. Methods

For detection of frequent mistakes of managers at crisis communication, it was performed the critical analysis of documents of companies on courses of crisis. They were identified mistakes, their causes and consequences of mistakes at crisis communications. The risk connected with the crisis communication is understood as the size of consequences for company (size of losses, damages and harms) normed to one year and percentage of total company property. For serious risks´ sources (huge losses, damages and harms, it was prepared the risk management plan [19] for improving the crisis communication.

6. Results

The company that proactively prepares itself for a potential onset of the crisis has communication with all key stakeholders incorporated and regularly updated in its risk management. It is because the company realizes potential risks that can emerge due to its ignorance of effective crisis communication as well as benefits of successfully managed crisis communication in all its phases. Risk management of the enterprise will first identify a risk in the risk assessment phase, which means that it describes in detail what risks there are in case of incorrect communication of the enterprise. Subsequently, it carries out analysis to discover mainly the sources of the identified risk. In the end, the assessment of the scope of the described risk takes place in order to take required actions.

Table 1 shows the measures for improvement the crisis communication for priority risks connected with crisis communication.

Table 1. Risk management plan for serious risks connected with crisis communication.

Risk	**Source of risk**	**The measures for reduction of risk**		
		Low risk	**Medium risk**	**High risk**
Loss of company goodwill	- negative media publicity, - defamation of the enterprise by its competition, - incorrect reactions of the company management, - excusing and disparaging mistakes and substantial breaches of laws by the company management, - neglecting public relations, - neglecting corporate social responsibility and others	prevention in the form of: - public relations regularity, - notifications of planned and performed activities of corporate social responsibility to individual stakeholders	- immediate response of top managers to negative publicity or defamation, - creating own web page for informing the public on current affairs taking place in the company	- setting EWS in order to eliminate any breach of law by the enterprise, - immediate apology for mistakes and substantial violations, - inspection of such cases and drawing consequences for violators
Incorrect reactions of management	- long-lasting stress, - pressure imposed by the company management, -panic of customers, employees, - ignoring and concealing important information and others	- preparation of pre-crisis communication and crisis communication as part of emergency plans	- providing for more crisis managers for individual tasks, - selection of managers with resilience, ability to cope with stress and respond to crisis situations, - handing over important information	providing for an interim manager with required experience, objectivity, flexibility and responsibility for the result, detached view and impartiality
Loss of business partners (suppliers /customers)	non-observing contractual terms and conditions and agreements, e.g.: - technical parameters, - ISO standards, - financial discipline and others.	systematic character of creating long-term and favourable partnership relations based	observing contractual terms and conditions agreed with business partners	searching for acquisition, global strategic alliances and corporations

		on the win-win result		
Loss of end customers	- -unknown and unsolved problem with a product or a service, - -missing feedback with regard to customers and their expectations and others.	- regular monitoring of customer satisfaction with products and services, - providing service	- investigating complaints, - staff trainings for successful work with customers	providing for required innovations of products and services
Threat of lawsuits	- damage to customers, employees, - fatalities, - enterprise violating legislation, - enterprise providing incorrect information during the crisis and others	- requiring a correction of an inaccurately described situation or causes of the company crisis in the media, - providing correct information	regular monitoring of legal compliance in key areas of occupational health and safety as well as integrated management systems	eliminating potential fatalities
Loss of best (key) employees	- pathological corporate culture, - tough bureaucracy, - managers informing against the company, - suspiciousness, - arrogance of managers, -internal fights within the workplace, - tolerating mobbing, - intimidation, - suppressing creativity, - withholding important facts in relation to employees, - low-quality personnel policy and others	- zero tolerance of any manifestation of mobbing within the workplace, - application of whistleblowing in case of employees	- quality and motivating employment policy, - staff trainings, - elaborating a quality social policy	- improving corporate culture, - creating corporate code of conduct with sanctions for its non-observance, - supporting creativity, - transparency of the staffing process
Loss of competitive-ness	- isolation from new streams in the area of the company core business, - no activity of the management in the area of innovations,	- supporting innovative thoughts, - investing into science and research	- purchasing licences, - new technologies	- innovations, - new products, services, service, - entering new markets,

	- satisfaction with the achieved state, - stereotypical behaviour, - creation of so called - "protected area" via lobbing and various secret deals			- diversifying risks

As pointed out by several authors [20, 21], existing corporate culture and the way crisis management communicates with employees play their role during the crisis onset. According to Markidan [22] "Crisis communication should always be centred around your customers, and what you've done, are doing, and plan to do to make things right for them."

Enterprises understand more and more that it is important not only to elaborate an emergency plan but also a code of conduct. However, it is necessary to put the code of conduct as such into practice as a set of values, principles, behaviour, expected moral attitudes. The code of conduct includes principles that the organization observes in its behaviour related to its partners, i.e. employees, customers, shareholders, suppliers and the like. The code of conduct usually includes moral standards expected of the company employees. These could relate to the matters such as: conflict of interests, giving and accepting gifts, polluting environment, health and safety, sexual harassment. The crisis often attacks the enterprise quickly and without previous warnings and the response to it is usually stress and shock. It is exactly in the crisis situation when the corporate culture is examined. If the corporate culture is firm and strong, positively focused on similar objectives, it will be positively reflected in the response to the crisis. In those enterprises where the corporate culture was purposefully created and formed, where there were no contradictions and requests of employees were met, the corporate culture becomes a stabilizing element in the course of the crisis. On the contrary, if the corporate culture is superficial only, or it is unstable or weak, its very essence is uncovered during the crisis and destruction occurs. This could result in creating groups that follow different interests and objectives. In the time of the crisis, personal and group antagonisms are brought to light, some employees deal with the situation by quickly leaving the enterprise, passivity in negotiations occurs, or high level of aggression of employees is shown.

7. Conclusion

The crisis represents reality of the business entity that is best dealt with by preparing for its onset. Honest, clear and transparent communication of the enterprise with every group of stakeholders before the crisis, during the crisis and after the crisis is one of the ways how to survive it. It is experience that can help the enterprise recover its reputation, get its customers back and maintain loyalty of its own employees. The enterprise that managed the crisis can obtain valuable experience and continue in further existence, can create values for the society. Crisis communication should therefore be part of emergency plans of companies.

Acknowledgement

The article was created as a contribution for IG-KEMM-02/2015-3.3.9.

References

[1] ICM. *ICM Annual Crisis Report for 2014.* http://crisisconsultant.com/crisis-intel-reports/icm-annual-crisis-reports/2014-crisis-report-download/

[2] SEDLÁK, M. *Manažment* (In Slovak). ISBN: 978-80-8078-238-2. Bratislava: Iura Edition, 2009, 438p.

[3] KUNZ, V. *Společenská odpovědnost firem* (In Czech). ISBN: 978-80-247-3983-0. Praha: Grada Publishing 2012, 201p.

[4] HVIZDOVÁ a kol. *Základy marketing (In Slovak).* ISBN: 978-80-89372-49-2. Prešov: International School of management Slovakia 2013, 219p.

[5] ZUZÁK, R., KÖNIGOVÁ, M. *Krizové řízení podniku* (In Czech). ISBN: 978-80-247-3156-8. Praha: Grada Publishing 2009, 256p.

[6] MÍKA, V. Špecifiká krízovej komunikácie s verejnosťou (In Slovak). In: *Zborník z 9. vedeckej konferencie s medzinárodnou účasťou „Riešenie krízových situácií v špecifickom prostredí".* ISBN: 80-8070-273-X. Žilina: FŠI ŽU 2004, 436p.

[7] KISLINGEROVÁ, E. *Podnik v časech krize. Jak se nedostat do potíží a jak se dostat z potíží: zkušenosti ze světové recese let 2007 až 2009* (In Czech). ISBN: 978-80-247-3136-0. Praha: Grada Publishing 2010, 206p.

[8] MIKUŠOVÁ, M. *Krízový management pro malé a střední podniky* (In Slovak). ISBN: 978-80-8168-106-6. Bratislava: Wolters Kluwer s.r.o. 2014, 307p.

[9] MIHOK, J., KÁDÁROVÁ, J. *Manažérske aspekty krízového riadenia podnikov* (In Slovak). ISBN: 978-80-553-1255-2. Košice: SjF TU 2012, 272p.

[10] MIHOK, J., PAŠKA, P. *Komunikácia v krízovom manažmente podnikov* (In Slovak) http://www.sjf.tuke.sk/transferinovacii/pages/archiv/transfer/13-2009/pdf /050-052. pdf

[11] REMIŠOVÁ, A. *Etika a ekonomika* (In Slovak). ISBN: 978-80-8101-402-4. Bratislava: Kalligram 2011, 495p.

[12] VYMĚTAL, J. *Průvodce úspěšnou komunikací. Efektivní komunikace v praxi* (In Czech). ISBN: 978-80-247-2614-4. Praha: Grada Publishing 2008, 328p.

[13] BEDNÁŘ, V. *Medialní komunikace pro management* (In Czech). ISBN: 978-80-247-3629-7. Havlíčkuv Brod: Grada Publishing 2011, 160p.

[14] STANOVÁ, I. *Krízová komunikácia. Čo robiť pred, počas a po* (in Slovak). http://www.institutik.cz/wp-content/uploads/2012/03/PMP_Marketing_krizova_ komunikacia.pdf

[15] CHALUPA, R. *Efektivní krizová komunikace* (In Czech). ISBN: 978-80-247-4234-2. Praha: Grada Publishing 2012, 176p.

[16] HUMENSKÝ, P. *Ako komunikovať, keď do firmy pride kríza* (In Slovak). https://www.etrend. sk/podnikanie/ako-komunikovat-ked-do-firmy-pride- kriza. html

[17] KAPLAN, T. *The Tylenol Crisis: How Effective Public Relations Saved. Johnson &Johnson.* http://www.aerobiologicalengineering.com/wxk116/TylenolMurders/ crisis.html

[18] VDOVIN, A. *Effective Communication Tips During a Company Crisis.* http://alert - software.com/effective-communication-tips-during-a-company-crisis/
[19] PROCHÁZKOVÁ, D. *Analýza a řízení rizik* (In Czech). ISBN: 978-80-01-04841-2. Praha: České vysoké učení technické 2011, 405 p.
[20] AMSTRONG, M. *Řízení lidských zdrojů* (In Czech). ISBN: 978-80-247-1407-3. Praha: Grada, 2012, 788 p.
[21] ZUZÁK, R. *Krizové řízení podniku* (In Czech). ISBN: 80-86419-74-6. Havlíčkuv Brod: Professional Publishing 2004. 179 p.
[22] MARKIDAN, L. *3 Examples of How Not to Handle Crisis Communication* (and What We Can Learn from Them). https://www.groovehq.com/support/bad-customer-service-crisis-communication-examples

Chapter 11

BUSINESS PROCESSES AND THEIR MAPPING AS BASE FOR BUSINESS CONTINUITY MANAGEMENT AND MAP OF RISKS

1. Introduction

In the context of corporate activities, we repeatedly face situations where it is necessary to monitor individual business processes from a risk perspective. Typical examples of such situations may include:

1. Making a risk map as a basic tool for risk management in the company. It is understandable that by activity and specific focus of the company, the processes, the resulting individual risks as well as their severity could be different. By severity we mean the possible probability of risk (i.e. the likelihood of harm) and its possible impact.
2. Management of the specific type of risk. For certain types of risk, e.g. credit risk, market risk, currency risk etc. the business process map is just an auxiliary tool. On the other hand, for managing other types of risks, especially from the operational risk category, an accurate view of business processes, their risk characteristics and context is absolutely necessary.
3. Business Continuity Management (BCM) and crisis management. By using the mapping of business processes, it is possible to determine which processes are crucial (critical) to the running of the business and must be secured in case of emergencies. For use in BCM and crisis management it is necessary to determine the characteristics of a critical period, the maximum allowable downtime (MAD), the possible impacts of failure, etc. for individual processes, as will be discussed below.

2. Background research

For the definition of *risk*, we refer to Smejkal, Rais [1]. The risk could be understood as:

1. Probability or possibility of loss, fail.
2. Variability of possible outcomes or uncertainty of their achievement.
3. Deviation of actual and expected results.
4. Probability of any result different from the expected outcome.
5. Situations where the quantitative extent of a phenomenon subject to a certain probability distribution.
6. Danger of negative deviations from the target (pure risk).
7. Danger of wrong decision.
8. Possibility of loss or profit (speculative risk).
9. Uncertainty associated with the development of the asset (investment risk).

Authors: Dipl. Ing. Martin Svítil, Ph.D. Expobank CZ, Praha, martin.svitil@seznam.cz, Assoc. Prof. , JUDr., PhDr. Ivo Svoboda, Ph.D., Vysoká škola regionálního rozvoje, s.r.o., Praha, dr.svoboda.ivo@seznam.cz

10. Median of a loss function.
11. Possibility that a specific threat exploits specific vulnerabilities of a system.

According to Smejkal, Rais [1] the ***risk management*** usually includes:

1. The analysis of risk(s).
2. The selection of countermeasures.
3. The analysis of cost / benefits.
4. The implementation of countermeasures.
5. The testing (the comprehensive screening) of countermeasures.

In this paper we mostly deal with ***credit risk*** and ***operating risk***. The credit risk is the risk of loss due to the inability or unwillingness of the contractor to meet the agreed contract terms. From the perspective of the lender we see the credit risk as the risk of default of the borrower in the way that the borrower fails to meet its obligations, thereby causing loss to the creditor. The operating risk (as classified by Cipra [2]) contains the risk of the transaction (losses resulting from errors in the execution of operations in accounting, settlement etc.), operational risk management (management activities of front-in, middleware and back-office, especially fraudulent, criminal and unauthorized conduct, money laundering, transactions over the limit, lack of control etc.) and, finally, risk of systems (errors in computer programs, mathematical models for data, system downtime, etc.)

For ***Business Continuity Planning*** (BCP) we refer to Smith and Sherwood [3] "The objective of the business continuity planning exercise is to ensure the recovery in an acceptable time frame of the business as a whole, following an incident which causes major disruption to business operations." In the same paper Smith and Sherwood [3] recommend to execute the ***Business impact analysis*** (BIA) and to identify critical business functions and operations.

Gibb, Buchanan and Shah [4] define the role of ***Business Continuity Management*** **(BCM)** "Business continuity management is concerned with identifying and managing the risks which threaten to disrupt essential business processes, minimising the effects of these risks and ensuring that recovery of a process is achievable without disruption to the business. BCM is more than just disaster recovery - while disaster recovery is a reactive activity, BCM is also about trying to prevent disasters occurring in the first place". We agree absolutely with this statement, especially with the last sentence. This is why our research is aimed both at the risk management as well as BCM and crisis management. The importance of the BCM is recently increasing. E.g. Herbane, Elliott a Swartz [5] see a „possibility of a role for BCM that can be more integrated with the more conventional strategic activities of a firm "and get „mission-critical strategic role ". More about BCM and BCP it is given for example by Herbane, Elliot a Swartz [6], Ernest-Jones [7] and Gibb and Buchanan [8]. More about BIA for example by Goldberg [9]. The basics of actual ***techniques and tools*** for ***process mapping*** are well described e.g. by Keller and Jacka [10] (primarily from the audit perspective). They propose the use of specialized worksheets (questionnaires), including in particular the name of the process, its objective, risks of the process, key controls, event for beginning and ending, input + sources, output + customers, measures of success. Alternatively, the summary of job duties of individual employees is included too.

3. Data description and methods

The subjects of research were two companies and their business processes. It was (1)

a medium-sized company in the financial sector, with roughly 150 employees. The company provides various financial services, using sales offices covering the entire territory of the Czech Republic. (2) Small universal bank with roughly 250 employees in Czech Republic.

In both cases the activities such as approving transactions, their processing and management, enforcement etc. (i.e. Back - office) are concentrated at the headquarters, performing these processes for all the sales offices.

The aim was to analyse and describe the procedure of mapping activities (processes) running in the enterprises and to provide recommendations for such mapping procedure.

A procedure of collecting empirical data in the parts of the enterprises, assess them according to criteria of verifiability and relevance was used. The application of method of induction was subsequently carried out to extend the conclusions to the entire enterprise.

4. Results

For the above situation, tracking business processes from a risk perspective, it is effective to map business processes and ***create a map of business processes from the perspective of risk***. The basic requirement is such a selection of criteria and procedures for the mapping of processes that makes the resulting process map not too detailed and therefore too large for planned uses, but also allows the map contain all relevant processes from the point of view of risk. The number of processes, in which all activities of the company is segmented, could be considerably influenced during the mapping process.

The primary criterion for mapping is the affiliation of the processes with different departments or divisions of the company. The analyst executing the mapping procedure usually goes through the standard (normal) and occasional (extraordinary) activities of every department and tries to describe it in the form of individual processes, usually ***in conjunction with the head or authorized employee of each department***. The individual activities are allocated from the overall picture of the function of the department.

Additionally, to recently used mapping techniques and tools as described e.g. by Keller and Jacka [10], we needed to rather expand the range of information, because our mapping of processes should be used (as above) for a wider than just an audit inquiry. So we added some more information into the questionnaire, which are important from our perspective and for our use of material. As the **main criteria** for the breakdown (separation) of activity into individual processes we include the following components:

1. Periodicity of the process: some activities, typically e.g. reporting, some control activities, maintenance and adjustment, etc. are carried out (or at least should be carried out) periodically. Usually the activities with different periodicity belong to different processes. For other activities the frequency is variable. The big advantage here is the experience of employees in the department who are involved in mapping.
2. A critical period of the process, i.e. the period during which process should be executed
3. The maximum permissible period of malfunction / downtime (sometimes referred to as MAD = Maximum Allowable Downtime): How long is the complete outage of the process allowable without affecting the functioning of society.
   Maximum Allowable Downtime = the point in time after a significant interruption at which the product or process can no longer be inoperable.

Sometimes the term MTPoD is used too: Maximum Tolerable Period of Disruption = the point in time after a significant interruption after which an organization's viability will be *irrevocably threatened* if product and service delivery cannot be resumed.
This is crucial information, especially for BCM and BCP. Let's mention for example the bank: if the making of new contracts with clients (e.g. opening new accounts etc.) would be prevented for several days, it would certainly be very unpleasant for the bank, especially in terms of reputation and loss of potential gains from new contracts and from new customers. But if, however, the bank would be for several days unable to pay deposits to clients, the impact would be much worse. In addition to the huge reputational risk, legal actions from customers (e.g. because of the loss of profit, etc.) could be launched. And with a high probability the bank would be exposed to sanctions from the regulator.

4. Personnel: how many employees usually perform the process, what number of them is required to ensure the basic operation of the process (e.g. if it is needed to relocate to an alternate site or work from home etc.)
5. The necessary technical equipment: what hardware and software is usually used, which HW and SW is required to provide at least basic functionality of the process for a limited time. It is closely related to the number of employees mentioned above: it can be assumed that almost every employee will need a PC or a workstation with some software equipment, data access, and possibly other essentials (printer, Internet access ...). The question is also equipping people with portable devices (laptops, smart phones) - the higher, it is obviously easier to find a solution to crisis situations if the usual working place is not available.
6. The possible effects of process failure (structured): usually comes up later, with the creation of map of processes and sorting of the processes into critical / non-critical - see below.

All activities of the department can therefore be divided into individual processes. Affiliation of the processes to individual departments or divisions of the company is the primary criterion, but not a dogma. In the practical implementation of process mapping it is useful to focus not only on the formal definition of department / division, but in conjunction with the employees to pay attention to the practical functioning of enterprise. Moreover, as stated for example by Neumaierová [11] (p. 50): "In most cases, the organizational structure, such as mentioned in the annual reports, reveal little about the actual style of management of the company. Only the allocation of the company employees in various functional specializations or fields in which the company conducts its business plans is described. But you can learn only a very little about the processes taking place in these organizational structures of these organizational charts." [translated by M.S.] If this view is respected and taken into consideration, it is possible to successfully map the processes in the organization that uses other than traditional hierarchical organizational structure.

There is also the possibility to exclude some individual activities / processes from the mapping process, that takes place within the enterprise across departments / divisions, and include them into the process maps separately. An example of such a process may be all the necessary activities related to AML (Anti - Money Laundering). In financial institutions, several departments are usually involved on AML (esp. risk management, compliance, legal and internal audit) and it may therefore make sense to monitor this process separately, instead of being classified under all participating departments are

therefore occur four times in the process map. It has much to do, of course, with the way the process of AML is organized in the company.

In case that the standard method of the mapping comes to too high and thus difficult-to-treat number of processes, there is the alternative to perform a ***primary selection processes*** directly at the primary mapping. This selection process should be configured to include only such processes to the map, with which the risk is or potentially may be associated. Such primary selection allows you to speed up and simplify the process of mapping and treating the data. On the other hand, it is logically associated with a risk of missing out a process that could show up to be danger, or (more commonly) turns out to be associated with other danger process.

If the standard mapping method attains such a number of processes with which it is possible to work further effectively, the ***selection of critical processes*** follows as a next step. In essence, this is a process very similar to the **BIA (*Business Impact Analysis*)**.

The basic criterion for the selection of critical process is the severity of possible impacts of the interruption (loss) of the process. The impacts are usually evaluated in several categories, namely:

1. Financial impact: this includes e.g. the loss of revenue, loss of profit, reducing CF, restrictions on the ability to collect receivables, increase financial obligations or the inability to make appropriate financial reports.
2. Impact on customers: the negative impact on company with regard to customer opinion and / or customer satisfaction, can lead to loss of customers.
3. The impact on third parties (employees, suppliers, shareholders / partners ...): the negative impact on company with regard to opinion and / or satisfaction of third parties, could lead e.g. to leave of important staff, disputes with employees or unions and similar organizations, the threat of a strike, etc., to the loss of suppliers, management changes etc.
4. The operational impact: the inability to provide services for internal customers, i.e. other departments within the company. May lead to inability to meet the objectives / deadlines, the accumulation of pending work, the need to intervene in the processes / systems, to loss of productivity, the ability to limit cooperation with third parties.
5. Legal / Regulatory Impact: negative impact on legal / regulatory environment can lead to non-compliance with external regulations (laws), regulatory requirements and consequently the legal penalties (fines or - in extreme cases - up to the withdrawal of its banking license, etc.).
6. Reputation impact: a negative impact on the image / brand of the company or its reputation.

In some categories it is possible to estimate the impact of interrupting of processes quantitatively or calculate it directly, usually in financial volume. In other cases, the impact may be quantitatively estimated only very roughly, or it is completely impossible (typically e.g. a reputation impact, where it can be extremely roughly to estimate what percentage of clients and potential clients could learn about a possible problem, etc.). The used scale and extent of degrees of quantitative evaluation depends, of course, on the individual processes, but also on the size and strength of the company, which processes we map. For example, for a small company the possible level of fines imposed by regulator or other authority in the millions of CZK could be liquidating. On the other hand, for large bank a fine in the same amount would represent a relatively less significant impact, the more important it could be related to her reputation risk.

In case of impossibility or unsuitability of the use of quantitative indicators, it is possible to qualitatively assess the possible impacts, e.g. on a scale limited / moderate / strong / disastrous.

Example categorization of interruption of processes in a financial institution is given in Table 1.

Table 1. Example of categorization of interruption of processes in a financial institution [GE Money].

Category of impact	**4**	**3**	**2**	**1**	**0**
	Disastrous	**High**	**Middle**	**Low**	**No impact**
Financial impact	Loss higher than 1 000 000 USD	Loss higher than 500 000 USD and lower than 1 000 000 USD	Loss higher than 250 000 USD and lower than 500 000 USD	Loss lower than 250 000 USD	No financial impact
Impact on customer	Affects more than 10% of the relevant customer base and / or matter requires notification more than 10% of the customer base	affects more than 5% and less than 10% of the relevant customer base and / or matter requires notification more than 5% and less than 10% of the customer base	affects more than 1% and less than 5% of the relevant customer base and / or matter requires notification of more than 1% and less than 5% of the customer base	affected less than 1% of the relevant customer base and / or requires no notice to customers	no impact on customers
Operational impact	Excessive accumulation of transactions / work; degradation of internal controls; unavailability of suppliers	Accumulated work requires the deployment of additional personnel; Internal controls are being met, but are not respected deadlines; Suppliers are working with limited capacity	Accumulated work requires the deployment of additional personnel; Internal controls are being met; Services or information from suppliers are delayed, but does not affect operation	Operation is not affected	Operation is not affected
Legal / Regulatory impact	Criminal sanctions and heavy fines; necessary investigation, the results of which are	Potential to cause criminal penalties and / or fines; may lead to investigation on the basis of the	Less legal risk increasing the possibility of an audit; coupled with the observation in the	No Legal / Regulatory impact	No Legal / Regulatory impact

	presented to the Board and on the basis of which it adopted a corrective action plan; It includes matters requiring immediate attention (MRIA), matters requiring attention (MRA), or their equivalents; the company faces severe penalties, loss of licenses and / or ability to function	adopted plan of corrective measures; by the regulator is recommended or required additional reporting	investigation; there is no need reporting or corrective action plan		
Impact on reputation	Significant negative impact on the Company's reputation; escalation on the corporate level and generate negative publicity	Leads to negative media coverage at the national level for a long time; long-term problem for the company's image; affected Corporation (Group)	Leads to negative media coverage at regional or local level	Unlikely to media coverage on any market	No impact on the Company's reputation

Typical examples of critical processes in financial institutions may be:

1. Maintain the communication and awareness of the key persons in the company (and outside the company, if needed)
2. Allow clients the access to their assets (esp. withdrawal from bank accounts, drawing of contracted loans, etc.).
3. Ensure the physical security of assets and functionality of IT security
4. Monitoring repayment of liabilities and other obligations from clients / debtors / business partners, early warning if they are not met and enforcement actions, where the risk of delay exist
5. Implementation of necessary legal steps in accordance with the deadlines in the context of legal proceedings (e.g. a timely application to the bankruptcy proceedings, filing of complaints, suggestions and appeals, reactions to the proposals of the other parties, etc.).

6. Ensure the compliance with statutory obligations (e.g. the protection of personal data, etc.).
7. Provide the reporting and control activities, whose failure to comply could result in a sanction from the regulator or other institutions
8. Receipt and registration of incoming mail / messages in data mailbox and response to, if the risk of delay exists

An important part of the selection of critical processes is also a consideration of ***succession of the processes***. If a process is recognized as a critical, we logically have to evaluate as critical all the preceding processes (if any), which create the necessary conditions and prerequisites for the original process. The danger of the primary selection of the processes during the mapping is evident here: some processes, not critical individually, but essential for other critical processes, can be omitted in the primary selection.

Some critical business processes may depend on external processes or conditions outside the surveyed enterprise and may be impossible for the company to influence. In such case, a situation like this has to be reported in the map of critical processes and taken into consideration within the follow-up. This is usually done within the framework of Business Continuity Management (BCM) and creating a Business Continuity Plan (BCP), as the company looks for alternative providers of critical services or goods, it creates a reserves etc.

The most obvious prerequisite for application of the process map is a ***regular update***. Usually it deems necessary to upgrade or check the validity of the process map at least once a year. However, the update rate may vary depending on the type of business, number and severity of processes like.

Of course, it is necessary to perform the update of process maps, selected critical processes and links whenever there's the significant change of the way in which the company operates (e.g. after a change of legislation), its internal structure and functioning (e.g. the extension of the activities of the company in a different industry) or when the Business process Reengineering was executed, as described i.e. by Řepa [12], as a fundamental change to the nature of the business process from the beginning.

5. Conclusion and recommendations

With proper selection of criteria, the mapping of company processes can bring universally applicable map of critical processes within the company, along with its expected impacts and other important information.

We especially recommend paying attention to following essential prerequisites for the successful mapping of processes:

1. Correct setting of the mapping process, that makes the resulting process map not too detailed and therefore too large for planned uses, but allows the map contain all relevant processes from the point of view of risk.
2. The proper criteria to breakdown all the activities in company's departments to individual described processes
3. Cooperation with key employees of each department
4. Correctly set selection of critical processes
5. Proper mapping of succession of the processes
6. Corresponding updates of process map, both periodic and ad hoc if needed

The resulting process map is then applicable to risk management in company as a whole, for the management of a particular type of risk (especially the operating risks) and for Business Continuity Management (BCM) and crisis management.

References

[1] SMEJKAL, V., RAIS, K. *Řízení rizika ve firmách a jiných organizacích* (In Czech). ISBN: 978-80-247-3051-6. Praha: Grada Publishing 2010.

[2] CIPRA, T. *Kapitálová přiměřenost ve financích a solventnost v pojišťovnictví* (In Czech). ISBN: 80-86119-54-8. Praha: Ekopress 2002.

[3] SMITH, M., SHERWOOD, J. Business Continuity Planning. *Computers & Security*, 14 (1995), 1, pp. 14-23.

[4] GIBB F., BUCHANAN, S., SHAH, S. An Integrated Approach to Process and Service Management. *International Journal of Information Management.* ISSN: 0268-4012, 26 (2006), 1, pp. 44-58.

[5] HERBANE, B., ELLIOTT, D., SWARTZ, E. M. Business Continuity Manage-ment: Time for a Strategic Role? *Long Range Planning*, 37 (2004), 5, pp. 435–457.

[6] HERBANE, B., ELLIOTT, D., SWARTZ, E. Contingency and Continua: Achieving Excellence through Business Continuity Planning. *Business Horizons.* ISSN: 0007-6813, 40 (1997), 6, pp. 19-25.

[7] ERNEST-JONES T. Business Continuity Strategy – the Life Line. *Network Security*. ISSN: 1353-4858, 20 (2005), 8, pp. 5-9.

[8] GIBB F., BUCHANAN, S. A Framework for Business Continuity Management. *International Journal of Information Management.* ISSN: 0268-4012, 26 (2006), 2, pp. 128-141.

[9] GOLDBERG E. M. Sustainable Utility Business Continuity Planning: A Primer, an Overview and a Proven Culture-Based Approach. *The Electricity Journal*. ISSN: 1040-6190, 21 (2008), 10, pp. 67-74.

[10] KELLER, P., JACKA, J. M. Process Mapping. *The Internal Auditor.* 56 (1999), 5, pp. 60-61.

[11] NEUMAIEROVÁ I. A KOL. *Řízení hodnoty podniku, aneb, Nedělejme z podniku záhadu* (In Czech). ISBN: 80-7099-701-X. Praha: Profess Consulting 2005.

[12] ŘEPA, V. *Podnikové procesy: Procesní řízení a modelování* (In Czech). ISBN: 80-7259-022-3. Praha: GRADA, 2007.

Chapter 12

A MENTAL DECISION RISK MODEL: THEORY AND EVALUATION*

1. Introduction

The aim of chapter is:

- to draw attention to the importance of *monitoring the evaluation* of individual parts of project proposal, and also to the review of way of solution of any assigned critical values exceedance and to the complete excluding the conditions endangering the project integrity,
- to draw attention to the *weak points* (smoothing down the time series of unexpected conditions) by the deterministic evaluation of parameters,
- to propose an alternative method for the *evaluation of any decision criterion*, or for data simulating.

More detailed explanation follows and is linked to the critical interpretation of relation (1), given below for practical applications. Technical-economic work is exposed to various influences. Further, the influences are identified as benefits, losses, risks, threats etc. [1]. For strengthening or diverting such influences, the management is responsible. It addresses process management, acquisition management, usage or removal control, design of technical work etc. The management target is to achieve a sustainable and competitive performance. The risk analysis and continual thorough risk assessment are essential for the conceptual design and evaluation of technical-economic variants.

To express risk management process mathematically, the total risk $\boldsymbol{R}$ is the sum over set of individual risks ri, where individual risk is computed as the product of potential losses l_i, and probabilities $p(l_i)$; the integrated risk is considered

The total risk of project is written as $\boldsymbol{R}_{(i)} = \sum_i r_i = \sum_i r_i \; p(l_i)$. Loss is expressed in financial units or a verbal description of the outcomes. A helpful survey is given in the introduction of papers [2, 3]. For example, to support the simulation of buildings designing there are many tools, but it is a lack of simple tools that can support the initial set of goals in the early phases of design and promote the dialogue between representatives of non-professional users and professionals in housing cooperatives, such as architects, contractors and consultants. Jensen and Maslesa [4] proposed the RENO EVALUE, a tool for targeted planning as a holistic qualitative tool for determination of objectives and, what is perhaps even more important, the tool for clarifying the expectations as a part of initial dialogue and decision-making process.

Subsequently, the management can choose different strategies for work with risk [3] and formulation of individual solutions´ evaluation, selection of decision methods and measures´ monitoring. The decision operates traditionally with chosen factors F_1, F_2, ..., F_i, ..., F_m and it has assigned to their evaluations [h_1, h_2, ...h_i, ..., h_m]. The matrix for

Authors: Assoc. Prof., Dipl. Ing. Petr Dlask, Ph.D., Czech Technical University in Prague, Praha, Czech Republic, dlask@fsv.cvut.cz; Assoc. Prof., Dipl. Ing. Václav Beran, Ph.D., D.Sc., Assoc. Prof., Dipl. Ing. Ivana Faltová Leitmanová, PhD., University of South Bohemia, České Budějovice, beran@jcu.cz; leitman@ef.jcu.cz

assessment [***h***] is subsequently used for the calculation of total evaluation ***U***. It is applied for the comparison of variants, alternatives, and the feasibility of various controlling measures etc. The presumption is the existence of significance w_j for the individual decisional factors F_i of assessment criteria. The resulting evaluation is determined by the matrix product

$$\boldsymbol{U}=[\boldsymbol{w}]\cdot[\boldsymbol{h}]^{\mathrm{T}} \qquad (1)$$

where $1\leq i \leq m$. This calculation is also known as *MCDA (*the *multi-criteria decision analysis)* of problem. Evaluation may take for decision factors F_i various practical forms. We can see the discrete evaluation value as scalar for real number of solitary cost evaluations, and as vectors (multidimensional evaluation), as matrix of probability densities, i.e. as a set of time series (process flow simulations in time), or as also a fuzzy set etc.

The problem solving the modern decision making nature is multidimensional. A new solution requires the complexity, sustainability, technical-economic (T-E) progress, efficiency, security, risk evaluation etc. Suitable examples might be documents of United Nations: Agenda 21 [5] and Rio+20 in [6]. Major reasons for the relatively slow progress are complicated aspects of topic, conflicting interests and many other factors. Nevertheless, the essential problem can also be seen as a bottleneck that is in the actual theory.

It is advantageous to use a hierarchical graph for the description of structures´ evaluation. It detects the factual structure of criterions´ evaluation. The interpretation of constant ***U***, in its internal structure, enables monitoring the weak and strong points of assessed solution. It thus opens the way for the evaluation of variants including the subsequent modifications. Generally, the supporting terminology is from the ISO/IES standard risk platform. For the needs of evaluation, it uses the IEC 31010: 2009 *Risk management – Risk assessment techniques* [7]. The chapter deals with a modified assessment tool based on the Monte Carlo simulation and a tree structure of evaluation criteria.

For both, the ongoing work and the right interpretation of explanation it is appropriate to define some terms:

- *project feasibility* – it is the project realisation assessment regarding to real conditions,
- critical value – it is the value beyond which the project is not feasible,
- scarce events – it denotes events with sporadic occurrence due to the external influence,
- project solver – it is a tool for calculation and integration of final project evaluation,
- decision process – it is decision based on criteria F and evaluation of technical-economic indicators x_i, (T-E),
- transfer function – it is the conversion of x_i set to $u_{i\,set}$; data to utility,
- risk (management) – it involves the identification, assessment, and prioritisation of risks,
- risk – it is the effect of uncertainty on objectives (ISO 31000) [7],
- risk management process – it is the monitoring and reviewing the risk.

Extensive information about category risk, also terminology concerning and legislation, is given in IEC 31010:2009 - *Risk Management - Risk Assessment Techniques* [7], and in ISO/Guide 73:2009 – Risk management – Vocabulary [7].

2. Background research and motivation – the process concept

Let us engage in a formal summation for the general purpose – i.e. a description of the factual problem. Let us refer to members (elements, components) of solution structure (A_1, A_2,..., A_n) and about links K_{ij} among them. Important for process structure, there are the components (elements, …) of physical (material) reality labelled as set ***A*** (described mostly by using nouns for commodities, assets, …). The interrelations between these elements are changes or progressions (mostly labelled as ***K*** expressed by the verbs describing doing, performing action, …). In most practical descriptions we deal with structures that proceed in *time*. In other words, we create a dynamic time dependent structure.

Let us express such a structure organizational chart $\boldsymbol{G_{org}} = (\boldsymbol{A}, \boldsymbol{K})$. The more advanced description of reality focuses on effects of *risk* ($\boldsymbol{G_{org}}$| *risks*) or *occurring phenomena*, and more. We may speak about process structures influenced only sparsely as ($\boldsymbol{G_{org}}$|*sparse phenomena*), etc. The $\boldsymbol{G_{org}}$ establishes some value network and enables analysis by visualizing sets of relationships and the dynamic of the process in prospect. For a hierarchical (tree) structure and the evaluation of projects, it is used SW called *PREV – Project Evaluation* [8]. The software *PREV* is based on two steps: generator of tasks; and solver of tasks that is a scenario based on risk analysis and risk decision making.

The generator of tasks uses the superposition principle for decomposition from the total (difficult) complex view to the detailed (simple) view. The entry data create the basis for the generator of tasks which will then create the initial calculating structure for the evaluation of new project. The data quality (correctness) comes from the nature of accessible information for the expert evaluation by means of SW application interface.

The internal SW – solver works further with the generated structure. Work with the solution concept asks necessarily to define the monitoring mechanisms, which appraise and check the evaluated structure and inform about the occurrence of critical data for the whole project structure (more in [8, 9]). Besides the structure of the decisional criterion, it is necessary to work with the structure (hierarchy) of evaluation. The chosen method comes from deterministic evaluations for u_1, u_2, ..., u_m. The historical data are mostly related to timeline [-*t*, 0] and factual sources are mostly hard data x_i as measurements, statistics, expert knowledge, research reports etc.

The relation of $x_i \rightarrow u_i$ (hard data towards utility or benefit) requires the transfer function $f(x_i)$ for decision-making in environment, which is exposed to risks. In such a case it is necessary to know the transfer function between the benefits/utility and risks for each *t* in the past. This can be denoted as $h(u_i)$. Data oriented to the future [0,*t*] are the data generated by the simulation model. A schematic distinguishing idea is:

REAL DATA FROM THE PAST – *t*

↓

CURRENT MOMENT OF TIME

↓

DATA SIMULATION OF FUTURE +*t*

(2)

Series {X} of [-*t*, 0] → ***Creation of model*** → *Forecasting s*eries {X} of [0, *t*].

Data describing the past have only limited validity. Such data demonstrate the features of past and tells us about the past, they help us to understand the past infrastructure, technology, organisation, etc. Any new solutions have to be carriers of new added values. New solutions for implementation industry need to be reflected in both, the existing and the future infrastructure, which also involves the future macroeconomics conditions. Therefore, "model-making" simulated data are the basis for decision-making.

It is appropriate to mention the interaction of macroeconomics – framing the national infrastructure – and microeconomics as based on enterprises and their management. Macro– and micro– relations are relatively reliable if external influences are stable. Difficulties arise if the external, unexpected risks are affecting the development structure. More macroeconomic examples are offered in more popular mode in the Taleb book [1]. On the other hand, many examples are tied in with microeconomic factors and applications; mostly in areas such as technical design, environmental impacts, medicine etc.; an example is given in [2].

Conditions for sectors are differentiated in terms of technology used and as well as in management perspective. The global environment may also change the conditions and risks in each country. Table 1 shows the possible terms for assessing the approach of authors in [10]. These authors refer to possible terms for assessing the level of risk in construction projects.

Table 1. View of evaluation [10].

Macro	**Mezzo**	**Micro**
Country	Project	Management
Industry	Enterprises	Organization

This chapter basically deals with risk processes. The approach focuses on technical-economic risk (T-E). Risks anchored in microeconomics and macroeconomics has long been elaborated especially for the consequences which impact on the efficiency of farm businesses and national economies. Technical processes have a closer impact, and risks are defined more clearly. Economic risks characterize accidents, disasters operation of technical equipment, for example database *Health and safety at work* of the Eurostat [11]:

- costs per fatality range between approx. € 0,5 million and 3 million Euro for EU 28,
- costs per serious injuries comprise a range of ca. € 880,000 (between € 80,000 and € 950,000). The range of monetised slight injuries amounts to almost € 65,000 (between € 220 and € 66,000).

Comparison of countries reveals, in most cases, the accident components. The EU 28 [12] indicated for the year 2014 a total of 3,739 fatal accidents at work; the Czech Republic 118. An accident in the economy is an economy of *scale* and consequences. Table set out in the Annex allows structural insight into the statistics of accidents in industry. Work related, non-fatal accidents, are presented by increasing index 9-10. The Eurostat is working with the value impact of 3,176,640 accidents at work for year 2014. The EU-OSHA – European Agency for Safety and Health at Work, presents in [15] data as costs of work-related injuries and illness. These data are more substantial. In the EU-27 in 2007, 5,580 accidents at the workplace resulted in death and 2.9 % of the workforce had an accident at work that resulted in more than three days of absence, Figure 1.

Additionally, approximately 23 million people had a health problem caused or made worse by work across a 12-month period.

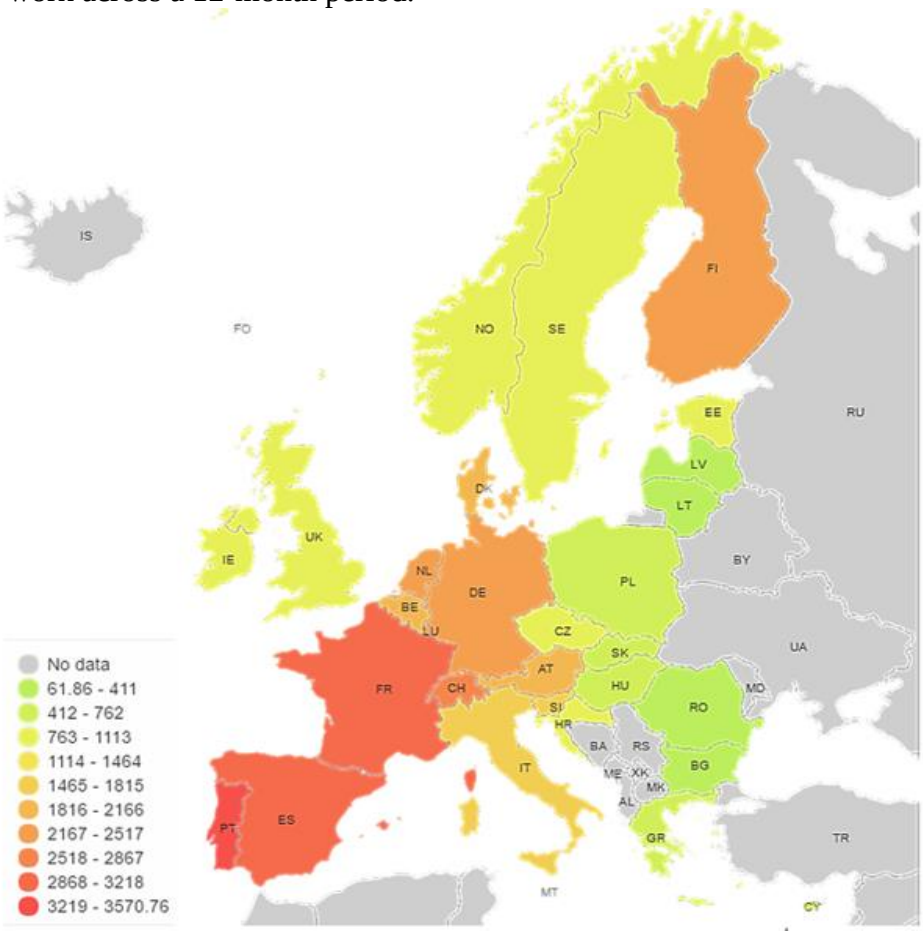


Fig. 1. Standardised incidence more details in Table given in Annex. The rate of accidents at work per 100,000 workers [12].

As an idea indicating the comparative problem scope was judged to be the most methodologically sound, these kinds of events are reported in Australia 2008/2009 as worth 4.8 % of GDP, in the Netherlands 3.0 % of GDP [13].

The economic risks are working of course within their own terminology. The causes are rooted in the technical area if they are traceable. If they are not traced, then economic disciplines use the wildcard term - uncertainty.

The model, which captures the shifts in investment demand, has been introduced by Baker et al. as variables around uncertainty [14]. Although, the standard economic theory explains the demand for capital in response to the user cost of capital and technology, the composite model captures the various dimensions of uncertainty, namely uncertainty as perceived by firms, financial markets and investors. In addition, the composite indicator is less "boisterous" than some of its component.

Although, a series of papers deals with qualitative and quantitative risk assessment, much less papers dealing with the risk identification are available. Salah and Moselhi introduced a developed method for identifying risks [15]. They define a matrix of responsibility for risk distribution among project participants, and they introduce a method for qualitative and quantitative evaluation of each item using the fuzzy logic and fuzzy probabilistic theory.

Lack of capacity, which would inhibit response to the existence of faults and failures, stresses the need to assess this resistance and its management, which can, however, be overcome according [16] by identifying and taking account the resistance factors, whereby in this context the developed model is significant in that:

- all uncertainty is relatively important in the business, and is certainly significant in terms of actual resistance factors and their values,
- the analytic hierarchy process is used for ranking the relative importance of business processes and factors of resilience is a process similar to human reasoning in general,

thus determining the values of variables is based on fuzzy pairwise comparison matrices with balanced decision making fuzzy groups. Finally, the accuracy of coefficient is based on the support of FTOPSIS software.

Projects aim at developing the new products, simultaneously they are full of uncertainties, which are caused not only by a chaotic surround, but also by scarcity of resources and strong competition. Screening the projects for development of new products that are competitive and have high potential market share is the most important business. For the effective implementation of this process, the authors [17] present a method of fuzzy multi-criteria group decision, i.e. a model called the project selection model potential (PPSM), which can serve as a decision-making mechanism to help businesses choose their projects in an uncertain environment.

Any incident data base for the EU 28 is affected by the diversity of national methodologies. These result from legislative differences and definitions of categories, etc. Comparisons are therefore of a limited nature. Interesting information connects the structure of economic activities to non-fatal and fatal accidents in EU28, 2013 [18]. The highest fatal activities are in the Construction and Manufacturing industries, followed by Transportation and Storage, Figure 2.

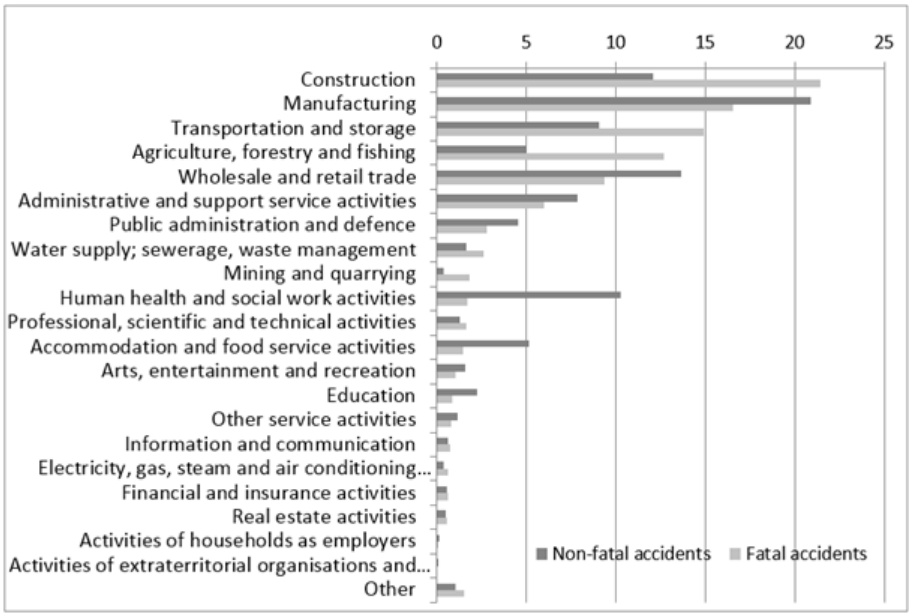


Fig. 2. Fatal and non-fatal accidents at work by economic activity, EU-28, 2013 [11, 12].

Risk analysis and decision making requires other statistical approaches than those already known classically. Especially rare phenomena (catastrophes) are in a T-E environment difficult to evaluate. There are insufficient data for such methods. Decision makers who are involved in catastrophic events use experts to evaluate risks and

consequences, and these are available in [19]. In this context subjective assessments are a natural part of decision process. Consequently, the Bayesian statistics seems to be suitable, since it offers a range of powerful tools utilising the concept of subjective probability which is, according to a Bayesian, a measure of a person's degree of belief; substantial contribution to the development has been done by a number of authors. One of the leading personalities of the discipline is Savage and already in 1954. This chapter attempts to contribute to a theory of how a decision maker may bring logic and system to their use of expert assistance.

The need for concerted action activities going beyond the national dimension is, with the given uncertainty, even more acute. One example which can serve here is the DynoTRAIN project, which was implemented under the 7th FP, in order to unify important open points in the technical specifications for the interoperability of the trans-European rail system and consequently capability to contribute to a "European" standardization. Reducing the cost of operating the process of assessing the dynamic properties is necessary for permission for entry into service according to an EU report Licciardello et al. [20], it requires to be in the form of quantitative results of experimental evaluation processes running through dynamic properties following the standard EN 14363 [21].

2.1 Input data and decisions and modification of decision method – MMM model

Most input data for decision making have their origin in measurements. Measurements are interrelated with some methodologies and devices. There exist a range of units, definitions, institutes that are responsible for control, time sequences of measurement, juridical correctness, and availability for users etc. Such time series $\{X_i\}$ have an improved background support and have mostly a better validity. The transformation (to be taken as process, method, model, theory, ...) to utility can be in general written as

$$\left\{\{X_i\} \xrightarrow{\boldsymbol{g}(X_i)} \{U_i\}\right\} \tag{3}$$

where $\{X_i\}$ **...** are measured data; time series for the criteria F_i , $g(X_i)$.. is a transfer (process, tool, way, function) of measured data to utility, within defined *critical values* (*min, max*), $\{U_i\}$ **...** are utility time series of criteria F_i .

The approach presented is dedicated to evaluation of risk. A transfer process $h(U_i)$ is required to facilitate relation

$$\left\{\{U_i\} \xrightarrow{\boldsymbol{h}(U_i)} \{R_i\}\right\} \tag{4}$$

where $\{R_i\}$ … are risk time series of risks based on utilities U_i , $h(U_i)$.. is a transfer process of utility data to risk data series.

Relations (3) and (4) give ability to get to decision criteria F_1, F_2, … corresponding time series $\{R_1\}$, $\{R_2\}$, ... Each time series contain in themselves the significance of the component. Risk is expressed in financial units, and therefore $\{R_1\}$, $\{R_2\}$, ... are additive ones for individual periods (years).

The criteria F(·) are understood as independent components. Very often there are risk associated decision models based on the relationship (1) or on its modifications. The calculations, which are reduced to aggregate technical-economic time series $\{X_i\}$, provide as a result simplified information – smoothed time series or simple averages etc. Such an approach addresses the suppression of internal information of series. The approach proposed in (2) and (3) keeps the information content of time series available and changes it only by its form and nature to risk, volatility, uncertainty, reliability etc.

If time series for decision making, gained in the past, are only partially valid for future technical-economic judgements, it is the role of experts to adapt them for further use. This means amenable to simulation of risk consequences, probab1ity evaluations, damage costs etc. An example of data implementation is presented in Table 2 to illustrate measurements obtained and the symbolism used.

Table 2. Measured data and example for theoretical background.

Variant 1	Variant 1: data series $\{X_i\}$ for criteria i = 1, 2, 3						
↓Criteria; Measurements in years -t →	$E(X_i)$	$\sigma(X_i)$	t-10	t-9		t-2	t-1
F_1 criterion and measurement series $\{X_1\}$	$E(X_1)$	$\sigma(X_1)$	$x_{1,t-10}$	$x_{1,t-9}$	…	$x_{1,t-2}$	$x_{1,t-1}$
F_2 criterion and measurement series $\{X_2\}$	$E(X_2)$	$\sigma(X_2)$	$x_{2,t-10}$	$x_{2,t-9}$	…	$x_{2,t-2}$	$x_{2,t-1}$
F_3 criterion and measurement series $\{X_3\}$	$E(X_3)$	$\sigma(X_3)$	$x_{3,t-10}$	$x_{3,t-9}$	…	$x_{3,t-2}$	$x_{3,t-1}$

Variant 1	Variant 1: data series $\{X_i\}$ for criteria i = 1, 2, 3											
↓Criteria; Measurements in years -t →	$E(X_i)$	$\sigma(X_i)$	t-10	t-9	t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1
F_1 – Investment (mil. €); time series $\{X_1\}$	96.20	19.0	99	100	90	120	70	110	60	105	87	121
F_2 – Durability (Years); $\{X_2\}$	26.20	11.3	25	22	30	17	15	30	10	50	23	40
F_3 – Local acceptability (+,...,-); $\{X_3\}$	6.00	1.7	8	5	7	4	6	7	6	5	9	3

Note: input measurement of technical-economic data for decision criteria F_1, F_2, F_3.

For some decision processes, if expert correction is necessary, the recalculation or prognosis is justified. An example is: the mean $E(X_1) = 96.2$ in Table 2 is a surrogate of measurements $\{X_1\}$. The dynamic properties of time series are then only figuratively apparent from $\sigma(X_1)$. Such surrogates in decision making are used frequently. Simplicity, however, it is paid for by the loss of information (time linkage, the substantive conditions etc.).

In the presented approach, we focus on preservation of properties for their transmission to utility and risk series quantification. If relations (3) and (4) are implemented on the mentioned basic series $\{X_1\}$ of measurements, the F_1, so investment, series $\{\boldsymbol{u}_1\}$, $\{\boldsymbol{r}_1\}$ enable more transparency for this decision criterion. Illustrative data of recalculation results are shown in Figure 3. A similar calculation is necessary for the criteria F_2, F_3.

Obviously at this point, it is necessary to note that there exist a number of decision-making methods. An approach differs for example according to dimension of criteria (the number of criteria). Let us be reminded – a one-dimensional decision (1D) criterion operates only on the basis of e.g. price or cost, profit, payback time, net present value (NPV), etc.

Multidimensional decision methods – (*n*D) are linked to the relation (1); however, in practice a time factor is omitted. The method, proposed here prefers to maintain the dynamic properties of time series for all hierarchical levels.

We call this approach the *Modified Multidimensional Model* (MMM); it works with the relationships (1) and (2), and it retains information data gathered in the original time series. The main aim of MMM is to preserve the informational substance of measured T-E indicators. In the example: F_1 – Investment (mil. €) in Table 2 is transformed by $\boldsymbol{g}(X)$ to U_1 – Investment utility and by h(U) to R_1 Investment Risk. Data are shown in Figure 3.

Both newly mentioned indicators in Figure 3 are modified to deterministic evaluations. The used approach based on $\boldsymbol{g}(\cdot)$ and $\boldsymbol{h}(\cdot)$ may be carried out in practice in more demanding forms. Recall that modifications, regulation, management activities, are in their origin actions or processes. They aim is to improve existing conditions. The results are new evaluated states, for example: benefit, utility, risk, etc.

The process in that case is understood in more general sense as a causal relationship. Its purpose may generally fulfil software needs, expert group or executive administration etc. The data for Figure 3 was transformed by means of experts. The expert group proposed the shape of functions $\boldsymbol{g}(X_1)$ and $\boldsymbol{h}(U_1)$.

2.2 Short interpretation of results

The interpretation of result measurements is given in Figure 3 and it is developed on this basis by input data – time series $\{X_1\}$. These time series data are adapted for further use (decision making) and preserve the time factor. As a convenient supporting result there are proposed qualitative sub-indicators U_1 - utility and R_1 - risk. Both indicators preserve the dynamic properties of the original - default - time series $\{X_1\}$. Aggregation without preserving the dynamic properties is contained in the report referred to in the Table 3. Loss of ability to watch deeper dynamic properties is balanced with simplicity and clarity. The dichotomy, involved in deciding whether aggregate information content, is more useful than the dynamic of time series, and it remains as a challenge for every decision-making body.

Table 3. Indicator F_1 – example, extension of indicators.

Indicator	**Value**
Total investment in period (-10 ... -1), (mil. €)	962.000
Total utility units acquired	31.300
Total risk expected (mil. €)	58.000
Risk per investment of mil. € and Year (%)	6.029
Utility per investment unit (%)	3.254

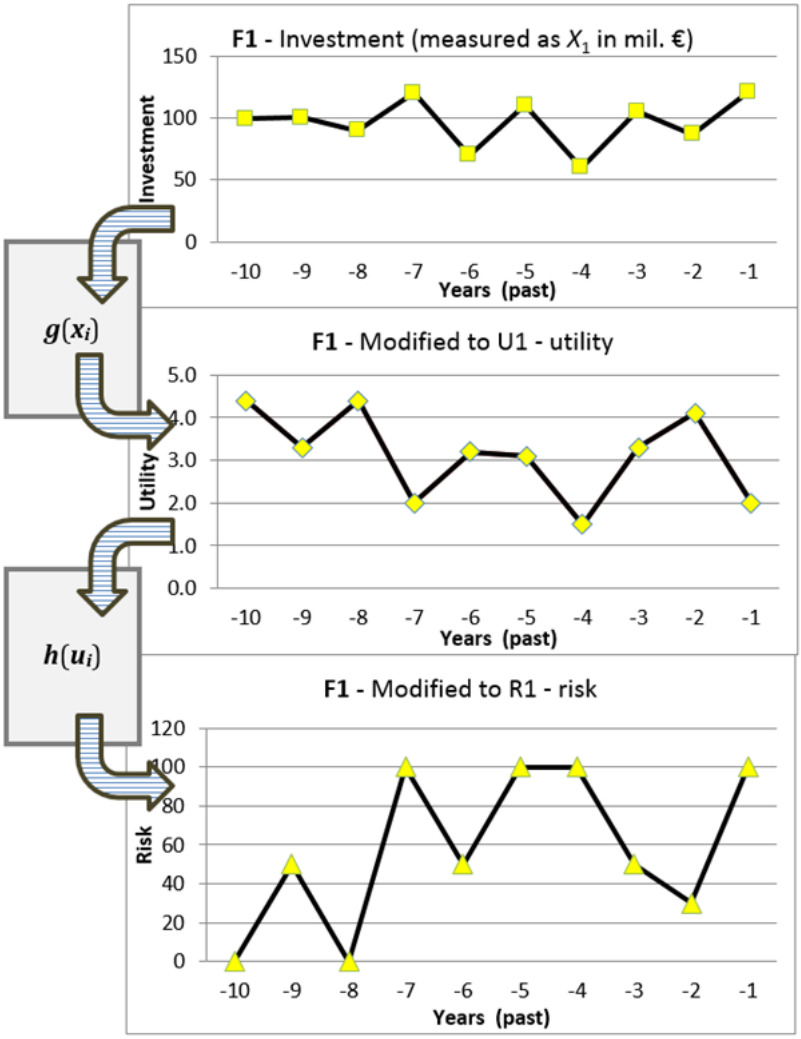


Fig. 3. Modification of time series measurement F_1 to U_1 – Utility and F_1 – Risk.

The same procedure is further addressed for more decision factors. Figure 4 shows another example of grouping decision criteria (F_1, ..., F_4). The decision maker is interested in evaluations for amalgamated evaluations (F_1 and F_2) mentioned in Figure 4 as an aggregation of second hierarchical level (F_1 and F_2)−*Project solution* and as (F_3 and F_4)− *Economic solution*.

The proposal (Example 1 in Fig. 4) shows the time dependent sequence (the horizontal axes) and decision criteria structure (vertical axes).

3. Description of data methods used

The assumption of expert evaluation is that the basic information is embedded for decision factor F_i in evaluation U_i. The basis of a credible U_i evaluation rests on past data (on physically measured data or statistical data) and in terms of future, it is somewhat misleading. The reality of decision making is that it focuses only on the future.

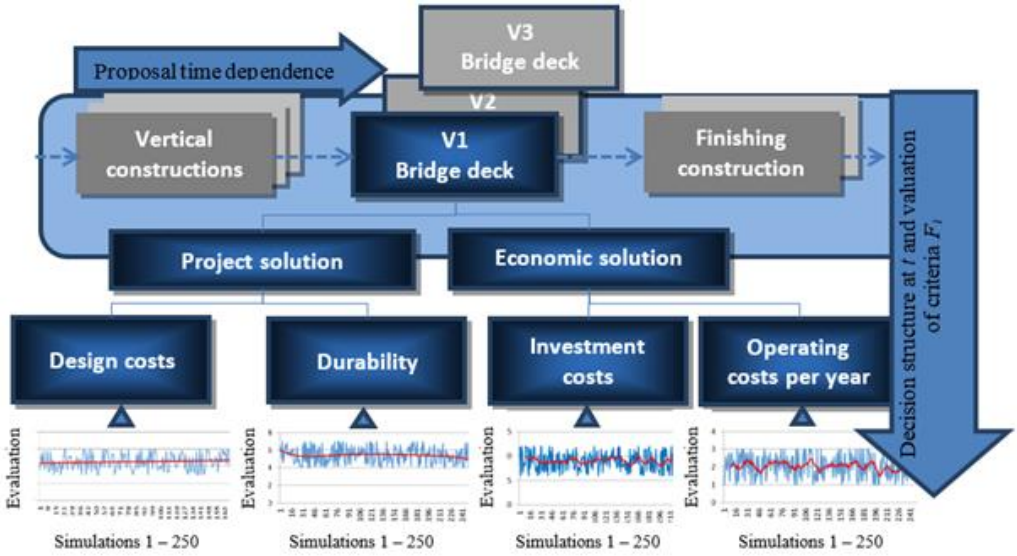


Fig. 4. The risk is embedded in evaluation of element bridge deck; V1, V2, V3 are the variants of construction solutions. The proposal shows time dependent sequence and decision criteria. Example 1.

Decision making disposed for a future interval $[0,\tau]$ requires an enrichment of past statistics by expert judgements regarding the future development. It is better talk about a dynamic model of expected future changes. In other words, it is necessary an expert *model*, which offers a prospective evaluation series for decision factor i for interval $[0,\tau]$ and time series $[u_{i1}, u_{i2}, \ldots, u_{i\tau}]$. The basis of such information is an adapted time series substitute $[x_{i1}, x_{i2}, \ldots, x_{i\tau}]$. Only hereby are the calculated (meaning as simulated, evaluated by experts) particular $x_{i\tau}$ plausible. The mentioned concept is illustrated in the example in Figure 3. The context of example is one single construction element, the bridge deck. The evaluation of four decision criteria $F_{1,\ldots,4}$ enables supplementary measures of statistical dispersion (variance, standard deviation, interquartile range etc.). Such a procedure leads to a reduction in informative content of the source information.

On the other hand, the series $[x_{i1}, x_{i2}, \ldots, x_{i\tau}]$ contain for example known risk, uncertainty etc. Bold thinking about the incidence of unexpected risks and their unexpected occurrence is appropriate. There is a poor level of reliable data on one site, and on the other it appears a quantity of unexpected unknown events. The paper [6] vividly recounts the problem and it speaks about black swans and data for post facto explanations without an existing statistical background. We may agree with Nafday [6] *…the likelihood of an event is usually estimated by using frequency of past similar events in event-tree methods but the likelihood for black swans cannot be estimated due to the lack of event knowledge and observed data. Expert opinions and subjective beliefs are also of minimal use since these are tainted by biases and constrained by finite human history and life span, which provides just a miniscule window to observe sparse events.* More is also provided in [5].

In this context, the flow of needs is evident. Specifically, it is necessary to improve the simulation methods and an implantation of experts´ doubts into utility evaluations $x_{i\tau} \rightarrow u_{i\tau}$. For management decision there are necessary further transformations to *risks* $u_{i\tau} \rightarrow r_{i\tau}$.

The techno-economics applications have close ties to timelines. Information content provided may be significantly damaged by changes such as, the reduction values on

average values, prognostic fitting curves and so on. On the other hand, it is objectively necessary to take into account the full range of decision criteria F_1, F_2, ... In any case, it is necessary to accumulate information from different sources in accordance with decision criteria. An example is given in Figure 3, where the concept shows criteria F_1, F_2, F_3, F_4 and their four-time series $\{X_1\}$, $\{X_2\}$, $\{X_3\}$, $\{X_4\}$. Aggregations are there designed to the middle level of decision tree, and is formulated as $(F_1 \cup F_2)$ – *Project solution* and modifies the series to $[\{X_1\} \cup \{X_2\}]$ evaluation. The amalgamation of $(F_3 \cup F_4)$ gives *Economic solution* evaluated as series $[\{X_3\} \cup \{X_4\}]$. The whole variant – *Bridge deck* – evaluation is obtained in a similar way.

The calculation methods are a mechanism that is preserving or disrupting the nature of initial information saved in the $\{X_1\}$, $\{X_2\}$, $\{X_3\}$, $\{X_4\}$; measured time series. Data are carriers of information. For calculation and T-E recommendations we use the simulation *PREV* (*Project Evaluation*). Software facilitates: assessment procedures; comparisons of assessments measured or evaluated by experts; corrections for improvements; and analysis of hierarchy of existing evaluations. The proposed tree structure and software support help to perceive past reality and expected tendencies. The possibility of collapses is part of reasoning for actual and future decisions. The illustrative input data are evident from the bottom in Figure 4. The evaluation of *base–node* of criteria is given in Table 4.

Schematic occurrence of unexpected events is given in Figure 5. Extreme evaluations are placed outside the expected range $\langle \bar{x}_j + \sigma_j; \bar{x}_j - \sigma_j \rangle$. For the labelling of what are and what are not unexpected events, it is appropriate to establish a definition level beyond the expected range.

The scheme of simulation for basic nodes is inserted in Figure 5. The vertical values that deviate away from the selected band are very danger and manageability is burdened with the costs consequences for each x_i.

The generation of the evaluation tree in Figure 6 is based on the data of Example 1 in Table 4. Important values for the *Base Nodes*: d*esign costs, durability, investment* time series are the inputs $\{X_i\}_t$ for risk oriented decision-making or factual series $\{X_i\}$ based on cross sectional data series relevant to a single time point (or interval), *costs, operating costs per year*. The values 999 indicate the calculated value (final evaluation). The extension or modification of the decision tree structure is in the hands of project management. In this case also the phase of transformation to deterministic evaluation values, $\bar{x}_{ij}$ and σ_{ij}.

The scheme was also presented before in Figure 3. The presentation discusses the extension of the measured input structure. The applied approach eliminates weights and works with the transforming functions. This procedure is applied over the entire hierarchy of the decision tree. The transition towards creation of a simulated time series is in the hands of the solver or researcher.

4. Results and analysis of outputs – example

In this part, the attention is focused on the extension of evaluations and some aspects of current practice in decision-making mechanisms respecting the risk. Data for decision-making are based on empirical data, i.e. real measurements. The proposed approach aims to rehabilitate the information contained in measured data for higher levels of decision-making tree structure and time horizons (decision life cycle). It is useful to point out the distinction between the time series inputs $\{X_i\}_t$ for risk oriented decision-making and the

factual series $\{X_i\}$ that are based on the cross sectional data series relevant to a single time point (or interval) and series of measurement or expert judgements.

Table 4. Description of project data (structure of the evaluation tree with main node, middle and base nodes) – Example 1.

Level	**Item ID**	**Parent ID**	**Weight** w_{ij}	**Evaluation** $\bar{x}_{ij}$	**Sigma** σ_{ij}	**Title**	**Description**
0	0	-1	999	999	999	Bridge deck	**Construction variant**
1	1	0	0.3	999	999	Project solution	Project technology
1	2	0	0.7	999	999	Economic solution	Purchase, operating costs
2	3	1	0.4	7.75	1.192	Design costs	*Design costs*
2	4	1	0.6	7	2.017	Durability	*Project duration*
2	5	2	0.5	7.3	1.46	Investment costs	*Bridge deck costs*
2	6	2	0.5	6.6	1.32	Operating costs per year	*Operating costs*

Note: number 999 indicates the calculated values (final evaluation).

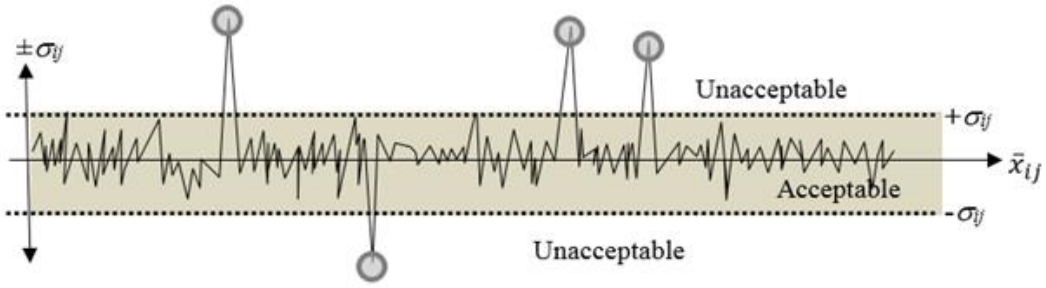


Fig. 5. The scheme of simulation with sparse (unexpected and unacceptable) events. Highlighted values are outside the main simulation zone of the expected simulation data flow (acceptable range).

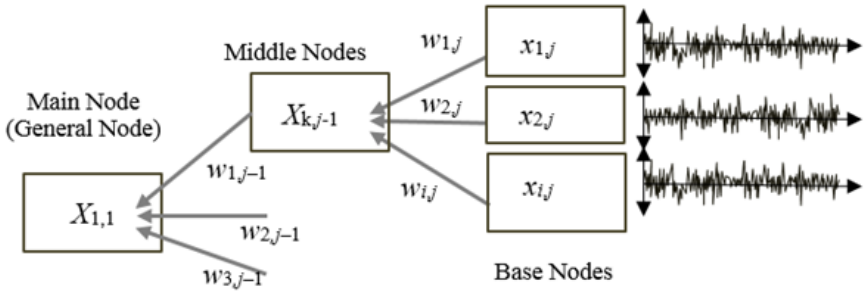


Fig. 6. The structure of project nodes (decomposition to levels of project evaluation).

The solution or the application is applied to the tree-decomposition of project evaluation criteria [23], which offers the standard calculation methods for example FTA (Fault Tree Analysis [24]), TOPSIS [25] or appropriately a type of the MCDM method [26]. The evaluation of the FTA tree allows the determination of conditions creating the fault situations. The structure of decision tree may be limited to simple methods

mentioned formerly, before application of MCDM or extended methods which works with time series on all levels of hierarchy tree. Multidimensional methods prefer, at least till now, weighting as a transformation tool. The evaluation of particular nodes, and elementary parameters are implemented there as:

w_{ij} - evaluation of weight of node (element) *i* on the decomposition level *j* significance),

σ_{ij} – standard deviation of evaluation of node (element) *i* on decomposition level *j* (specified size of dispersion),

$\bar{x}_{ij}$ – evaluation of node (element) *i* on decomposition level *j*.

Defined values are applied on the nodes of the criteria tree, which are named as:

- main node (general node),
- middle nodes,
- base nodes.

All the parameters w_{ij}, σ_{ij}, $\bar{x}_{ij}$ are embedded in *Base Nodes*. The evaluation of the aggregation weights w_{ij} is defined for *Middle Nodes*. The top *Main Node* does not contain any evaluation parameter.

$$X_{k,j-1} = \sum_{i=1}^{n} w_{i,j}\bar{x}_{ij} \tag{5}$$

where: $X_{k,j-1}$ *is* node (element) on level *j*–1, *n* is number of nodes on level *j*, w_{ij} is evaluation of the weight of node (element) *i* on the decomposition level *j* (significance), $\bar{x}_{ij}$ is evaluation of node (element) *i* on decomposition level *j*.

The range of element evaluation is appropriately defined into the closed interval for example 1 to 10 (according to the evaluation methodology). With defined parameters there operates the aggregating calculation. The evaluation of the end-nodes parameters makes it possible to obtain two basic methodological approaches:

- ensure an adequate amount of experts,
- simulate pattern of evaluation, which has defined parameters.

The approach No. 1 requires a group of individual experts. The calculation demands a sufficient count of experts with professional knowledge. The second approach No. 2 is not so demanding in terms of range/number of experts, but requires the right parameter settings for creating a simulation pattern. The parameters for simulation must be validated by competent estimation (calculation). We are referring to the acquisition parameters mentioned before as w_{ij}, σ_{ij}, $\bar{x}_{ij}$.

Both approaches in evaluation of *end nodes* conceal the possibility of sparsely occurring values (unusual values, unusual events...). The reasons for their existence can be different. In the case of approach, No 1. It may be an (actual person) expert with:

- poor knowledge,
- incomplete knowledge,
- misleading knowledge,
- dishonest intent,
- misunderstanding of the facts and the assignment.

The danger of these sparse values increases with the number of experts (evaluators). In the case of simulation approach No. 2, all these aspects are associated with the human factor category and are eliminated down to a single evaluation (estimation) or to a parameters dependent simulation pattern. The simulation pattern is software generated and it is not burdened by human influences and other negative consequences. For the values that are beyond the acceptable risk area (mentioned on Figure 5, Example 2), we

are required to implement according to reports about appearance of *sparse* events. The result is the risk assessment, labelling the situation as unacceptable and consequently the designated variant solution as inadmissible.

The data for Example 2 are described in Table 5. This is a different type of project compared with Example 1. The main node is describing an investment project of a Residential house (RH03). The second hierarchical level is named *Facade and Doors/Windows*; details are in Figure 7. The evaluations of base nodes are created on the statistical data (real measurements). The solution of Example 2 is in foregoing section.

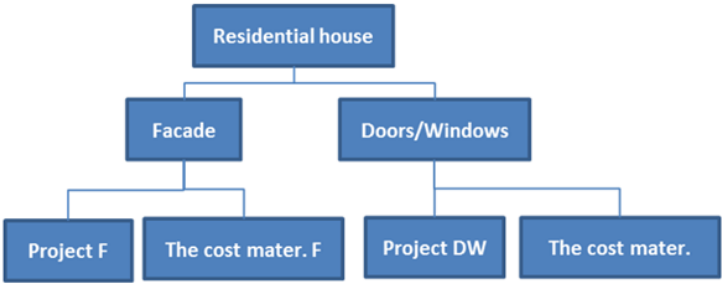


Fig. 7. The tree structure for project of Residential house (RH03), Example 2. The tree is generated according to data described in Table 5.

Table 5. Description of project data (structure of the evaluation tree with main node, middle and base nodes) – Example 2.

Level	Item ID	Parent ID	Weight w_{ij}	Evaluation $\bar{x}_{ij}$	Sigma σ_{ij}	Title
0	0	-1	0,15	999	999	Residential house RH03
1	1	0	0,6	999	999	Façade
2	2	1	0,45	7	1,5	Project F
2	3	1	0,55	6	2	The cost mater. F
1	4	0	0,4	999	999	Doors/Windows
2	5	4	0,3	6	1,3	Project DW
2	6	4	0,7	7	2	The cost mater. DW

5. Results and evaluation

The approach mentioned in the previous parts is applied to Example 1 (*Bridge deck*). The example is aimed at selecting the most appropriate technical-economic standards in a design project. For illustration there is chosen a decision about the best convenient variant of *Bridge deck*. Assuming that it is necessary to improve the collection of experts' judgements or, input data which are not satisfactory for validation into the future. The final pattern of input data is incomplete (high differences, poor quantity of judgements, etc.). For evaluation of project tree, it is chosen the second simulation approach (see Part 4, ad 2) on the basis of already existing inputs completed with new information (such as statistics, studies, and additional expert evaluations). The results of simulation for node *Design costs* we can follow on Figure 8. For comparison there are given the results in a

common chart with evaluation, which show the presence of sparse events (example is given in Figure 9). The simulated evaluation is aggregated according to formula (2) into the higher *Middle nodes* to the *General node* depicted on Figure 6.

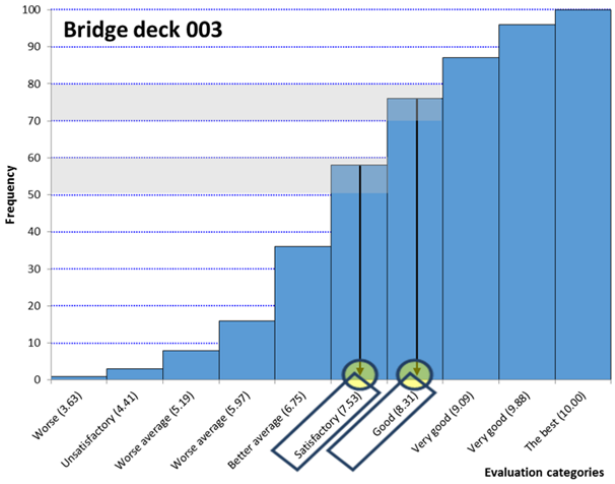


Fig. 8. Evaluation of Bridge deck – simulation results. On the level 80 % we can read evaluation Good (8.31). On the level 50% we can find evaluation satisfactory (7.53).

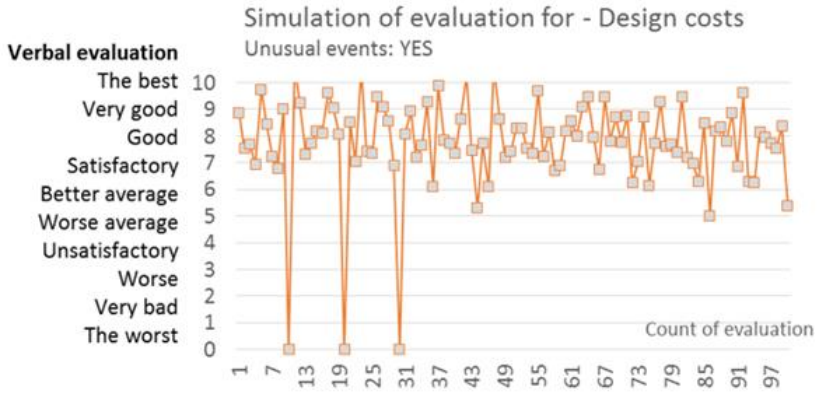


Fig. 9. Simulation of evaluation for project part Construction costs with sparsely events.

In the Figure 10 we can see a simulated-evaluation with limit 3% occurrence of unexpected events. The further question that can be posed is: how significant is this when the final evaluation reaches a higher occurrence of the unexpected events than 3%.

The practical impact of the given example should be seen in the fact that the occurrence of sparse events influences the evaluation only minimally in this particular case (see the difference in Figure 11). However, it is not possible to be content with this statement and it is necessary to search for the causes of their occurrence. The reason is to gain warning signals for evaluators or for other causes stated in section 4, with more in [27].

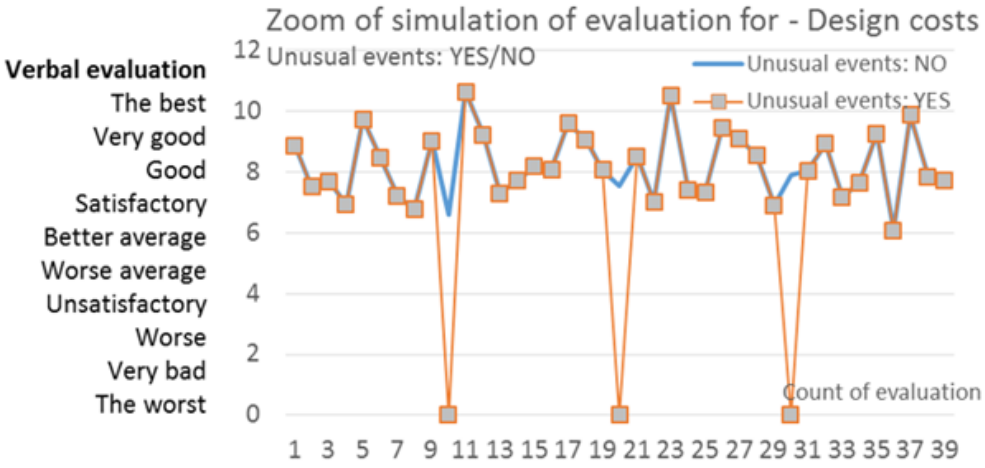


Fig. 10. Comparison simulation of evaluation. Simulation with/without sparsely events (data series YES/NO).

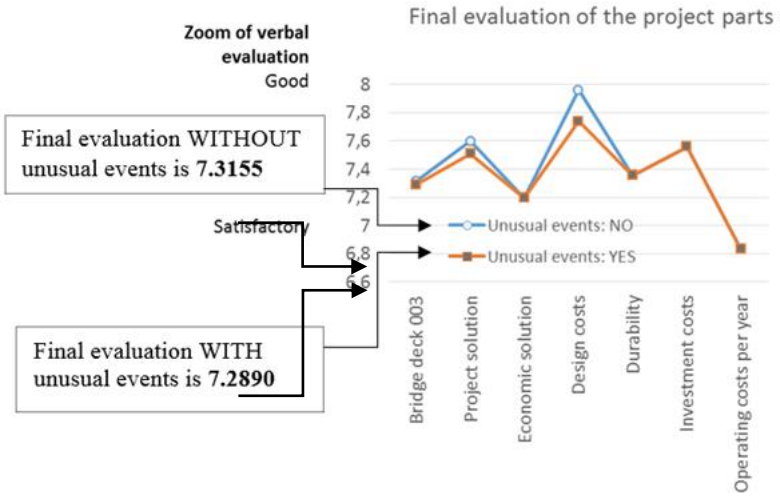


Fig. 11. The final evaluation of the project parts in the case of sparse events: YES/NO.

In Figures 12 and 13 there are the results of simulation with different frequency of occurrence of unexpected events. The initial precondition was that the occurrence of unexpected events has a massive impact on the final evaluation of design project. This initial assumption has not been confirmed.

In the final evaluation of Example 1, Table 6, we see that there are a large number of unexpected evaluations for evaluated element *Design costs*. The evaluation of project shows in the 10% evaluations occurrence of unexpected events that is written as $X_{10\%}$ = 7.2190. In the case, when the part "*Design costs"* is theoretically absolutely eliminated by unexpected events is the final evaluation $X_{100\%}$ = 6.3603. Verbal description for $X_{100\%}$ is *Better average* and for $X_{10\%}$ is *Satisfactory*. The project with this verbal description is acceptable, but from the point of view of unexpected events (risk) it is absolutely unacceptable.

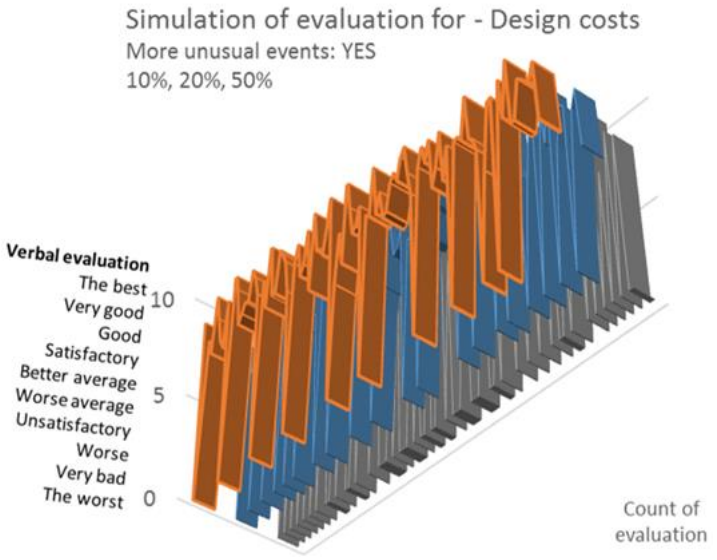


Fig. 12. Comparison simulation with different number of unexpected events. There is 10%, 20%, 50% occurrence of the unexpected events in element Design.

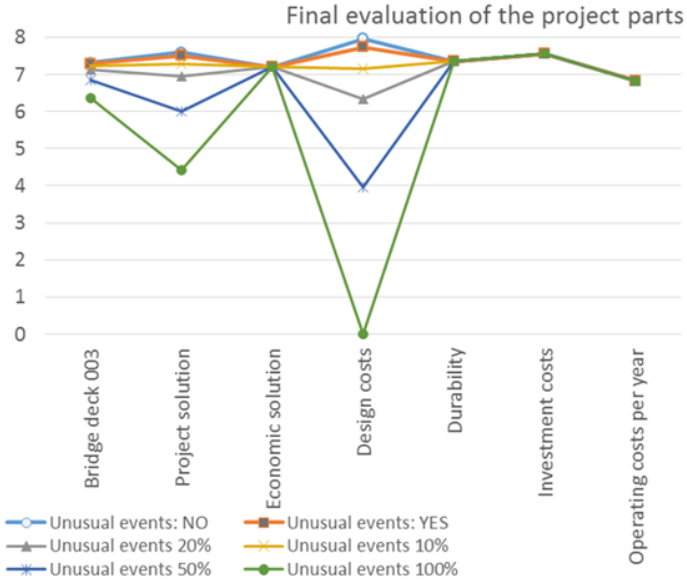


Fig. 13. Comparison of the final evaluation of the project part. The occurrence of the unexpected events is gradually 10%, 20%, 50%, 100%.

Table 6. Final evaluation with different number of sparse events (unexpected events).

Final project evaluation	
Without sparse events for *Design costs*	7.3155
With sparse events for *Design costs* 3%	7.2890
10%	7.2190
20%	7.1199
50%	6.8352
100%	6.3603

From this reason, we implement at evaluation of Example 2 the costs considering the risk. From historical data the evaluation in Table 4 is performed and then implemented the project tree in Figure 7. After simulation we get progress in evaluation for base nodes, middle nodes and main node of the project. Simulation of the parameters for *Project Facade* and *Material of Facade* we can see in Figures 14 and 15.

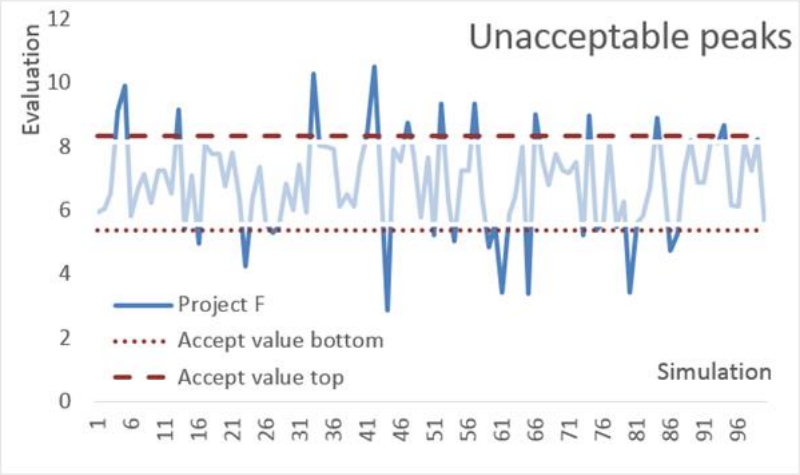


Fig. 14. Simulation of evaluation for Project Facade with highlighted non-acceptable peaks of evaluations.

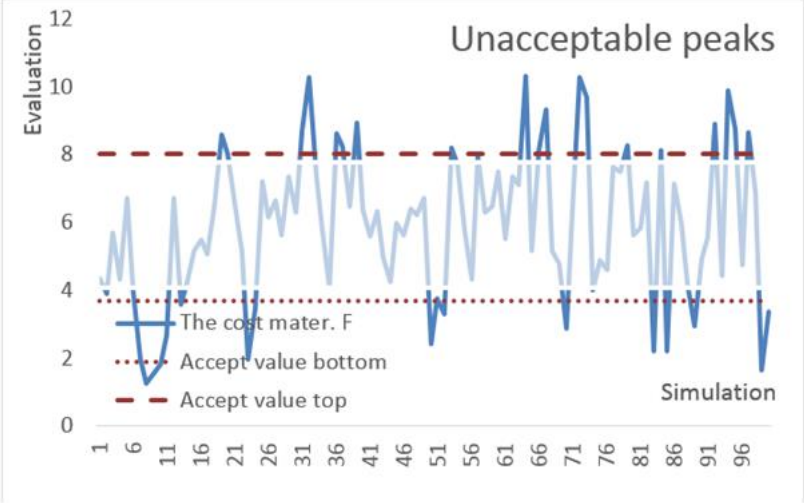


Fig. 15. Simulation of evaluation for Material of Facade with highlighted non-acceptable peaks of evaluations.

The non-acceptable peaks highlighted in Figures 14 and 15 are interpreted as unexpected events. In the next step, it is necessary to transform the dimensionless evaluation to the risk costs and to financial units. It is necessary to define a transformation function with which graphic interpretation is presented in Figure 17, the used source code is available in Figure 16.

```
Function EvalRisk(AEval As Double, APositive As Boolean) As Double
EvalRisk = 0
If APositive Then // part for positive value
If (AEval > 0) And (AEval <= 0.5) Then
EvalRisk = 200000
ElseIf (AEval > 0.5) And (AEval <= 1) Then
EvalRisk = 230000
ElseIf (AEval > 1) And (AEval <= 2) Then
EvalRisk = 300000
ElseIf (AEval > 2) And (AEval <= 3) Then
EvalRisk = 400000
ElseIf (AEval > 3)
EvalRisk = 500000
End If
Else // part for negative value
If (AEval > 0) And (AEval <= 0.3) Then
EvalRisk = 100000
ElseIf (AEval > 0.3) And (AEval <= 2) Then
EvalRisk = 220000
ElseIf (AEval > 2) Then
EvalRisk = 300000
End If
End If
End Function
```

Fig. 16. Source code of the transformation between evaluation and risk costs.

In Figure 17, there is presented an illustrative source code of the transformation function between a dimensionless evaluation and risk costs (in financial units). In the transformation function there are defined two parts. The first one pays attention to the positive values of evaluations and the other deals with the negative values of evaluations. Intervals of evaluations for positive values was defined by a specialist as $(0;0.5\rangle$, $(0.5;1.0\rangle$, $(1.0;2.0\rangle$, $(2.0;3.0\rangle$, $(3.0;\infty)$. Intervals for negative values are defined as $(0;0.3\rangle$, $(0.3;2.0\rangle$, $(2.0;\infty)$.

Figure 18 gives the graphic relation between dimensionless evaluation and risk costs. Risk costs over the limit for unexpected events and under a defined limit are visualized in Figure 18.

The last step in calculation of risk costs for the project is the creation of the frequencies and distribution function to the risk costs, Figure 19. The level of reliability is defined as P = 0.8. The value of risk costs on a defined level of reliability is $X_{P=0.8}$ = 200000Eur.

6. Conclusions

Let us focus on the decision making process which is based on knowledge embedded in some *ex post* data. The evaluation (based on knowledge as the statistical characterisation, correlation, etc.) represents the core of useful information for current decision making about techno-economic processes or other T-E future activities. The chapter as such presents two stimuli.

The first one is an *idea about information content* of time series based on measurement of original techno-economic process data. The data series can be transformed to *utility* and subsequently to *risk* or other streams through the process of evaluating indicators. The decision factor F_i is proposed to be calculated and evaluated as a three dimensional quantity (variable) – *value, utility, risk.* The method proposed avoids weighting indices and *recommends the transfer function* as a more general tool.

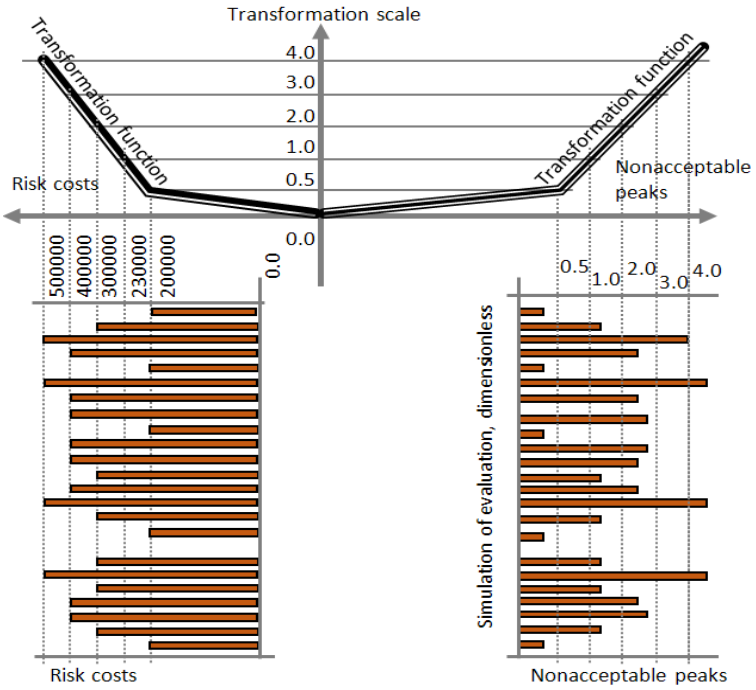


Fig. 17. Scheme of the transformation scale between non-acceptable peaks and risk costs.

Fig. 18. Graphic representation of non-acceptable peaks in financial units. Transformation is realized by the risk costs transformation function.

The second stimulus is to open up the question about validity of decisions based on simplified decision-making evaluations without a time factor−it is incorporated into the proposed approach, as an important part of all long-lasting processes.

Implementation for the multidimensional decision making is given in Example 1 and Example 2. The first example deals with conversion of techno-economic units: to *utility and risk* by means of transfer functions (avoiding use of probabilities or weights).

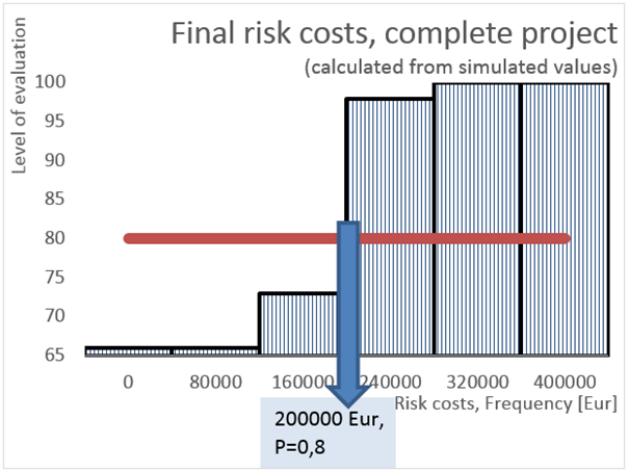


Fig. 19. The cutting of risk costs - final calculation for the entire project and defined confidence levels.

The second example proceeds with simulation and usage of the past, historical data as a precondition for framing data for the *ex ante* decisions.

It is matter of fact that the implementation and correct use of past data for decisions valid in the future is often overestimated. However, all the decision applications will operate in the future. It remains that the decision methods with long life require more sophisticated methods and computer support.

The horizontal time axis in most decision situations is running in long time unit t (weeks, months, years) and the decision making process is running in time $\tau << t$ (hours, days).

The dichotomy in description of the factual elements distinguishes the past versus the future. This view is an advanced challenge to currently used methods and calculations. Development and decision making of technical-economic processes is very diverse. It extends to raw materials, energy, and labour allocated over time. In terms of development the modern society is an open society. This means modern solutions and associated activities (processes) are in fact non- linear, and not in equilibrium states.

Project security evaluation is applied on many levels of business management. Correct decisions lead to savings on all types of resources linked to time stretch and personnel impacts. The introduction of the appropriate methodology for the evaluation does not signify a result, however, to improve T-E security, risk recognition and implementation of early timed security measures. The application examples demonstrate that the occurrence of distinctively negative expert estimates lead only to a small distinction in the final evaluation. The rationally thinking evaluator, however, cannot be content with such a conclusion and should look also for the causes behind the occurrence of critical and danger sparse events.

Mathematical symbols used in text

F_i ...verbal description of decision criteria i,
U ... utility of a technical-economic solution,
w vector of weights of technical-economic decision factors,
h ... vector of evaluation of decision criteria

$\{X_i\}$ **...** are measured data; time series of criteria F_i,
$\boldsymbol{g}(X_i)$.. is a transfer (process, tool, way, function) of measured data to utility,
$\{R_i\}$ … are risk time series of risks based on utilities U_i ,
$\boldsymbol{h}(U_i)$.. is a transfer process of utility data to risk data series,
$\{X_i\}_t$ .. are time series inputs for risk oriented decision-making,
$\{X_i\}_s$ .. is factual series based on cross sectional data series to a single time point (or interval).

Annex

Number of non-fatal and fatal accidents at work, 2014, details in [11]. (*), (persons)

	Accidents at work involving at least four calendar days of absence from work			Fatal accidents at work
	Total	Men	Women	Total
EU-28	*3 176 640*	*2 183 494*	*992 870*	*3 739*
Belgium	65 587	46 812	18 771	52
Bulgaria	2 246	1 600	646	117
Czech Republic	42 306	29 797	12 509	118
Denmark	54 157	31 920	22 041	38
Germany	847 370	631 819	215 552	500
Estonia	6 288	4 097	2 191	16
Ireland	18 115	12 503	5 583	47
Greece	3 410	2 551	859	28
Spain	387 439	264 010	123 430	280
France	724 662	454 997	269 664	589
Croatia	11 669	7 686	3 981	26
Italy	313 312	226 263	87 049	522
Cyprus	1 613	1 145	468	5
Latvia	1 725	1 154	571	41
Lithuania	3 120	2 025	1 092	55
Luxembourg	7 183	5 701	1 482	10
Hungary	19 491	12 674	6 817	81
Malta	2 632	2 235	397	4
Netherlands	87 964	55 567	32 397	45
Austria	65 418	51 352	14 066	126
Poland	76 274	50 294	25 980	263
Portugal	130 153	93 003	37 150	160
Romania	3 396	2 629	767	272
Slovenia	12 314	9 312	3 002	25
Slovakia	8 552	5 910	2 642	40
Finland (')	47 432	32 630	14 802	22
Sweden	35 296	19 596	15 700	40
United Kingdom	244 948	156 842	88 064	239
Iceland (')	1 787	1 182	605	0
Norway	10 108	6 243	3 865	61
Switzerland	86 346	68 492	17 854	74

References

[1] TALEB, N. N. *The Black Swan: The Impact of the Highly Improbable*. ISBN: 978-1-4000-6351-2. London: PENGUIN, 2007, 366p.

[2] CARGALO, C., CARVALHO, A., GERNAEY, K., SIN, G. A Framework for Techno-Economic & Environmental Sustainability Analysis by Risk Assessment for Conceptual Process Evaluation. *Biochemical Engineering Journal*, ISSN: 1369-703X, 12 (2016), pp. 146-156.

[3] JODL, H., G. Risk in the Implementation of Construction Projects –Defining the Risk. *Geomechanics and Tunnelling*, ISSN: 1865-7389, 7 (2014), pp. 709–714.

[4] JENSEN, P. A., MASLESA, E. Value based building renovation – A tool for decision-making and evaluation, Building and Environment, ISSN: 0360-1323, 92 (2015), pp. 1-9.

[5] COMPTON, P., DEVUYST, D., HENS, L., NATH B. *Environmental Management in Practice*. Routledge 2002, p. 544.

[6] GB PARLIAMENT. *Outcomes of the UN Rio+20 Earth Summit, 2013-14*, 1 (2013), p. 83.

[7] ISO. *IEC 31010:2009 Risk Management – Risk Assessment Techni*ques, Zuerich: International Organization for Standardization – ISO, 2009.

[8] BERAN, V. DLASK, P. *PREV – Mosaic – Theoretical Guide*. ISBN: 978-80-01-04880-1. Praha: CVUT 2011, 26p.

[9] TALEB, N., N. *Anti-fragile*. ISBN: 978-0-8129-7968-8. London: Penguin 2012, 519p.

[10] TAMOŠAITIENĖ, J., ZAVADSKAS, E., K., TURSKIS, Z. Multi-criteria Risk Assessment of a Construction Project. *Procedia Computer Science*, ISSN: 1877-0509, 17 (2013), pp. 129-133.

[11] EU. *European Statistics on Accidents at Work (ESAW) — Summary methodology*. ISBN: 978-92-79-28419-9, ISSN: 1977-0375., Luxembourg 2013, pp. 59, http:// ec.europa.eu/eurostat/web/main

[12] EUROSTAT *Fatal Accidents at Work by NACE Rev. 2 activity*, (*Database file* [hsw_n2_02], http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=hsw_ n2_ 02 &lang=en.

[13] KASNATSCHEEW, A., et al. *Review of European Accident Cost Calculation Methods – With Regard to Vulnerable Road Users*. Federal Highway Research Institute (BASt) 2016.

[14] BAKER, J., CARRERAS, O., KIRBY, S., MEANING, J., PIGGOTT, R. Modelling Events: The Short-term Economic Impact of Leaving the EU. Economic Modelling. ISSN: 0264-9993, 58 (2016), pp. 339-350.

[15] SALAH, A., MOSELHI, O. Risk Identification and Assessment for Engineering Procurement Construction Management Projects Using Fuzzy Set Theory. *Canadian Journal of Civil Engineering*, ISSN: 0315-1468, 43 (2016), pp. 429-442.

[16] MACUZIĆ, I., TADIĆ, D., ALEKSIĆ, A., STEFANOVIĆ, M. A Two Step Fuzzy Model for the Assessment and Ranking of Organizational Resilience Factors in the Process Industry. *Journal of Loss Prevention in the Process Industries*. ISSN: 0950-4230, 40 (2016), pp. 122-130.

[17] CHIU-CHI., W., AGUS, A., HOUN-WEN, X., CHIOU-SHUEI, W., TING-CHANG., L. A New Fuzzy Decision-Making Approach for Selecting New Product

Development Project. *Concurrent Engineering.* ISSN: 1063293X, 24 (2016), 3, pp. 240-250.
[18] EUROSTAT. *Statistics Explained – Accidents at Work Statistics*. Luxembourg 2017. ISSN: 2443-8219. http://ec.europa.eu/eurostat/statistics-explained/index.php/Accidents_ at_ work_ statistics. Last update: 29 November 2016.
[19] SAERS BIGÜN, E. Risk Analysis of Catastrophe Using Experts´ Judgements: An Empirical Study on Risk Analysis of Major Civil Aircraft Accidents in Europe. *European Journal of Operational Research.* ISSN: 0377-2217, 87 (1995), pp. 599-612.
[20] LICCIARDELLO, R., FUNFSCHILLING, C., MALAVASI, G. Accuracy of the experimental assessment of running dynamics characteristics quantified through an uncertainty framework. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, ISSN: 0954-4097, (2016), pp. 567-569.
[21] EU. *EN 14363:2016 Railway applications. Testing and Simulation for the acceptance of running characteristics of railway vehicles.*
[22] FLAGE, R., AVEN, T. Emerging Risk - Conceptual Definition and a Relation to Black Swan Type of Event. *Reliability Engineering & System Safety.* ISSN: 0951-8320, 144 (2015), pp. 61–67.
[23] GÜRLÜK, S., UZEL, G. An Evaluation of Agri-Environmental Indicators through a Multi-Criteria Decision-Making Tool in Germany, France, the Netherlands, and Turkey. *Pol. J. Environ. Stud.* ISSN: 1230-1485, 25 (2016), 4, pp. 1523–1528.
[24] RODRÍGEUZ, A., ORTEGA, F., CONCEPCIÓN, R. A Method for the Evaluation of Risk in IT Projects. *Expert Systems with Applications*. ISSN: 0957-4174. 45 (2016), pp. 273–285.
[25] NAFDAY A., M. Consequence-Based Structural Design Approach for Black Swan Events. *Structural Safety*. ISSN: 0167-4730, 33 (2011), pp. 108–114.
[26] LIN, J., YUAN, Y, ZHANG, M. Improved FTA Methodology and Application to Subsea Pipeline Reliability Design. *PLoS ONE Access.* ISSN: e93042, 9(2014), 3, pp. 1–10.
[27] KOLIOS, A., MYTILINOU, V., LOZANO-MINGUEZ, E., SALONITIS, K. A Comparative Study of Multiple-Criteria Decision-Making Methods under Stochastic Inputs. *Energies.* ISSN: 1996-1073, 9 (2016), 566, pp. 1–21.

Chapter 13

THE RELIABILITY EVALUTION OF ASSEMBLY LINES USING MODELS*

1. Introduction

A significant case of discontinuous devices with relatively high failure rate are the automatic assembly lines for the mechanical and electrotechnical production of components and devices. The failure rate of an assembly process has an impact on the economic efficiency of the line. For typical assembly operations are used modular units, they are arranged in a one-lane or multi-lane automatic line with a fixed or variable attachment. Each assembly node includes an assembling work station, component feeder, and conveyor where the semi-finished product moves on and the information system that registers fault modes such as binary signals from the sensors. The failure rate is affected by the line construction, operator skills and scrap rate of supplied components.

The objective of this paper is to analyse the impact of the components' scrap rate and the assembly line's downtime period in relation to its performance. The formulations of the relative performance are shown graphically for clarity. Based on experimentally identified data about the node failure rate and also the whole line, which are being registered by monitoring and information system, the work is further focused on mathematical-statistical evaluation. It is necessary to obtain the most accurate approximation of activity duration distribution and downtime duration from the histograms of relative downtime frequency for a typical assembly node and the line for cumulative relative activity frequency in different periods of running-in stage of the line, and simulate its behaviour in various modes and in more complex arrangements [1].

2. Background research and solution concept

The paper extends into the following areas:

- reliability and failure rate of machines,
  Reliability is a significant characteristic in real setting. With complexity of the device, and with number of components the risk of failure occurrence is increasing. Reliability can be enhanced by control measures, replenishment of the automatic machine and implementation of maintenance works [1-5].
- mathematical-statistical reliability evaluation,
  Reliability of individual automatic machines and assembly lines is described on the basis of mathematical probability theory. As a characteristic of reliability we define as a time of seamless operation and resumption of operability using the distribution

Authors: Dipl. Ing. Miloslav Linda, Ph.D., Dipl. Ing. Gunnar Kűnzel, Dipl. Ing. Monika Hromasová, Ph.D., Jiří Prokopec. Czech University of Life Sciences Prague, Praha, linda@tf.czu.cz

function and probability density function. The most commonly used are experimental, Weibull, Gamma, normal and log-normal probability distribution. When applying the exponential distribution, there is an advantage of using the Laplace transform and the theory of Markov processes for modelling automatic machines with reserve [6-8].

- design of automatic manufacturing systems,
  It contains variant configuration of technological lines in various fields, optimizing storage capacity of feeders, control of technological processes using computers and behavioural simulations of the proposed system [9-11].
- sensors, measuring systems and software,
  To record the failure rate and reliability, it is necessary to address a selection of suitable sensors with double-value signals (e.g. optoelectronic, inductive, capacitive) and the circuits for the integrated measuring system that is part of the assembly line [12-13].

Using appropriate software enables us to collect and continuously process data about the node failure and the whole line failure. For behavioural simulation is convenient to use i.e. an interface Scilab Xcos for dynamic calculations and statistics [14-15].

The assumed reliability solution of the line is based on block diagram of a simple serial line, equipped with control and measuring system (Fig. 1). From the available data registered in the form of tables we plotted histograms of relative frequency of both the assembly node period and the assembly line period, and also the downtime duration. Based on identification methods we determined the distribution function and probability density, provided that a superposition of two exponential probability distribution. The possibilities of using this methodology are set out in conclusion [1].

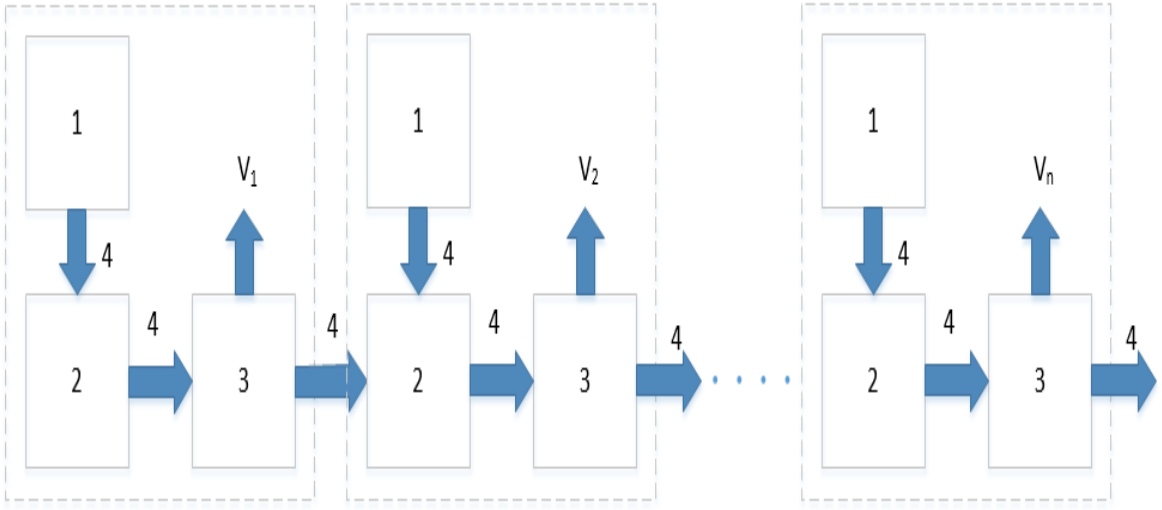


Fig. 1. Block diagram of the automatic assembly line part [1]. 1 – a component feeder, 2 – an assembling work station, 3 – control and measuring system, 4 – conveyor, V_1, V_2 … V_n – output signals for registration of the failure modes.

3. Data description

Data were repeatedly obtained during the operation on a real assembly line (Fig. 1). Mean values are shown in Tables 1 - 3.

Table 1. The relative frequency values of the assembly node's activity period.

Number of tacts (-)	Relative frequency of activity period (-)
0	0.34
100	0.15
200	0.09
300	0.06
400	0.05
500	0.025
600	0.03
700	0.015
800	0.019
900	0.025
1000	0.015
1100	0.013
1200	0.013
1300	0.014
1400	0.015
1500	0.015

Table 2. The relative frequency values of the whole line's activity period.

Number of tacts (-)	Relative frequency of activity period (-)
0	0.035
5	0.015
10	0.016
15	0.013
20	0.011
25	0.009
30	0.01
35	0.008
40	0.009
45	0.007
50	0.005
55	0.004
60	0.003
65	0.0025
70	0.0025

Table 3. The relative downtime-frequency values of the assembly node and the relative downtime-frequency values of the whole line.

Number of tacts (-)	Relative frequency of downtime periods of the assembly node (-)	Relative frequency of downtime periods of the whole line (-)
0	0.025	0.07
1	0.045	0.09

2	0.075	0.092
3	0.06	0.087
4	0.09	0.084
5	0.1	0.07
6	0.095	0.06
7	0.09	0.056
8	0.085	0.05
9	0.065	0.043
10	0.07	0.037
11	0.03	0.031
12	0.025	0.025
13	0.02	0.023
14	0.017	0.02
15	0.025	0.018
16	0.013	0.015
17	0.014	0.012
18	0.006	0.01
19	0.003	0.014
20	0.003	0.014

4. Methods

4.1. Analysing the effect of scrap rate on the automatic line performance

In case that we assess the automatic assembly lines V_1 (pc.min^{-1}) only by the number of correctly assembled products per unit of time, we obtain a simple relation (1)

$$V_1 = \frac{60}{T_t}\prod_{i=1}^{m}(1-q_i)\,, \tag{1}$$

where: T_t (s) - a tact time of the line, q_i - a probability of serving a defective component from i-th feeder (it corresponds with the scrap rate), m (each) - a number of assembled components, coefficient $\frac{60}{T_t}$ - represents a theoretical performance of the line V_t, provided that there is a good product in each tact, coefficient $(1-q_i)$ - represents a probability of serving a good component from i-th feeder. To illustrate the impact of the components' scrap rate, we use relative performance V_r (-) (2) for a simplified case when the scrap rate of all components is the same

$$V_r = \frac{V_1}{V_t} = (1-q)^m\,. \tag{2}$$

In case the defective components cause stopping the line, the performance decreases due to downtime periods. Downtime is characterized by the mean time T_p (s). Then the line performance (3) will be

$$V_2 = \frac{60}{T_t + T_p.[1 - \prod_{j=1}^{k}(1 - q_j)]}, \quad (3)$$

where: k - the number of components of the assembled product (-).

Dependence of the relative performance on the number of assembled parts (4) is

$$V_r = \frac{V_2}{V_T} = \frac{1}{1 + \frac{T_p}{T_t}[1 - (1 - q)^k]}. \quad (4)$$

Downtime period is determined largely by the operator. It consists of time required to identify the fault location from defective component and of time required for its elimination. Increasing performance is possible only by shortening the tact time T_t. While the complexity and cost of the line increases, simultaneously the performance does not increase permanently but stabilizes at the limit value (5)

$$V_{2u} = \frac{60}{T_p.[1 - (1 - q)^k]} \doteq \frac{60}{T_p.k.q}. \quad (5)$$

4.2. Experimental determination of failure rate.

As already mentioned in the part 3, the control and measuring system are a part of the automatic assembly line. Because the tact time is short, it can be considered as a unit of time for formulation of periods of activity as well as downtime periods in discrete form (by number of tacts). Defining the concept of the line allows us to segment, in a suitable manner, a reliable line model. Recording the failure rate of the states provides us with data which, when processed by a computer, were arranged in histograms (Fig. 7 - 10), they show a distribution of the activity and downtime periods for each tact. These sets of values are illustratively demonstrated in different histograms in Chapter 5.

4.3. Mathematical-statistical analysis of experiments

High failure rate of assembly lines allows obtaining a relatively smooth course of cumulative relative frequency. Furthermore, the described techniques are based on these waveforms and their approximations by statistical functions based on analogy with the transition characteristics of physical systems. This identification approach is known from management theory.

For approximating the distribution of the line's activity period, after a goodness of fit test of multiple waveforms with distribution functions, the best appears to be the superposition of two exponential functions of probability distributions with different mean periods of activity. Analysis of the assembly process enables us to create a certain interpretation of the obtained waveforms. Error-free operation of each assembly node depends on two independent quantities - on scrap rate of assembled components, and on failure rate of the line.

Distribution function of superposition of two exponential distributions (6) is in a form

$$F(t) = 1 - [c_1 . e^{-\frac{t}{T_1}} + c_2 . e^{-\frac{t}{T_2}}] \quad (6)$$

and

$$f(t) = \frac{dF(t)}{dt} = \frac{c_1}{T_1} . e^{-\frac{t}{T_1}} + \frac{c_2}{T_2} . e^{-\frac{t}{T_2}} \quad (7)$$

is probability density (7). It is a three-parameter distribution, of which the distribution function is formally identical to the transient characteristics of two parallel blocks with unit amplification (Fig. 2).

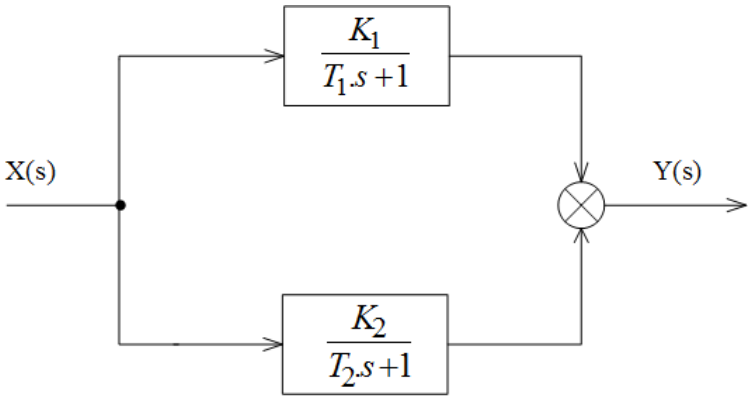


Fig. 2. Block diagram of parallel blocks of I. order (s - Laplace Transform Operator).

With inverse Laplace transform during a unit step response on the input, we achieve an analytical expression of the transition characteristic in a form

$$Y(t) = K_1 (1 - e^{-\frac{t}{T_1}}) + K_2 (1 - e^{-\frac{t}{T_2}}) \quad (8)$$

After implementation of $K_1+K_2=1$ we obtain a formal compliance with equation (7) $K_1=c_1$; $K_2=1-c_1$. The analogy also applies to the constants. In equation (7) are T_1, T_2 mean periods of activity, in equation (8) it regards to time constants.
For approximating the distribution of downtime periods would be appropriate to use i.e. Gamma distribution but even better conformity can be achieved when comparing the cumulative relative frequency waveforms of downtime periods with transient characteristics of dynamic systems of I. order, connected in series (Fig. 3) with different time constants.

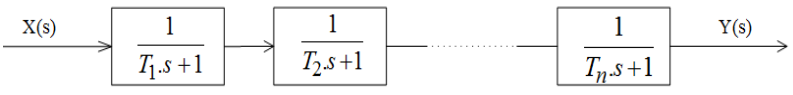


Fig. 3. Block diagram of the higher-order system.

Transient characteristic of system of II; order is (9)

$$Y(t) = 1 - \frac{T_1}{T_1 - T_2}.e^{-\frac{t}{T_1}} + \frac{T_2}{T_1 - T_2}.e^{-\frac{t}{T_2}}. \quad (9)$$

The time constants T_1, T_2 are again corresponding with the mean periods of time of individual tasks during downtime period. This analogy again allows the use of identification methods of management theory. There is clearer concept of physical causes of observed processes. It is interesting that with complexity of the assembly node, the order of distribution function is increasing.

4.4 Reliability of automatic machines

Reliability of automated production machines can be examined on the basis of reliability of individual machines, which the production system consists of. For the most important reliability characteristics the machine operation will be considered as a random period-alternation of failure-free operation τ_1, τ_2 ... and periods of operability restoration Θ_1, Θ_2 … Operational and organizational downtime is excluded. To describe the reliability we use a mathematical apparatus of probability theory [2], [5], [8], [15] which defines the essential reliability characteristics of the machine as shown on Fig. 4.

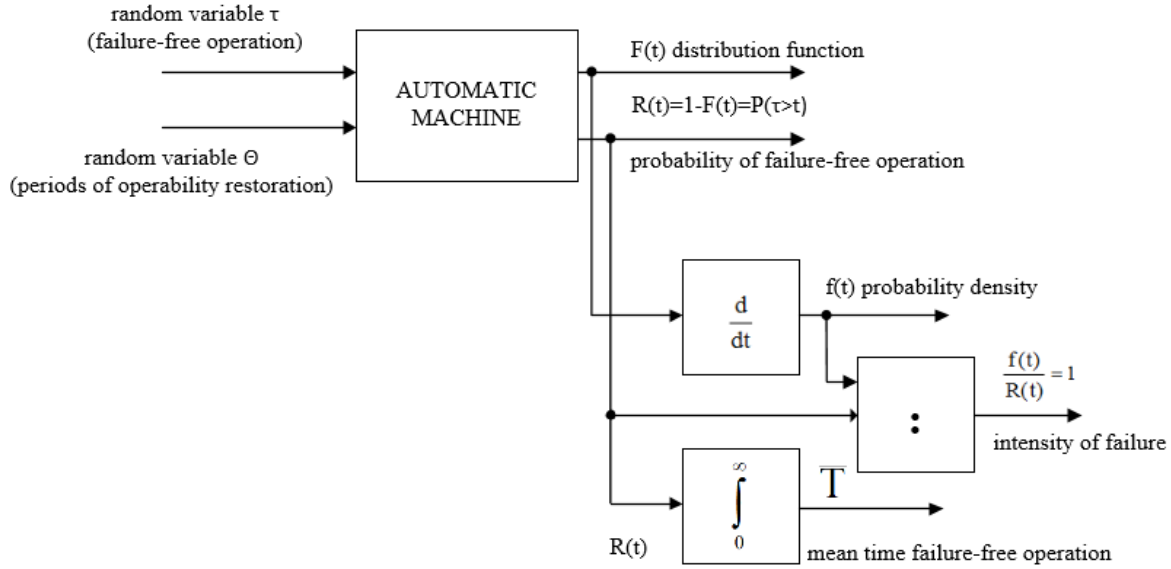


Fig. 4. Machine characteristics in terms of failure-free operation.

A random variable Θ - the period of operability restoration leads to an expression of the machine properties after its failure. We assume that after operability restoration, the device is in its default condition. During the period of operability restoration, we carry out the repairs of mechanisms and machinery equipment, and replacements of parts, and in extreme cases, even replacement of the entire machine by an equivalent machine. By analogy we can define the characteristics of continuous random variable Θ.

Distribution function (10)

$$G(t) = P(\Theta \leq t)$$
(10)

Probability density (11)

$$g(t) = \frac{dG(t)}{dt} \tag{11}$$

The probability N(t) (12) does not implement a restoration in time t

$$N(t) = P(\Theta > t) = 1 - G(t) \tag{12}$$

The intensity of restorations μ(t) (13) (the analogy of failure intensity of λ(t))

$$\mu(t) = \frac{g(t)}{1 - G(t)} = \frac{N'(t)}{N(t)}$$
(13)

Mean time of operability restoration (14)

$$\Phi = \int_0^\infty N(t)dt \tag{14}$$

If the random variable τ (resp. Θ) has an exponential distribution, the failure rate is defined by the constant λ and the intensity of restorations by the constant μ. This operation of machines can be described by Markov processes [1], [2] which substantially facilitates all the calculations of the dynamic alternation of failure-free operation and the period of machine's operability restoration. When evaluating a production system, we are interested in the effect of machine's reliability on the workplace performance, and in finding out reserves of the production system's performance, and in the level of utilization of workplaces for a machine restoration (resp. the adjusters' restoration). These problems can be solved by using an experimental data from operation, preferably solved using a mathematical model. A formation of the model, and its implementation on PC, will be shown on a specific case.

Task: Determine the absolute probability distribution, and other reliability characteristics of the production system, consisting of two machines where $\lambda=0.1\ hr^{-1}$ and $\mu=1\ hr^{-1.}$ Determine the actual performance V_s of the system if only one setter is available. The theoretical performance of each machine is in the $V_t=650\ PPH^{-1}$ (pieces per hour) and d=14 hrs (two-way operation). We expect an exponential foundation τ and Θ.

Formulation of a mathematical model: The system of automatic machines n is in time t at the state k if a fault occurs in the machine ($0 \leq k \leq n$).

In view of the assumptions given, the system's behaviour can be modelled by the homogeneous Markov process, which is sometimes referred to as a birth-death process and can be also used outside the field of technology. Using the markings common in the literature [3], [15] it is possible, for the absolute probability distribution of a Markov process' states, to formulate Kolmogorov system of differential equations (15)

$$\pi_0'(t) = -\lambda_0\pi_0(t) + \mu\pi_1(t)$$
$$\pi_1'(t) = \lambda_0\pi_0(t) - (\mu + \lambda)\pi_1(t) + \mu\pi_2(t)$$
$$\pi_2'(t) = \lambda\pi_1(t) - \mu\pi_2(t)$$
(15)

where the initial probability distribution is defined in line with usages and practices (16).

$$\pi_0(0) = 1; \pi_1(0) = \pi_2(0) = 0 \qquad \text{and} \qquad \lambda_0 = 2\lambda \tag{16}$$

After reaching values of λ_0, λ, μ we get the system of (17)

$$\begin{aligned}
&\pi_0'(t) + 0.2\pi_0(t) - \pi_1(t) = 0\\
&\pi_1'(t) - 0.2\pi_0(t) - 1.1\pi_1(t) + \pi_2(t) = 0\\
&\pi_2'(t) - 0.1\pi_1(t) + \pi_2(t) = 0
\end{aligned} \tag{17}$$

Using a Laplace transform where we introduce (18)

$$\begin{aligned}
&\mathrm{L}\{\pi_k'(t)\} = sL\{\pi_k(t)\};\ \mathrm{k=1,\ 2\ is}\\
&(s + 0.2)a_0(s) - a_1(s) = 1\\
&-0.2a_0(s) + (s + 1.1)a_1(s) - a_2(s) = 0\\
&-0.1\mathrm{a}_1(\mathrm{s}) + (\mathrm{s} + 1)\mathrm{a}_2(\mathrm{s}) = 0
\end{aligned} \tag{18}$$

This system can be solved analytically e.g. using determinants (Cramer's rule), and an inverse Laplace transform, or a PC simulation e.g. in Scilab Xcos. For limited probability distribution (steady state in $t=\infty$) is $\pi_0=0.820$; $\pi_1=0.164$; $\pi_2=0.016$, which can be proven by the inverse Laplace transform, and it can also be documented on graphical waveforms of absolute probability distribution $a_0(t)$, $a_1(t)$ and $a_2(t)$), as seen in part *Results*.

The mean value of the examined Markov process is generally given by relation (19) [3, 16]

$$m(t) = \sum_{i=1}^{n} i\pi_i(t) \tag{19}$$

For dissipation applies (20)

$$\sigma^2 = \sum_{i=1}^{n} i^2\pi_i(t) - m^2(t) \tag{20}$$

The mean performance of the system V_s for two shifts is determined by using a limit probability that can be determined in relation (21)

$$V_s = dV_t\sum_{i=0}^{n-1}(n - i)\pi_i \tag{21}$$

where: V_t (PPH^{-1}) - theoretical performance of one machine, d (hr) – operation time.

Block diagram on Fig. 5 shows a computer model structure of three first-order differential equations system for a simulation of time waveforms of the absolute probability distribution as well as waveforms m(t) and $\sigma^2(t)$ of a random process.

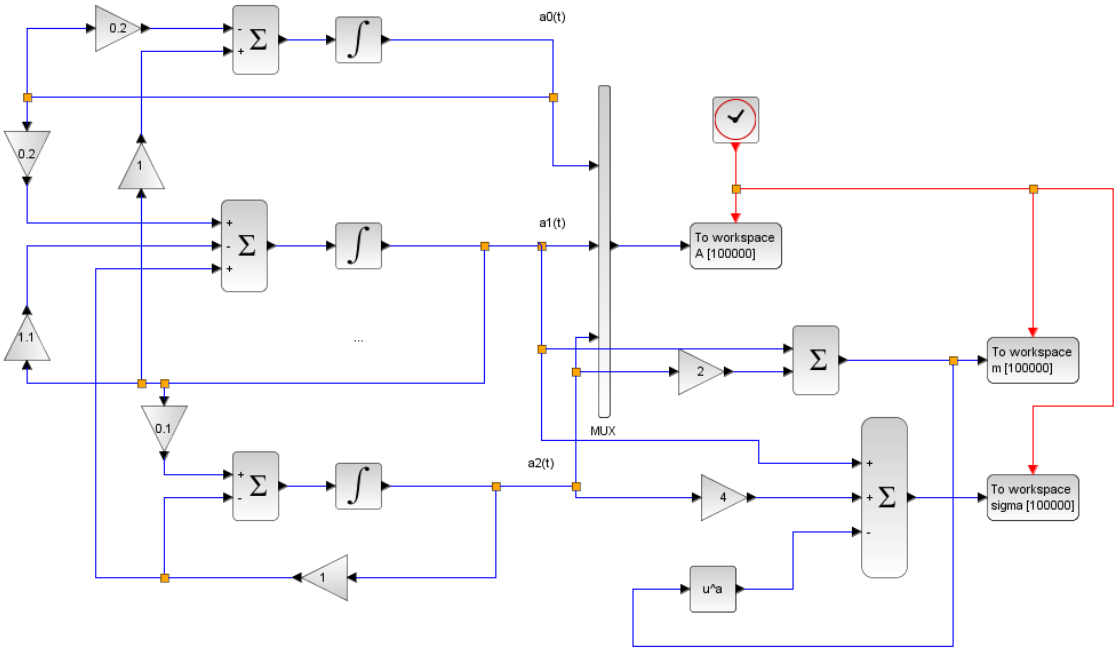


Fig. 5. Block diagram in Scilab Xcos.

5. Results

Achieved results are shown in form of graphs and relevant comments. From them it follows:

1. An impact of line's relative performance in proportion to the number of assembled components with different scrap rate according to equation (2) shown in Fig. 6. The performance also decreases at low values of q, considerably when medium complexity products are introduced.
2. An impact of line's relative performance in proportion to the number of assembled components k (q - parameter) for the line's tact period T_t=6 s and T_p=30 s (downtime period) according to equation (4), is shown in Fig. 7.

   After implementation $a = \frac{T_p}{T_t}$ it is possible to draw a dimensional graph V_r=f(a,k) for parameter q_i (Fig. 6).

   Histograms of the relative frequency of activity period as well as downtime periods of the assembly node and the whole line are shown in Fig. 8 - 11. A dimensional graph of performances V_r proportional to downtime period ratio and to the tact time and also to the number of assembled parts, a) q = 0.01 and b) q = 0.02

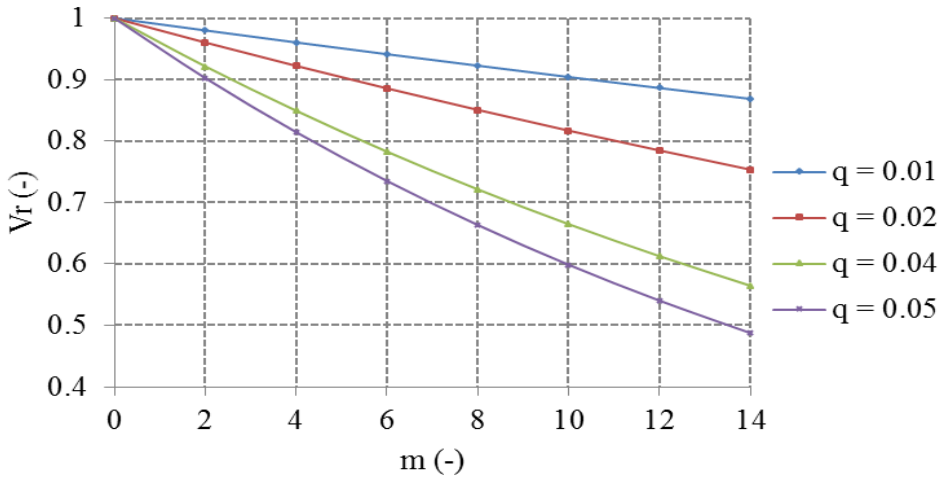


Fig. 6. Dependence of the line's relative performance V_r on the number of assembled parts. (q – scrap rate parameter).

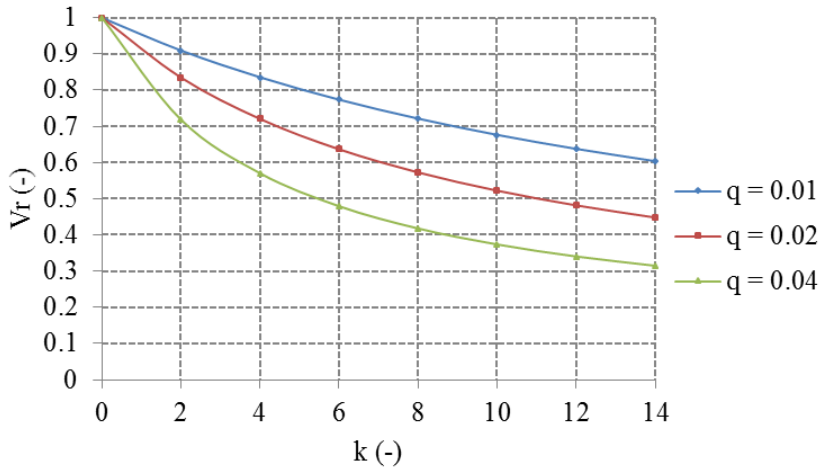


Fig. 7. An impact of line's relative performance in proportion to the number of assembled components when $\frac{T_p}{T_t} = 5$ for parameter q.

3. The assembly line was observed in different modes under this procedure. The unstable mode is the line's running-in period and staff training. During the mode stabilization, there is both the distribution function's order reduction (the number of mean periods of time), and also a value change of the mean periods of time of both the activity and downtime periods. Fig. 14 shows three cumulative frequencies of the line's activity period, obtained in different periods of the lines running-in stage.
   The course A represents putting the line into service, B is from a period after ending the running-in stage and C is a course after a year of service. A reduction of the mean time of activity is explicable by a substantial decrease of the failure proportion of the assembly facilities, yet the failure rate of defective components varies negligibly.

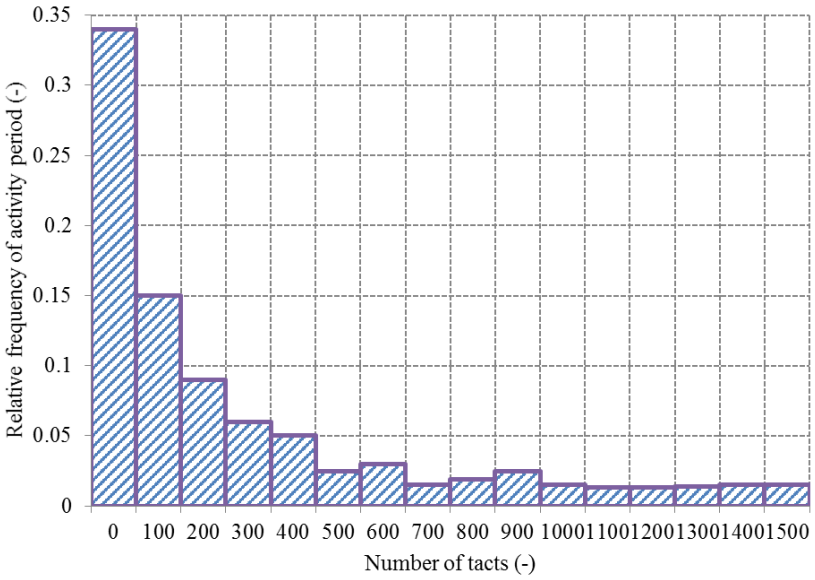


Fig. 8. Histogram of the assembly node.

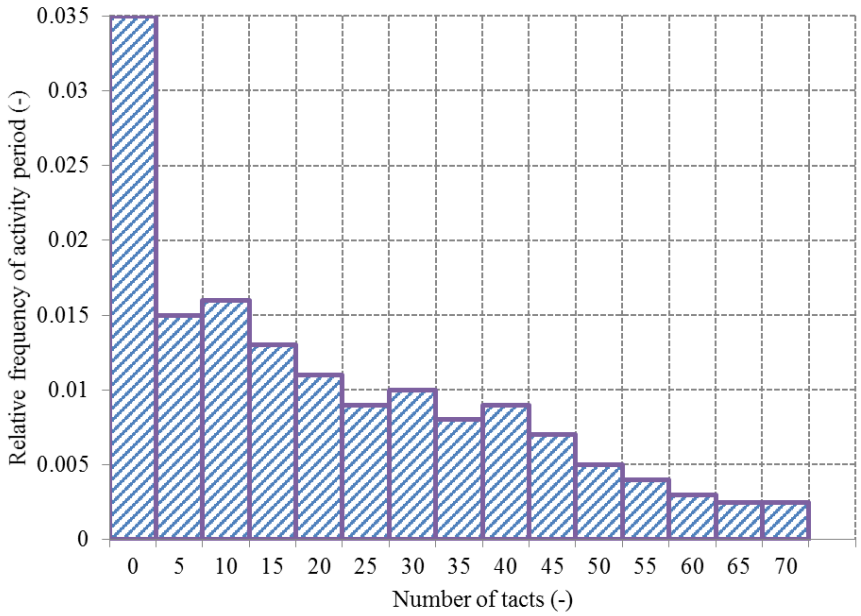


Fig. 9. Histogram of the whole line.

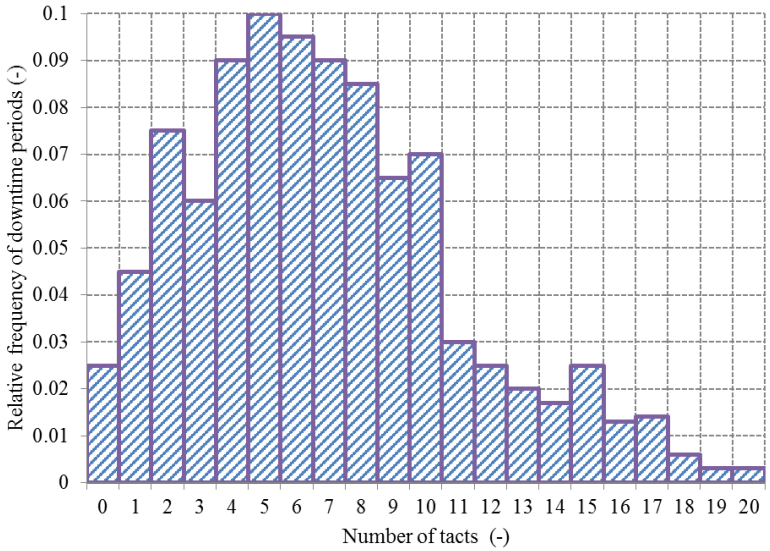


Fig. 10. Histogram of downtime periods for the assembly node.

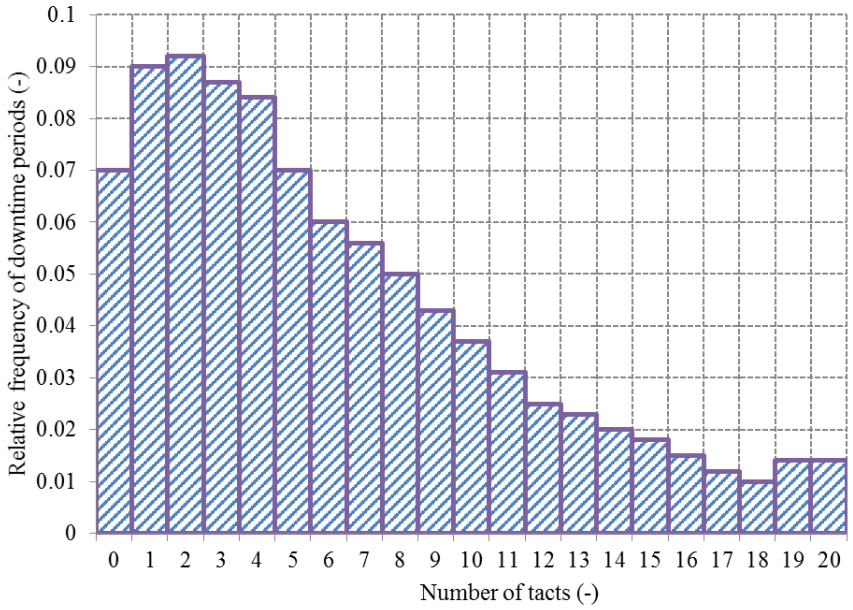


Fig. 11. Histogram of downtime periods for the whole line.

4. From the histogram of relative frequency of the line's activity period (Fig. 9) it was derived a course of the cumulative frequency of line's activity period (Fig. 12). From the histogram of relative frequency of the assembly node's downtime period (Fig. 9), was drawn a course of the cumulative relative frequency of the assembly node's downtime period (Fig. 13).
   The assembly line was observed in different modes under this procedure. The unstable mode is the line's running-in period and staff training. During the mode stabilization, there is both the distribution function's order reduction (the number of mean periods of time), and also a value change of the mean periods of time of both the activity and downtime periods. Fig. 14 shows three cumulative frequencies of the line's activity period, obtained in different periods of the lines running-in stage.

The course A represents putting the line into service, B is from a period after ending the running-in stage and C is a course after a year of service. A reduction of the mean time of activity is explicable by a substantial decrease of the failure proportion of the assembly facilities, yet the failure rate of defective components varies negligibly.

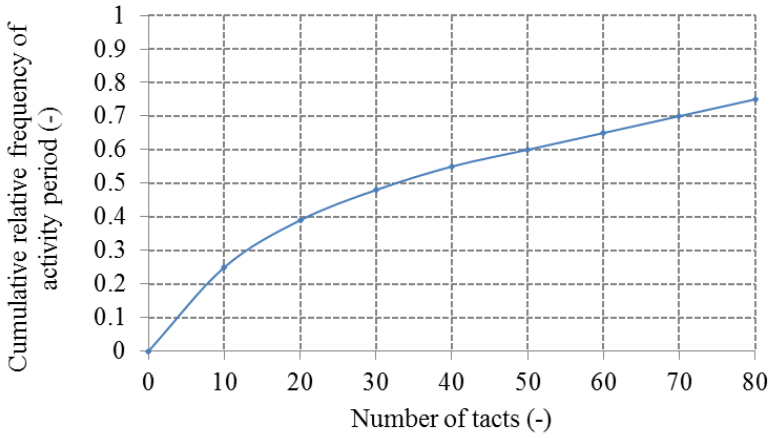


Fig. 12. The course of cumulative relative frequency of the line's activity period.

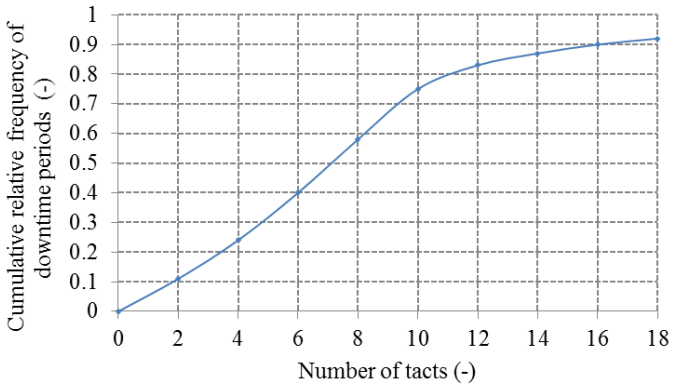


Fig. 13. The course of cumulative relative frequency of the assembly node's downtime period.

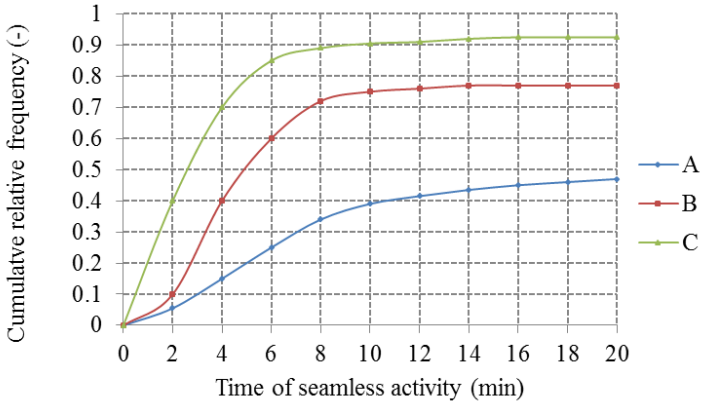


Fig. 14. Courses of the cumulative relative frequency of the line's activity period in different running-in stages.

5. In part 4.4 we created a model of production system reliability, consisting of two independent machines. For specified parameters was implemented a computer model in Scilab Xcos [17] in accordance with the block diagram in Fig. 5. For specified parameters were stated time waveforms $a_0(t)$, $a_1(t)$ and $a_2(t)$ (Fig. 15) of an absolute probability distribution with a marking of steady values. On Fig. 16 are graphs of mean values m(t) and $\sigma^2(t)$ of monitored random process with respect to time. Calculation of mean performance V_s for two shifts can be determined from the Table 4.

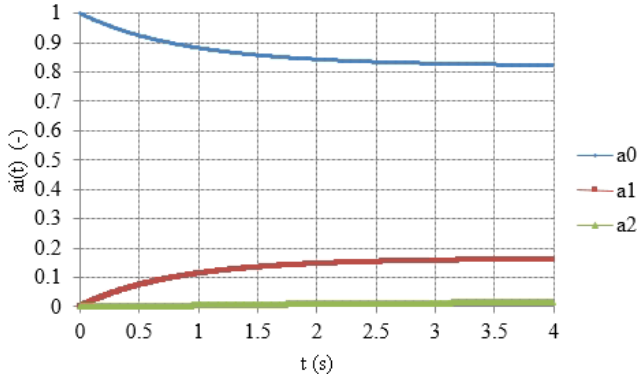


Fig. 15. The time waveforms $a_0(t)$, $a_1(t)$ and $a_2(t)$.

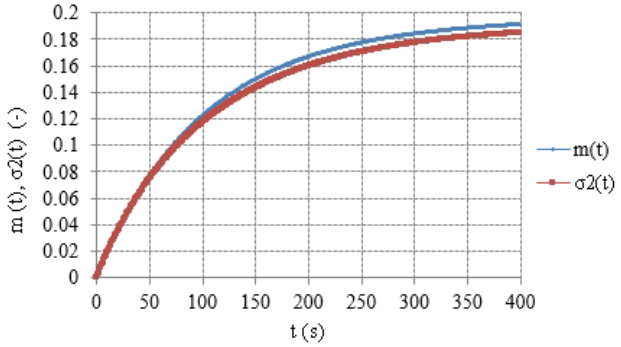


Fig. 16. The graphs of mean values m(t) a $\sigma^2(t)$.

Table 4. The calculation of mean performance V_s.

i (-)	π_i (-)	dV(2-i) (-)	dV(2-i)π_i (-)
0	0.820	18200	14924.0
1	0.164	9100	1492.4
2	0.016	-	-
Σ	1.000	-	16416.4

In accordance with results in Table 4 V_s=16416.4 pieces per two work shifts.

6. Conclusions

When designing the line, the economic effectiveness is important in addition to a technical and technological solution. It is necessary to determine the theoretical performance of the line so as to achieve the desired real performance. It is also necessary

to determine the length of the line and appropriately set the tact time of the line. Most of these problems can be solved using the results of experiments during prototype testing of the individual modular assembly nodes.

Monitoring the settling of cumulative relative frequency of activity period in different periods of the line's running-in stage is important to establish the terms and conditions of testing when the line is handed over to the customer. When the line is submitted to the operation, all the parameters should be stabilized. The performance of the line depends also on staff training. This usually requires to pass and entrance exam by the customer later, when there is a sufficient period of time from the line's installation. The stated methodology can also be used when designing more complex lines where some of the operations are backed up. In this case, to describe their activities we use probabilistic approach by so-called Markov process. The system of differential equations is then advantageously addressed by the Laplace transform.

The system of three first-order differential equations expressing the absolute probability distribution of a production system with two independent machines (for specified parameters) was addressed by using a PC model in the Scilab Xcos environment. Time waveforms are showing particular layouts of reliability distribution of a production system including the mean value and dissipation of a random process. Table 4 enables us to state the mean performance of the machines during production time.

References

[1] LINDA, M., KŰNZEL, G., PROKOPEC, J., HROMASOVÁ, M. Analysis and Evaluation of Reliability of Automatic Assembly Lines. In: *Risks of business and territorial processes.* ISBN: 9788075610218. UJEP: Ústí nad Labem, 2016, pp. 51-59.

[2] MYKISKA, A. *Bezpečnost a spolehlivost technických systémů* (In Czech). ISBN: 978 8001028681. Praha: ČVUT 2006, p. 206.

[3] BEDNAŘÍK, J. *Technika spolehlivosti v elektrotechnické praxi* (In Czech). Praha: SNTL 1990, p. 336.

[4] HØYLAND, A. *Reliability Theory. Models and Statistical Methods*. ISBN: 0471471-3X. New York: Wiley 2014, p. 643.

[5] http://www.reliability-magazine.com.

[6] LEITL, R. *Spolehlivost elektrotechnických systémů* (In Czech). ISBN: 800300 408X. Praha: SNTL 1990, p. 287.

[7] https://www.quanterion.com/KnowledgeBase/ReliabilityToolkit.shtml.

[8] BARUH, H. *Applied Dynamics.* ISBN: 9781482250732. New York: CRC Press 2014, p. 872.

[9] MAIXNER, L. *Navrhování automatických výrobních systémů* (In Czech). Praha: SNTL 1980, p. 210.

[10] KLAS, A. *Krok za krokem k výnosné automatizaci montážních linek* (In Czech). MM průmyslové spektrum 2004, p. 28.

[11] ZLOCHOVÁ, M. Optimalizace výrobních buněk. *Úspěch - Produktivita a inovace v souvislostech* (In Czech). ISSN: 1803-5183, (2012), 1, pp. 18-21.

[12] MICHAELI, L. *Modelovanie analógovo číslicových rozhraní* (In Slovak). ISBN: 80968555018. Košice: FEI TU 2001, p. 159.

[13] BUSCH-VISHNIAC, I. J. *Electromechanical Sensors and Actuators (Mechanical Engineering Series).* ISBN: 9780387984957. Berlin: Springer 2012, p. 339.

[14] SZYLAR, J. Inteligentní informační systém řízení údržby (In Czech). *MM průmyslové spektrum* 2006, p. 40.
[15] KUPKA, L., JANEČEK, J. *Matlab & Simulink: řešené příklady* (In Czech). ISBN: 978 8023995329. Lanškroun: SOŠ a SOU Lanškroun 2007, p. 224.
[16] ANDĚL, J. *Statistické metody* (In Czech). ISBN: 978-80737-803-6. MatfyzPress 2007, p. 299.
[17] GROSS, D., SHORTLE, J. F, THOMPSON, J. M., HARRIS, C. M. *Fundamentals of Queening Theory*. ISBN: 978-047179-1270. New York: John Wiley & Sons, Inc, Hoboken2008, p. 528.
[18] https://www.scilab.org/content/view/full/957.

Chapter 14

SIZE OF HAZARD DEPENDS ON DATA FILES EXTENT

1. Introduction

Sizes of risks for human society depend on sizes of hazards cause the disasters and on the vulnerabilities of public assets. Due to the human population increase and the increase the number of interconnected complex systems and technologies the human system vulnerability to disasters is increasing and this causes large losses, damages and injuries to public assets at great disasters origin. Therefore, in connection with the protection of humans and the development of human society there is very important the occurrence of extreme disasters.

The impacts of extreme phenomena usually cause the huge losses, damages and injuries to the public protected assets, which are: the human lives, health and security; the property (material and immaterial values); the public good (welfare); the environment; and also the infrastructures and technological facilities, which are for the humans the life-giving assets because they providing the energy, water, food, services etc. [1].

For the extreme phenomena we now use the designation:

- the Black Swan,
- the Royal Dragon,
- atypical disaster or atypical accident,

see e.g. the papers given in book [2].

The detailed study of disasters [3] processed for improving the safety of complex technological facilities as nuclear power plants and big chemical plants documents that the extreme events occur sparsely and irregularly; and their mean return periods in Central Europe are between 420 to 460 years. With regard to this reality, their occurrence cannot be revealed by tools of classical mathematical statistics by help of data only obtained from instrumental disasters monitoring; the data and methods using for prediction have not sufficient power to distinguish them; i.e. they seem as unpredictable (unforeseen) phenomena.

The extreme disasters occurrence has been explained by several theories, e.g. the theory of largest values [4], theory of extreme values [5], theory of evidence [6], theory of possibility [7], complexity theory [8] and the theory of options [6, 9].). For description of their occurrence in practice they are at present also used the methods based on conditional probability, expert methods for capturing the knowledge uncertainties and Bayes' theory. On the example of earthquakes, for which the authors compiled the wide-ranging data files (catalogues, isoseismals maps, maximum earthquake intensity maps, seismotectonic maps etc.) for the last 1000 years for the whole Central Europe and adjacent areas [3] , it is shown that it is more one reason for explanation of sudden big earthquake origin at present.

Authors: Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc., RNDr. Jan Procházka, Ph.D., Czech Technical University in Prague, Praha, Czech Republic, prochazkova@fd.cvut.cz

The results show that the big role plays the length of disaster observation period from which we use the data for determination of maximum expected disaster. When we use for the prediction the data from too short time interval we cannot obtain the correct size of maximum expected disaster, and then we may erroneously talk on extreme event, even though equally large disaster occurred in past, sometimes even nevermore.

2. Findings on disasters and on disaster management aim

Data on disasters are important for technological practice, because we need to build the safe facilities and safe infrastructures. For earthquakes and other natural disasters in broad vicinity of Central Europe we derived at preparation of terms of references for building the complex technological facilities the mean return periods 420 - 460 years, which is in harmony with the values used by Swiss Re [10-12]. From this reason we use long time series of disasters, i.e. also the historical data that are not as precise as present instrumental one but allow understanding the occurrence of great disasters that occur seldom and irregularly.

Analyses of many databases of disasters [3, 13, 14], show the general knowledge that extreme phenomena occur rarely and irregularly, which affects the technical-methodological ways of prediction [3, 15]. From the detail study of disasters, it follows that each disaster is the product of some process being in the Earth or in the human society that are understand as open systems of systems [1]. Due to the dynamic development of this human system the processes have been changing in space and time, which resulted in disaster parameters changes. This reality causes that assumption of mathematical methods for prediction (requiring the stable process) is not quite fulfilled.

Because we have not enough knowledge on this domain we need to take into account the existence of uncertainties, namely random and knowledge; just knowledge uncertainties of ongoing physical processes in the Earth and its surrounding are the causes of our incompetence to predict the origin and size of extreme disasters. We will show this reality on the data set for earthquakes because authors have good data set for last 800 years; the data set has been very carefully collected for ensuring the protection of complex technological facilities in Central Europe; i.e. for the determination of their terms of references, rules for designing, building, construction, operation and pulling off critical conditions if they occur.

Omission of historical data leads to incorrect terms of references used for building the complex technological facilities, as shown Fukushima accident [16, 17].

For protection of humans and other public assets on which the human security and development are dependent we need to perform qualified disaster management, the demands of which are summarised in [1]. For this purpose, we determine the disasters´ characteristics and regimes (especially we interested in prediction of maximum expected disaster sizes and their occurrence probabilities), so we might be capable to apply correct countermeasures in advance; the given aspect is especially important in case of complex technological facilities that present problem for their vicinity.

3. Determination of size of maximum expected disasters for ensuring the technological facilities safety

The task dealing with determination of maximum possible or maximum expected disaster for solution of problems in real practice, in detail described in works [1, 3, 10-

12] is of principal importance for both, the safety management and the insurance domain. Therefore, the attention has been paid to this domain for a long time.

The methodology development in time progressed conformable with the knowledge development, roughly by the following way:

- maximum expected disaster size = size of maximum observed disaster in historical period,
- maximum expected disaster size = size of maximum observed disaster in historical time + certain correction on the indeterminateness (random and knowledge uncertainties) or on the reality that extreme disaster has not had to occur yet. The correction always depended on experience and knowledge of assessor,
- maximum expected disaster size = disaster size that corresponds to intersection of graph showing the disaster frequency occurrence with the disaster size axe. Challenges to this method mainly consisted in reality that results of such assessments might be distinctly physically impossible in some cases,
- maximum expected disaster size = result of methods for extreme value determination [1, 3, 10-12].

Extreme value determination is widely used in many disciplines, such as earth sciences, structural engineering, finance, traffic prediction, geological engineering and biological sciences. Applications of method for extreme value determination usually go from the Gumbel distribution [5] that is a particular case of generalized extreme value distribution.

The applications for earthquakes and other disasters for needs of terms of references for nuclear power plant site locations authors started in 80s of last century and step by step they were spread for building the other complex technological complexes; the real values are in the safety documentation of these complexes. In practice connected with complex technological facilities [1, 3], it was successfully tested the following relations:

$$R_t(I_0 \geq I_{0i}) = 1 - \left\{ \frac{T}{T + t.P(I_0 \geq I_{0i})} \right\}^{n+1}, \quad (1)$$

$$P(I_0 \geq I_{0i}) = \frac{e^{-\beta I_{0i}} - e^{-\beta I_{0\max}}}{e^{-\beta I_{0\min}} - e^{-\beta I_{0\max}}}, \quad (2)$$

in which: $R_t = (I_0 \geq I_{0i})$ is the probability that the size of disaster I_0 does not exceed the size I_{0i} in the time interval t; $P_t (I_0 \geq I_{0i})$ is the probability that the size of disaster I_0 exceeds the value I_{0i} ; P is defined by the equation (2); T is the disaster observation time interval; n is the observed disaster number; I_{0min} is the minimum disaster size (from which the catalogue is homogeneous; it represents the data set homogeneity limit); and I_{0max} is the maximum disaster size in the given region.

It means that the relations hold for intensities from interval $I_{0min} \leq I_0 \leq I_{0max}$. Parameter β is determined using the numerical parameter b_c from the cumulative frequency equation

$$\log N_c = a_c - b_c I_o , \quad (3)$$

in which N_c is the cumulative frequency of disasters, I_0 is the disaster size, a_c and b_c are numerical parameters calculated for intensity interval $I_{0min} \leq I_{0i} \leq I_{0max}$. It holds $\beta = b_c \ln 10$. The mean value of return period η for the disaster with the intensity of I_0 is equal to time t for which it holds the relation $R_\eta = 0.633$(expressing the probable mean value of normal distribution).

The impacts of disaster on the territory and on the complex technological facility depend on the type of disaster and on the vulnerability of given assets; real data are shown e.g. in quoted works of authors.

From the safety reasons we in practice use the conservative deterministic approach for all disasters because the theory of extreme values is based on the following assumptions:

- the conditions that prevailed in the past, need also to apply in the future,
- the largest observed phenomena in a given time interval are independent,
- the largest phenomena size in a given interval will be the same in the future as in the past.

It is necessary to note that these assumptions are not in reality fully veridical [1, 3, 13, 15, 18], which influences the results of predictions of large (extreme) disasters.
In practice, according to the theory of extreme values there are determined two quantities the return period and the annual probability of non-exceedance by which the disaster hazard is determined.

4. Data on earthquakes in broad vicinity of Central Europe used for research

The earthquake is a physical phenomenon that is a result of certain dynamic processes in the Earth´s interior. It originates by a sudden release of mechanical energy in the Earth's interior. During the earthquake there are originated irreversible deformations in the earthquake focus and from the focus there are emitted seismic waves (longitudinal and transversal).

Outside of earthquake focus the earthquake predominantly manifests by seismic waves and we observe them in the form of vibrations of the Earth's surface of a different size that from a certain intensity cause the harm on human lives and health, property, infrastructure and environment, and the stronger ones caused huge harms.

With regard to present knowledge the total energy of seismic waves is expressed by the relation

$$E_0 = \int_0^\tau \int_S \varepsilon \, \mathrm{d}S \, \mathrm{d}t$$

in which S is the surface through which the seismic energy flows from earthquake foci, τ is the time for which the seismic energy flows and ε is a flux of seismic energy for which it holds the relation

$$\varepsilon = e \cdot v \, \mathrm{d}\Omega,$$

in which e is the seismic energy density, v is the progressive wave velocity and $\mathrm{d}\Omega$ is the cross-section of the ray tube.

The model of seismic energy spreading from earthquake focus is expressed in the form

$$E_n = E_0 \, e^{-d\,Dn} \, D_n^{-c} \,, \qquad (4)$$

in which E_0 is the seismic energy emitted from the earthquake focus, E_n is the seismic energy in the hypocentral distance D_n for which it hols

$$D_n = (r_n^2 + h^2)^{1/2}$$

where h is the focal depth, r_n is the epicentral distance), c and d are numerical parameters; d *is* the seismic energy attenuation coefficient and c is the numerical parameter, the value of which depends on the geometry of real problem.

The relation between seismic energy E_n and macroseismic intensity I_n in the broad vicinity of Central Europe according to [18] is given by relation

$$\log E_n = 12.40 + 1.13\, I_n.$$

The seismic energy attenuation derived for the Bohemian Massif conditions is expressed by relation (4) with parameters: $c = 2.8;\ d = 0.061$; derivation is in [18].

For the qualitied determination of seismic terms of references for complex technological facilities in broad vicinity of Central Europe there were ensured:

- qualified data sets (earthquake catalogues, isoseismal maps, epicentre maps, maps of maximum observed intensities,
- detailed study of strong events,
- delimitation of focal zones,
- determination of geological, tectonic, geophysical and seismotectonic features

[3].

The form of isoseismals (scenarios of earthquake impacts) in the epicentral zone depends on the fault-plane mechanisms of earthquake, and in distant zone on material properties of Earth´s crust in which the seismic waves are spreading; the boundary between these zones is given by empirical relation

$$ir \approx 2.5\, h\ ,$$

in which ir is the isoseismal radius in km and h is the focal depth in km. Sizes of isoseismal surfaces depend directly on the earthquake size and on the focal depth and indirectly on the intensity attenuation [18].

Seismic (earthquake) regime is the set of relations among the earthquakes in a given focal region. One of the basic relations is an empirical function describing the earthquake frequency distribution by earthquake size:

$$\log N = a - b\, S,$$

where N is the number earthquakes with size S, a and b are numerical parameters. This relation has the same form as equation (3) but the numerical parameters differ because simple and cumulative frequencies are not the same [18].

If we need to consider data on historical earthquakes, we need to use the intensity I (° MSK-64) as the measure of earthquake size; details and relations with other measures are for example in publication [18].

The types of dependences of relation $N_c(I_0)$ given by equation (3) shown in Figure 1 authors derived on the basis of investigation of 87 focal zones, Comparison of ten graphs shows that earthquake intensity intervals and observed maximum earthquake sizes are

very different. It is also seen that the numerical values of graph slopes b are different, which cause the differences in parameter β and through this parameter it also influences the maximum expected earthquake size that is determined by help of $P_t\,(I_0 \geq I_{0i})$ and $R_t = (I_0 \geq I_{0i})$, equations (1) and (2). The differences in maximum expected disaster sizes cause the differences in seismic hazard, namely not negligible as show the data in [3].

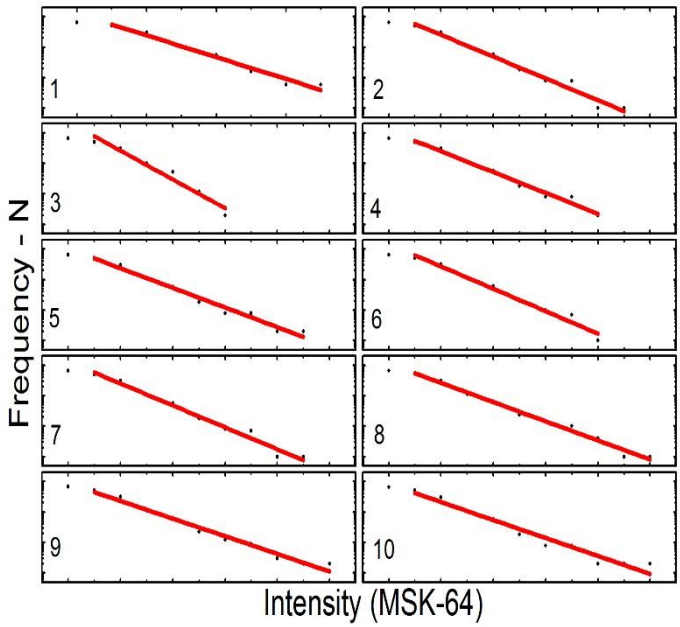


Fig. 1. Scheme of observed types of distributions occurrence frequency on earthquake intensity - $log\ N_c = a_c - b_c\ I_o$.

The numerical values of parameters a_c and b_c describe the seismic regime of individual focal regions; i.e. because they vary in a broad interval it is evident that the seismic regimes of focal regions in Central Europe are not the same. Apart from in one focal region they also depend on the calculation method [3], which also influences the results connected with application of equations (1) and (2), in which we use the numerical value of slope.

Findings from the seismic regime of focal zones research in broad vicinity of Central Europe are in harmony with results from other world parts, which is documented by comparisons given in [3]. Their summarisation is:

- the seismic regime of each focal zone is variable in time and space,
- the seismic regime has a certain prevailing character in each focal zone,
- the seismic regime is well described by the Benioff´s graphs which expresses the dependence of released earthquake energy on time in a given focal zone

$$\sum_i E_{si}^{1/2} = f(t),$$

where E_{si} is the seismic energy i-th earthquake and t is the time.

The Benioff´s graphs (example is in Figure 2) indicate that the tectonic stresses are released usually after a prolonged period of inactivity, either in the form of one very strong earthquake or in group of several stronger shocks with comparable size. In one focal area both forms often are observed [3,18].

The active periods (i.e. the interval characterised by release of great seismic energy) in all focal areas have not the same duration (e.g. in the Eastern Alps active and quiet periods take several centuries), and they do not happen at the same time in all focal regions (particularly not in neighbouring focal areas).

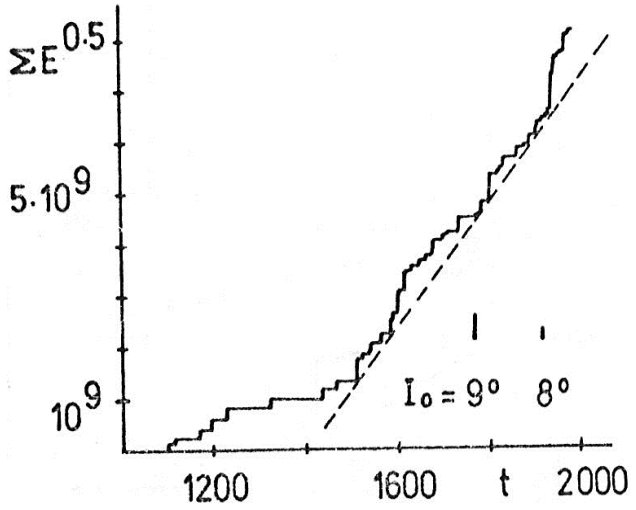


Fig. 2. Example of Benioff´s graph – South Eastern Alps.

Detailed studies of Benioff's graph in broad vicinity of Central Europe [3, 18] showed that in some time interval the seismic energy releases in the form of one very strong earthquake and in another one in the form of several middle size earthquakes. This physical fact shows that at determination of seismic hazard we need to consider data from time intervals with duration of several centuries so the result may have the acceptable credibility. The other characteristics of real seismic regimes of individual focal zones that also influence the seismic hazard of real localities for the followed region are given in works [3, 18].

On the basis of above mentioned data we determine the seismic hazard of site under account by the following procedure:

- on the basis of catalogue, we determine the set focal regions the strong foci of which can threaten the site – due to earthquake characteristic in Central Europe [18] we need to consider all earthquake foci in distance 400 km from the site under account,
- on the basis of all earthquakes from these focal regions we calculate parameters of cumulative frequency distribution according to relation (3) for selected observation period *T*,
- by application of formulas (1) and (2) we determine the sizes of maximum expected earthquake in the followed region for time intervals *t*, e.g. *t = 2, 5, 10, 20, 50, 100, 200 …*years on the 95% credibility level,
- considering the maximum expected earthquake size for given time interval, the attenuation curve between the possible earthquake focal zone and the followed site, considering the shortest distance between the earthquake focal zone and the followed site we obtain the result; the real attenuation curves for 16 directions are summarized in [3].

On the basis of other parameters influencing the earthquake size in a real site (e.g. anomalies in intensities, Earth´s structure anomalies, tectonic features etc.) we prepare

the seismic terms of references as input data for designers of complex technological facilities. After proposal of design we test seismic vulnerability of facility to the maximum expected earthquake.

During the operation of complex technological facility we regularly test its resilience to earthquakes and after some accident we also realised complex walk downs in facility with aim to check if its safety is on required level [1, 3]. For reader information the described procedure is in harmony with demands [19] and with demands of complex technological plans land use planning that are in the SEVESO directive.

5. Data and method used for research

For our research we used earthquakes from the author´s earthquake catalogue that is completed to 2015 and contains the earthquakes since 400 AD.

It is reality that the data in the used earthquake set have not the same homogeneity boundary in the history; in broad vicinity of Central Europe the homogeneity boundaries are:

- 6° MSK-64 in last 200 years,
- 6.5° MSK-64 in last 400 years,
- 7° MSK-64 in last 800 years.

The main characteristics of investigated region are:

- the earthquake epicentres distribution in investigated region for $I_0 \geq 5°\,MSK\text{-}64$ and last 800 years is shown in Figure 3,

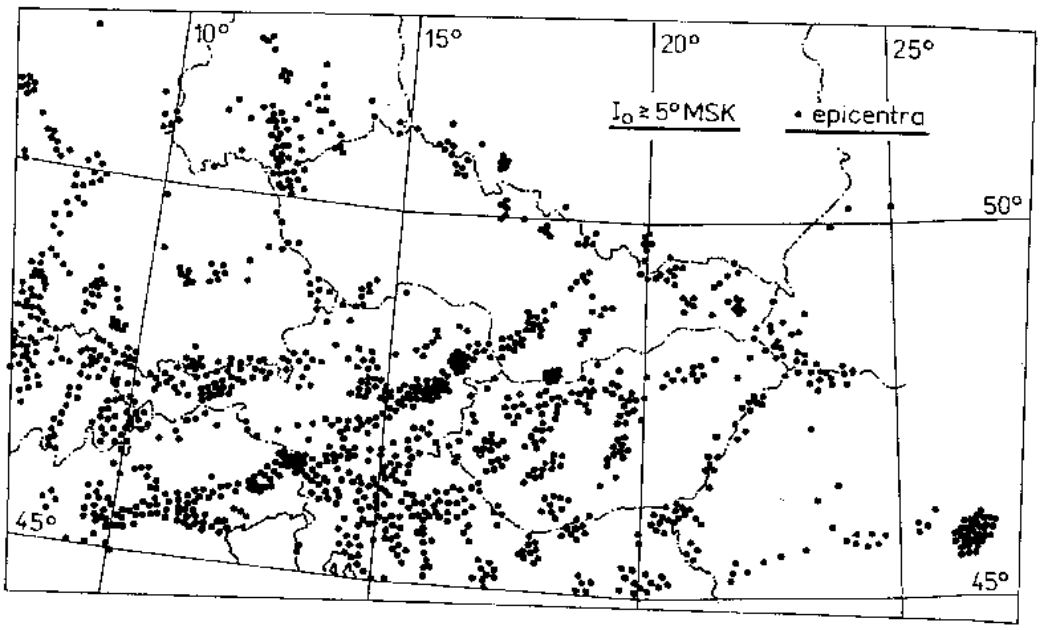


Fig. 3. Earthquake epicentres with intensity $I_0 \geq 5°\,MSK\text{-}64$ occurring in last 800 years.

- the earthquake focal zones delimited according to seismic, tectonic, geological, gravimetric and geomagnetic characteristics by the methods that are in great detail described in [3] are in Figure 4.

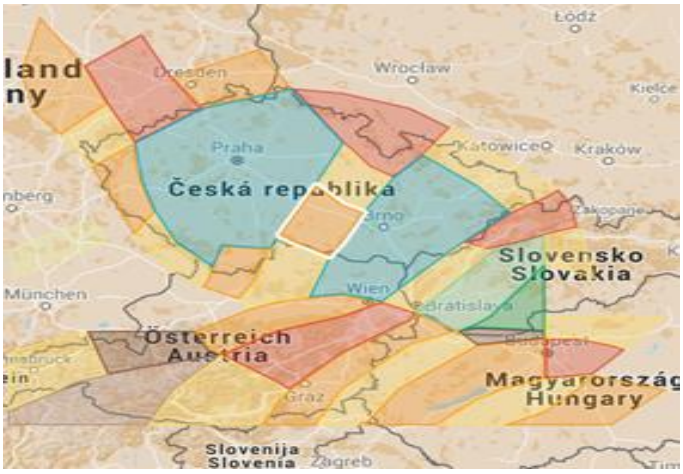


Fig. 4. Focal zones in Central Europe important for seismic hazard.

The seismic hazard assessment is based on analytical function expressing the occurrence of strong earthquakes based on theory of extremes; equations (1) and (2). For calculation there need to be use data from specified region and specified time interval; from the physical reasons usually from the region defined by circle with the centre in a given site and with radius more than 100 km.

In practice there are used: the deterministic approach considering the stable earthquake occurrence rightfulness and from safety reasons the most adverse (bad) conditions; and the probabilistic approach considering the random uncertainties in earthquake occurrence and their statistical evaluation – there are used median, median + σ; the comparison of both ways based on real data is in [1, 3]. In case that we show in next paragraph the deterministic approach results are given.

Seismic hazard values go on from determination of maximum expected earthquake size value calculated with help of equations (1) and (2). They have been calculated for many localities in Central and Eastern Europe in which they are located the complex technological facilities.

On the basis of their values and real conditions in place of siting and its vicinity there are determined:

- vulnerabilities and possible risks for public assets and complex technological facility itself,
- terms of references for complex technological facility etc.

Because the maximum expected earthquake size value is very important for the seismic hazard value in real place we show its dependency on the data range; the other sources of seismic risk values variability are possible to find in [1].

6. Variability of seismic hazard values with data range

To show the dependence of seismic hazard value on the data range we select locality in Central Bohemia. Using the formulas (1) and (2) and the procedure described above we calculate the maximum expected earthquake size value, from which we go on at determination of seismic hazard values for localities in Central Bohemia; i.e.:

- by application of formula (1) we determine the earthquake sizes for time intervals, e.g. *t = 50, 100, 200 …* years on the 95% credibility level,

- considering the intensity attenuation curve between possible focus and site and the distance between focus and site equals to 300 km we determine the site seismic hazard for selected time intervals.

In presented research we use the data from different observation periods:

- T = last 100 years,
- T = last 200 years,
- T = last 300 years,
- T = last 500 years,
- T = last 800 years.

Figure 5 shows the curves calculated on the basis of data from the last 100 years. The curves describe the probability of occurrence of earthquake of sizes 6 – 10.5° MSK-64. The predictions of maximum expected earthquake size value estimations are for times t = 2, 5, 10, 20, 50, 100, 200, 500, 1000 and 10 000 years.

We can see that the 5% credibility level line crosses the probability curves of non-exceedance of intensity value at intensity values:

- 9° MSK-64 for t = 2 years,
- 9.9° MSK-64 for t = 5 years,
- 10.4° MSK-64 for t = 50 years,
- 10.5° MSK-64 for t = 100 years and further time intervals.

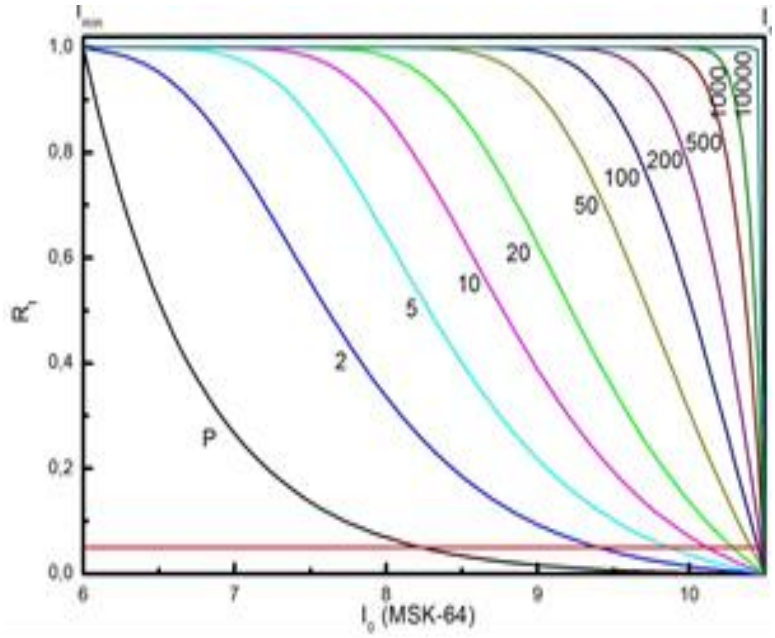


Fig. 5. Assessment of maximum expected earthquake size by help of data set from observation period T = last 100 years and predictions for t = 2, 5, 10… years that determined the seismic hazard in sites in Central Bohemia.

Considering the intensity attenuation curve [3] and the distance of 300 km, the intensity decrease is 5.5 °MSK-64; i.e. in the Central Bohemia (e.g. also in Praha capital) the seismic hazard prediction for time interval:

- t = 50 years is 4.9° MSK-64,
- t = 100 and more years is 5.0° MSK-64.

Figure 6 shows the curves calculated on the basis of data from last 800 years (*T*). The curves describe the probability of occurrence of earthquake of sizes 6 – 11.5° MSK-64. The maximum expected earthquake size value estimations are for times *t* = 5, 10, 20, 50, 100, 200, 500, 1000 and 10 000 years. We can see that the 5% credibility level line crosses the probability curves of non-exceedance of intensity value at intensity values:

- 10.7° MSK-64 for *t* = 5 years,
- 11.3° MSK-64 for *t* = 50 years,
- 11.4° MSK-64 for *t* = 100 years,
- 11.5° MSK-64 for *t* = 500 years and further *t*.

Considering the same intensity attenuation curve and the distance of 300 km, the intensity decrease is 5.5 °MSK-64; i.e. in the Central Bohemia (e.g. also in Praha capital) the seismic hazard for time interval:

- *t* = 50 years is 5.8° MSK-64,
- *t* = 100 years is 5.9° MSK-64,
- *t* = 200 years and higher *t* is 6.0° MSK-64.

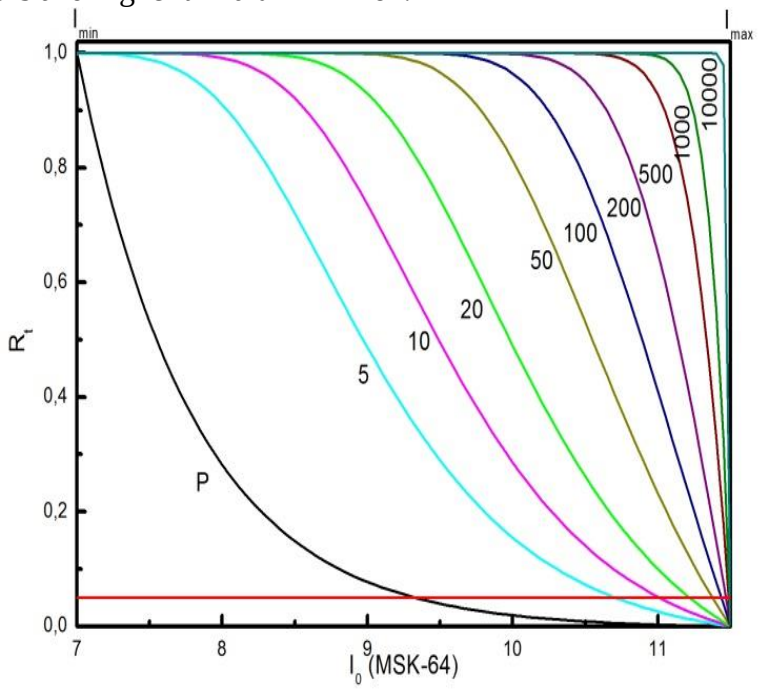


Fig. 6. Assessments of maximum expected earthquake size by help of data set from observation period *T* = last 800 years and predictions for *t* =5, 10, 20, … years that determined the seismic hazard in sites in Central Bohemia.

Table 1 shows the numerical results for more observation periods *T*. We see that:

- the longer time interval *t* is, the higher maximum expected earthquake size (i.e. the seismic hazard base value) is,
- the longer observation period *T* is, the higher maximum expected earthquake size (i.e. the seismic hazard base value) is,
- the relation between the seismic hazard base value *H* and earthquake observation time interval *T* is roughly given by relation

$$H = (10.375 \pm 0.003) + (0.001 \pm 0.0003)\, T,$$

i.e., at large earthquake observation time interval T the increase of H has been slowed.

Critical evaluation of numbers in Table 1 shows that for complex technological facilities it is necessary to use the correct values of both quantities, i.e. T and t. The value of t is important for the life cycle of facilities and the value T is important for the safety reasons.

From practical reasons it is very big difference if we build the complex technological facility with life cycle 60 - 100 years with regards to maximum expected earthquake size value estimations 10.4° MSK-64 or 11.4° MSK-64; i.e. if the site seismic hazard value for determination of seismic risk for site in Central Bohemia (including the Praha capital) is 5° MSK-64 or 6° MSK-64.

Table 1. Maximum expected earthquake sizes that create base for determination of seismic hazard in Central Europe; T – observation period, t – time for which prediction is done.

Data	**T\t**	**50**	**100**	**200**	**500**	**1000**	**10000**
6 - 10.5	100	10.4	10.4	10.5	10.5	10.5	10.5
6 - 10.5	200	10.4	10.4	10.5	10.5	10.5	10.5
6.5-10.5	300	10.4	10.4	10.5	10.5	10.5	10.5
6.5-10.5	400	10.4	10.4	10.5	10.5	10.5	10.5
7 – 11.0	500	10.9	10.9	11.0	11.0	11.0	11.0
7 - 11.5	800	11.4	11.4	11.45	11.5	11.5	11.5

Considering the requirements of EUROCODE 8 included in building standard [20], so in the cases of intensities $I > 5° MSK\text{-}64$ we have from safety reasons at designing, construction and operation of complex technological facility to do the correction for seismic loads (which leads to rise of cost of facility construction). In other words, the given results mean that when we take into account the seismic hazard:

- calculated on data from the past 100 years, so we do not have to do the correction for seismic loads, i.e. they are not additional costs on facility construction,
- calculated on data from the past 800 years, so we have to do the correction for seismic loads and costs on facility construction increase.

Real data show that the costs for ensuring the complex technological facility safety in the second case are two times higher [3].

The experience from practice and the precautionary principle suggest for the latter solution. This is confirmed by results obtained from Japan in connection with nuclear power plant Fukushima accident [16]; for Fukushima NPP safety it was used data on tsunami since 1890 and for Onagawa NPP since 840, and therefore, the Onagawa NPP withstands the earthquake and tsunami without serious problems and the Fukushima NPP was destroyed by the tsunami.

7. Conclusion

Security and development of humans depend on the way by which the humans manage the disasters, i.e., how they know disasters and with what quality they perform the preventive, mitigating, responding, and renovation measures and activities. For obvious reasons it goes on establishing the maximum expected sizes of real disasters, with which the humans need to count on their protection, which means ensuring the protective measures not only for the human individuals, but for all the essential public assets.

On one side, many mathematicians and theoretically efficient experts trying to predict the major phenomena on the basis of sophisticated theories. However, at predictions of sizes of great phenomena they are using the data files from the past 10 to 20 years, with the substantiation that these data are very precise. At the origin of disaster with size greater than they calculated, they talk about the extreme phenomena, which call by names of mystic figures that invoke fear.

Otherwise, to the problems of today's world they are accessing the engineers who create and care for public assets in the territory, i.e. their task is to create works that are safe (i.e. even at their critical conditions they do not destroy themselves and their surroundings) and for their life cycles they fulfil the required functions in the certain level of quality. Therefore, the engineers calculate with: the existence of disasters, the sources of which are inside and outside the facility and with the human factor; and the reality that available resources, forces and resources are always limited. In the design, construction and operation of works they go from the system nature of world. They give the care to general and specific knowledge and experience, and they lean on real data.

Present work shows by help of data on earthquakes, as it is important to consider in practice the data on disasters from the historical times, even if they are not as accurate as the data of last years. Neglecting the data on major historical phenomena, causes that they are not established sufficiently effective protective measures ensuring the facility safety. Consecutively, in the origin of great phenomena there are occurred great losses of human lives, damages and injuries to the other public assets.

Finally, it is necessary to note, that even when the precautionary approach associated with the use of long time series of disasters is used, it could not be overestimated the skills and capabilities of humans, because it is the reality that the great planetary phenomena disturb the processes in sub-systems, and by that they are changing their regimes for shorter or longer time period (such as the earthquake in Indonesia on Dec. 26, 2004 or on March 11, 2011 in Sendai.

Acknowledgement

Authors thank to the Czech Technical University in Prague for grant on protection of critical infrastructures and complex technological facilities in frame of which this detailed research was performed.

References

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

[2] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KROEGER, W. *Safety and Reliability of Complex Engineering Systems.* ISBN: 978-1-315-64841-5. London: Taylor &Francis Group 2015.www.crcpress.com

[3] PROCHAZKOVA, D. *Principles of Risk Management of Nuclear Facilities.* ISBN: 978-80-261-0173. Plzen: University of West Bohemia 2016, 56p.

[4] NORQUIST, J. M. Theory of Largest Values Applied to Earthquake Magnitudes. *Trans. Am. Geoph. Un.*, 26 (1945), 29.

[5] GUMBEL, E. *Statistical Theory of Extreme Values and Some Practical Applications.* New York: Columbia University Press 1954.

[6] SHAFER, G. A. *Mathematical Theory of Evidence*. Princeton: Princeton University Press, Princeton 1976, 292p.

[7] DUBOIS, D., PRADE, H. *Possibility Theory*. New York, London: Plenum Press 1986.

[8] LUCAS, Ch. *Quantifying Complexity Theory*. 2006. www.calresco.org/lucas/quantity.htm

[9] RAKOWSKY, U. K. Fundamentals of the Dempster-Shafer Theory and Its Applications to System Safety and Reliability Modelling. *Special Issue. RTA 3-4.* Oslo: Balkema 2007.

[10] LUCK, P. H. *Schweizer Rueck – Sonderrisiken*. Zuerich: Swiss Re Publishing 1998, 23p.

[11] MUELLER, S. ET AL. *Safety Culture – a Reflection of Risk Awareness*. Zuerich: Swiss Re 1998, 45p.

[12] ZIMMERLI, P. *Natural Catastrophes and Reinsurance*. Zuerich: Swiss Re 2003, 46p.

[13] BEN MENAHEM, A. *Historical Encyclopaedia of Natural and Mathematical Sciences.* ISBN: 978-35-40-68831-0. Berlin: Springer 2011. 5988p.

[14] EM-DAT. *The OFDA/CRED International Disaster Database* – www.emdat.net. Brussels: Université catholicque de Lou-vain. www.emdat.be

[15] BEN MENAHEM, A. *Probability in Physics.* ISBN: 978-04-86-40465. Berlin: Springer 2011. 324p.

[16] EPSTEIN, W. Not losing to the rain: What I Learned when I learned about Onagawa. In: *Safety and Reliability of Complex Systems.* ISBN: 978-1-138-02879-1, London: Taylor &Francis Group 2015, pp. 365-371. ISBN: 978-1-315-64841-5, www.crcpress.com

[17] KUMAR, M., WIELENBERG, A., RAIMOND, E. Post Fukushima Lesson Learned for Probabilistic Safety Assessment. In: *Safety and Reliability of Complex Systems.* London: Taylor &Francis Group 2015. ISBN: 978-1-138-02879-1, pp. 489-496. www.crcpress.com

[18] PROCHAZKOVA, D. Earthquake Pattern in Central Europe. *Acta Universitatis Carolinae - Mathematica et Physica*. 34 (1993), pp. 3-66.

[19] IAEA. *Seismic Hazards in Site Evaluation for Nuclear Installations. Specific Safety Guide No. SSG-9*. ISBN: 978–92–0–102910–2. Vienna: IAEA 2010, 62p. www.iaea.org/books

[20] CR. Building norms. EU - 1998-1, ČSN EN. *Eurocode 8.* Praha: UÚTNMSZ 2013.

Chapter 15

ASSESSMENT OF CAPABILITIES OF CONVENTIONAL TOOLS FOR ANALYZING AND ASSESSING OF RISK IN CONTEXT WITH DYNAMIC RISKS*

1. Introduction

Firstly, it is necessary to unify the issue of risk nomenclature. The risk definition may be introduced in connection with different branches, such as economy, human health, environment etc. As it was mentioned in foregoing chapters, the general definition of risk is: the measure of unfavourable events with unacceptable consequences. The study is focusing on the problems of dynamic risk assessment. In this connection it is necessary to define this type of risk. The dynamic risks have an occasion in the surrounding changes (political, industry, economy etc.) of evaluating system, but also inside of this system. These risks may affect a large number of individuals and their threat is an irregularity.

Risk management and decision making under risk is a complex issue, especially in situations in which there are rapid changes due to external and internal factors that may influence the system functioning positively and negatively influence. A human being is able to identify, analyse and assess the risks leading to their minimization or complete elimination. If the risks and sources of danger are constantly searched for and evaluated, precautions that may reduce the overall level of risk are generated.

Specific risk scenarios for a specific system may in some cases be repeated and their scenario may be predictable. These scenarios of dangers, however, can be affected by many other factors that are not easily predictable, whether it is a human decision or situations with which man has not yet met (new technologies, waves of migration, etc.). The classical model of hazard scenarios and risk level may be in these conditions significantly changed.

This may not always happen only at extreme situations, affecting the entire country or region. It may be a significant event that will affect the individual elements of critical infrastructure locally, enterprises and their functionality, etc. It is not possible to rely solely on management of known risks, which are usually predictable. It is necessary to assess the threats and risks, which are dynamic and although their significance may not be great, they can, in some cases, under the effects of other factors become very serious risks. Meaning and principles for managing of these risks are, therefore presented below.

Authors: Dipl. Ing. Barbora Schüllerová, Ph.D., Assoc. Prof. , Dipl. Ing. Vladimír Adamec, PhD., Assoc. Prof., Dipl. Ing. Aleš Vémola, Ph.D., University of Technology, Brno, barbora.schullerova@ usi.vutbr.cz, vladimir.adamec@usi.vutbr.cz, ales.vemola@usi.vutbr.cz, Dipl. Ing. Petr Skřehot, Ph.D., Expert Institute of Health and Safety, Pardubice, skrehot@zuboz.cz, Dipl. Ing. Michaela Melicharová, T-SOFT, Praha, michaela. melicharova@tsoft.cz

2. The importance of dynamic risks

Currently the development of new technologies, materials, chemical substances and mixtures, as well as changes related to unexpected phenomena (drought, extreme heat, waves of migration, political conflicts, etc.), are a source of new threats and hazards that the current society is not properly ready for. Risks which the society encounters can be divided and characterized on the basis of different approaches. One of these approaches is the division of risk into static and dynamic. Static risk is defined as a possible loss, the causes of which do not originate in the economy, but for example due to losses caused by natural phenomena. The current problem is how to assess the dynamic risks. Approaches and methods for risk assessment are often focused on the statistic risk and a negative factor is also application of outdated data.

Dynamic risks are caused by changes in the reporting system in the area (political changes, industry and economy), but also inside the system. These risks may affect a large number of individuals and their big threat is their irregularity [1]. They can become so-called black swans for the whole system and its consequences can be fatal [2, 3]. Dynamic risk assessment is most often applied to describe the process of a changing (dynamic) environment within which the development of the system itself is described. The urgency of dealing with dynamic risks, their changes and the impact on functional systems are dealt with not only from the economic point of view [4, 5].

A man often perceives the risks which he is aware and which he can identify. Methods for identifying the risks in connection with a particular process are detected on the basis of knowledge from the perspective of the evaluator or external entity. We must not, however, forgot other risks, that can significantly affect the process. Three main strategies are currently selected which are generally known in risk management. They are information, safety and preventive measures, and discursive strategies. The security strategy is also known as a strategy of robustness and adaptability, especially when a method of constant monitoring of the situation, adequate knowledge and research of emergencies are chosen, providing alternative sources and measures to maintain the function of the affected system. Discursive strategy is based on building the measures to ensure the certainty and reliability through the reduction of uncertainties, clarify facts related to the origins and effects of risks, engagement of the parts concerned, vigilance and responsibility [6, 7]. The strategies and approaches mentioned appear to be insufficient for the problems in question, as is highlighted in the following text.

2.1. Approaches to dynamic risk management

This approach is applied in many areas where there are varying conditions, for example, during the year. Examples are studies [8-10], which reported that these conditions may, in the normal application of quantitative assessment and risk management, give rise to errors and distorted data. The importance of the dynamic approach to risk management is occasional especially in the areas of effective prevention [8]. This approach is able to take into account a new perspective on risk and early warning signals and systematically evaluate the related risks.

One of these approaches is the Dynamic Risk Management Framework (DRMF), the aim of which is to highlight, describe and implement the needs related to improving and updating processes related to risk management. DRMF uses two methodologies in the context of hazard identification. The first is the Dynamic Procedure for Atypical

Scenarios Identification (DyPASI), arising from the project of EC iNTef-Risk [12]. The aim of this method is to create a complete risk assessment process, the creation of scenarios accident events, which differs from conventional expectations [11, 12, and 13].

The second approach is the dynamic risk assessment (Dynamic Risk Assessment (DRA) using the Bayes Theorem (1), based on abnormal situations and figures about accidents [19].

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} = \frac{P(A \cap B)}{P(A)} \quad (1)$$

where are A and B are events in sample space. The meaning of the dynamic approach to risk assessment finds application not only in the prevention of accidents but also in the prediction of upcoming events, both positive and negative [12]. The importance of this approach is described, for example, in [14].

The application of this approach is explained using the case of a support system based on geographic information, which is used for the analysis of natural disasters and their modelling time. The aim is to provide the most accurate basis for population protection acts such as the evacuation of residents. It also enables the modelling and monitoring of environmental risks and impacts [15]. The application of dynamic risk assessment within the Human Reliability Assessment (HRA) method using systems such as Accident Dynamics Simulator-Information Decision and Action in Crew (ADS-IDAC), which is able to dynamically simulate various events such as the threat of a blackout. This system is chosen in such complex areas as energy and other critical infrastructure elements [16, 17].

Human reliability and neglect of certain obligations are a general major threat. The human factor is described as the sum total of human abilities and characteristics which may have a significant impact on the assessed system both in terms of efficiency and productivity. A man is capable of creative thinking and can react promptly to the situation. The most common cause of errors is stressful situations. However, it can happen even in another extreme situation that a person makes mistakes, if there is a complete absence of the stress factor throughout its operations, which may be based on monotonous activities which can lead to omission of important steps [18].

The system of dynamic risk assessment is able to monitor, detect, assess and propose and apply subsequent measures as was indicated in [39]. This system is based on the method of safety assessment by the following equation:

$$R_{New} = R_{Current} + \sum rf_{New} - \sum ri_{Old} \quad (2)$$

where R_{New} is the current risk level and Σrf_{New} is the sum of scores signed to new risk factors discovered by the assessing, and where Σrf_{Old} is the sum of scores assigned to old risk factors of $R_{current}$ that are no longer discovered by the assessing, and where ri_{New} is a new risk increment based on a combination of the new risk factors, and where ri_{Old} is an old risk increment based on a combination of the old risk factors [39].

The European Commission also highlights the importance of risk management by the dynamic approach in real time [40]. It refers to new research which combines two different techniques leading to threat identification and risk assessment within one dynamic process being assessed. The choice of this approach enables information updates

and risk assessment, which are subsequently used for precise calculations corresponding to the real situation.

2.2. Methods of analysis and modelling of dynamic risk

Methods of assessment and risk analysis are in many cases based on the risk assessment of static risks. As stated in [19], the main drawback of the traditional Quantitative Risk Assessment (QRA) is the inability to update the risk over time for developing conditions. The techniques used in this evaluation determine the probability of occurrence of a specific event and determine the potential loss of life caused by undesirable events.

Therefore, for dynamic risk assessment, models based on methods of the tree and flow diagrams or other calculation methods such as the Bayes theorem [20-23] are used. Among the models allowing a description of the behaviour of dynamic phenomena in time are the Markov models, the Dynamic Event Logic Analytical Methodology (DYLAM), providing an integrated framework for explicit handling of time, the procedural variables and system behaviour, further, the Dynamic Event Tree Analysis Method (DETAM) tracking the time-dependent evolution of a hardware device status, the values of process variables and the state of the operator during the development of a scenario [21]. The methods mentioned are based on the development and description of an event through the logical Event Tree Diagrams (ETA). This diagram enables to create a logical view of the relationship between the causes and effects. In [22], the authors applied this method to create a complete scenario of risk and in [23-26] the authors used this method for the analysis of traffic safety, etc. The "butterfly" approach mentioned is chosen especially in situations where it is necessary to make immediate decisions based on events changing in time.

In real time, the monitoring of these risks is necessary, especially from the perspective of the implementation of effective preventive measures. An early and effective identification of process faults is crucial in the prevention of major accidents. In this case, for example, principal components (PCA) or the method of the probability factor (GLR) or multidimensional detection and fault diagnosis techniques [5, 27-30] are applied. These methods have been created for specific systems and processes (oil industry). The possibility of identifying risks within the dynamic processes can be based on these methods. Compared to the traditional static risk assessment, Dynamic Risk Assessment (DRA) has a lot of advantages, such as uncertainty quantification (FTA method, etc.) which may lead to improvements in the accuracy of risk calculations in real-time. By constant updating of the information, risks can be assessed better and thus also managed better. Thanks to an early identification of abnormal risks, it is possible to respond to them in a suitable way [30-35].

2.3 Software for simulation of development and impact of risks

Currently, there is software which seeks to work with a dynamic environment and with associated risks. However, this software has mainly been developed for the assessment of economic risk and the related optimization processes within the enterprise system. An example is the Risk Dynamic Analyser (RDA), which is intended for regular or immediate risk analysis in operation. The software is able to analyse risks in the process and highlight them in advance, so that they can be averted in time or the rate can be

reduced [21]. The Czech Republic has also developed new programs and software that allow dynamic simulation, which is a tool for optimizing and improving business processes. The aim is to increase the utilization capacity, increase the flow and speed up production time, reduce inventory and work in process, optimal configuration of facilities, equipment and operating personnel, increase competitiveness. The software is especially applied in the field of logistics and risk identification in economy enterprises [22-25].

The very frequently used software tools for modelling emergencies in the CR, especially in terms of releases of hazardous substances, include the TerEx (Terrorist Expert) program and the freely available ALOHA software. Other programs suitable for the modelling of hazardous substances are, for example, ROZEX Alarm (CR), Phast (NR) EFFECTSGIS (NL), RMP Comp and [26-31]. The total impact analysis (leakage, evaporation, dispersion, fire, explosion, vulnerability) can be further evaluated using the following software tools: WHAZAN, PHAST, SAFETI; RISKAT; EFFECTS / DAMAGE, RISKCURVES SOCRATES, Chemical Accident Index - an index of toxicity (CEI), IAEA -TECDOC - 727, FlUIDYN [32, 33].

The software products focused on the calculation of risks in projecting, industry and the environment include, for example, RMPlanner, HazardReview, Risk Radar, FaultrEASE, Cegis FaultrEASE, AgRisk, SiteSafe, BOSS, DNV Risk Management Software, EQUIS - Environmental Quality Information System RBCA, in the financial and business areas, then COBRA, Algo Suite Solutions, Quantum Sierra, Sierra Treasury, Sierra ASP, CORA - Cost-of-Risk-Analysis, financial Software Lattice, STP, SunGard, DATA. Furthermore, there is software created for specific areas of tools for calculating risk in the areas of pipelines (Bass-Trigon Software, BOSS) hydrology (HFAM, HYDRON, HYDRA) and the like [34-37]. Currently, a large development of information technology is available to many software products, resulting in risk assessment. Software products are based on physical models of varying complexity, which can result in obtaining inaccurate and unreliable results. Most of the existing software tools can be used only to evaluate certain type of cases.

2.4 Dynamic risk in context with so called black swans

Risk analysis and assessment should not overlook risks with very low probability which may seem to be improbable for the evaluator. Taleb in his book [40] discusses the so-called false sense of security. It is likened to the life of a turkey that is fed, which gives it a sense of satisfaction and safety without realizing that in the end it will be the main course at dinner. The same is true even for the man who does not perceive the risk, does not realize it or ignores it. It could be caused by the fact that the threats are known or previously do not occur in this process. However, it does not mean that similar cases have not already occurred in the same or similar processes. In these cases, it could be neglected and the warning signals may not be perceived as well as the subsequent manifestation of threats.

Also, the threat assessment and the preventive measures must be applied in accordance with reality (e.g. not expect a tsunami from the ocean in an inland state). Therefore, it is important to determine when risk assessment and so-called limits of acceptability and the implementation of risk could cause serious damage [1]. Identification and analysis of black swans is a very complicated problem, which is discussed by many experts [41, 42, 43, and 44]. It is the need for finding a combination of the warning signs, early detection and rapid response. Continuous monitoring of signals could be suitable as prevention of

their ignorance and re-examination of the already existing events, which can lead to timely preventive measures for the threats of black swans or at least mitigate their impact. There are recommended general approaches that include the possibility of forming hypotheses and the application of a combination of risk analysis methods. As seen above, the issue of the dynamic risk and so-called black swans is not only associated with accidents in industrial processes but it could appear at different levels (individual, company, locality etc.), which means individual and society risk. With regard to the current rapid development of society and the changes that are happening, there has been a search for possible ways and methods which would help to increase prevention and the prediction of threats that are particularly dynamic.

3. Data

The problem situation for this study was a model municipality with 3000 habitants with fictitious infrastructure. This type of municipality was chosen as a typical system without special crisis planning and experience with solving undesirable events, especially in context with dynamic risks. As a model problem situation, a non-periodical cultural event with more than 250 attendees was dealt with. This cultural event was organized for the first time. It was a short term event (5 hours of preparations, 2 hours of performance, and 3 hours of cleaning after the event). The most danger parts are the phase of preparations and then especially the phase of the performance. Risk assessment included the connections of this system with the surroundings, historical experience not only from this municipality, undesirable events, current state, available preventive measures of the integrated emergency system, etc. Data collection is recommended from the local documents, methods, legislative, expert experience, etc. Due to the fact that there was a lot of data, it was necessary to choose suitable methods and approaches for the assessment and evaluation of the problem.

4. Materials and methods

It is necessary to choose suitable approaches and methods for dynamic risk assessment as was found out during the analysis of the current state. Also, methods based on the combination of a qualitative and quantitative approach were chosen. Due to this fact, the methods were chosen in accordance with the common practice and were proposed with the aim of an easy and effective monitoring of the development of a specific situation. These methods are based on the systematic approach, which is compatible with risk engineering methods for solving the problem.

4.1. Systemic approach

This approach was chosen because of its comprehensive and integrated approach, which helps to achieve an objective manner to get the optimal process. The basic attributes of the system approach are:

1. The definition of the area of interest.
2. The approaches to problem solving.
3. The assessed specifications of the area of interest.
4. The definition of methods for analysing the considered area.
5. The ethical standards and compliance with them.

What is important is the assessment of properties and the entity and its binding (internal and external) with the ongoing processes that positively or negatively affected the system under evaluation. The systematic approach is also implemented in methods of risk engineering and therefore these methods were chosen to match the requirements of the individual attributes and assist to fulfil them. Selected methods are listed in the following chapter.

4.2 Risk engineering methods

Qualitative methods are the first step in risk analysis by which the identification of risk sources is done and the probability of occurrence of a specific phenomenon and losses is determined. The methods are based on the deterministic approach and it is suitable to complement them by another risk analysis like the quantitative method [46]. The method suitable for the identification of risk is, in cases of dynamic risk events, primarily the so-called tree diagram analysis with a logical division. Using these methods, it is possible to detect possible risks and their causes, which can have undesirable consequences leading to the disruption of the process or system. Due to this fact, the following methods have been chosen:

1. Fault Tree Analysis, FTA, which analyses the causes of undesirable events using logical gates. FTA could be applied as a quantitative approach with calculation of the probability of causes [47]. Other methods which are applied in the first step of analysis – risk identification, are also Check List Analysis, What if Analysis. These methods are able to determine the area of interest and closely specify the elements which are evaluated.
2. Quantitative methods are suitable for detailed analysis of the whole process. As was mentioned in the previous chapters, one of these suitable methods is another one based on the tree diagram analysis. *Event Tree Analysis*, *ETA*, which analyses the final status of undesirable events after the initiatory event. The methods mentioned are applied in the area of risk and safety engineering and together with other methods they will be used for dealing with the risk of damage occurrence and its prevention.

5. Results

Based on the analysed methods, the methodology of dynamic risk assessment with application on the real system as autonomous units has been proposed. The reason why it is necessary for these systems to do this assessment are processes that are realized in these whole systems and that are influenced by external and internal environment. These systems have dynamic progression and specific manifestation. These processes could be:

- short-term
- long-term
- periodical
- repeated without periodicity
- random

These long-term processes or periodical events could be thoroughly analysed and suitable preventive measures could be proposed for them to reduce or eliminate the risk of undesirable events occurrence. However, the processes should be influenced by other

factors and processes, which may significantly change their course in a positive or negative manner. With regard to these facts, methods aiming to monitor the manifestation of dynamic risk were chosen and applied within the proposed methodology.

5.1. Systemic approach application

In context with the chosen approaches and methods for dynamic risk assessment, it has been evaluated that it is necessary to choose the common approach in the first step. Other methods are chosen based on this method. A systemic approach is suitable for these requirements and it is a suitable choice for solving the determined aim because it is created logically and with a step by step methodology. A systemic approach by the author of [48] is created using twenty attributes, divided into five subgroups (Figure 1). The attributes, which are defined in connection with the solution, are characterized in the next part and the categorization has been created by the author mentioned.

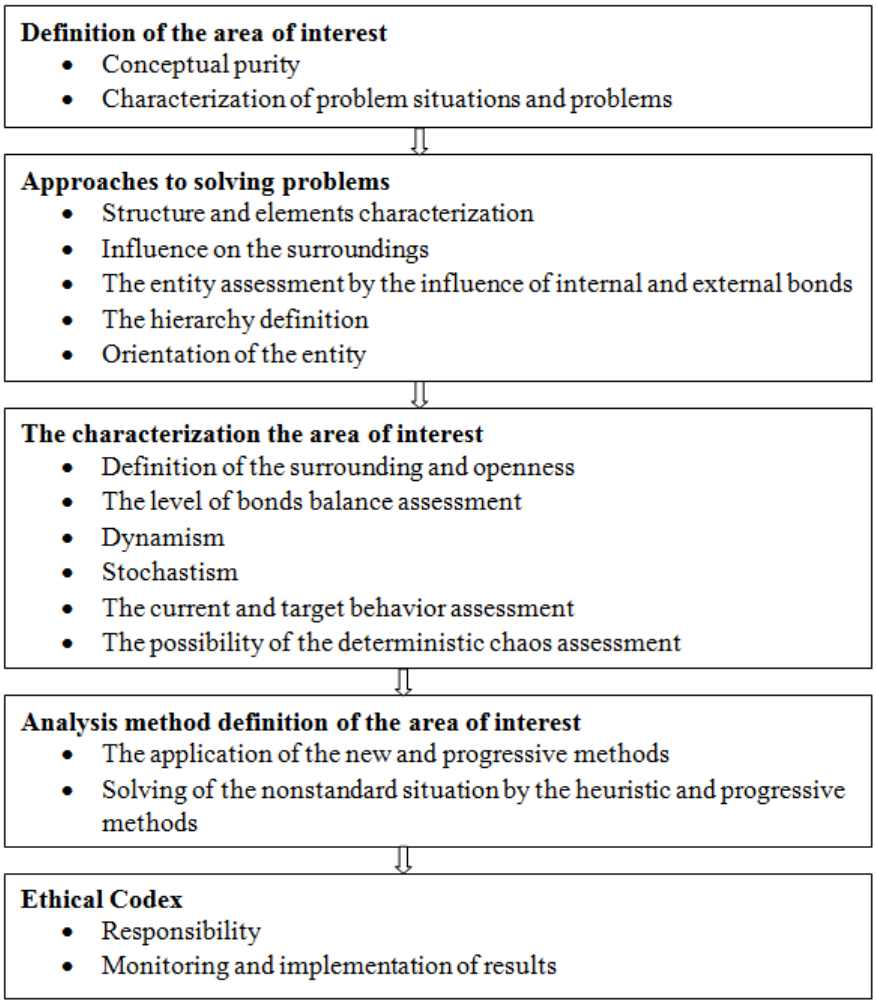


Fig. 1 Attributes and subgroups

Attributes should be different with respect to the problems being solved. Their assessment and registration are also important as they make it possible to unify the approach to solving specific problems such as the dynamic risk assessment in this issue.

5.2. Application of risk engineering methods

To assess and join the various attributes, risk engineering methods were chosen. These methods help to identify threats and risks. However, this approach allows a relatively rapid application and thereby creates risk scenarios for their identification. As was mentioned in part 4, the chosen methods include the Event Tree Analysis and the Fault Tree Analysis to identify potential threats. The approach is shown in Table 1 and the method in Figure 2.

Table 1. Example of subgroups of systematic approach of authority unit (municipality).

Subgroups	**Attribute**	**Characterization**
Area of interest	centre of culture	reconstruction
		cultural event (> 250 people)
Approaches to problem solving	multifunction centre, non-periodical events with > 250 people, safety measure	included in crisis plan, internal safety measures, accessibility, duration of the event, another event at the same time etc.
Specifications of the area of interest	city centre, traffic, objects of interest	road with high density of traffic, petrol station, bus station, shops, river
Methods for analysing the considered area	qualitative risk analysis methods	What if, ETA, FTA
Ethical standards and compliance with them	Legislation	local regulation

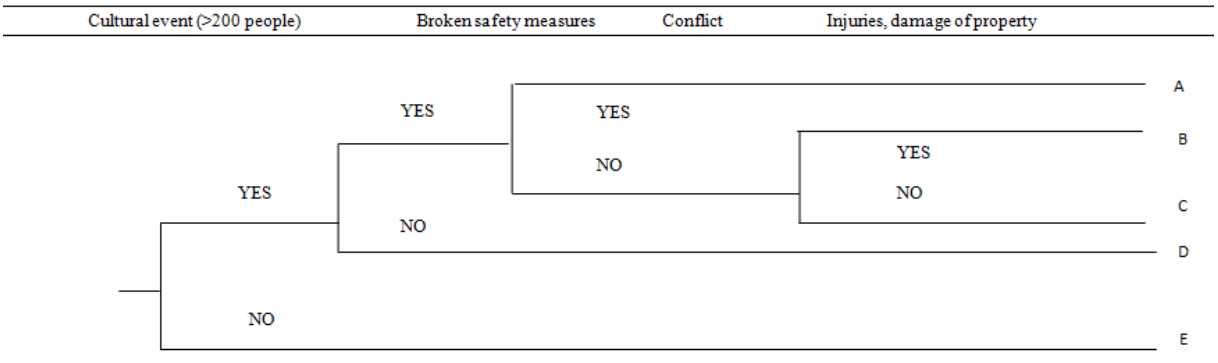


Fig. 2. Example of the ETA method application

The end events are indicated by letters A-E, the characteristics of which are set out in Table 2. In some cases, there may be the same ending element more than once, and therefore the aim of this indication is to clarify and simplify the results interpretation.

Table 2. Example of impact assessment in context with ETA.

Impact	**Significance**
A	Highly dangerous event with risk of injuries, life and property damage
B	Dangerous event with risk of injuries and property damage
C	Risk of small injuries and property damage
D	Risk of inadequate safety measures
E	Function of safety measures

In the second case, the FTA method was applied with the aim of controlling the origin of risk. The FTA method is suitable in cases after known events and their impact. It is possible to find the root events which are responsible for these damages. It is then possible to control the right procedure for creating the risk scenarios by the ETA method. The FTA method could be applied with a qualitative approach. This method is applied with the logic knots of AND and OR. It is possible to apply the Caused and Consequences Analysis (CCA) known as the butterfly method. In this case, it is also possible to use the Caused and Consequence Analysis with the so-called butterfly approach. The ETA method is used to create the risk scenarios and estimate the possible consequences in case of the threat realization. Specifically, the possible effects of undesirable events related to the processes which occurred during the evaluated system.

After the application of these methods, it is suitable to create the risk registration. In this register, notes are the elements of the assessment system and threats and risks which are connected with them. The structure of this register is similar to the register in OSH with the application of the elements of the FMEA method and the Check List analysis (Table 3). The register is suitable for controlling known and appropriate threats connected with them. The periodical control is highly important for prevention of risk and for detailed creation of risk scenarios.

Table 3. Example of risk identification by Check List.

System/ Subsystem	**Hazard identification**	**Source of risk**	**Consequences**	**S**	**O**	**D**	**RPN**	**Measures**	**Date**	**Responsibility**	**Control**
Auditorium	conflict	audience	serious/ fatal injuries					layout of security guards, choosing conflict individuals	regular during performance	management of security guards, security guards	+
			numerous injuries								+
			property damage								+
			thefts								+
			cancelled show								+
	terrorist attack	individual/ society	numerous injuries, fatal injuries					layout of security guards, choosing conflict individuals,			+

System/ Subsystem	Hazard identification	Source of risk	Consequences	S	O	D	RPN	Measures	Date	Responsibility	Control
								cooperation with rescue services, security measures, monitoring of security situation			
	spread of disease		mass infection					monitoring of individuals with symptoms of disease, cooperation with health care services, monitoring of health situation in and around the city		management, health care service	-
	fall of subjects	human factor/ mechanical damage	numerous injuries, fatal injuries					layout of security guards, control before and during performance, cooperation with police services	Regular before and after performance	management of security guard, technical management, maintenance	+
	fire	human factor/ technical failure	serious/ fatal injuries, property damage					layout of security guards, control before and during performance, cooperation with firefighting services		management of security guide, technical management, maintenance, fire service	+
	explosion		serious/ fatal injuries, property damage					layout of security guards, control before and during performance, cooperation with firefighting and police services			+

The creating of the register as a database of threats, risks and near misses (almost undesirable events) including the measures and responsibilities should be based on the areas of interest and sources of threats (Table 4).

This database allows the identification and monitoring of threats and risks in various areas which occurred or may occur with respect to the assessed entity. In the register, preventive measures and responsibilities are also determined by the guarantors. Determining responsibilities and creating the overview also helps to capture a broad portfolio and provide the ability to minimize identified threats. The assignment of responsibilities must be performed in accordance with the local regulations. If it is necessary to choose more responsible persons, it is important to define the affected areas with respect to their inclusions.

Table 4. Example of threats and risk database by their source.

Source of	Risk	Scenario	Conse-quences	Date on event	Measures	Preven-tion	Respon-sibility-	Current
Anthropogenic	Fight	conflict between personal and attendees of cultural centre	injuries of 3 attendees and 2 employees	10/1993	police and security intervene-tion	Reinfor-cement of security guard	Manage-ment of cultural centre	
	intentional damage	damage of equipment and security measures	fall of decoration and injuries of 20 attendees	06/1975	security intervene-tion	more security guards, sector distribution		
	suspicious subject	finding suspicious sacks	false alarm	09/2014	police and security intervene-tion	often security patrol, thorough inspection before perfor-mance	Manage-ment of security guard	
Natural	Flood	flooding of centre	property damage, cancelled performan ces	04/1997	Interven-tion of rescue services	preventive flood protection measures (active, passive, continual)	rescue services, manage-ment of cultural centre	
	steady rain	roof damage	property damage,	03/2003	Interven-tion of rescue services, improved roofing	stronger roof construction, regular inspections	rescue services, manage-ment of cultural centre, maintena-nce manage-ment	
	snow calamity	roof damage	serious injury of employee,	01/1930, 12/2001				
Economic	want of money	expensive performa-nce	cancelled performa-nce	02/2007	refund tickets	insurance of cultural events, financial reserve, estimated budget	financial manager of cultural centre	

Source of	Risk	Scenario	Conse-quences	Date on event	Measures	Preven-tion	Respon-sibility-	Current
Technology	power damage	stoppage of operation	delay of performance and financial expense	09/2014	electrician service	stronger power site, regular control before performance	technical manager	

5.3. Results evaluation

The above mentioned practices respond to the results of the current state where, apart from the stationary risks, it is more and more frequent for dynamic ones to appear. The reason could be: inadequate attention to warning signals, ignorance of the newly introduced process and inexperience with this process, insufficient analysis of internal and external factors that has impact on the evaluated objects of interest/ entity, not placing the responsibilities of competent persons, ignoring past events and near misses etc.

The reasons mentioned are related to the risk of the so-called black swans. Therefore, the methodology of the dynamic risk management was designed in accordance with the requirements for minimization and prevention. These requirements could include: secondary measures for planning the creation of a functional communication network, investigation of any undesirable event or near misses incl. their causes, monitoring events in similar systems, sharing the gained experience with the common guidelines and local regulations etc.

The solution method is based on the comprehensive and dynamic complexity of assessing the risks with regard to the source of threats and the related risks. Applying this method is useful for the systems and processes that may be affected by external factors or processes without periodicity. It therefore represents for example businesses or municipalities and other local authorities. Of course, changes and further applications depend on the input data and the time period of the evaluation with respect to the size of the system. The whole principle of using the systematic approach which is also part of risk engineering methods remains unchanged.

6. Conclusions

Dynamic risk management is a difficult task that cannot be solved using only one method of risk analysis. As in the prediction and reduction of highly improbable events called Black swans [1], it is necessary to follow a few basic rules. It is the perception of the threats and risks as probable, which must be registered in the related system. An example is the risk register, which should be conducted, reviewed and updated only at regular intervals such as once a year but also with every change that occurs and is associated with the evaluated systems (e.g. business, municipality or region). In this register, records of incidents and threats that have occurred or almost occurred should also be maintained. In the case of OSH, they are, for example, the records about the near-misses [38]. It is not only the OSH where such abnormal situations should be recorded and kept in mind by employees.

The next step is to monitor the events retrospectively which have already occurred in history and may not be directly related to the event system being evaluated. The knowledge of this information may help in the identification of threats and risks, their assessment and implementation of appropriate preventive measures. In the case of dynamic risk, the knowledge of the period in which they occur is also important. This may be the known threats and risks. For example, an enterprise focused on agricultural activities has the highest productivity in the season but out of the season, the production is reduced as well as the number of employees. Threats and risks for these periods are different and their approximate interval duration is known. In these periods, the monitored threats and risks vary. If they are continuously monitored, they can also be detected early and as negative factors that could significantly increase the threats and risks. The paper presented the current approaches, methods and software tools that can be applied to control the dynamic risks in complex systems like municipality. It depends on the individuality of each system which has its own distinctive characteristics and must apply these methods and approaches adapted. The solving of this problem is currently focused on the possibility of dynamic risk management of risk within the local government. The aim is to increase efficiency in risk management, strengthening prevention, reducing or preventing adverse events and the ability to support preventive obligations and liability.

References

[1] AVEN, T. On the Manning of a Black Swan in a Risk Context. *Safety Science.* ISSN: 0925-7535. 201 (2013), 57, pp. 44-51.

[2] TALEB, N. *Černá labuť – Následky vysoce nepravděpodobných událostí.* ISBN: 978-80-7432-128-3. Praha: PASEKA 2007, 478p.

[3] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* ISBN: 978-80-247-4644-9. Praha: Grada 2013, 483 p.

[4] ANAGNOSTOPOULOS, T., KOLOMVATSOS, K, ANAGNOSTOPOULOS, CH. ZASLAVSKY, A, HADJIEFTHYMIADES, S. Assessing Dynamic Models for High Priority Waste Collection in Smart cities. *Journal of Systems and Software.* ISSN: 0164-1212, 110 (2015), pp. 178-192.

[5] KHAN, F., RATHNAYAKA, S., AHMED, S. Methods and Models in Process Safety and Risk Management: Past, Present and Future. *Process Safety and Environmental Protection.* ISSN: 0957-5820, 98 (2015), pp. 116-147,

[6] SHAFAGHI, A. Equipment Failure Rate Updating-Bayesian Estimation, *J. Hazard. Mater*. ISSN: 0304-3894. 159 (2008), 1, pp. 87–91.

[7] HARROU, F., NOUNOU, M. N., NOUNOU, H.N., MADAKYARU, M. Statistical Fault Detection Using PCA-based GLR Hypothesis Testing, *Journal of Loss Prevention in Process Industries,* ISSN: 0950-4230. 26 (2013), 1, pp. 129-139.

[8] PALTRINIERI, N., DECHY, N., SALZANO, E., WARDMAN, M., COZZANI, V. Towards a New Approach for the Identification of Atypical Accident Scenarios. *Journal of Risk Research,* ISSN: 1466-4461. 16 (2013), 3/4, pp. 227- 354.

[9] MEEL, A., SEIDER, W. D. Plant-Specific Dynamic Failure Assessment Using Bayesian Theory. *Chemical Engineering Science.* ISSN: 0009-2509. 61 (2006), pp. 7036-7056.

[10] SHALEV, D. M., TIRAN, J. Condition-Based Fault Tree Analysis (CBFTA): A New Method for Improved Fault Tree Analysis (FTA), Reliability and Safety

Calculations. *Reliability Engineering and System Safety*. ISSN: 0951-8320. 92 (2007), pp. 1231-1241.
[11] PALTINIERI, B., KHAN, F., AMYOTTE, P., COZZANI, V. Hoeganaes Metal Dust Accidents. *Process Safety and Environmental Protection*, ISSN: 0957-5820. 92 (2014), pp. 669-679.
[12] PALTRINIERI, N., TUGNOLI, A., BUSTON, J., WARDMAN, M., COZZANI, V. Dynamic procedure for Atypical Scenarios Identifications (DyPASI): A New Systematic HAZID Tool. *Journal of Loss Prevention in Process Industries*, ISSN: 0950-4230. 26(2013), 4, pp. 683-695.
[13] PALTRINIERI, N., QIEN, K. M., COZZANI, V. Assessment and Comparisons of Two Early Warning Indicator Methods in the Perspective of Preventive of Atypical Accident Scenarios. *Reliability Engineering and System Safety*, ISSN: 0951-8320. 108 (2012), pp. 21 – 31.
[14] GAO, L. Collaborative Forecasting, Inventory, Hedging and Contract Coordination in Dynamic Supply Risk Management. *European Journal of Operational Research*, ISSN: 0377-2217. 245 (2015), pp. 133-145.
[15] FULI A., COMFORT, L. K., DONG, Y., ZNATI, T. A Dynamic Decision Support System Based on Geographical Information and Mobile Social Networks: A Model for Tsunami Risk Mitigation in Padang, Indonesia, *Safety Science*, ISSN: 0925-7535 (2015).
[16] CHANG, Y., MOSLEH, A. Cognitive Modelling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents, Parts 1-5. *Reliability Engineering and System Safety*, ISSN: 0951-8320. 92 (2007), pp. 997-1101.
[17] COYNE, A. *Predictive Model of Nuclear Power Plant Crew Decision-Making and Performance in a Dynamic Simulation Environment*, College Park, MD: University of Maryland PhD Dissertation, 2007.
[18] DOLEŽAL, R. et al. Analýza a hodnocení rizik s ohledem na lidský faktor: materiály z 50. semináře odborné skupiny pro spolehlivost (In Czech). Praha: Česká společnost pro jakost, 2013, 32. sISBN: 978-80-02-02434-7. www.csq. cz/fileadmin/user_upload/Spolkova_cinnost/Odborne_skupiny/Spolehlivost/Sbor niky/Sbornik _2013_02_26_Lidsky_faktor.pdf.
[19] KALANTARNIA, M., KHAN, F., HAWBOLDT, K. Dynamic Risk Assessment Using Failure Assessment and Bayesian Theory, *Journal of Loss Prevention in Process Industries*, ISSN: 0950-4230.22 (2009), 5, pp. 600-606.
[20] MARSEGUERRA, M. RICOTTI, M, ZIO, E. Approaching System Evolution in Dynamic PSA by Neural Network, *Reliability Engineering and System Safety*, ISSN: 0951-8320. 49 (1995), 1, pp. 91-99.
[21] KALANTARNIA, M, KHAN, F., HAWBOLDT, K. Dynamic Risk Assessment Using Failure Assessment and Bayesian Theory, *Journal of Loss Prevention in Process Industries*, ISSN: 0950-4230. 22 (2009), 5, pp. 600-606.
[22] YANG, X., ROGERS, W. J., MANNAN, M. S. Uncertainty Reduction for Improved Mishap Probability Prediction: Application to Level Control of Distillation Unit, *Journal of Loss Prevention in Process Industries,* ISSN: 0950-4230, 23(2010), 1, pp. 149-156.
[23] SHAFAGHI, A. Equipment Failure Rate Updating-Bayesian Estimation. *Journal of Hazardous Materials,*159 (2008), 1, pp. 87-91.

[24] MARKOWSKI, A., AGATA, K. Bow-tie Model in Layer of Protection Analysis. *Process Safety Environmental Protection*, ISSN: 0957-5820. 89 (2011), pp. 205-213.
[25] ESLINGER, K., URE, D., KUTLAY, S. Risk Management and Analysis of Driving Hazard Using Bow Tie Model. *SPE International Conference*. Alberta: SPE 86846.
[26] WIERENGA, P. ET AL. Application of the Bow-Tie Model in Medical Safety Risk Analysis. *Drug Safety*, ISSN: 1179-1942, 32 (2009), pp. 663-673.
[27] ELHDAD, R., CHILAMKURTI, N., TORABI, T. An Ontology-Based Framework for Process Monitoring and Maintenance in Petroleum Plant, J *Journal of Loss Prevention in Process Industries*, ISSN: 0950-4230, 26 (2013), 1, pp. 104-116.
[28] XU, Q., ZHANG, L., LIANG, W. Acoustic Detection Technology for Gas Pipeline Leakage, Proc. Saf. Environ. Prot., 91(2013), 4, pp. 253-261
[29] ZADAKBAR, O., IMTIAZ, S., KHAN, F. Dynamic Risk Assessment and Fault Detection Using a Multivariate Technique. Proc. Saf. Prog., 32 (2013), 4, pp. 365-375
[30] FLAGE, R., BARALDI, P., ZIO, E., AVEN, T. Probability and Possibility-Based Representations of Uncertainty in Fault Tree Analysis, *Risk Analysis*, ISSN:1539-6924. 33 (2013), 1, pp. 121-133.
[31] KARDA, L., KUDLÁK, A. *Analýza, metody a nástroje na řešení krizových situací*. České Budějovice: Jihočeská univerzita 2007, 44 p.
[32] PROCHÁZKOVÁ, D. MV GŘ HZS ČR. *Seznam – Přehled metodik pro analýzu rizik* (In Czech). 2004, 15 p. http://krizport.firebrno.cz/file/122.
[33] KHAKZAD, N., KHAN, F., AMYOTTE, P. Dynamic Risk Analysis Using Bow–Tie Approach, *Reliability Engineering and System Safety*, ISSN: 0951-8320, 104 (2012), pp. 36-44.
[34] YOU, X., TONON, F. Event-Tree Analysis with Imprecise Probabilities. *Risk Analysis*, ISSN: 1539-6924, 32 (2012), 2, pp. 330-344.
[35] SINNAMON, R. M., ANDREWS, J. D. New Approaches to Evaluating Fault Trees. *Reliability Engineering and System Safety*, ISSN: 0951-8320, 8 (1997), 2, pp. 89-96.
[36] KHAKZAD, N., KHAN, F., AMYOTTE, P. Dynamic Safety Analysis of Process Systems by Mapping Bow–Tie into Bayesian Network. *Process Safety and Environmental Protection*, ISSN: 0957-5820, .91 (2013), 1-2, pp. 46-53.
[37] SHALEV, D. M., TIRAN, J. Condition-Based Fault Tree Analysis (CBFTA): A New Method for Improved Fault Tree Analysis (FTA), Reliability and Safety calculations. *Reliability Engineering and System Safety*, ISSN: 0951-8320. 92 (2007), pp. 1231-1241.
[38] BÍLEK, E. Sedm kroků ke stanovení rizik a co se za nimi skrývá (in Czech). *BOZPInfo.cz* http://www.bozpinfo.cz/knihovna-bozp/citarna/tematicke_prilohy/ rizika/ postup040319.html
[39] PRADEEP, B. Dynamic risk management (In Czech). *US 7908660 B2*. 2011-03-15, US 11/702,974 https://www.google.com/patents/US7908660
[40] PALTRINIERI, N., KHAN, F., AMYOTTE, P. ET AL. Dynamic Approach to Risk Management: Application to the Hoeganaes Metal Dust Accidents. *Process Safety and Environmental Protection*, 92 (2013), 6, pp. 669-679.
[41] HANSON, D., WARD, T, IVES, N. Responding to a Black Swan: Principles and protocols for responding to unexpected catastrophic events. London:

Ernst&Young, 13.1.2011, http://www.ey.com/Publication/vwLUAssets/Responding_ to_a_Black_Swan/$FILE/Responding_to_a_Black_Swan-5_Insights.pdf
[42] MURPHY, J. F., CONNER, J. Black Swans, White Swans, and 50 Shades of Grey: Remembering the Lessons Learned from Catastrophic Process Safety Incidents. *Process Safety Progress*, 33 (2012), 2, pp. 110-114.
[43] AVEN, T. Implications of Black Swans to the Foundations and Practice of Risk Assessment and Management. *Reliability Engineering and System Safety*, 134 (2005), pp. 83-91.
[44] NILSSON, J. Introduktion till riskanalysemetoder, Lund University for Risk Analysis and Management, LUCRAM. *University of Lund*, Sweden, 2001.
[45] WANG, W., X. JIANG, S. XIA a Q. CAO. Incident Tree Model and Incident Tree Analysis Method for Quantified Risk Assessment: An In-Depth Accident Study in Traffic Operation. *Safety Science*. 48 (2010), 10, pp. 163-180.
[46] JANÍČEK, P. *Systémová metodologie*. *Brána do řešení problémů* (In Czech). ISBN 978-80-7204-887-8. Brno: Akademické nakladatelství CERM, s.r.o. 2014, 374p.

Chapter 16

SUPER PROCESSES FOR MANAGEMENT OF RISKS IN TERRITORY AND IN TECHNOLOGICAL ENTITIES DIRECTED TO HUMAN SECURITY AND DEVELOPMENT*

1. Introduction

The main goal of all human effort is ensuring the human life, i.e. all human needs, interests, and wishes. Human needs, interests and wishes are fulfilled by intangible and material goods that have a utility value. Unfortunately, in the world it is not just a human society, but also other systems, which are not subordinated to the human society. Therefore, the conflicts originate: human vs. the environment; technology vs. the environment; human vs. technology; human vs. human, human vs. PC etc. Because the human kind is based on its education, as well as in the present case, it needs to realize that, in a given situation it needs to be based on knowledge, which have been accumulated by science and historical experience of life, which shows that it is a limit for the human activities, which could not be exceeded, in order to prevent the destruction of mankind.

Christianity and Eastern philosophies perceived rightly that the human basic problem is the answer to question: „How to live?" The question connected with the existence of human in today's civilization runs: „How is human going to exist?" It is necessary to state that, for example, ***in minds of humans the relation between human and human society towards the nature still means the domination and exploiting of natural resources for the sake of satisfaction in their needs***. But from the view of knowledge and experiences it is necessary for the humans to realize that they are not the rulers of the Universe and they should, by their status, participate on securing the existential conditions for both, themselves and the future generations, which requires certain behaviour and certain responsibility for their manners and activities.

The strategy of sustainable development is comparable to other systems of values, which do not have a terminal form (e.g. the system of human laws and freedom). It is heading towards the securing the highest possible quality of life for the present generation and towards the creation of preconditions for quality life of following generations and with being conscious of fact that ideas of future generations concerning the quality of life can be different from ours.

From this reason the UN defined the strategic goal for human society *"safe human system"* in 1994 [1], consecutively the EU defined *"safe community"* in 2004 [2]. The present knowledge [3] shows that it is necessary to care on both, the public assets (human lives, health and security; property and welfare; environment; critical infrastructures and technologies) and their interfaces that are realised by natural and by human made linkages and couplings by help of various flows. Precisely, the interfaces among assets are the causes of permanent increase of vulnerability of present world, and therefore, today the management of entities in the world is based on the system concept [3-5].

**** Author:*** Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc., Czech Technical University in Prague, Praha, Czech Republic, prochazkova@fd.cvut.cz

The present world we understand as the set of open mutually interconnected systems that dynamically develop in time (the system of systems). Its foundation stones are: the environment; the human society; and the technological system [3, 4]. These principal systems and another systems and their sub-systems have own targets that they realise by help of internal processes. It is reality that all results of some of these processes are not positive for the humans, and therefore, we denoted them as disasters [3, 4].

Owing to existence of such phenomena, the humans need to try to create the favourable conditions for life. From the logical reasons, the humans need to direct their protection against phenomena that have the huge impacts on them and also on the assets that they need for the life. In this context the term "risk" is used and it is defined as the rate of probable size of disaster impacts on humans, namely directly or indirectly through the public assets on which the humans are dependent [4].

From reason of human development, it is necessary to apply the strategic management to each important entity (state, territory, object, organisation) directed to the long-term sustainability, which on our knowledge means the targeted work with risks of all kinds. Therefore, ***the risk is now the dominate concept of our society.*** It is connected with complex phenomena, conditions or factors: uncertain natural hazards, technological accidents and other disasters [3]; uncertainties that are in science and technology findings and their action on health and quality of human life human vulnerability and lack of consistent explanation of living sorrows and their sense; and also with the human play with fear, chances and opportunities [3-5].

For quality human life it is necessary both, the co-existence of mentioned essential systems and the provision of humans needs that in hierarchical Maslow pyramid [6] (needs: physiological, security; social; sociable assertiveness, self-realization).
From this reason, the humans need to consider at management: the system interconnection of living assets; mutual interconnections among many open systems; and development dynamics vs. human ways of problem solutions.

The human hierarchy of problem solution has the levels: technical; operative (functional); tactic; strategic; and politic. For general aims´ reach, the goals on all levels need to be targeted in same direction and to be co-ordinated [3-5]. With regard to different development of structural open systems in the world, there is necessary to expect the conflicts, and therefore, the human needs to monitor the changes in the world and to be prepared the originated conflicts to solve in time [3, 5].

Basic tools of human society for provision of needs there are: correct control of human society (from urgency reason, the problem solving is divided in [3] to:

- management of security and development,
- emergency management,
- crisis management),
- good asserting the knowledge and exercises at negotiation with risks directed to public interest respecting [4, 5].

In this respect, the big roles prove to managerial and engineering disciplines that have capability to ensure the human existence, human security and the potential for human development [4].

2. Summary of findings on advanced management, processes and their risks

As it was said above, the world is dynamically developed in time and space that is manifested by different processes that are inside and across of its structural systems. The

different phenomena, having the various sizes, are the products of these processes. These phenomena cause the changes that have often highly unacceptable impacts on humans, namely directly or indirectly over the public assets that humans need for quality life and development. This reality causes that the accent is put on the management type called "disaster management" in which considering all disasters is denoted as „All Hazards Approach "[7].

2.1. Disasters as processes outputs

Among the disasters, we classify the phenomena that cause damage, losses and harms to humans and other public assets on which the humans are dependent. These phenomena are the results of five different processes in the human system that represents the world [3]. The results of processes:

- running in and out of the Earth are: *natural disasters* (earthquake, floods, drought, strong wind, volcanic activity, land slide, rock slide etc.); *epiphyte; epizootic; land erosion; desertification; fundament liquefaction; sea floor spreading etc.*
- running in the human body and in human society are: *unintentional:* illnesses; epidemic; involuntary human errors etc.; and *intentional*: robbery; killing; victimization; religious and other intolerance; criminal acts; terrorist attacks; local and other armed conflicts, bullying; religious and other intolerance; criminal acts such as: vandalism and illegal business, robbery and attacking, illegal entry, unauthorized use of property or services, theft and fraud, intimidation and blackmail, sabotage and destruction, intentional disuse of technologies, such as: improper application of CBRNE substances; data mining from social networks and other cyber networks used for psychological pressure on a human individual etc.
- connected with the human activities are: *incidents; near misses; accidents; infrastructure failures; technology failures; loss of utilities; etc.*
- that are reactions of the Planet or environment to the human activities are: man-made earthquakes; disruption of ozone level / layer; greenhouse effect; fast climate variations; contaminations of air, water, soil and rock; desertification caused by human bad river regulation; drop of the diversity of flora and fauna (animal and vegetal) variety; fast human population explosion; migration of great human groups; fast drawing off the renewable sources; erosion of soil and rock; land uniformity etc.
- connected with inside dependences in the human society and its surrounding separated to: *natural*: changes in stress and movements of territorial plates; changes in water circulation in the nature (environment); changes in substance circulation in the nature (environment); changes in the human food chain; changes in the planet processes; changes in the interactions of solar and galactic processes; *and human established*: the failure of human society management (organizational accidents caused by: mutual improper behaviour of an individual or groups of individuals as illegal migration of great groups of people; incorrect governance of public affairs - as: corruption, abuse of authority, the disintegration of human society into intolerant communities; and failures in organization of education and upbringing etc.); the failure of correct flows of raw materials and products; the failure of correct flows of energies (harmful is e.g. blackout); the failure of correct flows of information; the failure of correct flows of finances etc.;*{word "correct" means the way in benefit of human interest, i.e. given by legislation}*.

The disaster list shows that disasters, according to the process, the product of which they are, have very mixed physical, chemical, economical, biological, social or cybernetic nature/basis. This mentioned fact is a clincher from the view of safety, because the preventive measures need to be targeted to the nature of disaster for the sake of being effective. Definitions, features and impacts of disasters are listed in the works [3, 8-10]. Generally, it stands that the disasters have certain characteristic features, which are the origin of impacts causing the damages, losses and harms to the important assets, links or flows and that from the human point of view, because this is de facto the only thing in which a human is interested (human aim is to make human to survive). Among the impacts it belongs e.g. vibration; directed fast air, water or soil flow; damage to a stability and cohesiveness of rocks and soil; displacements of materials; outburst of liquids; anomalies in the temperature etc.

The impacts effect directly or vicariously through links and flows of human system. Humans, thanks to their intellect, deliberately create the resilience of areas, buildings, infrastructures and technologies against disasters. They do with a help of both, the choice of elements, links and flows and their interconnection; and the specific preventive measures and activities until the specific disaster extent (which is given by human knowledge, abilities, financial and technical possibilities etc.) [3]. It makes why the impacts of interconnections in the system (interdependences) appear only with beyond design disasters, which by their extent lays above the border size of disaster against which the humans systematically provide resilience [3]. Understandably, there is a big difference - rich technically developed and quality managed countries or organizations (generally entities) have the threshold of assets resilience set higher that the counties with a lower standard.

Disasters cause or from certain extend cause damage, loss and harm on assets, i.e. they are the reasons of situations falling on a human and that is why human has to handle with them. By the reason of big variety of disasters, the arising situations classified as "the emergency situations" have either the same or highly specified impacts. The relation between a disaster and an emergency situation is the relation *"cause-consequence"* [3]. This relation is not simple because the intensity (destructiveness, severity, criticality, cruelty) of emergency situation in a given place is predetermined not only by the size of disaster but also by the local vulnerability of assets, failure of implemented protective systems (e.g. the system of warning in the area, security mechanism etc.) which were created for increasing the assets resilience, the humans' mistakes during the response etc. [3, 5, 8].

2.2. Danger, hazard and risk

In domain connected with the disaster management, there are three terms that are by given way interconnected. They are not often distinguished in spoken language, which leads to misunderstanding at critical moments, and by this to huge harms. In professional terminology they have exactly the given sense, and therefore, we here deal with them; it goes on terms: danger, hazard and risk.

Danger marks the conditions of human system at which the origin of harms on protected assets has the high probability (it is almost sure that the harm will origin) [4], i.e. the term marks the rate of conditions. It means that it goes on mark of possibility of origin of harm, loss or damage of one or more assets. The danger is predetermined by substance properties that are in facility, object or territory and by properties of processes that are

running in facility, object or territory. It is immediate, if the course uncontrollably goes to the disaster origin that causes the emergency situation; and it is creeping, if the course goes to disaster origin inconspicuously and without clear-cut precursors [4]. The danger for human means both, the big phenomena (e.g. natural disasters, industrial accidents, environmental or social disasters) and the seemingly small phenomena from the daily life (slump of snow, icicle or roofing from roof, rough pavement etc.) [4].

Hazard marks the disaster potential to cause the harms, losses and damages on protected assets in a given site that is prescriptively determined. It goes on prescriptive measure of danger that is connected with the given disaster. For the strategic planning needs, the centennial disaster is often considered, i.e. the hazard is size of disaster that occurs once in hundred years, or professionally exactly, the disaster size that has return period 100 years; at special buildings and facilities it is considered from safety reasons the hazard, which is connected with thousand years' disaster or ten thousand years' disaster [4].

Risk connected with a given disaster is the probable size of damages, harms or losses on protected assets that originate in given place at origin of disaster with size of normatively determined hazard, which is normalized to the certain territory unit or number of individuals and the time unit [4]. The difference between risk and danger is the following: the danger is specific (it denotes the topical conditions) and the risk is only expected opportunity.

The humans ensure the protection of human society and populated territory against the risks by the way that for each disaster they determine the certain size (so called design disaster). They perform the preventive measures to design disasters and by which they ensure so the possible risk size may be acceptable. The problem arises if disasters with size greater than design disaster occur, because great damages, harms and losses origin as the consequence of failure of man-made technological systems [3-5, 10].

2.3. Process management and risk management

The entity (territory, object, plant, state etc.) governance has been developed during the history [3]. At the beginning of the 20th century, the methods of scientific management were introduced. After the Second World War, the start-up of development of impoverished countries was need, which meant to ensure the fast recovery of businesses and areas. For this purpose, it was needed an initiative of wide inhabitant mass and more dynamic way of management. Therefore, the special management was introduced (this type has been still used for solving the critical situations). Its fundament is the management of processes; the process is mutual interconnection of partial sets of actions (mechanisms) by which the set of events is under way.

The mentioned management type presents the targeted management (programmes are split into projects which are further divided into processes; each process manifests itself under the project coordination – new types: project management; and process management). The characteristic feature of this management type [11] is the orientation on: the priorities and the use of planning; the methods of setting the goals; and the initiative of managers / leaders.

From the 70s of last century: it comes in useful the employee participation in the management, profit and ownership; and the demands on a qualification at all professions have been increasing. The beginning the 90s is characterised by: the wide usage of

automate and office technics; the flexible manufacturing system; telecommunication and informatics.

Reforms in the public governance, i.e., marking by the transition from the bureaucracy management to the targeted management, i.e. the project management based on process management, were the response to the big problems in the EU regional policy, and they were being started-up by the Maastricht treaty in 1989 [12].

At present, the goal of project management of entities from both, the profit and the non-profit (public) sector, is ensuring the safe entities with sufficient development potential, and therefore, it is strategic, proactive and systemic [3]. However, it is necessary to consider that it is not possible to use the same criteria for the management of public and private sectors, because e.g. the human protection, the education and research need the investment without consideration of profit. The main differences between public and private sectors are:

1. *A difference in goals*. In the public sector that is represented by municipalities and regions, the profit or another gain for any legal or physical person is not the main goal, but the main goal is the public interest and its procuration.
2. *Legislation.* The public sector has a greater connection to justice, which leads to significant constraints in domain of decision making. It is caused by the need to respect and satisfy the duties and the principles of governance, to respect the elected bodies, the adjustment and the position of state organizational units, rights and duties of their employees, requirements on financial and property management, etc.
3. *A profit absence at public sector has consequences* that some benchmarks and indicators, which are used in private sector for support of more quality management, are not possible to use.

For both mentioned sectors, however, it holds that it goes on the process management, on which all stakeholders are participated. The process management leans on the partnership, it is based on negotiation with risks and at the decision making it goes from the variant assessment on the basis of qualified criterion [12].

Currently, the three types of project management are used [3], i.e.:

1. New Public Management.
2. Total Quality Management (TQM).
3. Common Assessment Framework.

In our conditions, the Total Quality Management (TQM) is used [3, 12]. For its success the ISO standards 9000, 14000 etc. had been set up. The TQM approach consists in the requirement that all employees, from the plain employee up to the top management employee, are participated in the process of quality improvement. The process of quality improvement (i.e., in its top level it goes on de facto on integral safety increase) comes from the impulses which come from customer/citizen needs.

The TQM comes from the assumption that the stable quality of products and services cannot be ensured by commands, supervision, partial programmes, organizational or economic measures, but it can be reached by seeking, measuring and evaluating of causes, why the productivity and quality do not improve [3]. De facto it goes on certain safety culture (in the other words it is a way of application of measures and human activities). Attention is focused on processes ongoing in the entity. At the TQM implementation, they are taken into account the entity specifics, because all measures need to reflect the structure of entity from the reason of efficiency [3, 12]; it means they shall be site specific.

The modern management, which leans on the project and process management, uses the general process (Problem Solving Process) that is the part of best-practice (i.e., the

best experiences) and it is worldwide used [13]. It goes on the process that is universal and it exceeds the problems of project and the project management; it involves ten points: problem identification; problem definition; analysis of present conditions; looking for causes; definition of target; proposal of solutions; solution selection; solution validation; realization; and evaluation.

In real practice, we distinguish three common management levels, which are needed to be harmonized. The strategic level determines the basic development directions, from which it follows: which processes are necessary to modify or create; which organizational changes are necessary to perform; and where to obtain know-how, financial sources, etc. The tactical level helps to sort activities, which are necessary for realization of long-term intentions. It looks for answers on questions: how to set up the processes; in which condition to maintain processes; and how the processes need to cooperate mutually. The operational management decides about the real allocation of sources in the process (human, technological, financial) and also about the execution of appropriate activities in the range of adjusted processes (how to perform the real operation). An effort is to ensure the knowledge transfer and skill transfer among workers.

The organisation can reach a competitive merit when it harmonises all three management levels. The aim is to achieve the state when the processes are defined and managed on the basis of strategy and the operational management does not mean only response to emergency conditions or other types of faults. The processes are improved on the basis of knowledge coming from the operational management. New findings coming from the management processes are then quickly reflected into the strategy and they invoke the next important change connected with the business development or another entity development.

The process management is based on the principle of integration of activities into the integral processes. It means that the partial operations are necessary to integrate. The processes are controlled by process teams. Each process team controls the processes on its level and it distributes the tasks which lead to aim achievement to subordinate groups. At the same time all process´ teams shall be motivated to achievement of optimal outcomes, and all management levels shall follow the final goal at achieving the particular aims. Within the process management, two management systems exist, namely, the functional one and the process one, which create the more complex management.

Processes for safety support need to be followed in each entity [3, 5, and 16]. Modern management types, which are the project and process managements, are only successful, when they properly deal with risks, which are inherent to human system and also to each its sub-system. If the risks are not properly managed, so it will not be possible to reach successfully targets, and therefore, the project feasibility is assessed in advance. The importance of risk role is caused by the matter that on the risk mastering it is dependent not only the project price, but overall successfulness of total project. Thus, it is needed, so that each project may own specific structure, risk separation and way of financing that corresponds to its character. Risk management deals with the risks in process, which shall be a part of each project and that shall run from the very beginning, because only by this way it can respond to originated risks.

From the logic thinking it follows that the risks have various sources [3, 5, 8, and 16] and they depend on: disasters; local vulnerabilities; methods of management and coping with risks; and they occur on the side of all stakeholders. For achievement of understanding the stakeholders and following the risks´ reductions, it is necessary properly to work with risks, it means to choice the right concept for the risk management

(five concepts exist in the risk context [5,16]); risk identification, risk analysis and evaluation [4], to correctly decide about risks and to perform the right risk allocation including the risks´ coping and the risks´ negotiation to stakeholders; to get over the risks; and to introduce the permanent monitoring, in which if necessary to apply the in advance prepared corrective measures [5].

The correct outputs for needs of proper management according to the TQM are the following:

1. The risk assessment document – it contains information about the appropriate risks.
2. The list of top risks – it contains the list of selected risks, the solution of which demand big claims on resources and time.
3. The list of retired risks – it serves as the historic link for decision making in future.

The technique of only risk management from the reason of economic handling with forces, resources and funds formally before work with risks reviews both, the risk management and the trade-off with risks in the context of benefits and costs on the outputs.

On the basis of present knowledge, the orientation to the process management leads to:

- better understanding and greater integration of entity,
- continuous management of linkages among the individual processes,
- stress on: comprehension of requirements and their fulfilment; needs to consider the processes from the viewpoint of added value; run into increase of performance and effectivity; and permanent putting forward the processes on the basis of their efficiency.

3. Data used at determination of super processes for risk management in dynamically variable world

For determination of supper processes for risk management in dynamically variable world we use data on both, the risks´ sources and the risk management procedures directed to human safety that are used in present practice.

In the first case, we use the detailed data on disasters and the results of studies of disasters that are in special projects, e.g. Switzerland - the PLANAT project, US – FEMA projects, Canada, the Netherlands, EMA (Australia), OCHA, the Czech Republic, IAEA, OECD, UN etc. – all real references (over 1000) are given in [3-5].

In the second case for some disasters (floods, earthquakes, chemical accidents, epizootic, epidemic, electro-energy net failure, industrial accidents, traffic accidents etc.), we use practical experience with tried-and-true tools for management and getting over the risks; e.g. the plans for risk reduction for more than 5000 accidents and failure of networks [9]. These data are in further paragraphs.

Because for practical purposes, there are necessary good technical solutions based on recent findings and experiences and correctly aimed governance of public assets supported by legislative with sufficient legal force, finances, qualified human personnel and material base, these data are also followed

3.1. Knowledge on risk, risk management and risk engineering

The fundamental facts on nature, principles, methods and tools of risk management and trade-off with risks, i.e. recent knowledge from management domain, entity structure

(role of interfaces among the human system assets and human system sub-systems), errors at decision-making and management are given in works [3-5, 8, 9, 10, 14, and 15]. Their summary is:

1. The principles for work with risks are: to be proactive; to think through possible consequences; correctly to determine the priorities of public interest; to think on overcome of problems; to consider the synergies; and to be alert.
2. The principles of work with risks come out from the stipulated demands that the risk management task is the safety increase, i.e. to find the optimum way how the evaluated significant risks may be reduced on demanded socially acceptable level, or to preserve the determined safety level. From this reason, the following facts need to be respected:
   - reduction of risk is practically always connected with increasing the costs,
   - risk management needs to be led by effort to find the boundary to which it is endurable to reduce the risk, so the spent costs might be socially acceptable,
   - on the basis of just given facts, it is necessary in each real case to establish the requirements that output from trade-off with risks needs to be fulfilled,
   - at real trade-off with risks, the stipulated requirements need to be kept and in case their non-observing, the reasons need to be given.

   Because the territory and each technological objects or facility are the complex systems of systems (set of open and mutually interconnected systems of various nature [3, 5]), it is necessary to consider the safety of whole complex, called the integral safety. For this purpose, it needs to work with an integral risk. The integral risk is influenced by reality that each followed entity has a range of protected assets of different nature that are interfaced by internal links and couplings created by flows. Because the goals of assets are not always the same, it is necessary to expect the conflicts. At several conditions (caused by occurrence of special disaster with size greater than design one, which creates the boundary value that assets withstand such disaster without greater losses and damages), low assets´ resilience and interfaces among the assets are the causes of another conflicts. Therefore, the entity integral risk also depends on the hazards from disasters of all kinds (natural, technological, social, financial, economical, legal etc.) that can threaten the entity; the disasters affected not only the individual assets but also their links and couplings, which lead to the cascade failures.

   For correct assessment of entity risk, it is important to consider all disasters that can damage the entity, and properly to determine the sizes of hazards connected with individual disasters. The risk connected with each disaster is probable size of losses, damages and harms on the entity for hazard connected with the design disaster divided to area unit and one year. The crucial is the correct determination of hazard connected with the design disaster. ***Both, the performed entity safety reports audits and the inspections after the entity accidents or failures, revealed that in evaluated cases:*** some possible disasters with potential to disrupt the entity were not considered at risk determination directed to the entity safety; and several faults in determination of correct value of hazard connected with design disaster were found (e.g. data from too short time interval on disaster, too limited knowledge).

   From the practical reasons it is necessary to consider that the entity risk connected with the given disaster does not represent only the direct losses on assets but also the indirect ones; the indirect losses are caused by: delays or errors in response, cascades

of failures caused by synergic and cumulative effects, which are caused by linkages and couplings among the assets; and by domino effects.
Due to the entity structure their risk is the integral risk that is expressed by following formula

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

where: $\boldsymbol{H}$ is the hazard connected with the considered disaster; $\boldsymbol{A_i}$ are the values of assets, $\boldsymbol{i = 1,2, ..., n}$ that are considered in connection with complex technological facility safety, where $\boldsymbol{n}$ is the number of monitored assets; $\boldsymbol{Z_i}$ are the vulnerabilities of assets taken under account, $\boldsymbol{i = 1,2, ..., n}$; $\boldsymbol{F}$ is the loss function; $\boldsymbol{P_i}$ is the occurrence probability of i-th asset damage – conditional probability; $\boldsymbol{O}$ is the vulnerability of safeguard measures; $\boldsymbol{S}$ is the size of followed territory / facility; $\boldsymbol{t}$ is the time that is measured from the origin of harmful phenomenon in facility; $\boldsymbol{T}$ is the time for which losses arise; and $\boldsymbol{\tau}$ is the return period for the given disaster.
Because the loss function $\boldsymbol{F}$ form is not known, we use for determination of total risk (i.e. the integral risk) the scheme given in Figure 1.

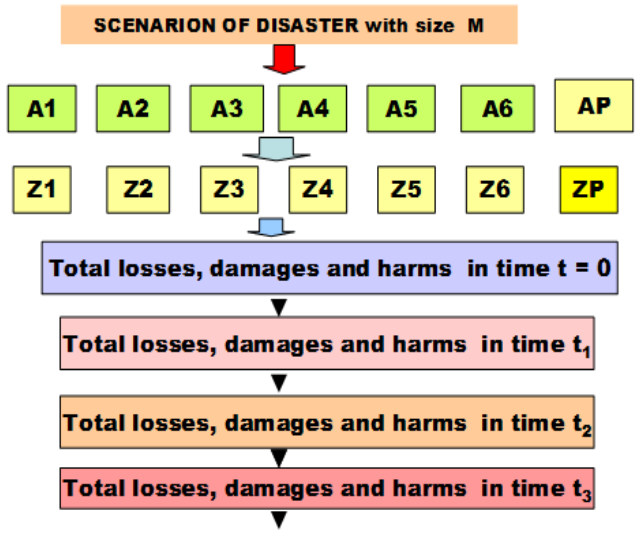


Fig. 1. Flowchart for determining the risks for the strategic management of safety; A – assets and Z losses, damages and harms to the assets; Description: 1-the human lives and health, 2- human security, 3 - property, 4 - the public welfare, 5 - the environment, 6 - infrastructures and technologies, P – private.

Onward, the problem is complicated by reality that the world is in dynamic development, i.e. both, the entity conditions and the risk sources are changing in time. Moreover, there is necessary to respect that the risk and safety are not complementary quantities – it holds that the risk reduction leads to safety increase but at the same risk value the safety can increase if humans perform special measures or at their behaviour use special manners following from correct safety culture.

Owing to differences in individual disasters nature, the countermeasures for assets´ protection being effective to one disaster, are not effective to another and even can increase vulnerability some of them; i.e. the countermeasures effectiveness depends on real entity and its disaster - see the rules given in Figure 8 in chapter 1.
Therefore, at solution of practical tasks connected with both, the entity safety and the entity risk, ***it is necessary to consider that risks are normal and for the entity safety it is necessary to apply*** not only the risk prevention measures and activities determined on the basis of correct intent and correct data and methods, but also: the safety culture by which the human behaviour in the entity and its vicinity is targeted to safety; and the tools that reduced losses and damages if some important disasters occur. Therefore, it is necessary to prepare the qualified response for important risks realizations, such as: the risk management plans for both, the entity and the entity vicinity for all relevant risks; the continuity plans for survive of important complex technological objects and facilities; and the operational crisis plans for both, the complex technological objects and facilities and their vicinities.

3. Process model for work with risks is shown in Figure 5 in chapter 1.
4. The risk management is the complex process that needs knowledge, experiences and skill from many fields. In detail, it is described in Figures 6 and 7 that are given in chapter 1. It is necessary to perceive the fundamental separation of tasks among the professionals (Risk determination), the decisive sphere (Decision Making) and the executive sector, i.e. engineers, technical workers and first responders (Risk Control and Mitigation) and also role of public. If decisive sphere does not respect the public interest correctly or if it has not enough knowledge or sources, the organizational accidents occur earlier or later.
5. The risk management is targeted to building the safe world. For this we perform the measures and activities during the prevention, preparedness, response and renovation, Figure 2.

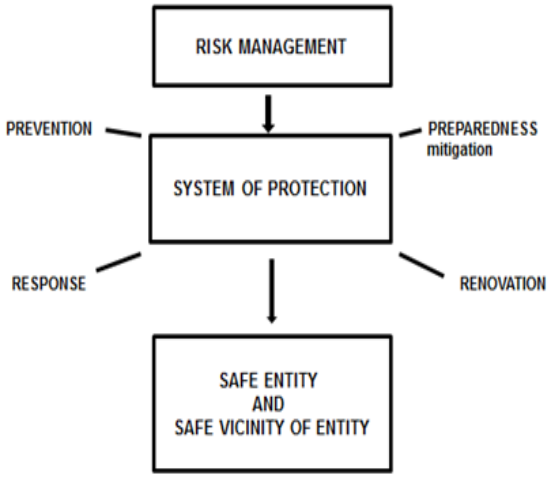


Fig. 2. Time sequence of phases in which the measures and activities for defending the risks are performed.

6. From the viewpoint of ensuring the human needs, namely including the human survival at critical situations, the four phases of each entity investigation are important:
   - in-depth knowledge of entity (protected assets, possible disasters, vulnerabilities),

- determination of risks, determination of concept of optimising the measures and activities in entity for getting over the expected risks,
- determination of weaknesses in management and trade-off with risks and in determination of measures of response and responsibilities for case of occurrence of great damages, losses and harms on protected assets, e.g. caused by lack of finances, knowledge, technology etc.; at least it is necessary to process the risk management plans for important risks,
- constitution of capability and preparedness to ensure the survival of humans and critical technologies at critical situations (crisis plans, continuity plans).

7. Present knowledge shows that it is not enough to manage the risks of individual disasters but it is necessary to understand and to manage the processes that product the disasters. Due to dynamic world development, the processes originating the disasters also change, and therefore, the attention to them is logical. Safety management concept formed at certain time on the basis of integral risk is not sufficient and it is necessary continually to adapt it to changes that are caused by internal and external processes by help of proactive targeted integral risk management.
8. The aim of all processes for risk management is the safe world. This management type is called the safety management. Its process model is in Figure 3. The safety is a set of anthropogenic measures and activities, which lead to ensure the followed entity security and development. Since the world is dynamically changing, so the management of safety of critical installations is focused on priorities. In the first place, it means the application of All Hazard Approach [7], determining the hazards posed by individual disasters, and according to the assessment of size of threat from real disasters and vulnerabilities of a site and of critical installations against real disaster the separation of disasters into the following groups: the disasters, which cannot have impacts on critical facility; disasters that have only an acceptable impacts on critical facility, for which we use the designation “relevant disaster”; disasters that have on a critical facility only impacts that are manageable at origin by prepared prevention and mitigation measures, for which we use the designation “specific disaster”; and disasters that have an unacceptable impacts on the critical facility and, therefore, it is necessary to carry out essential preventive measures in the field of technical, organizational, legal and educational and it is necessary to have the possibility to activate all of the resources and the means to cope with their impact and jump-start further development, for which we use the designation “critical disaster”. The last mentioned disasters have the potential to cause extreme emergency situations and for their defeat it is necessary to use the tools for crisis management. ***To achieve the desired level of safety it is necessary well to manage and properly to decide.*** Good management and good decision making is possible only when we have relevant data and when we use relevant tools. The term “*relevant data*” means: to be correct (it is known their size and accuracy); to have explanatory power for the problem (i.e. to be validated). The data files need to be representative (i.e.: complete; contain the correct particulars; have a sufficient number of particulars; the particulars need to be spread homogeneously throughout the reference period and need to be validated. In the application of models, random and epistemic uncertainties in the data need to be properly considered.

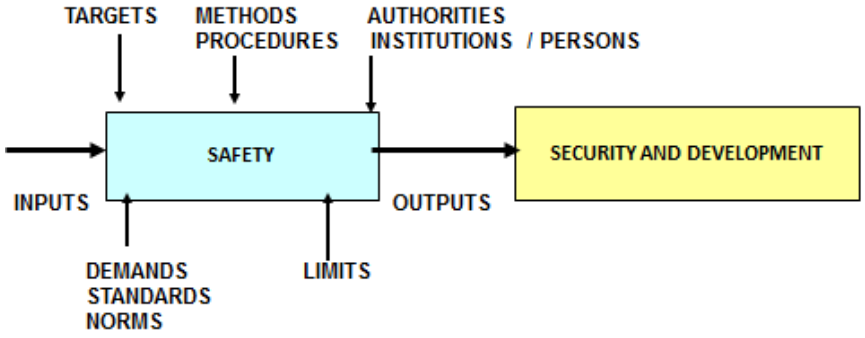


Fig. 3. Process model for ensuring the security and development.

9. Present advanced management of socio-technological entities is based on the processes management; details are in Annex. Model for entity safety management in time [5] is shown in Figure 4. It is necessary to coordinate six processes: 1 - concepts and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. The main processes are further divided into sub processes:
   i. The first process consists of sub processes for: the overall concept; achieving the intermediate objectives of safety; leadership / management of safety; the safety management system; personnel staff including the sections for: human resources management, training and education, internal communication / awareness and working environment; review and evaluation of the implementation of fulfilment of objectives in the safety.
   ii. The second process consists of sub processes for: identify of hazards from potential disasters and risk assessment; documentation of procedures (including work permits); management of change; safety in conjunction with contractors; and supervision of product safety.
   iii. The third process includes the sub processes for: research and development; design and mountings; inherently safer processes; technical standards; storage of hazardous substances; and maintenance of integrity and maintenance of equipment and buildings.
   iv. The fourth process includes the sub processes for: cooperation with the administrative authorities; cooperation with the public and other stakeholders (including the academic institutions); and cooperation with other facilities.
   v. The fifth process includes the sub processes for: planning of internal (on-site) preparedness; facilitate the planning of external (off-site) preparedness (for which it corresponds the public administration); and the coordination of the activities of the departmental (resort) facilities at ensuring the departmental emergency preparedness and at response.
   vi. The sixth process has sub processes for: processing of reports on disasters, accidents, near misses and other learned experience; investigation of damages, losses and harms and their causes; and the response and follow-up activities after disasters (including lessons learned and information sharing).

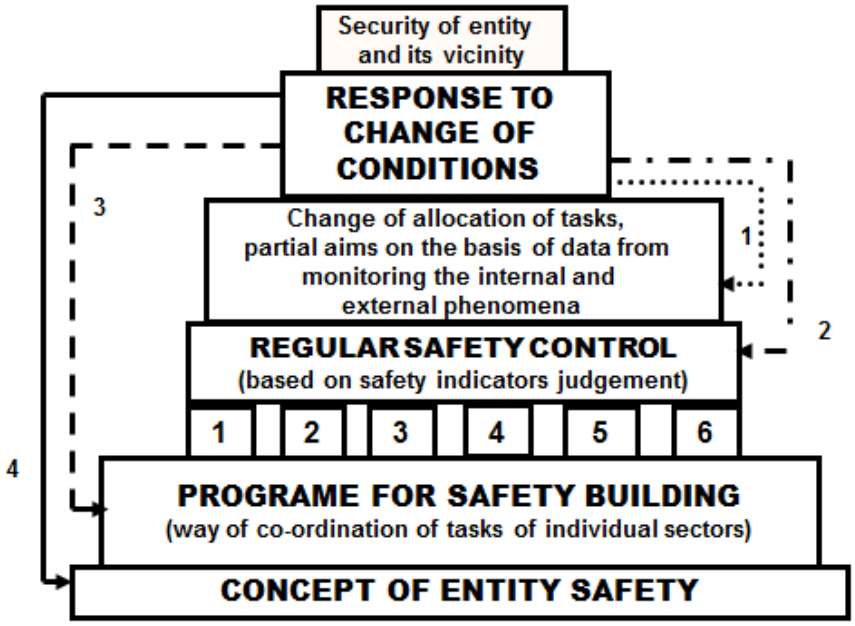


Fig. 4. Model of management of critical complex facility safety; black block – concept for specification of important processes of critical complex facility; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4

Coordination of processes is targeted at ensuring the safe complex facilities under the conditions of normal, abnormal and critical (Figure 5).

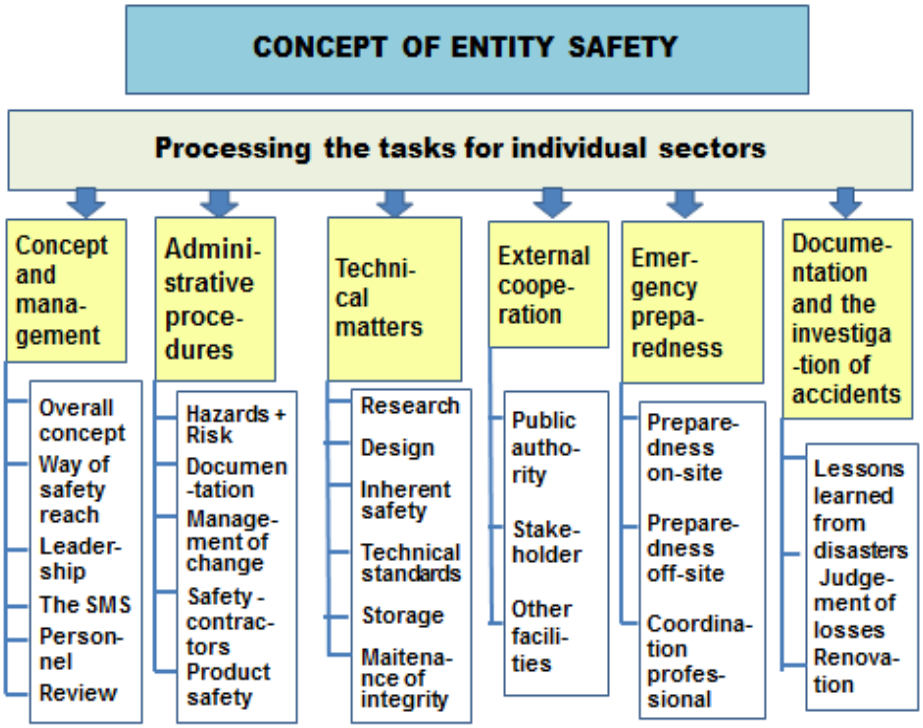


Fig. 5. Concept of entity safety and its main parts.

10. Only at known and frequent disasters the risk level perceived by humans is near to real risk level. At infrequent and low known disasters the humans perceive the risk level as shadowy and remote. Perception of risk is also influenced by further factors – e.g. at activities that we perform voluntarily (mountaineering, ski jumping etc.) we consider the insignificant level of risk. The risk acceptability is the result of comparison of several types of acceptability – technical acceptability (reliability and complexness of technologies, machines and devices), economic acceptability (costs) and socio-political acceptability (general risk perception).

    Generally, it is possible to say that acceptable risk is determined on social and knowledge base, and that the social, economic and political factors are considered during the risk level determination. It also means that level of acceptable risk is not same for all countries.

    Because the required level of safety is possible also to reach by special education, installation of warning systems, it holds that acceptable risk level is not safe risk level at which the probable losses and damages are negligible.
11. According to the theorization of present philosophers the risks have in society the objective and subjective features, and moreover there are not out of culture and value connections (in this direction they are not pure scientific problem and they need to be considered also from viewpoint of civic involvement). Even, if the modern society enforces the indolent strategy of insurance and reimbursement, it is not possible to rely on it fully because some risks can affect the core of social system, which it is truth for some security risks.

    Against scientism of security politics nothing can be say to the extent that we prove to be reflexive, which means to reveal consequences of individual activities and we do not yield to illusion on opportunity of perfect solution. Reliance on experts (and institutions) can induce the reduction of capability to participate actively on solution and to finish the separation of private and public (which manifests as inherent risk on which the expert opinion fails). According to professional concept all participants (i.e. all interest groups) have duties and responsibilities at trade-off with risks.

    From this reason the humans need to have possibility to participate in decision-making, to manifest their needs and opinions, namely without fear from punishment. It is necessary to involve many humans (in spite of great costs in the process beginning) and to try accomplishment of consensus.

    Problem comes in professional matters in which the ground documents are based on evaluations that are complicated and for current humans non-understandable. The decision-making in these cases is often influenced by the lobbies of various groups that strive on commission.

    From this reason it is necessary so that: all evaluation procedures need to be lean on legislative; the selection criteria need to be directed to publicly aims and need to be transparent at decision with regard to dispositional sources, forces and means of public administration. In practice we use risks of several types: partial if we consider one asset; integrated if we consider several assets and the total risk is the aggregation of individual assets risks; and integral (systemic) if we consider more assets and total risk includes also indirect impacts on assets that are caused by linkages and couplings in system.
12. The assignation of real work with risks in good governance is given to person or organisational part that is well prepared for such work. This approach is possible only in organization with qualified process management in which activities and measures

are applied on knowledge base, namely matter-of-fact and from management domain (i.e. the activities are mutually interconnected, no errors in communication, each participant knows what to do and how to do).

Because, it does not exist the general consensus on formulation of problems of sustainability of welfare of human society in context with system utilities, each problem solution is provisional, because it continually balances among the rival interests and society goals (if they are stipulated). It is difficult to give explicit decision on problem owing to the alternating decision process character [3]. During the decision, the following dilemmas are solved: relation between risks and profits (often greater benefit for human means greater risk for ecosystem); time conflict between needs of present and future generations; and social conflict (relation of needs of individuals and the society). It is difficult to solve inverse problems owing to the systems´ complexness. If some symptoms connected with risks are stipulated and sorted out, the new symptoms will emerge. From this it follows that the real approach to sustainability management by help of risk management needs to be iterative, interactive and adaptive [3, 4].

The aim of complex management is to ensure at each situation the protection of human lives and security, property, environment, infrastructures and technologies that are necessary for human survival. It means always to ensure:

- the mobilisation and co-ordination of all national sources (energy, labour force, production capacity, food and agriculture, resources, telecommunications etc.),
- the co-ordination of such activities as notification system, warning system, rescue system and first responders´ system, which reduce the disasters' impacts and supporting the state administration activities and adherence of legal rules.

The planning types that form fundamental methodical tools of individual mutually interconnected management types need to create the base in which all given aims are embedded [4, 5].

For reaching the human society aims, i.e. security and sustainable development, the mutual combination of measures and activities is necessary at vulnerabilities´ reduction, resiliencies upgrade and adaptation capability; all public assets in detail and in complex need to be respected. The present tool based on knowledge and experiences means to apply on all management levels to implement the proactive safety management system based on work with risk respecting above mentioned knowledge; especially: All-Hazard-Approach, Defence-In-Depth strategy, interdependences, time and space variability [3-5].

3.2. Categories of causes of risk management failures

From the critical analysis of emergency up to critical situations in human system, in detail described in [10], it follows that:

- the cause of critical situations are the organisational accidents that are connected with a human factor; especially with the phenomena as corruption; abuse of power; suppress of the public interest; low respect to knowledge and engineering experiences; and low professional level of management,
- the organisational accident consequences are: government default; technologies failures; infrastructure failures; research failure; social system failure; decay of human society into intolerant groups; increasing number of impoverished people – seniors, dossiers, jobless – problem young people who are out of work and without education; disturbances of daily civil protection human needs; disturbance of daily civil

protection, human security and public welfare; disuse of technology, space militarization.

From this reason we pay the attention to these phenomena that cause the disturbance of social relations, public welfare and human security [10] – Table 1.

Table 1. Phenomena that cause the disturbance of social relations, public welfare and human security.

Domain	**Defects leading to critical situations**
Top governance	The domain management: is predetermined to political and military aspects; is short of human dimension and gives low support to the EU inhabitants; does not governed on the basis of qualified data processed by qualified methods; is often determined by fixed ideas without real assessment of their realisation; is based on image that all is stationary and it does not respect dynamic development of world that means to prepare possible extreme scenarios and measures for human's survival; and is not realised on the principle "Safety management system for system of systems".
Technical domain	In domain: no standards and norms for underground and high-rise buildings with regard to human security and public welfare; missing essential services provided to the citizens; scenarios for decision-making are prepared only by simulation without verification with use of real data – sometimes scenarios used were derived for different conditions, i.e. conditions of technology transfer were not fulfilled; no norms and standards for interoperability; no standards and norms for co-operation of diverse systems; no co-ordinated emergency plans on all levels (EU-wide to regional) – all must be on professional level respecting knowledge and experiences, continuity and contingency plans.
Organisational domain	In domain: missing the effort directed to reduction of weakness (low number of resources, contamination of environment, work price, unemployment) and to use of strength (qualified technician population); no effective tool against to corruption, power disuse, lobbying etc.; missing the support of co-operation on mutual partner principle; missing base for mutual understanding and mutual co-existence; no effective international teams of first responders; no base for close co-operation of first responders; no norms and standards for interoperability.
Knowledge domain	In knowledge base used for decision-making: missing systematic respect to present world nature – dynamic open system of systems; low effort directed to collection of qualified data on disasters and on lesson learned from responses to extreme disasters; underestimation of disasters at disasters´ management; neglecting the creeping disasters as ground water stores, contamination of human food chain etc.; no qualified disasters´ scenarios for decision making.

4. Methods used for determination of super processes for risk management in dynamically variable world

The outputs of our task are created by application of methods as: the critical analysis and critical evaluation of knowledge that is gathered in professional publications and summarized in foregoing section; consideration of experiences from everyday life; logical interconnection of knowledge; classification of obtained facts; synthesis of obtained facts; application of methods of creative thinking and expert judgement (panel discussion, brainstorming, Delphi method, criticality assessment etc.) on data as:

- risk nature and features,
- risk scenarios change in time and space,
- risk management change in time and space; special attention is paid to management failures,
- trade-off with risks change in time and space; special attention is paid to failures caused by incorrect or insufficient measures.

At individual investigations the analytical and heuristic methods [15, 16] are used.

The results from own direct research are based on: systematic investigation and evaluation of disasters and accidents in technological objects and facilities; judgement of impacts of real accidents on technological objects and facilities; simulations performed by the risk engineering methods (What, If and Fishbone [16]); and performed professional inspections in real technological objects and facilities.

The aim of inspections was the determination of main deficiencies in complex technological facilities. For this aim it was used the special checklist, which was compiled according to the technique described in [5]. Its form for i-th disaster is shown in Table 2. All mentioned data were critically considered and synthetized according to the principles of strategic process models [3-5, 14], i.e. by help of procedure that is in agreement with procedure described in famous works as [17-22].

Table 2. Identification of deficiencies for i-th specific disaster, i.e. disaster that can have important impacts on entity and its vicinity, i = 1, 2, ..., n, i.e. assessment of criticality rate of viewpoint of application of All-Hazard-Approach and Defence-In-Depth. Safety rate = 1 – criticality rate [5]. For assessment of criticality it was used the value scale 0-5 [5] was used (0-negligible, 1-low, 2-middle,3-high,4-very high,5-extremely high) and the median of values determined by inspection members (usually 5-7).

	Question	**Assessment of criticality**	**Reasons of criticality**
i	1. Has the technological object or facility to incorporate the principles of inherent safety, i.e. safe design?		
	2. Has the control system of a technological facility (SMS) set the basic control functions, alarms and the response of the operator set up so that the technological facility in normal (steady) state?		

	3. Has management system (SMS) instrumentation (built-in safety instructions) and relevant physical barriers, which at derogate from the normal state to keep technological system in a good condition, i.e. they prevent the occurrence of unwanted phenomenon? The operation is successful, when, after the occurrence of the abnormal state the technological facility will return to normal as a result of resilience or after the application of corrective measures (clean-up, repair, replacement of parts).		
	4. Has management system (SMS) for the case of loss of control, i.e. critical conditions measures for emergency response that mitigate impacts on technological facility system and ensure the capability to return to a normal state? Operation of a technological object is successful, if it is a good continuity plan ensuring that the technological facility shall ensure all the necessary tasks.		
	5. Does management system (SMS) for the case of loss of control, i.e. supercritical (beyond design, extreme) conditions the measures for: - maintaining the operability of the technological system following its repair and maintenance, - and measures to ensure the protection of public assets (people, the environment and other assets) in the surroundings of technological facility?		

5. Advanced principles of risk management and risk engineering

With regard to knowledge [3, 4, and 23] the present possibilities of human society for dealing with risk are:

- part of risk is reduced, i.e. by preventive measures the risk realisation is averted in advance,
- part of risk is mitigated, i.e. by purpose-built measures, activities and by preparedness (warning systems and another measures of emergency and crisis management - response personnel, response systems, material, technical and finance reserves) at response to risk realization reduce the impacts or avert the unacceptable impacts,
- part of risk is re-insured, i.e. the insurance ensures the cover of possible loses and damages,
- part of risk for which there are prepared procedures and resources for response and renovation; i.e. the reactive measures and activities ensure the human survival, the territory protection, the situation stabilization and the renovation,
- part of risk for which there is prepared contingency plan; i.e. the reactive measures for suppress of critical unforeseeable situation (contingency plan) for case if non-controllable or too costly or low frequent risks occur.

To this it is joined the distribution of risk defeating among all stakeholders [3]. The distribution in good governance is performed according to rule that all stakeholders have responsibility for the risk defeat and that the defeat of a real risk is assigned to a subject the preparedness of whom is the best.

The key concepts of present engineering directed to human safety derived in [16] are the following:

1. The approaches are based on risk – the work intensity and documentation is adequate to risk level.
2. The professional approach is based on reality that only the critical attributes of quality and the critical parameters of process are considered.
3. The problem solution is oriented to critical items – the critical aspects of technical systems ensuring the consistence of system operations are followed and managed.
4. Verified quality parameters are included in the project proposal.
5. The accent on quality engineering procedures – it needs to be proved the accuracy of selected procedures under given conditions.
6. The aim of a safety upgrade – permanent improving the processes with a use of analysis of the root causes of malfunctions and failures.

For respecting these items there should be used relevant data sets and only verified methods that provide outputs with a designated testified competence. Because in the group of cases there is not well coped with vagueness in data, in practice there are used the procedures designated as good practice procedures / good engineering practice procedures. Modus operandi procedures in individual domains go on that on the basis of experience lead to a good result. The given procedure is used in cases in which there was not approved any unified procedure. It is often used at measurements in laboratories, negotiation with humans etc.

Owing to a lot of factors, including the human factor, influencing the problem solving at real conditions exist; and these factors are not only random but also epistemic, the measures, activities and procedures denoted as good engineering practice are typical for engineering disciplines.

Good engineering practice (good engineering procedure) is then defined as a set of engineering methods and standards that are used during the life cycle of technical system with the aim of reaching the appropriate and cost- efficient solution. It is supported by fit documentation (conceptual documentation, diagrams, charts, manuals, testing reports etc.).

In a given context the engineering expertise is the expression of the capability to:

- apply the knowledge of mathematics, science and engineering,
- propose and realize experiments,
- analyse and interpret data,
- propose components or the whole system according to requirements and under the frame of realistic limitations identify, formulate and solve engineering problems,
- ensure the effective communication,
- comprehend the impacts of engineering solutions in a broader context,
- use the advanced tools and methods in engineering practice,
- adhere professional and operational responsibilities and ethics,
- lead the interdisciplinary team.

Most of the demands give above is directed to correct the human factor negative manifestation.

From given facts it follows that all considered engineering types are multidisciplinary and interdisciplinary disciplines, and therefore, they use very various methods, tools and techniques because the safety management targets cannot be reached only technically and or by mastery, but the methods, tools and techniques respecting the data logic, technological, financial, managerial and decision-making needs to be used, because their integral part is the decision-making over technical problems, human factor, costs and time planning.

The special attention of advanced risk management and risk engineering targeted to the human safety is targeted to the technological objects and networks that are in principle the socio-technological systems. According to knowledge concentrated in [5] it is necessary to use the following principles:

- the risk is followed and considered during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition,
- the risk determination is directed to user's demands and to the level of provided services,
- the risk is determined according to the criticality of impacts on facility processes, provided services and on assets that are determined by public interest,
- the unacceptable risks are mitigated by tools according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up.

The advanced risk engineering directed to human system safety respects the co-existence of systems with different nature (SoS), and so fulfils present demands of humans [3]. To prepare groundwork it is necessary to combine analytical methods with expert judgement by which we remove vagueness in data. The problems that we need to solve in this consequence consist in acquisition of knowledge and in assignment "who is expert"; the last mentioned problem was broadly discussed in world conference ESREL2011 [23]. For the first problem solution we need systematically to monitor human system and obtained data process by qualified methods [14].

6. Super processes for management of risks in dynamically variable world

It needs to be noted that in the real world we work at ensuring the safety of critical facilities with the non-trivial problems, i.e.: several protected assets, the objectives of which are sometimes conflicting. The assets vary in time and space; and the human system, in which the assets are, is in dynamic development.

6.1. Design of super processes

As above said, for ensuring the entity safety, the priority risks need to be considered. The negotiation with risks comes out from the present possibilities of human society and it consists is separation of trade-off with risks into several parts containing the measures and activities for given risk part control. The measures and activities of individual parts differ in time application. Their goals are mentioned in section 5.

As it was said above, the present knowledge shows that due to dynamic world development it is not sufficed to control the risks connected with individual disasters, but it is necessary to manage the processes that produce the disasters (the scientists have been trying to do tis since 50s of last century – e.g. technical polygons round the faults with

which great earthquakes are connected - Kamchatka, Central Asia, California etc.). It means that the complex view is necessary.

Taking into account the nature of world, i.e. many open mutually interconnected systems having the proper goals that end up in conflicts from time to time, it is logic that human reaction needs to be also the process that is controlled in space and time. On the basis of logical interface of knowledge and experiences from practice by help of strategic planning principles there are proposed two super processes for management of risks in time and space. The first one is for ensuring the safe territory and the other one for ensuring the safe technological objects or facility. These super processes ensure the continual control of risks.

For ensuring the safe territory and safe public assets it is necessary to apply the super process that consists from five processes (Figure 6):

1. The process for obtaining the sufficient knowledge on territory includes: determination of assets in territory; determination of territory parameters and assets characteristics in the extent of land-use planning documentation; and determination of list of disasters that affected the territory (the input list of disasters being under the term All-Hazard-Approach is in [10]).
2. The process of risks assessments and risk controls includes: the determination of hazards for all disasters that can have impacts on the given territory and their return periods; determination of vulnerable sites in territory and vulnerability of public assets with regard to determined sizes of hazards (ways of hazard determination are e.g. in [4, 5]); determination of design disasters (normative determined disaster size); determination of impacts of disasters on territory and assets (it is suitable to determine the normative impact scenarios for design disasters); determination of integral risks for all important disasters (i.e. to consider the both, the direct disaster impact on assets and the indirect disaster impacts on assets through the linkages and couplings among the assets); put the work with risks.
3. Process of evaluation of quality of risk management and trade-off with risks includes: judgement of levels of effectiveness of prevention, preparedness, response and renovation with regard to integral risks connected with important disasters; determination of critical points in risk management and in trade-off with risks and determination of these points criticalities with regard to integrity and effectiveness of applied measures and activities and their control (i.e. it goes on the reveal of sources of possible organizational accidents); proposal of corrections for high critical points.
4. Process of determination of safety management includes: determination of measures and activities for points with high criticalities and their implementation in the frame of short-term, middle-term and long-term realization plans, namely including the responsibilities for realization and sources for realizations; introduction of safety culture on the level of assets, assets´ management and on the territory safety management (from top management to individual citizens) [3, 5,14]; and determination of response procedures to emergency situations with demand that at each response to critical up to extreme situation there are solved the human survival and the continuity of critical objects, facilities and infrastructures.
5. Process of preservation and upgrade the safety includes: systematic formation of capability to perform early and effective response to critical situation, to ensure the renovation and continuity of services in territory; determination and implementation of strategic programme for safety increase in time including the monitoring the

effectiveness of processes for risk management and trade-off with risks; regular detail assessment of territory safety every 10 years; and immediate territory safety judgement after critical situation occurrence.

Fig. 6. Structure of super process for risk management and trade-off with risk for profit of safe territory and safe public assets. The numbers denote the feedbacks that need to be realised if problems occur. From the economy reasons the firstly the feedback 1 is applied, and only if it fails the feedback 2 etc.

Because the dynamic development of world it is necessary to monitor the territory and to have prepared the procedures for correction of unfavourable situations. From economy reasons it is necessary firstly to use the cheapest procedure that feedback 1 in Figure 6 shows; in case of its failure the feedback 2 etc.; at huge harms immediately it is used the feedback 4, which means the change of territory safety concept. In each case denoted by feedback some of adjusted processes change:

- in case denoted by feedback 1, it is pursued the change of process of territory safety management (e.g. they are change the rules for territory safety management, the allocation of roles of participated persons, management priorities etc.),
- in case denoted by feedback 2, it is pursued the change of process of evaluation of quality of risk management and trade-off with risks (e.g. they are changed the ways of risk control in territory, separation of tasks of trade-off with risks among the participated persons, priorities for risk management and trade-off with risks, allocation of means for measures leading to risk reduction – it does not only rely on response but more on prevention etc.),
- in case denoted by feedback 3, it is pursued the change of process of evaluation of risk assessment (e.g. they are introduced the further criteria for risk assessment, the value scale is transformed, they are considered the contributions to integral risks from further linkages and couplings among the assets that were revealed as originators of huge damages, losses and harms on public assets etc.),
- in case denoted by feedback 4, it is pursued the change of process of knowledge on territory (they are added and introduced into practice new findings, e.g. into the set of risk sources are added the further harmful phenomena that were revealed as the

sources of huge damages, losses and harms on public assets, the size of disasters criticalities changes, the size of assets´ vulnerabilities changes etc.).

For ensuring the safe technological objects or facilities (or more precisely socio-technological entity because each such entity was invented and set up by humans) that are located in real territory it is necessary to apply the super process that consists from four processes (Figure 7):

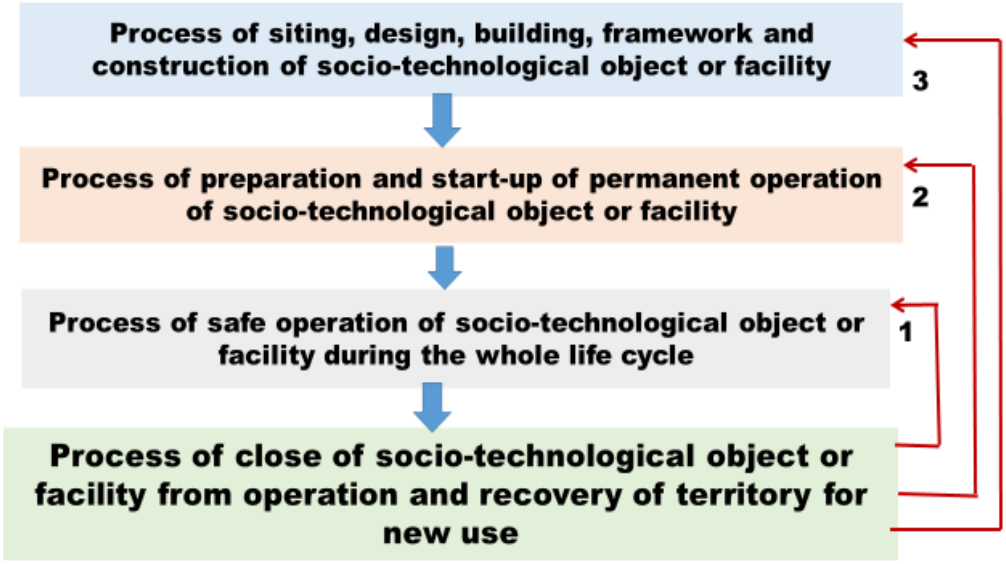


Fig. 7. The structure of super process for risk management and trade-off with risks for profit of safe technological entity during its life cycle and its safe vicinity. The numbers denote the feedbacks that need to be realised if problems occur. From the economy reasons the firstly the feedback 1 is applied, and only if it fails the feedback 2 etc.

1. Process of siting, designing, building and construction of technological entity (building, facility, network) includes: assemble of data on territory and its assets in which technological entity might be located in the extent of land-use planning documentation; assemble of data on disasters affecting the territory, their hazard sizes and their impacts character (the input list of disasters being under the term All-Hazard-Approach is in [10]); determination and judgement of integral risk, and determination of vulnerability of the technological entity against to disasters affecting the territory and the estimation of integral risk increase after technological entity realization; entity siting, designing, building and constructions with regard to site risks, technology risks and human factor risks with the respecting the Defence-In-Depth principle (in detail described in [5]) and the trade-off with risks connected with linkages and couplings between entity and its vicinity; and determination of way of technological entity safety management in time during the technological entity life cycle (documentation: preliminary safety report [5]).
2. Process of preparation and start-up of permanent operation of technological entity (building, facility, network) includes: tests of functional capability of individual buildings, facilities and devices and elimination of revealed sources of technical and organizational risks; semi operation during which the risks connected with linkages

and couplings (realised by different flows realizing at operation) inside and outside the entity are traded-off; trial operation during which the risks connected with linkages and couplings (realised by different flows realizing at operation) inside and outside the entity are traded-off; realization of proposal of safety management of technological entity (processing the preoperational safety report and proposal of operational safety report [5]); and start-up of permanent operation.

3. Process of safe operation of technological entity (building, facility, network) during the life cycle includes: installation of operating procedures for normal, abnormal and critical conditions, safety culture, risk monitoring process; programme for upgrade of safety in time and procedures for continuity plan realization at critical conditions (operational safety report [5]); adjustment of optimal maintenance of buildings, facilities and devices; establishment of regular inspections of buildings, facilities and devices and rules for implementation of early repair of detected defects on buildings, facilities and devices, especially those important from safety reasons; modernization of buildings, facilities and devices; regular audits of safety of technological entity and its impacts on vicinity, which including the judgement of safety culture level, and realization of measures for getting over the detected important risks and for removing the sources of organizational accidents; and early response to critical situations and ensuring the continuity of technological entity operation after repair [5].
4. Process of close of technological entity (building, facility, network) from operation and recovery of territory for new use includes: determination of sources and responsibilities for measures and activities that are necessary for remove the entity (building, facility, and network) and decontamination works; remove of buildings, facilities and networks from the territory; performance of decontamination of territory. It goes on the process on which it is often forgotten in practice as the brownfields show, and therefore, it needs to be followed during the whole technological entity life cycle.

Because the dynamic development of world it is necessary to monitor the technological entity and to have prepared the procedures for correction of unfavourable situations. It is also necessary to consider that each technological entity has limited life cycle, and therefore, for preservation of conditions for human security and development it is necessary to forestall to depreciation of territory. From this reasons there need to be prepared procedures and corrections in each technological entity for averting the unfavourable situation. From economy reasons it is necessary firstly to use the cheapest procedure that feedback 1 in Figure 7 shows; in case of its failure the feedback 2 etc.; at huge harms immediately it is used the feedback 3 that means the change of safety concept. In each case denoted by feedback some of adjusted processes change:

- in case denoted by feedback 1, it is pursued the change of technological entity safety management process (e.g. they change demands of public administration on operation of technological entity, rules for technological entity safety management, priorities in technological entity safety management – Figure 8 shows that often it is necessary to solve conflicts between security of public assets and the number of products, etc.),
- in case denoted by feedback 2, it is pursued the change of process of preparation and start-up of permanent operation of technological entity (e.g. they change ways of revealed risk management and trade-off with revealed risks and further trial operation is performed, allocations of trade-off with risks among participants, priorities in risk management and in trade-off with risks, allocation of means for

Fig. 8. Basic conflict in the management of technological entities from safety reasons (details in [5]).

measures leading to risk reduction - it does not only rely on response and more means is given for prevention etc.),

- in case denoted by feedback 3, it is pursued the change of process siting, designing, building and construction of technological entity (e.g. they are considered further sources of risks, introduced further criteria for risk assessment, changed the value scale, considered the further contributions to integral risk from linkages and couplings among the assets that were revealed as sources of great losses, damages and harms on public assets etc.).

Due to dynamic world development it is necessary regularly to evaluate in each territory the co-existence of territory and all technological entities located in it, because it is necessary to preserve the conditions in territory that enable the safe life of future human generations. At finding the significant problems it is necessary to find sources, forces and means for removing the important impacts on future territory conditions and future generations. It is necessary to determine the measures, sources for their realizations and responsibilities for their implementation, in the frame of public interest it is necessary to use all resources for performance of remedy in acceptable time horizon.

6.2. Deficits that reduce the effectiveness of super processes

The interface of processes for works with risks during the time, in individual parts of super processes is logical and today has support in many legal rules, norms and standards. The present problem is that it is not required the logical interface of different sectors that is very exigent. It needs the co-operation of specialists from many fields, which needs the common terms, mutual understanding, common effort at finding the consensus etc. that are missing. This reality confirms the results obtained for:

- energy infrastructure in [24, 25],
- drinking water infrastructure in [26, 27],
- transport infrastructures (road, rail, subway, air) in [28-36],
- communication, information and cyber infrastructure in [37-39],
- finance infrastructure in [40],

- supply chain infrastructure in [41-43],
- emergency services infrastructure in [44],
- public administration management in [45, 46]

and other studies that are in many other publications, which are in the CVUT archives [9]. The same shows the deficits given in Table 1. These facts reveal big deficiencies in work with the risk, namely in details and in whole processes.

The results of accidents investigation and inspections that were performed in twelve complex facilities: bulk power station; metro station; important central bus station; air control operation facility, airport; waterworks facility; big chemical plant; hazardous material storage facility; important highway bridge; important road tunnel; important artificial lake; and nuclear power plant [9, 47] revealed the main causes of organizational accidents in domains, e.g.:

- old style of entity management concept,
- old style of entity safety management (omission of system structure, human resources qualification, low safety culture),
- omission of some disasters, too simple risk assessment, low level of safety documentation in investigated technological object or facility operation control,
- insufficient control of individual processes and sub-processes,
- insufficient technical standards and norms,
- low level of cooperation among sectors in entity (e.g. delay and errors in information transfer at important facts), among other entities including the public administration,
- missing or low level plans for on-site and off-site preparedness,
- no documentation on near misses and on investigation of damages, losses and harms and their causes and on the response and follow-up activities after disasters (including lessons learned and information sharing).

With regard to results given above the super processes´ correct applications are good prevention of organization accidents. However, it is clear that the super processes application fulfils the expected targets only if all processes on lower hierarchical levels will be correctly applied and will be meaningfully interconnected and co-ordinated. It is necessary to note that problems connected with good application of both super processes, inhere in reality that neither present professional education nor present legislation do not require the connectivity of actions and measures that are important for success of super processes. The next problem is that partial processes contain sub-processes that are not interfaced in reality or their interconnections are insufficient as shown results of accidents investigation, failures of networks and conclusions from inspections of safety documentations mentioned above.

From above mentioned reasons it is necessary to introduce in education the branch of knowledge on management of hierarchically interconnected processes in vertical and horizontal structure and to prescribe the mandatory discussion of specialists responsible for management of individual sections from the level of sub-processes, over processes up to sub-processes, namely with participation of public administration and general public. The discussion needs to follow the public interest and to be performed by the suitable method of risk engineering on several professional levels (according to participants´ knowledge); the method needs to ensure the fair-mindedness and correctness; for professional discussion the more stages Delphi method [16] is suitable, according to experience the panel discussion [16] is unsuitable because at its use the special interest groups (lobby) can have chance.

7. Conclusions

Because the ideal of today's world designated as "the safe community" can be, according to the current knowledge, reached only by ensuring the human system integral safety, it is necessary not to be afraid of new conceptions and new objectives and to start constructing the complex system safety management in the communities and other entities concentrated on all the known disasters including the corruption and other phenomena belonging to organizational accident category which is ready to transform if there is the occurrence of new risks along with a mutual respect of coexistence of various systems. As always, the problem is in humans, i.e. how to force them, so they may consider the public interest, mutual help and similar values as the top value of individuals.

It is necessary to pay attention to safety culture which means that humans in all their roles (manager, employee, citizen or the victim of a disaster) keep the safety principles, i.e. they behave in a way that they don't cause a realization of possible risks and when they become the participants of risk realization they need to contribute to the effective response, stabilisation of the assets and their renovation and to initiating of their further development. It is true that the complex of attitudes, speculations, norms and values existing in the community which is the reflection of a way of how the community is managed, i.e. these are the general principles of dividing of the power and responsibility, the managing principles and a certain relation between the stress on a work results, authority, human care, keeping the safety principles and ensuring the function of the community.

The effective culture of safety is the basic element for the safety management. It reflexes the safety conception and originates from the values, attitudes and actions of the head managers of a community and from their communication with all the involved. It is an obvious obligation to actively participate on the solution of the safety questions and to promote among the others involved keeping of the authorized legal directives, standards and norms. The rules of safety culture must be elaborated into all the actions of a community. Their basis isn't the concentration on the delinquents'/mistakes originators' punishment but on the lesson from the mistakes and on instituting the corrective measures so that the mistakes couldn't be repeated or so that the rate of their occurrence was reduced.

On the basis of present knowledge, the world needs to be understood as the open system of systems and for security and development of humans the human communities (villages, municipalities, regions, states, association of states etc.) need to work well with risks. The work with risks targeted to human security and development is necessary to realize by super processes that are defined above. These super processes´ correct applications are good prevention of organization accidents.

Due to world variability in space and time there is necessary regularly to evaluate the conditions of co-existence of territory and all technological entities located in it from the viewpoint of human safety. Interconnection and co-ordination of super processes has not capability to ensure permanent territory safety and human safety, but it at least reduces the number of sources of organizational accidents by which it reduces the costs of human society on elimination of damages caused by technological accidents and infrastructure failures. For ensuring the correct interface and co-ordination on individual hierarchical levels, there is necessary to develop knowledge on knowledge uncertainties that are sources of risks that suddenly emerge, which of course influences the effectiveness of

super processes, and causes unpleasant surprises to humans in the form of extreme disasters occurrence.

Annex

On the basis of present knowledge, the technological (correctly socio-technological) facilities and infrastructures are open systems of systems, i.e. the sets of mutually interconnected open systems [3]. Each of these systems is made up from elements and interconnections among elements; the interconnections are set up by linkages among elements and by flows of different nature (material, energy, information, finance etc.) among elements.

The human, as a system developer, ensures that socio-technological system fulfils given tasks (it produces commodities or it furnishes a service) by using the logical linkages and the couplings set up by flows. Apart from the required interconnections, there can occur under certain circumstances the unacceptable interconnections, which lead to a lesser or higher damage of system. Such system damages cause that the system does not fulfil tasks and furthermore it endangers itself and its vicinity. Therefore, at present the technological facilities and infrastructures are made up as secured or safe systems.

On the basis of work [3], the safe system is constructed as the system that is ensured against all internal and external disasters including the human factor, i.e. to all harmful events and so that at its critical conditions it may not endanger itself and its vicinity (i.e. the place in which people live). It means that the safety is the system property, which is put above the system dependability. Therefore, the parameters which determine the system quality are arranged into the following order:

- ***safety***, i.e. the system capability to precede the critical system conditions (active safety uses the elements of control; passive safety uses the elements of protection) and even at its critical conditions does not endanger its vicinity,
- ***dependability***, i.e. the system capability to provide the required functions under the given conditions in the given quality and in the given time interval,
- ***availability***, i.e. the system capability to provide the required functions at the occurrence of process that uses the given function,
- ***integrity***, i.e. the system capability to provide the time correct and valid report on system faults,
- ***continuity***, i.e. the system capability to provide the required functions without disruption at the process initiation,
- ***accuracy***, i.e. the system capability to ensure the required system behaviour in the required range.

At the complex socio-technological systems that have the form “systems of systems” the other parameter of quality is supplemented, namely the interoperability as the interconnected systems capability to carry out the required tasks in required quality correctly and in-time in a given place and time.

As was said above, the safety is a set of measures, which are performed by human with goal to ensure the safe system, i.e. also the system security and human security in dynamically variable conditions of present world [3]. Origination and operation of the safe system is substantially more exigent on knowledge, sources, forces and means, and therefore, in current practice the secured systems are mostly used. If needed, these secured

systems are replenished by the organizational measures, which ensure the protection of public assets, when these systems endanger themselves and their vicinity [3, 48].

The secured system is understood as the system that is secured against all internal and external disasters including the human factor, i.e. to all harmful phenomena. In comparison with the safe system, the secured system can endanger itself and its vicinity under its critical conditions. With regard to human security, it can only be operated under certain conditions – so called limits and conditions [3].

As it is mentioned above, the secured systems involve commonly used technological systems, which can damage themselves and their vicinities under certain conditions. From this reason we follow their special property, i.e. the ***criticality***. This quantity is consistently related to size of impacts of function losses of system or system of systems targeted to fulfilment of certain goals for society [3]. According to this work, the determination of criticality in the territory of serviceability goes out from: the possible disasters´ hazard analyses; consideration of territory and system vulnerabilities; and from consideration of mutual interconnections among partial systems in the territory, i.e. vulnerabilities of whole system of systems. At criticality determination they are considered the following assets: public; technological system; territory; and the State, and the following questions:

1. How does the facility or infrastructure react to certain types of disasters?
2. How is the facility or infrastructure robust, resilient and rubbery?
3. How the behaviour of facility or infrastructure can be improved?
4. What management mechanisms in the sense of control are suitable?
5. What rules can be used for the self-regulatory or tolerable deflections?
6. Which parts of facility or infrastructure are critical?

For ensuring the safety, including the functionality, dependability and stability of facility or infrastructure, it is necessary to know certain threshold – the criticality, which determines the conditions at which the system of systems focused on certain targets´ fulfilment, does not ensure expected functions in a required time, in a required site, and in a required quality. Therefore, with regard to results of analyses of: important and dangerous faults and failures; losses and damages caused by system malfunctions; external disasters´ impacts; failures of mitigating measures; reactions of substances in a given facility; leakage or discharge of substances (pipelines) etc., the limits and conditions of facility or infrastructure are determined [3, 48].

Limits and conditions are tools for safety management of these technological facilities. Their observance ensures the safe operation of technological facility. They are the set of positively defined conditions, for which it is proven that the technological facility operation is safe. The appropriated set includes data on permissible parameters, requirements on operation capability, setting the protection systems, demands on the workers´ activities and on the organizational measures leading to the fulfilment of all defined requirements for design operation conditions [3, 48].

For ensuring the safety, i.e. also the reliability and the functionality, the control system of given technological facility or infrastructure needs to keep the determined physical quantities (parameters of appropriate subsystems) on values determined in advance. During the process of regulation, the control system changes the conditions of individual controlled systems by bearing upon the efficient quantities, with aim to reach the required state of whole system. In terms of integral safety [3], the following properties of control system are pursued in the order:

- level of observance of established operation conditions and prevention of damaging (unacceptable) impacts on the system itself and its vicinity,
- functionality (level of satisfaction of required tasks),
- operability, i.e. level of fulfilment of required tasks at normal, abnormal and critical conditions,
- operation stability, i.e. level of observance of established conditions during the time,
- inherently included resilience to possible disasters.

From above mentioned facts it follows that management and control systems determine quality and performance of systems. They have decisive influence on safety, and therefore, their following factors are considered: responsible autonomy; adaptability; integrity; and meaningfulness of tasks. Because the human behaviour is not deterministic, the main characteristics of considered systems are: the emerged properties; non-determinist behaviour; and complex relations among the organizational targets. People, maintenance, renewal and changes decide about each followed system. From the engineering viewpoint the followed systems are characterized by structure, hardware, procedures, surround, information flows, organization (problem of organizational accidents) and interconnections among the mentioned items [3].

Acknowledgement:

Author thanks to the Czech Technical University in Prague for support (grant SGS2015-17).

References

[1] UN. *Human Development Report*. New York 1994, www.un.org
[2] EU. Safe Community. PASR projects. Brussels: EU 2004.
[3] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organisation* (In Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.
[4] PROCHÁZKOVÁ, D. *Risk Analysis and Risk Management* (In Czech). ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405p.
[5] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities.* ISBN: 978-3-659-74632-1. Lambert Academic Publishing, Saarbruecken 2015, 244p.
[6] MASLOW, A. H. *Motivation and Personality*. Haper, New York 1954, 236p.
[7] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[8] PROCHÁZKOVÁ, D. Principles of Mitigating and Managing Human System Risks. *Information & Security*, 28 (2012), No 1, 21-36, ISSN: 0861-5160, e-ISSN 1314-2119, http://infosec.procon.bg
[9] CVUT. Czech Technical University archives.
[10] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Their Control* (In Czech). ISBN: 978-80-01-05479-6. Praha: ČVUT 2014, 234p.
[11] US. *A Guide to the Project Management Body of Knowledge*. Washington: US Project Management Institute 2004.
[12] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991
[13] GLENDON, I.A et al. *Human Safety and Risk Management*. ISBN: 0-8493-3090-4. Boca Raton: CRC Press 2006.

[14] PROCHÁZKOVÁ, D. *Principles of Safety Management of Critical Infrastructure* (In Czech). ISBN: 978-80-01-05245-7. Praha: ČVUT 2013, 223p.
[15] PROCHÁZKOVÁ, D. *Methodology for Assessment of Costs on Renovation of Property Affected by Natural or Other Disaster* (In Czech). ISBN: 978-80-86634-98-2. Ostrava: SPBI SPEKTRUM XI 2007, 251p.
[16] PROCHÁZKOVÁ, D. *Methods, Tools and Techniques for Risk Engineering* (In Czech). ISBN: 978-80-01-04842-9, Praha: CVUT 2011, 369p.
[17] ARMSTRONG, J. S. Review of Corporate Strategic Planning. *Journal of Marketing*, 54 (1990), pp. 114-119.
[18] BRYSON, J. M. *Strategic Planning for Public and Non-Profit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. London: John Wiley & Sons 2011.
[19] EPPLER, M. J., PLATTS, K. W. The Systematic Use of Visualization in the Strategic-Planning Process. *Long Range Planning* 42 (2009), pp. 42-74.
[20] JUDGE, W. Q., DOUGLAS, T. J. Performance Implications of Incorporating Natural Environmental Issues into the Strategic Planning Process: An Empirical Assessment. *Journal of Management Studies*. ISSN: 1097-0266. 35 (1998), 2, pp. 241–262.
[21] MOORE, M. H. *Creating Public Value: Strategic Management in Government*. Cambridge: Harvard University Press 1995.
[22] OECD. *Guidance on Safety Performance Indicators, Guidance for Industry, Public Authorities and Communities for Developing SPI Programmes Related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191p.
[23] BÉRENGUER, Ch., GRALL, A., SOARES, C. G. (eds): *Advances in Safety, Reliability and Risk Management.* ISBN: 978-0-415-68379-1. London: Taylor & Francis Group 2012, 3068p.
[24] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Causes of Failure of Electroenergy Infrastructure and identification of Domains that Need Prevention and Preparedness (In Czech). In: *Rizika podnikových procesů 2015.* ISBN: 978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, pp. 114-123.
[25] KRÁKORA, J., PROCHÁZKOVÁ, D. Impacts of Electric Energy Outage on Metro (In Czech). In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 83-90.
[26] PROCHÁZKA, J., VAŠATOVÁ, L. Failure of Drinking Water Supply (In Czech). In: *Proceedings.* ISBN: 978-80-214-5336-4. Brno: VUT 2016, pp. 278-286.
[27] PROCHÁZKA, J., VAŠATOVÁ, L. Risks of Drinking Water Failures. In: *Risks of Business and Territorial Processes*. ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, pp.92-104.
[28] PROCHÁZKOVÁ, D., MOCKOVÁ, D. Impacts of Failure of Selected Elements of Transportation Infrastructure (In Czech). In: *Ochrana obyvatelstva – nebezpečné látky 2012***.** ISBN: 978-80-7385-109-5, ISSN:1803-7372, Ostrava: SPBI 2012, pp. 148-152.
[29] PROCHÁZKOVÁ, D., LÁNSKÁ, M. Case Study Simulating the Impacts of Accident in Vítkov Tunnel (In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7835-115-6. Ostrava: SPBI 2012, pp. 253-256.
[30] PROCHÁZKOVÁ, D. Principles of Protection of Transportation Infrastructure (In Czech). In: *Požární ochrana 2013*, ISBN: 978-80-7385-127-9, ISSN: 1803-1803, Ostrava: VŠB-TU 2013, pp. 214-218.

[31] PROCHÁZKOVÁ, D., PATÁKOVÁ, H., PROCHÁZKA, J., STRYMPLOVÁ, V. Problems of Hazardous Substances Transport in the Czech Republic (In Czech). In: *Crisis Management - Strategy, Safety, Research*. ISBN: 978-80-86710-79-2. Brno: VŠKE 2014, pp. 225-237.

[32] STRYMPLOVÁ, V., PROCHÁZKOVÁ, D. Results of Analysis of Critical Spots at Passengers Control at Airport (In Czech). In: *Crisis Management - Strategy, Safety, Research.* ISBN: 978-80-86710-79-2. Brno: VŠKE 2014, pp. 238-247.

[33] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PATÁKOVÁ, H. The Results of Systematic Study of Risks Associated with the Transportation of Hazardous Substances. In: *Safety and Reliability: Methodology and Application*. ISBN: 978-1-138-02681-0. CD ROM. CRC Press 2014 (London: Taylor & Francis Group 2015), pp. 1663-1670.

[34] KERTIS, T., PROCHÁZKOVÁ, D. Reduce of Criticality of Critical Infrastructure Facilities in the Railway Domain. ISBN: 978-1-4673-6727-1/15/531.00©2015 European Union. *Smart Cities Symposium Prague (SCSP).* IEEE, 2015, 8p.

[35] REMEŠ, P., PROCHÁZKOVÁ, D. Compilation of Check List for Identification of Critical Spots on Highway (In Czech). In: *Rizika podnikových procesů 2015.* ISBN:978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, pp. 151-160.

[36] PROCHÁZKA, J., PRAŽAN, M., PROCHÁZKOVÁ, D. Causes of Organizational Accidents in Civilian Skyborne Operation (In Czech). In: *Young Transportation Engineers Conference 2016*. ISBN: 978-80-01-06016-2. Praha: ČVUT 2016, 10p.

[37] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Cyber Infrastructure – Identification of Critical Spots and Impacts of Its Failure (In Czech). In: *CYTER2012*, ISBN: 978-80-01-05072-9, Praha: ČVUT 2012, 10p.

[38] SRP, J., PROCHÁZKOVÁ, D. Analysis of Cyber Networks in System Concept. In: *CYTER2012*, ISBN: 978-80-01-05072-9. Praha: ČVUT 2012, 12p.

[39] PROCHAZKOVA, D., SRP, J., PROCHAZKA, J. Analysis of Cyber Networks in a System Concept. In: *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics. Recent Advances in Systems, Control, Signal Processing and Informatics*. ISBN: 978-1-61804-204-0, Rhodes Island 2013, pp. 102-109.

[40] PROCHÁZKOVÁ, D., KOPECKÝ, Z. Problems of Bank Sector (In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 250-252.

[41] PROCHÁZKOVÁ, D., ŘÍHA, J. Selected Security problems of Supply Chains (In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 266-269.

[42] PROCHÁZKOVÁ, D. Model for Supply Chains´ Safety Management. In: *Proceedings of the 11th European Transport Congress*. Praha: CTU in Prague. ISBN: 978-80-01-05321-8, pp. 213 -219. www.etc.2013.fd.cvut.cz

[43] PROCHÁZKA, J., RETAMOZOVÁ, P. Accidents of Oil Pipeline (In Czech). In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 164-173.

[44] BINKOVÁ, P., HORÁKOVÁ, A., PROCHÁZKOVÁ, D. Comparison of Strategies Used in Internal Safety in the European Union and the Czech Republic in Criminal-Police Sector (In Czech). In: *Požární ochrana 2012.* ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 21-25.

[45] PROCHÁZKOVÁ, D., PEŠKOVÁ, I. Open Problems in Social Domain Management (In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 257-261.
[46] PROCHÁZKOVÁ, D., ŠENOVSKÝ, M., MOZGA, J. Problems of Public Protection in the EU (In Czech). In: *Požární ochrana 2012*. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 270-274.
[47] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Results of Inspections of Risk Management Quality in Facilities of Critical Infrastructure. *International Journal of Mechanical Engineering*. ISSN:2367-8968. www.iaras.org/iaras/journals/ijme
[48] CR. *Act. No. 183/2006 Coll., on Spatial Planning and Building Regulation (Building Law).*

Chapter 17

CONCLUSION WITH PROPOSALS FOR IMPROVEMENT OF WORK WITH RISKS CONNECTED WITH PROCESSES*

1. Introduction

Publication „Risks of processes and their management“ is issued on the ground of significantly supplemented findings given in papers collected in collections [1-4]. Papers in question from the domain of management and cope with risks containing the original results from series of sectors, are here processed by uniform procedure, so they clearly may show the ways for control of risks in fields to which matter-of-factly belong. Such facts´ processing enables to generalize the cognition and to perform general proposals for improvement of work with risks of processes.

Present book contains seventeenth chapters separated to fife special parts, which are professionally and logically interconnected. The overview of their results is in the following section.

2. Summary of chapters´ content

The first part is the introduction to problems of risks. It is created by one-chapter *Outline on risk, risk management and trade-off with risks* that summarizes the present findings on risks, risk managements and fight with risks. It works with key words: disasters; hazard; risk; risk management; risk engineering; complex system; processes; variability of processes; variability of risks; system monitoring. *Author abstract is*: Disasters damage the humans and other public assets that humans need for life. The risk is a measure of losses, damages and harms that the disasters cause. For human safety and development, we need to negotiate with risks, so their impacts might not disturb the conditions in the world that humans need for life. For this purpose, special types of risk management and risk engineering are used in the practice. Present knowledge and experiences show that realisation and size of risks depend on the properties of disasters that are the results of processes that are going in our world. Due to world dynamic development, the processes are varying, and therefore, we also need to control the risks in this context. This reality needs new approaches in risk management and in risk engineering.

The second part deals with risks connected with selected processes. It contains ten chapters, i.e. chapters 2 – 11, which the authors processed by uniform way and on the same insight to risk. For individual chapters we give the key words and abstracts prepared by the chapters' authors.

The second chapter *Risks of drinking water failures* works with key words: drinking water supply; failure of supply; distribution network disruption; contamination. *Authors´ abstract is:* The chapter describes the impacts of drinking water supply in

***Author:** Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc., Czech Technical University in Prague, Praha, Czech Republic, prochazkova@fd.cvut.cz

Central Bohemia region if the failure is caused by two different origins, i.e. by: the disruption of distribution network; and contamination with toxic substance in one of drinking water source.

The third chapter *Risk management directed to safety of metro control systems* works with key words: transportation system; metro; system of systems; risk management; safety; security; metro safe operation. *Authors´ abstract is:* Risk management directed to safety is very important for transportation systems operation. Transportation systems in the context of various modes are meant as systems of systems, cyber-physical systems related to informational technologies and socio-technical systems related to human aspects. We concentrate to the urban guided transportation management system, based on knowledge on metro system in Praha. The critical assets and priority risks are given for both, the technological domain and the cyber one.

The fourth chapter *Evaluation of risks in transportation of items* works with key words: container; multimodal transport; risk; smart container. *Authors´ abstract is:* The development of trade has created higher demands on transport in terms of quality, speed, capacity and safety. During the securing process of goods, all means of transport that are to be used as well as any anticipated risks must be assessed. It is important to design all measures to mitigate the risks. The contribution lists the types of risks that might incur during the transportation of goods, and, in addition, usable methods of securing goods. Furthermore, the contribution provides an account of methods of protection against damage (safety) and theft (security). The individual measures are drawn from characteristics of the transport modus that is used in the logistics chain. For this reason, the contribution compares characteristics of individual types of transportation and very risky situation which can occur in unlikely occurrence, but with critical impact, too.

The fifth chapter *Economical and technical evaluation of machinery enterprise and system risks connected* works with key words: rating; evaluation of machinery enterprises; financial (quantitative) method; non-financial (qualitative) method; small and medium enterprise (SME); experiment. *Authors´ abstract is:* This chapter focuses on the current condition of economic and technical evaluation of small and medium enterprises with the use of domestic as well as international rating, emphasising the sector of machine industry. There is a need to get an objective tool for enterprise evaluation in the complexity. The task and aim of the work is to create functional practically applicable rating evaluating model of enterprise´s quantitative and qualitative data including creation of methodology for their domestic and international comparison. It was based on research. The functionality of academically suggested model including the methodology was tested by benchmarking in the time period of years 2009 - 2011 using the statistically validated financial data from the file of 21 anonymous domestic small and medium enterprises (next also „SMEs "), which operate in the field of machinery industry. Discovered results were compared by the benchmarking with the esteemed Rating of SME - the product of the company CCB – Czech Credit Bureau, a. s. from the multinational group CRIF, whose concrete calculation and methodology are its own know-how and a trade secret. The suggested model is more easily calculated using the less input data while providing high accuracy against the SME Rating. In conclusion of the article there is also an overview of risks connected with the subject and a proposal for their minimisation.

The sixth chapter *Risk assessment of project of implementation of video tolling for the fee collection system within the roads network of the Czech Republic as a part of regulatory impact assessment* works with key words: regulation, risk, roads, tolls, video

tolling. *Authors´ abstract is:* The Regulatory Impact Assessment (RIA) is a tool to support decision-making. The aim of the RIA is to determine the best option to achieve the objective of a rulemaking activity while minimising the potential negative impacts. The paper presents the RIA procedures and methodology from the view of the risk assessment, which is an obligatory part of each RIA. Specific application of the RIA risk assessment is presented on the case study of the project of implementation of the video tolling for the fee collection system within the roads network of the Czech Republic. The risk assessment consists of these parts: risk identification, evaluation of probability of its emergence, assessment of the potential impact on the proposed solution (probability and severity).

The seventh chapter *Employees fluctuation risks and how to measure them* works with key words: fluctuation; employee; human capital; job satisfaction; risk. *Author´ abstract is:* The aim of this chapter is to show risks of employees' fluctuation. In 2016 there is one of the lowest unemployment rates in the history of Czech Republic and companies are trying to preserve and prevent their key employees from moving to another employer. One of the tools which could help reduce this risk is providing additional education and qualification with laying great emphasis on most valuable and essential personnel. Process of selecting right employees, identification of unsatisfied employees and evaluation of provided courses should be important part of human resources management.

The eighth chapter *Assessment of economic security in enterprises* works with key words: risk, economic analysis, enterprises´ economic security, method of variability of indexes. *Authors´ abstract is:* The economic security is a state in which the economy of an object, whose security should be assured, is not faced by risks and threats which could significantly reduce (or are reduced already) their efficiency necessary to meet the basic functions and objectives. The main aim of the enterprise management should be the identification of the micro- and macro environment changes affecting the tangible and intangible sources of the enterprise economic security and the implementation of measures that allow achieving the defined objectives of an enterprise efficiently and effectively. One of the possible approaches to identification of risks affecting the enterprises´ economic security is an intercompany comparison. The chapter submits the theory of this risk identification method and the framework of indexes characterizing the criterion of enterprises´ economic security on the base of financial risks.

The ninth chapter *Marketing communication related to carrier – customer relationship in emergency situations* works with key words: carrier-customer relationship; emergency situation; marketing the communication; effectiveness; risk; risk monitoring; risk analysis. *Author´ abstract is:* The chapter deals process of information transfer at with the emergency transport in terms of marketing communications. It focuses on communication related to carrier – customer relationship and provides examples of usable communication channels. It briefly describes the basic types of emergency situations in traffic and defines them for basic communication objectives, and in that context it also touches upon problems in measuring the effectiveness of communication.

The tenth chapter *Risk connected with communication in critical situation* works with key words: communication, critical situation, stakeholders. *Author´ abstract is:* The issue of communication in a critical situation and its management represents a consistent part of emergency plans of companies which have decided not to ignore potential threats and which prepare themselves for a possibility of the emergence of the crisis. It is one of the proactive techniques and is based on the best experience of business entities that have already successfully managed the crisis. As people influenced by the crisis react similarly,

crisis communication involves mostly common characteristics, regardless of the economic sector in which the company operates. The present article analyses pre-crisis, crisis and post-crisis communication techniques. Their successful management makes it easier to overcome stressful times by crisis managers as well as by other stakeholders.

The eleventh chapter *Business processes and their mapping as a base for business continuity management and map of risks* works with key words: BCM (Business Continuity management), business processes, map of risks. *Authors´ abstract is:* The chapter deals with mapping of business processes from a risk point of view, in such a way that the final overview of the processes is useful for creating maps of risks, management of selected risks (especially operational risk) as well as for BCM (Business Continuity Management) and crisis management. The essence of the solution is the choice of criteria and procedures for mapping processes, so that the resulting process map was not too detailed and therefore too large for other planned uses, but also that contains all relevant processes from the point of view of risk. The primary criterion is the affiliation of the processes to individual departments or divisions of the company, further the frequency of the process, the critical period, the maximum allowable downtime (MAD), the possible effects of failure of the process (structured), etc. With proper selection of criteria and procedures arises universally usable map of risk processes.

The third part concentrates to theoretical and methodical aspects connected with selected activities performed in the frame of negotiation with risk, namely software tools. It contains four chapters, i.e. chapters 12 – 15, which authors processed by uniform way and on the same insight to risk. For individual chapters we give the key words and abstracts prepared by the chapters' authors:

The twelfth chapter *A mental decision risk model: theory and evaluation* works with key words: mental model; simulation; risk; risk management; sparse phenomena; volatility; uncertainty; reliability. *Authors´ abstract is:* Risk, uncertainty, and other terms have today much space and attention among thought-provoking intellectual constructs ranging across all disciplines in the humanities and social sciences (HSS). Physics, as a branch of science has been pre-occupied with relating the material objects, in space and time, for the last two centuries. The interest in this area appears to be primarily due to practical applications for rare events with high impact and large scale consequences. These mentioned events are particularly dangerous for technical-economic processes. Such examples can be found in critical infrastructure, energy production, chemical production, supply chains etc. Mental models devoted to risk can help to create a better understanding of reality and to help to more accurately reality simulation. The practical benefit is the efficient decision making probability increase which helps to avoid the risk underestimation.

The thirteenth chapter *The reliability evaluation of assembly lines using models* works with key words: assembly line, reliability, scrap rate, Scilab Xcos, step response. *Authors´ abstract is:* This paper focuses on the impact of scrap rate on performance of automatic assembly lines. Relations of relative line performance and a number of assembled components, and the ratio of line timing to median downtime at certain scrap rate are presented graphically. The automatic assembly line is equipped with measurement and information system that provides sufficient data on failure rates and reliability of lines. Mathematical-statistical evaluation uses identification method of control theory in Scilab Xcos which is based on analogy with step responses of physical systems. The paper aim is analysis and evaluation of reliability of automatic assembly lines.

The fourteenth chapter *Size of hazard depends on data files extent* works with key words: risk; disaster; hazard; data file extent; extreme theory application. *Authors´ abstract is:* Sizes of risks for human society depend on sizes of hazards cause the disasters and on the vulnerabilities of public assets. Due to the human population increase and the increase the number of interconnected complex systems and technologies the human system vulnerability to disasters is increasing and this causes large losses, damages and injuries to public assets at great disasters origin. Therefore, the prediction of extreme disasters´ sizes is of interest to experts who plan, built and operate technological facilities, or ensure the civil protection. Prediction is currently being carried out on the basis of mathematical methods as mathematical statistics working with random uncertainties, and more recently on methods based on the theory of extremes and on further more advanced theories (as chaos theory, complexity theory and the theory of options) that, in addition to random uncertainties can express a part of knowledge uncertainties, helping to identify the occurrence of extreme atypical disasters that afflict the human community irregularly and rarely. On the basis of results for prediction of great earthquakes calculated by authors for real data file from Europe, the authors show how the prediction of great earthquakes depends on the data files extent, and how it affects the safety of technological facilities.

The fifteenth chapter *Assessment of capabilities of conventional tools for analysing and assessing of risk in context with dynamic risks* works with key words: risk, dynamic, management, system, assessment. *Authors´ abstract is:* Risk management is an essential part of maintaining the functionality of systems, such as for example company, constituent of state administration or local government. Individual steps of the management can generate effective, preventive and safety measures which, also depends on the experience and knowledge of the main evaluate manager and his team of experts. It is necessary to maintain the objective approach and considering all possible risks arising from the entity activities. However, a situation can arise when all scenarios associated with the ordinary activities and events that at the first sight seems to be almost without risk are not taken into the account, but their impact could be very significant. These are associated with so-called dynamic risks, the manifestation's rate of which and the severity are changing in time. The aim of this chapter is to highlight the importance and possible ways of managing the dynamic risks.

The fourth part proposes two super processes, by help of which the humans can reduce or mitigate the risks that are connected with originators of organizational accidents, i.e. they are under human control. It contains one broad chapter, *Super processes for management of risks in territory and in technological entities directed to human security and development* that works with key words: security; development; safety; risk; risk management; process; super process; process management; territory; technological (socio-technological) entity (object or network. *Author´ abstract is:* On the basis of present knowledge, the world and each its entity (natural, social and technological) makes up the set of open and mutually interconnected systems. In these systems the processes are always under way that makes up the ground of dynamic development of both, the individual systems and their complexes. With these processes it is connected the occurrence of phenomena that harmed the humans and the territory in which the humans live. From this reason, the humans since their origin have been trying to comprehend harmful phenomena, to discover their causes and later also to manage the risks connected with them. Present tried-and-true management is based on management of processes, and therefore, the target of present paper is to determine the super processes for management of risks in territory and in technological entities directed to human

security and development. To this purpose it is performed the synthesis of verified knowledge and experiences from work with risks. On the basis of experiences from professional inspections and from analyses of accidents and failures of technological entities, there are given the most frequent causes of organizational accidents, i.e. bad applications of one or more processes that belong to followed super processes. The chapter proposes two super processes, the correct applications of which are the best prevention of organization accidents.

Last part is this conclusion, i.e. the present chapter, which summarizes the results and gives the proposals for improvement of work with risks connected with the processes, which are given in next sections.

3. Uniform evaluation of findings given in foregoing chapters

The first chapter shows that findings on risks´ originators, risks´ impacts, risk management and getting over the risks are today a lot. They are systematically followed in branch called *"risk engineering"*. The topical engineering measures and activities need to be correctly applied in right time and site in practice. From this reason, it is important the education of humans in which they will be teaching how to diagnose the priority risks and the ways of getting over them in domain of prevention, preparedness, response and renovation. It is also necessary to teach humans how to perform the correct safety culture in a given entity.

The data in the second chapter shows that the very great care needs to be directed to distribution of drinking water in the territory. It is shown that the drinking water network and its operation can be disturbed by great number of phenomena. The impacts of some disturbances (e.g. contamination of drinking water by high hazardous chemical or biological agents) are very critical, i.e. they lead to human lives losses and to damages of human health and other public assets. From this reason, all concepts of urban development of human settlements need to contain the tools for ensuring the safe infrastructure for drinking water distribution.

From the third chapter it follows that in Praha metro system, the critical assets and priority risks are in both, the technological domain and the cyber one. The selected cyber risks are studied in detail and some countermeasures are proposed. It is also shown, that there is available neither tool nor standard, which would specify the procedure for security practices in this specific field of cyber systems. They are used the standards from the industry sector that do not contain the railway specifics.

The fourth chapter is concentrated to problems connected with transportation of goods. It shows the overview of phenomena that damaged the supply chain of goods at its transportation. It goes on disasters of different types and also on human errors, namely both, the intent ones and the unintentional ones. In detail, they are followed the human failures that are very important sources of risks at goods transportation. For improvement of supply chains safety in the domain of transportation, they are proposed the special mode measures. These measures need to be systematic, interfaced and met by all participants of supply chain.

The topic of the fifth chapter is concentration to risks in economic domains that seriously threaten the competitiveness and goodwill of businesses. For business risk assessment, they are used three models that differ by approach to risk. By help of appurtenant formulas of models, they are determined the business capabilities in trading-off with expected economic risks. The comparison of obtained values for 21 SME shows

that the method The Domestic Rating KMEP provides the verified results with an average accuracy of 95 %.

The sixth chapter concentrates to risks connected with tolling the fee collection on roads. It follows partial risks from domains: legal, economic and politic. For their estimation it uses the current verbal classificatory scales for determination of occurrence probability and size of impacts on the State at risks realisation, however, the transfer of verbal scale to finances is not given. The results for six different possibilities of tolling the fee collection are given in the risk matrixes form. On the risk matrixes data, the order of tested variants of tolling the fee collection is determined. The lowest risk is connected with the variant of tolling the fee collection based on video detection system.

The seventh chapter objects are the risks from the human sources domain. The data on selection of human sources for businesses are processed by heuristic analysis. On obtained results, it is determined the variant for selection of human sources that has the lowest risks from the view of business stability. For estimation of variant, the index method is used. Results based on real data show that the work with risks in the human source domain is the key item for stability and competitiveness of each business. The critical item is the scale by which the indexes are defined.

The eight-chapter goal is to trade-off with risks that are important for the business economic safety. It goes from the economic characteristics of 41 businesses in the Slovak Republic. The sizes of their economic risks are determined by values of indicators that are used at the business management. From results, it follows that the management of business economic security need to be performed on the correct risks values. Because the determination of correct risks values requires the complex economic analysis of business that is timely and costly exigent, it shows the use of benchmarking method, the results of which are sufficient in many cases.

The ninth chapter is concentrated to risks in the communication domains at critical situations at roads and railways. It gives the basic principles of communication, and on real examples it shows the communication failures at critical situations. On real data from the Czech Republic, they are revealed the possible sources of risks that have potential to create the emergency situations or increase their severity. Among the losses caused by followed risks, it also includes the loss of carrier reputation. For carrier reputation losses reduction, it is recommended to carriers, so they might stop the underestimation of communication at critical situations. It is shown that right information transfer at traffic accidents is very important process that reduces the losses and damages connected with the traffic accident. To perform the correct response, it is required to ensure *"correct person obtains correct information at correct time"*. This shows the importance of marketing connected with the emergency situation, i.e. the negotiation with appurtenant risks for support of benefit of both, the public interest and the carrier profit.

The tenth chapter target is concentrated to crisis communication in businesses. On real examples, it is shown the necessity of proactive approach in this domain. On the basis of real data from businesses, the sources of relevant risks in appurtenant domains are determined. For successful work with these risks, it is given the risk management plan. It contains the measures for trading-off with risks if the appurtenant risks are realised.

The eleventh chapter target is the problem of credit risk and operating risk in businesses. For medium-size companies, the appurtenant risks are mapped. For their overcoming, it is compiled the business continuity plan. The core of correct risk solution is the correct selection of criteria and the correct way of determination of processes that can cause the phenomena that can seriously damage the business.

The 2 - 11 chapters are in appurtenant problem domains performed by professional approach that is used at the integral safety management [5]. They contain the answers on research, methodical and practical questions at risk management that are targeted to territory safety and especially to critical facilities and networks safety. They give the real measures leading to: the elimination or reduction of risks; risk management targeted to safety increase in transportation; risk management aimed to conservation of business competitiveness; reduction of cyber threats; protection of humans and property; and successful trading-off with further phenomena that threaten the Europe security and safety. They contain analyses of real events, models, case studies, examples, graphs, possible scenarios of impacts of failure of technological and organizational processes with the accent on examples of risk management in practice.

The authors of above considered chapters clearly or latently follow the integral safety concept in the human system [5]. They give the system characteristics and problems of management of safety in a given system, and ways of problems´ solutions in considered system based on present knowledge of science and especially information technologies. In chapters, there are new findings from theoretical application domains which work with terms as risk, risk management, disaster, safety etc. It enables to couple the basic theoretical and methodological foundations for complex safety management, and further to propagate the methodical and methodological apparatus for ensuring the individual safety aspects, and particularly the application of system measures in the practice.

The twelfth chapter deals with problems of decision-making at determination of models by which the reality is depicted at building the technological and social entities. It goes from reality that each used entity model has certain limitations that cause the entity failure at conditions that were not considered in the entity design; it verifies the assertion given in [6, 7]. From this reason, it is necessary at the selection of entity model to adhere the certain principles that specify the way of trade-off with risks. Therefore, the economic risks might be followed not only in the entity building but also in future, when as a consequence of conditions change, it will occur the failures in economic domain that will have also impacts in technological and social domains. It describes several software, which supporting the decision-making at the entity design selection. On real case, *bridge deck,* it compares the results of simulations according to used software in practice; the risk of each design is measured by finance expenses that exceed the expected costs. The most suitable procedure naturally seems the procedure based on integrated risk (sum of economic and technological risks) determination, in which it is used the mathematical algorithm MCDA (the multi-criteria decision analysis), probabilistic approach and the assumption that the risk is manifestation of knowledge uncertainty (vagueness).

The thirteenth chapter is related to the domain of automatisation of management of big technological entities. It presents the approach in which it is unlimited belief in good software. It propagates the Scilab Xcos software that is based on advanced knowledge that considers the Markov´chains, the Kolmogorov equations and probabilistic behaviour of systems. With regards to knowledge given in [7], this approach really enables to maintain the technical system reliability at normal conditions and to curb the random deviations caused by changes of internal conditions. It does not consider the external disasters, and therefore it has not capability to trade-off with all possible risks. Therefore, in practice, it might be supplemented by risk management plan or on-side and off-side response plans.

The fourteenth chapter shows that at determination of risk connected with a certain disaster, it is necessary to use the correct data on input parameters, i.e. on the hazard size

and on real vulnerabilities of assets in site, in which the risk is determined. On real case for earthquake, it is shown that the hazard size substantially depends on the time interval from which the data are considered. If we perform the assets´ protection on the incorrectly determined risk value, so sooner or later it is possible to expect huge losses and damages on public and private assets; e.g., it shows the consequences of several medium earthquakes in central Italy in last years (there were damaged new buildings because at their design the big historical earthquakes occurred in region were not considered). This knowledge is based on detail disaster research that shows that great phenomena occur sporadically and very irregularly, e.g. data in [8].

The fifteenth chapter deals with the capability of individual risk engineering methods, and mainly the appurtenant software products, at determination of risks of processes that change in time. It gives the theory based on the famous Bayes theorem and the basic equation for assessment of entity safety in a given time interval. The practical assessment is performed by the systemic approach, however, only for classic methods for risk assessment, i.e. for those for which the software is gettable. The results confirm the conclusions that owing to the world dynamic variability, it is necessary to monitor the each entity conditions as the open system of systems, and according the obtained facts to change the tools for management and trade-off with risk [7]. By other words, the classic methods for risk assessment, especially those in which the results are outputs of some software algorithm without logical thinking, have not the capability to express the risk values in the dynamic world.

The sixteenth chapter reacts on present findings on dynamic world development that manifests by changes of processes, which are the originators of phenomena that are the risks´ sources. Because the human factor at decision-making is one of important risks´ source, it proposes two super processes for management of human activities. Their adherence reduces the origin the organizational accidents and it ensures the quality management and trade-off with risks.

Used uniform view on risks in different partial domains enables to compare the approaches, methods and key procedures connected with work with risks. It removes the dissimilarities that are in many publications caused by disunity of terms or indistinctly determined aim of work with risks. Therefore, it can be said that aims of works with risks are same in all human activities domains, it is necessary to ensure the safety of activity or entity, i.e. the building, human settlements, sector, territory or the State; thence they respect the public interest.

The experience from practice obtained at assessment of disaster impacts on entities [1-4, 7-9] and above mentioned facts show that at work with risks a lot of deficiencies occur, e.g. :

- in many entities´ concepts, on which the risks or activities connected with management or trade-off with risk, it is not considered the system nature, interconnections of individual systems, existence of some internal and external disasters and changes in time and space (usually only direct selected disaster impacts are considered). It proves series of famous failures of technological and social entities, e.g. recent finance crisis that affected the majority of world,
- continually, the managers, technicians and scientists have great confidence in power of software that were really processed on theoretically well-founded models, but are not based on sufficient amount of real data describing the behaviour of followed entity during the sufficient time interval length; i.e., the appurtenant software can just contain the measures for adaptation of entity behaviour to changes in time and space,

and therefore, the have not capability to avert or mitigate great disasters impacts that are beyond their designs. From the risk engineering knowledge, such entities need to have emergency plans, continuity plans and operational crisis plans for protection of assets being in the entities vicinities,

- for risk assessment there are often used indistinctly determined criteria and classificatory procedures from which the real size of losses and damages on public and private assets is not recognizable (on risks they often adjudicate administrative and politicians who have low knowledge on risks and their impacts, or they have not real responsibility),
- at risk determination, it is often neglected the accent on use of relevant data and relevant methods; i.e. only exceptionally it is performed the judgement of representativeness and validity of data sets and sensibility of methods used for data processing, which in practise is manifested by errors in both, the risk determination and the measures for risks suppress,
- at ensuring the entity security and development, it is often considered to partial risks and exceptionally the integrated risks are considered. The integral (systemic) risks are considered only singularly.

4. Proposal of measures for improvement of management and trade-off with risks

On the basis of above given facts and knowledge, the proposals for improvement of control of risks connected with the processes need to come out from our findings, experiences and logical thinking, they are the following:

- reconnaissance of important assets in real entity and its vicinity, the safety of which is the target,
- determination of disasters that can have unacceptable impacts on the studied entity, their possible scenarios at different conditions in and out of entity; it means to consider the possible occurrence of several disasters mutually interconnected (amplification of impacts by bad maintenance, cascade effects),
- determination of processes that have capability to cause to happen the worse scenarios; determination of their criticalities and occurrence probabilities,
- evaluation of risks connected with processes with different scenarios, and mainly those that have capability to cause to happen the worse scenarios,
- judgement of human capability at copping with risks, namely critical ones, according to human possibilities and tools that are to disposal; the CBA is important tool,
- to perform correct decision on measures for coping with risks that were selected as important,
- to select the correct procedures suitable for given site for measures application in this site at prevention, mitigation and response (none of measures is suitable for all sites [9]),
- to determine correct procedure of realisation of measures of all kinds – technical, organizational, finance, legal and human sources,
- to ensure the prompt performance of measures,
- to introduce the monitoring that will follow the effectiveness of accepted measures and ensure the prompt correction measures.

From above concept it follows that the high quality work with risks represents the process which is challenging on knowledge, real data and time, and therefore, it requires the relevant interface of:

- deep findings and experiences,
- independent decision-making and management for public interest benefit,
- quality implementation of measures,
- support from all participants.

In case of lack of time, detail data or professionals the method based on comparison of entity safety level with another paradigmatic entity is possible to use. ***Benchmarking*** is the method of systematic comparison of processes, organizational structure, products and power of a given entity with other globally successful entities with aim to reach the excellency. It usually uses at risk management at cases if the goal is ideal and according to the good practice principles, it is suitable to manage the risks as the best operators in the given sector carry out it.

It is important continuously to consider that for whole human society welfare, the risks need to be managed in benefit of public interest, i.e. human security and development. From epoch of F. Taylor, the founder of scientific management and his successor H. Fayol [10, 11], the basic functions of management are not changed; the management goes on to lead (executors of management are people) the controlled organization or organizational part to prosperity and efficiency, and some change in this direction has not been predicted.

During the time, they have been changing the methods, the techniques and tools, how manage and lead, i.e. coordinate the human working activities so they may be performed effectively and efficiently. The social, technical, economic and globalization changes are reflected into changes of management of businesses and regions. This trend is permanent and it will also continue in the future. It induces the need of new development strategies based on smart technologies, new ways of work with risks, use of mutual active interactions among the research and business communities at creation and dissemination of knowledge. The successful development is more and more complex and depends on level of trade-off with risks in all entities.

In all entities, it goes on achievement of conditions at which the entity has the capability to dampen famous and foreseeable internal and external disasters that can damage some entity elements (or whole entity). It mainly goes on preservation of entity structure, entity stability, entity reliability and entity behaviour that is in harmony with entity mission, i.e. strategic targeted direction. It goes on level of entity stability and on its primary and secondary adaptation. In harmony with this mission, it is possible the entity safety management to structure and to define as:

- domain of management of relatively self-reliant (independent) activities with aim preventively to precede the risks or to minimize the risks consequences if risks realize,
- institutional set of subjects – actors ensuring the safety in regions, businesses that are from state administration and private entities,
- use of methods, procedures, directions, standards, norms and tools of management including the special methods and technologies for institutional (team) co-operation of individual actors ensuring the entity safety,
- systematic, functionally arranged, recurrent cycle of interconnected activities with the accent on permanent improvement of trade-off with risks which leads to entity safety upgrade.

The human security and entity development depends on level on which we trade-off with risks in processes that are round us; if we are capable existing and foreseeable risks to identify, to analyse, to assess and to control, i.e. effectively manage. The appurtenant sources – human, finance, information and time would be also the motive power of

positive human society development. But they can be limited factor or even by destructive factor if they are missing.

Generally, it is necessary to improve the safety culture and human learnedness on risks of citizens, administrators and politicians on all levels as the organizational accidents problem [7] shows.

5. Conclusion

As it was several times said, the world conditions permanently change, which means that the assets´ vulnerabilities and the processes being under way in the world also change. From this it follows that disasters´ characteristics and their impacts' scenarios also change. The consequence is the transformation of both, the risks´ rates and the human communities' possibilities. It means that each measure for tame of risks is provisional, and therefore, the humans' measures and activities need to be adapted to situation on the basis of lessons learned from critical situations. By research and increasing learnedness, the humans need furthermore to make up their capability to survive the extreme disasters that they are not identified in advance by present tools.

Safe world for humans can be only arranged by right work with risks. It is necessary to select proper concept on which we determine, manage and defeat the risks. In all cases, it is necessary to understand the world and each its entity as open system, to consider changes in time and space and proactively to solve problems. In cases, in which we neglect given facts from any reasons, we need to prepare the regime measures for fight with emergency up to critical situations.

The present book is synthetic source of knowledge for further development of integral safety concept in human system and for management of risks targeted to safety of both, the territory and the critical facilities, i.e. for human security and development. It may be useful for students of profile branches as the source of current findings in this domain. It also contributes to improvement of professional level, systemic thinking and behaviour in safety domain. It has all setups to be profitable part of library of many security professionals in theoretical and application spheres.

Finally, the author indicates that she would not evocate the impression at readers that she approves only her works because in this chapter she mainly uses the references to her works. She declares that she respects all professionals who work with risks in theoretical and practical spheres as the quotations in her books demonstrated; the reason of situation in this chapter is that her works are processed on one general concept od work with risks; references to other sources would require to explain the interfaces, because these sources describe the problems by other words, though concept principles, management and trade-off with risks are consistent.

References

[1] PROCHÁZKOVÁ, D. (ed.). *Selected Risks of Business Processes.* ISBN: 978-80-01-05831-2. Praha: ČVUT 2015, 190 p.

[2] PROCHÁZKOVÁ, D. (ed.). *Risks of Business Processes 2015* (In Czech). ISBN: 978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, 212 p.

[3] PROCHÁZKOVÁ, D. (ed.). *Risks of Business and Territorial Processes and Findings for Crisis Management* (In Czech). ISBN: 978-80-01-06033-9. Praha:

ČVUT, 2016, 507p.
[4] PROCHÁZKOVÁ, D. (ed.). *Risks of Business and Territorial Processes.* ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, 204p.
[5] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organisation* (In Czech). ISBN: 978-80-01-04844-3. ČVUT, Praha 2011, 483p
[6] PROCHÁZKOVÁ, D. *Analysis and Management of Risks* (In Czech). ČVUT, Praha 2011, ISBN: 978-80-01-04841-2, 405p.
[7] PROCHAZKOVA, D. *Safety of Complex Technological Facilities.* ISBN: 978-3-659-74632-1. Lambert Academic Publishing, Saarbruecken 2015, 244p
[8] PROCHÁZKOVÁ, D. *Risks Connected with Disasters and Engineering Procedures for Their Overcome* (In Czech). ISBN: 978-80-01-05479-6. ČVUT, Praha 2014, 234p.
[9] PROCHÁZKOVÁ, D. *Methodology for Estimation of Costs for Renovation of Property in Territories Affected by Natural or Other Disaster*. (In Czech). ISBN: 978-80-86634-98-2. Ostrava: SPBI SPEKTRUM XI 2007, 251p.
[10] TAYLOR, F. *The Principles of Scientific Management*. ISBN: 0-415-27983-6. Routledge 1911.
[11] Fayol, H. *General and Industrial Management: Henri Fayol's Classic Revised by Irwin Gray.* Belmont: David S. Lake Publishers 1987.

Title:	RISKS OF PROCESSES AND THEIR MANAGEMENT
Leading author:	Assoc. Prof., RNDr. Dana Procházková, PhD., D.Sc.
Reviewers:	Prof., Dr., Dipl. Ing. František Holešovský Asoc. Prof., Dipl. Ing. Václav Jirovský, PhD. Asoc. Prof., RNDr. Miroslav Rusko, PhD. Dipl. Ing. Karel Dach, PhD.
Publisher:	Czech Technical University in Prague
Number of copies:	200
Number of pages:	295
Year of issue:	2017

Professional reviewers´ and leading author´ comments to chapters were performed by authors. Format corrections, basic language corrections and reference corrections were performed by leading author.

ISBN 978-80-01-06186-2