Validity of Use of Various Concepts of Risk Management and Risk Engineering in Practice

Dana Prochazkova
Department of Security Technologies and Engineering
Czech Technical University in Praha,
Praha, Czech Republic
Email: prochazkova {at} fd.cvut.cz

Abstract— **Paper passes the judgement of concepts of management disciplines and the engineering disciplines directed to trade-off (negotiation) with risks that have been used with aim to ensure the safety of buildings, territories and human communities considered as systems. Individual concepts of these disciplines fulfil different goals, are based on various assumptions, have different demands on knowledge, data, forces, sources and means, and therefore, they involve different measures and activities for implementation in practice. The investigation, the results of which are furthermore presented, categorizes tasks in practice in which it is necessary to use very advanced procedures and in which simple ones are sufficient. The special attention is paid to engineering domain and to cases in which advanced procedures may be used for ensuring the safety of both, the system of systems and the system of systems´ vicinity.**

Keywords- **risk management; risk engineering; security engineering; safety engineering; process safety; system safety**

I. INTRODUCTION

Present goal of humans is to live in a safe space. The UN [1] formulated the human society target as a human system safety and the EU [2] formulated it as a safe community. The goal of both concepts is the human security and sustainable development. 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. Present cognition shows that it means to take care on public assets: human lives, health and security; property and welfare; environment; critical technologies and infrastructures [3]. To reach these targets the problems are on several levels: technical, functional (organisational, operative), tactical, strategic and political [4], and all problems must be solved and solutions on all levels must be interconnected. Robustness and capacity of solutions on technical level are aspects that under critical conditions guarantee the safety of objects and that are the important for ensuring the protection and survive of inhabitants [5].

The ground of human effort is to tame the risks. The term "*risk*" has the origin in the Middle Ages and our present knowledge on trade-off with risks has been collected since 30s of last century. Obtained knowledge and experiences have been influenced the management of risks and its measures and activities have been introduced step by step into practice by engineering disciplines [5]. At present work 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, i.e.: classical risk management / engineering; classical risk management / engineering including the human factor; security management / engineering; safety management / engineering, i.e. risk governance / trade-off for security and sustainable development of system; and safety management / engineering determined for system of systems (SoS) [4, 5]. It is evident that each more advanced type keeps the higher demands on knowledge, tools, times, finance, personnel qualification etc. For each management / engineering concept there has been developed 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. In next paragraphs we compare mentioned concepts, especially in engineering disciplines and judge the validity of their use with regard to their capability to ensure the human system safety, i.e. human security and sustainable development.

II. STATE OF ART

State of art of problems´ solution according to knowledge summarizes in works [4, 5] is: 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 at occurrence of extreme (beyond design, severe) disasters, Figure 1 [3-6]. The nature of such interdependences is physical, cyber, organisational and territorial [5]. Recent cognition 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 [3-5].

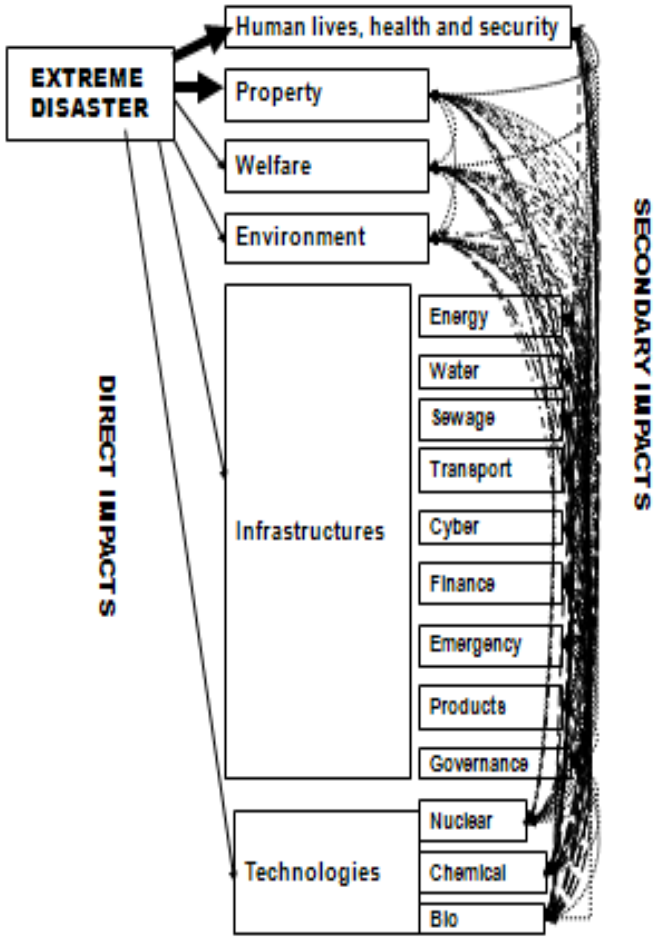

Figure1. Impacts on human system at extreme disaster

A system according to its core means more than only a sum of parts [4], and therefore, the stress is put on: study of the interactions and associations; non-linear thinking, interactions; inductions; feedbacks; and experiments or realistic simulations. E.g. feedbacks cause 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 the possible states of a system.

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 a 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 the 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 are 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 and their behaviour is described by results of simulations taking note of existence of epistemic uncertainties. The system of systems, i.e. a set of several overlapping systems (often also complex systems), 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.

Owing to consideration of problems of complex systems and the SoS, the system thinking is the fundamental principle of research. It 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 a feedback;*** to consider the relativity of possible situations; and to think in a long-term way [4, 5].

For management / engineering of complex systems and systems of systems it is then necessary to use the multi-criteria approach and in case of system of systems it is also necessary to consider the cross-sectional risks, the causes of which are emergent interdependences originating at certain conditions. The attention of advance engineering disciplines is concentrated to their disclosure. At their problems´ solution the tools are based on: the theory of chaos; theory of fuzzy sets; complexity theory; and theory of possibilities – references are in [5, 6]. In case of management of SoS we must also respect 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.

According to present standards the risk expresses the probable size of undesirable and unacceptable impacts (losses, harms and detriment) of disasters with the size equal to a normative hazards on system assets or subsystems in a given time interval (e.g. 1 year) and a given site, i.e. it is always site specific [4]. The typical risk properties are random and epistemic uncertainties (epistemic uncertainties = vagueness). If we want to manage risk, we must 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 task, we must use a lot of different methods, tools and techniques and also principles of good practice (good engineering practice). Basic aspects are included in following definitions of basic terms.

Work with risk is expressed by model shown in Figure 2 [6]. Feedbacks denoted in this Figure are used if risk level is not on required level [6]. For human safety and for human

system safety (i.e. territory, organisation, plant) we must 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 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.

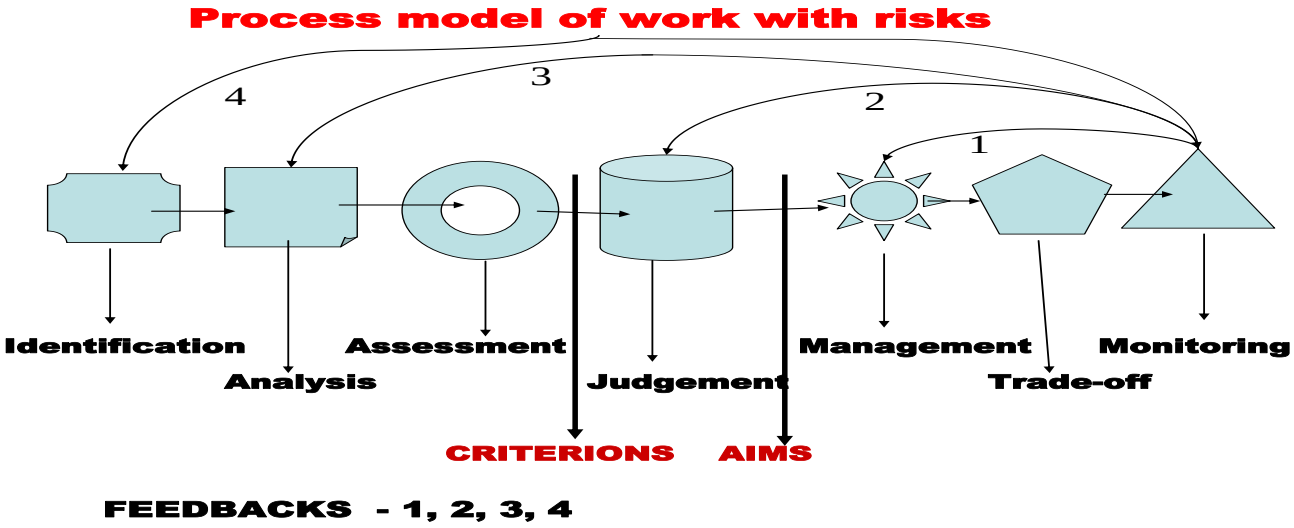

Figure2. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks

Considering the critical present knowledge evaluation, we recognised that one from many causes of interdependences, inducing the failure cascades in the human system or in its parts, is the human error (intentional or unintentional) in management. Therefore, in both, the management activities and the engineering activities we must do all the procuration with the aim to avert human failures, especially at the decision-making. Because consequences of errors caused at decision making are often huge, the human failure causes at management level, are now under a big attention at work with risk [8].

Security is the state of system at which the occurrence of harm or loss on system assets (protected public interests) has an acceptable probability (it is almost sure that harm and loss do not arise). It means that it ensures a certain stability of a 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 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.

System security means that system and its assets are not threaten by none of disasters with origin inside and outside of system.

System safety means that system, its assets and the system vicinity are not threaten by none of disasters, i.e. the system security and system vicinity security are ensured.

Secure human system is represented by a territory including the human society that is well protected against internal and external disasters.

Safe human system is represented by a territory including the human society, the assets of which (public assets are: human lives, health and security, property, welfare, environment, infrastructures and technologies) are in security and they can develop in a sustainable way. The system is protected against internal and external disasters and the system itself does not threaten its vicinity because the good symbiosis of each system with its vicinity is necessary for the system existence. Similarly, *a safe organisation* is the organisation, the protected assets of which are in security and they can develop in a sustainable way and the organisation does not threaten its vicinity.

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. As it was given above, 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 (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 20th 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 the protection of human lives, environment, property and economic assets, i.e. for the optimum reach of security and

sustainable development of human system; and 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.

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 must be respected that both, the assets and the 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 must 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].

Special requirements on methods, tools and techniques are given by further given facts:

- at problem solving it is considered: all processes under account are dynamical, and therefore, it must be used special appliance that is created by research procedures for optimal risk management; it is many disasters and they affect on different assets variously, and therefore, the vulnerabilities of assets, linkages and couplings in a system play big roles,
- on the basis of evaluation of accessible data sets, above all their random and epistemic uncertainties, it is necessary correctly to select at practical problem solution the approach to: a problem according to problem nature - deterministic, probabilistic, heuristic; risk and system safety that on general level is composed of steps: definition of system and its vicinity; identification of dangers; determination of hazards at extreme disasters; risk determination; proposal of corrective and remedial actions according to criterions for safety with goal to ensure acceptable security; and verification of risk acceptance.

Then it is necessary to structure methods according the data quality and according to goals of risk management because from practical viewpoint it is necessary to separate tasks for: risk identification; risk analysis; risk determination for different goals, i.e. the case in which we need precise value for strategic decision-making, or the case in which we only need rough value for check or immediate defeat of risk of real process at tactical or operational decision-making (sometimes verbal value is sufficient). Then methods, tools and techniques are selected with respect to a number of assets and in case of consideration of two or more assets it must be determined whether it is necessary to work with integrated or integral risk, and which disasters at real site we consider as sources of risk. Correctly, it is necessary to apply approach „All Hazard Approach"[9]. It is a reality that at all methods that we use in practice, we must distinguish two factors: certain integration into mathematical apparatus and the reality how certain method can be used at risk management / engineering based on work with risk in a certain concept of problem solution.

The key principles of present engineering directed to safety are: the approaches are based on risk, i.e. the work intensity and documentation is adequate to a risk level; the professional approach is based on reality that only the critical attributes of quality and the critical parameters of process are considered; the problem solution is oriented to critical items, i.e. the critical aspects of technical systems ensuring the consistence of system operations are only followed and managed; the verified quality parameters are included in the project proposal; the accent is put on quality of engineering procedures, i.e. it must be proved the accuracy of selected procedures under given conditions; and the aim of a safety upgrade is permanent improving of the processes with the use of analysis of the root causes of malfunctions and failures. For respecting these items there must be used relevant data sets and only verified methods that provide outputs with a designated testified competence.

Owing to existence of a lot of factors, including the human factor, that influence the problem solving at real conditions and the reality that these factors are not only random but also epistemic, the measures, activities and procedures denoted as good engineering practice are typical for engineering disciplines. 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 and it is often used at measurements in laboratories, negotiation with humans etc.

Good engineering practice (good engineering procedure) is then defined as the 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; and lead the interdisciplinary team. Most of these demands are directed to correct the human factor negative manifestation.

III. MATERIALS AND METHODS USED FOR CRITICALITY ASSESSMENTS OF FOLLOWED CONCEPTS

Concepts of risk management / engineering used in practice are mentioned above. We further judge them according to the criteria that enable to evaluate their capability with which they carry out the human targets that are human security and sustainable development. According to present knowledge the acceptable level of human system safety (representing the human community composed of territory and human society) is ensured by tools, which are risk management and risk engineering. Because the human system is composed of incommensurable assets, it is a system of systems, so effectiveness of tools in a various concepts is possible only performed by multi criteria approach [4, 6]. In analogy with procedures used at assessment of critical infrastructure safety and protection [10], where the assessment is targeted to safety and protection of human system, ***we use the criticality rate of individual concepts of risk management / engineering***, and for its determination the following factors: **1**-rate of capability of protection of human lives, health and security inside the system; **2**-rate of capability of protection of human lives, health and security outside the system; **3**-rate of capability of protection of property inside the system; **4**-rate of capability of protection of property outside of system; **5**-rate of capability of protection of welfare inside the system; **6**-rate of capability of protection of welfare outside of system; **7**-rate of capability of protection of environment inside the system; **8**-rate of capability of protection of environment outside the system; **9**-rate of capability of protection of live-giving infrastructures and technologies inside the system; **10**-rate of capability of protection of live-giving infrastructures and technologies outside the system; **11**-rate of capability of protection of human lives and health against disaster impacts caused by interdependences; **12**-rate of capability of protection of environment against disaster impacts caused by interdependences; **13**-rate of capability of protection of human society against disaster impacts caused by interdependences; **14**-rate of capability of protection of live-giving infrastructures and technologies against disaster impacts caused by interdependences.

The data for assessment were obtained from six experts selected according to criteria used in the EU [6] from domains: public protection; territory protection; environment protection; public administration; protection of technological systems; and first responders (Integrated Rescue System). The experts evaluate 14 factors given above according to their knowledge and experience, the following scale that is analogical to that used for risk assessment in CSN norms [6]:
0 point - factor ensures extremely high capability of protection (expected damages are lower than 5%, concept application means no significant risk for assets, i.e. negligible concept criticality),
1 point - factor ensures very high capability of protection (expected damages are in interval 5-25%, concept application means low risk for assets, i.e. low concept criticality),
2 points - factor ensures high capability of protection (expected damages are in interval 25-45%, concept application means median risk for assets, i.e. median concept criticality),
3 points - factor ensures median capability of protection (expected damages are in interval 45-70%, concept application means high risk for assets, i.e. high concept criticality),
4 points - factor ensures low capability of protection (expected damages are in interval 70-95%, concept application means very high risk for assets, i.e. very high concept criticality),
5 points - factor ensures negligible capability of protection (expected damages are higher than 95%, concept application means extremely high risk for assets, i.e. extremely high concept criticality).

Resultant value for each factor is determined as the median from data obtained from experts. Resultant assessment of capability of protection for all factors with assumption that all factors have the same weight can take on values from 0 to 70. If we again apply approach used in the CSN norms we obtain values given in Table I.

TABLE I. SCALE OF VALUES FOR DETERMINATION OF RATE OF CRITICALITY OF CONCEPT USED FOR RISK MANAGEMENT/ ENGINEERING

Rate of concept criticality	**Values in %**	**Number of points for factor**
Extremely high	More than 95%	More than 66.5
Very high	70 - 95%	49 – 66.5
High	45 - 70%	31.5 – 49
Median	25 – 45%	17.5 – 31.5
Low	5 – 25%	3.5 – 17.5
Negligible	Less than 5%	Less than 3.5

IV. RESULTS

Strategy of management for ensuring the security and sustainable development of managed subject consists of the negotiation with risks. We apply several ways of dealing with risk [4]:

- part of the risk is reduced, i.e. by preventive measures the risk realisation is averted,
- part of the risk is mitigated, i.e. by prepared measures (as warning systems and another measures of emergency and crisis management) non-acceptable impacts of risk realisation are reduced or averted,
- part of the risk is re-insured,
- part of the risk is covered by reactive and renovation measures and actions, i.e. there are prepared resources, forces and means for response and renovation,
- and residual part of risk remaining without human attention, i.e. it is a part of the risk that is non-controllable or too expensive at its averting or low frequent – in very advanced risk management it is prepared contingency plan and continuity plan.

The trade-off with risk is supplemented by distribution of risk defeating among all stakeholders.

The process of system safety management is shown in Figure 3. The safety management system is given in Figure 4. Feedbacks denoted in this Figure are used if safety level is not on required level [6].

It is necessary to give that management of risks has not been uniformly understood yet [4]. In our research we consider the interpretation given in Figure 2 that is consistent with definition of the FERMA (Federation of European Risk Management Associations), EMA (Emergency Management Office of Australia), UK Cabinet Office, USA Presidential / Congressional Commission on Risk Assessment and Risk Management, OECD, IAEA etc. Types of risk management and their characteristics summarized in work are given in Table II that was constructed according to results of critical analysis of publications [7, 11-16]; the other ones are in [4].

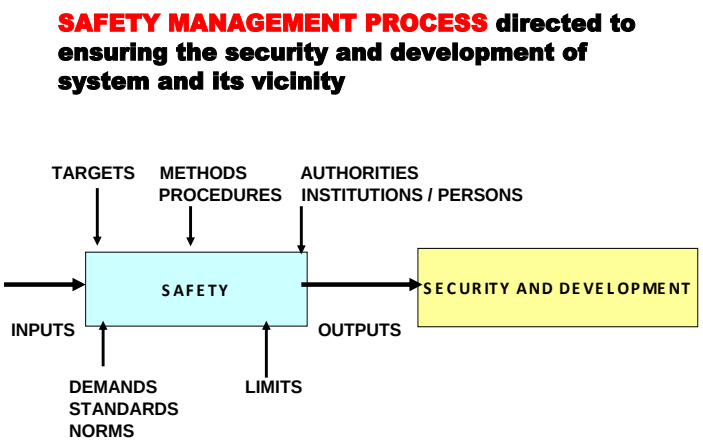

Figure3. Process of system safety management

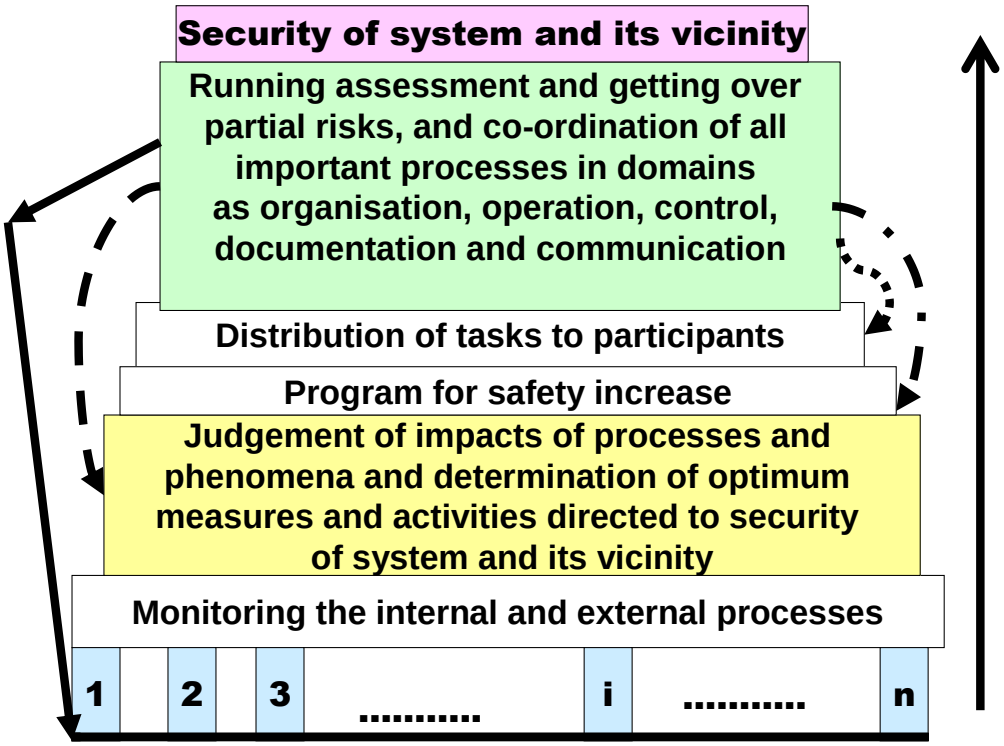

Figure4. Safety management system; numbers denotes internal and external processes that affect the system safety and lines (dotted, broken, dashed and full) denoted feedback

Types of risk engineering and their characteristics obtained by a critical analysis of works [17-30] are summarized in Table II; the other details as description of standards and norms and quotations of their authors are in [5]. The graphical scheme of risk engineering types is in Figure 5.

As it was shown above the five various concepts of risk management / engineering are used in practice and they were the subject of our reseach. They were assessed by methods described above and by help of data obtained from 6 experts. The resultant assessment representing the median from data obtained from experts described in foregoing paragraph is given in Table III.

Comparison of data in Tables III and II shows that the criticality rate of:

- both, the classical system risk management / engineering and the classical system risk management / engineering considering the human factor are very high,
- system security management / engineering is high,

- system safety management / engineering is median,
- system of systems safety management / engineering is low.

It means that the system of systems safety management / engineering is the most effective concept of work with risk with regard to our present knowledge and experience directed to human system safety from the viewpoint of ensuring the human security and sustainable development.

Taking into account the reality that the use of various concepts are differ by requirements on knowledge, data, personal qualification, material, finance and technical solutions, it is evident that the most effective concept is the most challenging. Therefore, it is necessary and important for strategic level of problems´ solution. For tactical and functional levels of problems´ solution is sufficient the concept ensuring the system safety management / engineering. The concept called as system security management / engineering is only suitable for technical level of problems´ solution, i.e. in cases in which high damage on system vicinity are not probable.

TABLE II. TYPES OF RISK MANAGEMENT / ENGINEERING AND THEIR CHARACTERISTICSABLE

Type of risk management / engineering	**Concept** **Characteristics**	**Aim of risk management / engineering**
Classical risk management / engineering	Object (plant, territory, organisational unit) is a closed system. Risk sources are internal technological phenomena in buildings. Formation in 30s of last century.	The target is to reduce the technological risks of a system to a certain level, given by standards and norms. The risk is determined after the design of the system, and therefore, there is no possibility to reduce risks connected with an inappropriate solution for a given site and system. The reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones [3].
Classical risk management / engineering considering the human factor	Object (plant, territory, organisational unit) is a closed system. Risk sources are internal technological phenomena and human factor in buildings. Formation at the end of 70s of last century.	The target is to reduce: the technological risks of a system to a certain level given by standards and norms; and to reduce risks connected with a human factor – safety instructions for danger works. The risk is determined after the design of the system, and therefore, for reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones [3].
System security management / engineering	Object (plant, territory, organisational unit) is an open system. Risk sources are external and internal phenomena including the human factor. Formation at the first half of 80s of last century. As risk sources also failures of decision-makings at risk management / engineering were included [4].	The target is to reduce risks for a system: from external and internal phenomena and a human factor, to a certain level given by standards and norms; i.e. to ensure the security of a system and its assets. No interest on system vicinity. Unacceptable impacts on vicinity can be only mitigated by special off-site emergency plans [3], i.e. by organisational measures and activities if state enforces such legislation.
System safety management / engineering	Object (plant, territory, organizational unit) is an open system. Risk sources are given by all hazards approach. Formation at the second half of 80s of last century. The advanced safety engineering uses at risk determination the following principles: • risk is determined 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, • risk is determined according to the criticality of impacts on processes, provided services and on assets that are determined by public interest, • unacceptable risks are mitigated by tool for risk management, i.e. according to technical and organisational proposals, by	The target is to ensure the security of a system and its assets and the security of system vicinity. The target is the safety, i.e. it is also necessary to trade-off with risks having low occurrence frequency if their impacts are unacceptable, and i.e. precaution principle is applied. The set of standards and norms exist especially for nuclear and chemical domain. Except of technical measures respecting the precaution principle, special technical problems solution there are continuity plans containing the procedures for overcoming the critical conditions in system and system vicinity, emergency plans and crisis plans. The risk management viewpoint by these characters: sitting – designing – construction – project with risk reduction; operation with the integration of early warning systems and of procedures for the management of the acceptable level of risks; and defeating the abnormal, emergency and critical conditions at the operation and at putting out of the operation [3].

	standardisation of operating procedures or by automatable check-up. To prepare groundwork, it is necessary to combine analytical methods with expert judgement by which we remove vagueness (epistemic uncertainties) in data.	
System of systems safety management / engineering	Object (plant, territory, organizational unit) is an open system of systems. Risk sources are given by all hazards approach and by interdependences among the partial systems and by those with vicinity. Formation at the beginning of third millennium.	Target is to ensure: the security of both, the system of systems including its assets and the system of systems vicinity; and the co-existence of individual systems crating the system of systems. The set of standards and norms are under discussion and preparation.

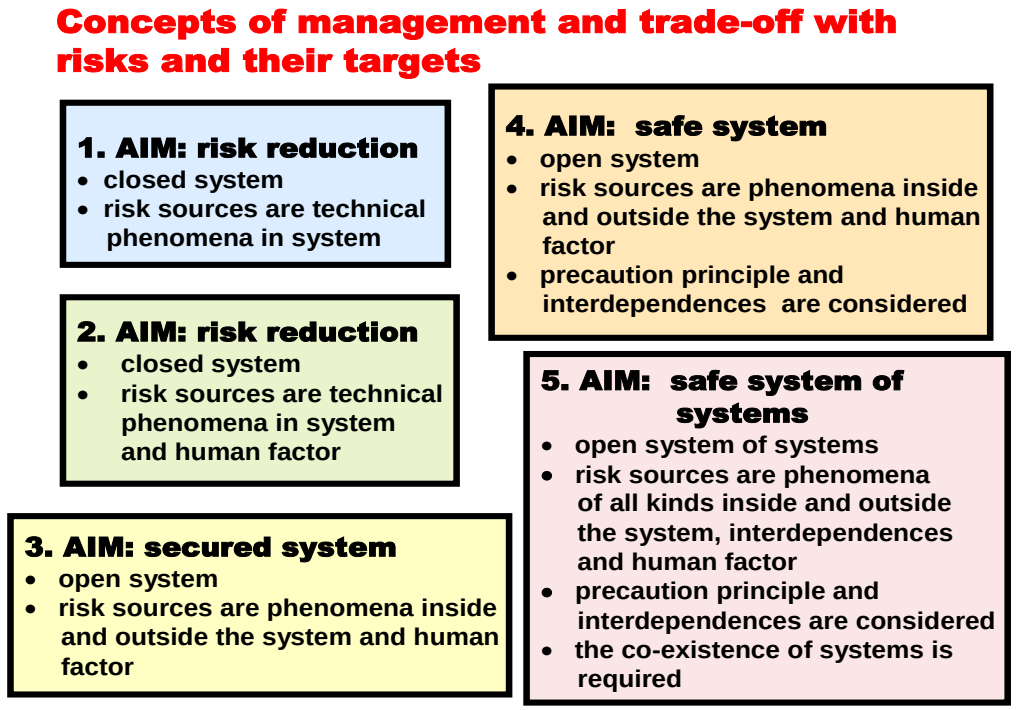

Figure5. Engineering types considering the risk

TABLE III. RATE OF CRITICALITY OF FOLLOWED CONCEPTS OF RISK MANAGEMENT / ENGINEERING

Factor	Classical system risk management / engineering	Classical system risk management / engineering considering the human factor	System security management / engineering	System safety management / engineering	System of systems safety management / engineering
1	4	3	1	1	1
2	5	5	5	1	1
3	4	3	1	1	1
4	5	5	5	1	1
5	5	3	1	1	1
6	5	5	5	2	1
7	4	3	1	1	1
8	5	5	5	1	1
9	4	3	1	1	1
10	5	5	5	1	1
11	5	5	4	5	1
12	5	5	4	5	1
13	5	5	4	5	1
14	5	5	4	5	1
All factors	66	60	41	31	14

V. CONCLUSION

Table III describes the risk management / engineering types used in a present practice. For each risk management / 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 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 given above show that at strategic level of problem solution it is necessary to use the system of systems safety management / engineering that fulfils demands of social engineers, technical engineers and environmental engineers. On the tactical and functional levels it is necessary to respect strategic concept recommendations and at site specific immediate problems´ solution it is possible to use the system safety management / engineering because character of solved problems is not so fundamental from the long term viewpoint. On the technical level it is necessary to respect recommendations of all higher concepts, i.e. relevant strategic, tactical and functional ones and at site specific immediate problems´ solution it is possible to use the system security management / engineering because character of solved problems is not so fundamental from the time viewpoint. The political problems solutions might respect strategic solutions if they want to respect public interests. The last one demand is often problem because politicians have not high professional knowledge and often they mean that they obtained godlike wisdom when became politicians.

It is also evident that at emergency management or at crisis management we have not time to determine the most suitable strategic solution, i.e. at emergency at simple case the risk management / engineering principles are sufficient, but at most of real cases the security management / engineering principles are applied if we *only* protect object under account and not its vicinity, ***otherwise*** the safety management / engineering principles or SoS management / engineering principles must be applied.

REFERENCES

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

[2] EU,"The Safe Community Concept". Brussels: EU, 2004, PASR project.

[3] D. Prochazkova, "Strategic Safety Management of Territory and Organisation". ISBN 978-80-01-04844-3. Praha: ČVUT, Praha 2011, 483p.

[4] D. Prochazkova, " Risk Analysis and Risk Management". ISBN 978-80-01-04841-2. Praha: CVUT, Praha 2011, 405p.

[5] D. Prochazkova: Critical Infrastructure Safety. ISBN: 978-80-01-05103-0, Praha: ČVUT, 2012, 318p.

[6] D. Prochazkova, " Principles of Critical Safety Management". ISBN: 978-80-01-05245-7. Praha: ČVUT, 225p.

[7] H. Bossel, "Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme". Books on Demand, Norderstedt/Germany, ISBN 3-8334-0984-3, 2004. www.libri.de.

[8] AIChE, "Guidelines for Preventing Human Error in Process Safety", American lnstitute of Chemical Engineers, New York, NY, 1994.

[9] FEMA, "Guide for All-Hazard Emergency Operations Planning". State and Local Guide (SLG) 101. FEMA, Washington 1996.

[10] D. Prochazkova and J. Prochazka, "Model for Critical Infrastructure Safety Management". Brno: UNOB 2013, in print.

[11] AFMC/ENPI, "Risk Management", AFMC Pamphlet 63-101, Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base 1997.

[12] AS/NZS, "Australia and New Zealand Standard: Risk Management, issued by Standards Australia, Guideline 4360", http://www.riskmanagement. com.au/Default.aspx?tabid=148 –116 pp.; b) Risk Management Guidelines - Companion to AS/NZS 4360:2004 available for purchase at http://www.riskmanagement.com.au/Default.aspx?tabid=157 – 28 pp.

[13] Canadian Standards Association, "CAN/CSA-Q850-97 Risk Management: Guideline for Decision-Makers – A National Standard of Canada". http://www.csa- intl.org/onlinestore/ GetCatalogItemDetails.

[14] EPA, "Guidance for Risk Assessment and Management: Off-site Individual Risk from Hazardous Industrial Plant. Environmental Protection Authority. State of Western Austria", 2000, pp. 21. www.environ.wa.gov.au/ downloads/Guidance_Statements/8.pdf

[15] NRC, "Science and Judgement in Risk Management". U.S. National Research Council 1994. http://www.nap.edu/books/030904894X/html/

[16] WB, "Natural Disaster Risk Management" The World Bank. Urban and City Management 2004. http://www.worldbank.org/wbi/urban/ paper disaster.htm

[17] R. Bris, C. G. Soares, and S. Martorell (eds), "Reliability, risk and safety: Theory and Application". ISBN: 978-0-415-55509-8, 2367p., CD ROM - ISBN: 978-0-203-85975-9, CRC Press / Balkema, Leiden 2009.

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

[19] Ch. Bérenguer, A. Grall, and C. G. Soares (eds), "Advances in Safety, Reliability and Risk Management". Taylor & Francis Group, London 2012, ISBN 978-0-415-68379-1, 3068p.

[20] CISP, "Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity", Commnon Standard. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch

[21] A. Kuhlmann, "Does Safety Science Fulfill the Requirements of Modern Technical Systems? In: Safety of Modern Systems". Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 9-17.

[22] H. J. Pasman and J. K. Vrijling, "Social Risk Assessment of Large Technical Systems". Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne: TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, pp. 151-162.

[23] IAEA, " Safety Guides and Technical Documents". Vienna: IAEA 1954 – 2013.

[24] COMAH, " Safety Report Assessment Manual: COMAH". London: UK- HID CD2 London 2002, 570 p.

[25] 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". ASCE, Washington 2001.

[26] H. E. Roland and B. Moriarity, " System Safety Engineering and Management". ISBN 0-471-6186-0. J. Willey 1990, 321p.

[27] R. Anderson, "Security Engineering – a Guide to Building Dependable Distributed Systems". ISBN 978-0-470-068552-6, J. Willey 2008, 1001p.

[28] F. P. Lees, " Loss Prevention in the Process Industries". Butterworths, London 1980.

[29] A. Kossiakoff and W. N. Sweet, "Systems Engineering. Principles and Practices!. ISBN 0-471-23443-5. J.Wiley, New Jersey 2003, 459p.

[30] DoD US, "DoD Security Engineering Facilities Planning Manual". Department of Defense US. DRAFT UFC 4-020-01, 3 March 2006. http://www.wbdg.org/ndbm /DesignGuid/ df/FINAL%20DRAFT_UFC_ 4-020-01.pdf