International Journal of Civil Engineering, Construction and Estate Management
Vol.5, No.1, pp.38-50, March 2017
Published by European Centre for Research Training and Development UK (www.eajournals.org)

MODEL OF CRITICAL INFRASTRUCTURE SAFETY MANAGEMENT

Dana Prochazkova, Jan Prochazka
Czech Technical University in Prague, Praha, Czech Republic

ABSTRACT: *The safe community is now at time of globalisation very dependent on a safety level of critical infrastructure ensuring the territory by basic services necessary for humans´ live as there are energy, water, food, information etc. Series of events from recent years connected with critical infrastructure failures showed its high importance. The critical infrastructures represent multistage mutually overlapping systems, i.e. big complex systems, the type of which is a systems system. The paper presents the model for critical infrastructure safety management based on this reality and it shows the way how simply to determine the criticality of individual infrastructures and the whole critical infrastructure.*

KEYWORDS: critical infrastructure; provision of territory services; security; safety; model for safety management.

INTRODUCTION

For ensuring the human security and development, there is necessary the safe human system [1-3]. Ensuring the safe human system is not easy, because the human system is a system of systems [4], i.e. system of several mutually interconnected systems of a different nature. Consequences of interconnections (interfaces) are mutual dependences, the character of which is physical, cyber, territorial and organisational [4-6]. Mentioned interdependences are the sources of further vulnerabilities of human system that magnify the integral risk of a given system by increase of cross-section risks in the system of systems [4-6]. As a consequence of growing globalisation the new sources of disasters take on force, they cause critical infrastructure failures. The paper deals with problems of critical infrastructure in the broadest concept, i.e. not only from the viewpoint of critical infrastructure itself, i.e. from the viewpoint of its structure and co-operation of its individual parts***, but also*** from the viewpoint of its impacts and profits for a given locality in it is in operation, i.e. for public assets in locality and region. By this feature the paper concept differs from the most of current works, and it is reality that its concept includes the public protection. From the reasons of fulfilment of targets of humans that may be realised only if human communities are in safe territory, the object of present paper is the critical infrastructure safety that ensures the safe infrastructures that do not threaten their vicinities, i.e. also another systems with which they are mutually interconnected or which they influence. The result of study, by help of methodology processed in the frame of project FOCUS [7-9], is the creation of model of infrastructure chains safety management.

ISSN 2055-6578(Print), ISSN 2055-6586(online)

Critical infrastructure

The critical infrastructure includes the infrastructures that are parts of different technological systems that ensure the human society needs [5]. Each of considered systems consists of the control system and controlled systems [9], which are for company processes, social system (humans, organisational structures, assets and values, knowledge), and for own technological system (tools, equipment, procedures, technologies). It means that they are multistage systems at which among the individual stages in both directions they run flows of materials, finances, information and decisions. From these reasons the systems needs to be also analysed from the viewpoint of interactions and interdependences among technical, human, social and organisational aspects of a system. The exception is the analysis of human survival that is either active or passive. The capability of passive survival is included in the system properties, there are based on knowledge on defects in environs; the defects are illustrated by causal chain. The capability of active survival manifests by system behaviour, it considers uncertainty in projection of future defects and failures.

From the methodological viewpoint the critical infrastructure and each its partial infrastructure is a system of systems [4, 5]. In engineering disciplines directed to risk at present we use two disciplines for trade-off with the risk [5]: a set of disciplines the target of which is the infrastructure security, i.e. security of infrastructure without regard to infrastructure vicinity (security management); and a set of disciplines the target of which is the infrastructure safety, i.e. security and development of both, the infrastructure and its vicinity. Many professional works deal with ensuring the first target, which has been pursued in engineering disciplines since the beginning of 80s [5]. The other discipline target is more ambitious on understanding, accessible data and methods of engineering disciplines. It has been pursued since a half of 80s but from reasons of big demands on: data (there are necessary data on: system, system vicinity, linkages and flows between system and its vicinity); comprehension of problems and their connections in a case of open system of systems; methods of problem structuring, analysis and solving the problems, it is only enforced in domain of nuclear technologies and astronautics [5], namely in spite of it solves interconnection of targets of humans in domains social, environmental and technological [3].

Relevant terms, infrastructures under account and safe critical infrastructure

Regarding to present way of problem solving given above, we use two concepts for ensuring the safe entity [4, 5]; i.e. security management and safety management. The first mentioned concept being simpler is more often used in practice; i.e. the target is the critical infrastructure security and impacts of critical infrastructure on its vicinity are out of interest. The other ensures both, the critical infrastructure security and the security of vicinity of critical infrastructure.
With regards to works [3-5, 9] the definitions of terms connected with security and safety are:

1. Each infrastructure belonging to the critical infrastructure and it alone is a multistage system in which among individual stages in both directions they run material, finance, information and decision flows.

ISSN 2055-6578(Print), ISSN 2055-6586(online)

2. The disasters for partial infrastructures and critical infrastructure are the phenomena that caused damages and losses. They include phenomena belonging to the category „all hazards approach" [10] and specific phenomena connected with humans and their behaviour that do harm the both, the critical infrastructure owners and operators prosperity and the fulfilment of tasks for which they were established (insufficient co-ordination of activities – organising accidents, failure of outsourcing activities, intent attacks etc.).
3. The infrastructure vulnerability is a predisposition of infrastructure (its protected assets) to harm / damage origination.
4. The infrastructure resilience is an infrastructure capability to overcome impacts of a given disaster.
5. The infrastructure risk is a probable size of losses, harms and detriment caused by a disaster with size of normative hazard (mostly design disaster) on infrastructure and public assets or subsystems rescheduled on selected time unit (e.g.1 year), site unit (e.g. 1 km^2) and on basic assets of owners and operators of infrastructure.
6. The infrastructure security is a situation / condition at which the probability of infrastructure assets´ harms, damages and losses is acceptable (it is almost sure that harms, damages and losses cannot origin).
7. The infrastructure safety is a set of measures and activities for ensuring the security and sustainable development of infrastructure, its assets and public assets.
8. The infrastructure security management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded security level of a supply chain.
9. The infrastructure safety management is a planning, organisation, allocation of resources, humans and tasks with aim to reach demanded safety level of infrastructure and its vicinity.
10. The infrastructure safety engineering is a set of engineering measures and activities by which the infrastructure safety is ensured in real conditions of a given site.

With regard to results from analyses of critical infrastructure safety and historical experiences, performed on the data given in the professional literature [1,5,9] and in sources quoted in given works, it is necessary to follow infrastructures for: energy supply, water supply, sewer handling, transport system, communication and information systems, bank and finance system, emergency services (police, fire rescue service, medical rescue service), basic services (food supply, waste liquidation, social services, funereal services), industry, agriculture, state and regional administrations, that are usually supported by the national legislative. To them there is necessary to join the infrastructures for both, the education and the research, which is supported by the EU legislation.

The safety and risk are not complementary quantities even though they together relate by a certain way. In each system both quantities depend on processes, acts and phenomena being under way in a given system and in its vicinity. In advanced concept the concentration to safety has higher targets than concentration to risk because it follows system security, system development, system existence, system vicinity existence and co-existence of different systems [4].

ISSN 2055-6578(Print), ISSN 2055-6586(online)

The risk sources are all phenomena included in the term „all hazards“[10], the phenomena specified in work [4] and further fulfilled during the FOCUS project (from 77 disasters followed now in 2035 the number of disasters increases to 105) [11]. The risks connected with infrastructures are: partial that include risks connected with individual protected assets; integrated that include risks connected with several assets aggregated by a defined way; and integral that include risks connected with all protected assets, with linkages and flows among assets that cause couplings among assets, partial systems and with vicinity. It is clear that to be able to ensure the system safety, the system integral risk needs to be considered, managed and traded-off.

Method of infrastructure safety management model building and method of criticality judgement

With regard to the present knowledge it is necessary to give that for infrastructure safety management fundament, it is the risk analysis, risk assessment and trade-off with risks connected with mutual interconnections in infrastructure sectors and in whole infrastructure (i.e. in agreement with [4] it is necessary to consider interdependences in a system of systems; i.e. at risk identification it is necessary also to use cross-sectional criterions). The procedure of work with risk is shown in Figure 1. It starts with definition of concept of work with risk (system characteristics, determination of assets, specification of aims), on the basis of which risks are identified, analysed, assessed, judged, managed, traded-off and monitored. Feedbacks denoted in this Figure 1 are used if risk level is not on required level [9].

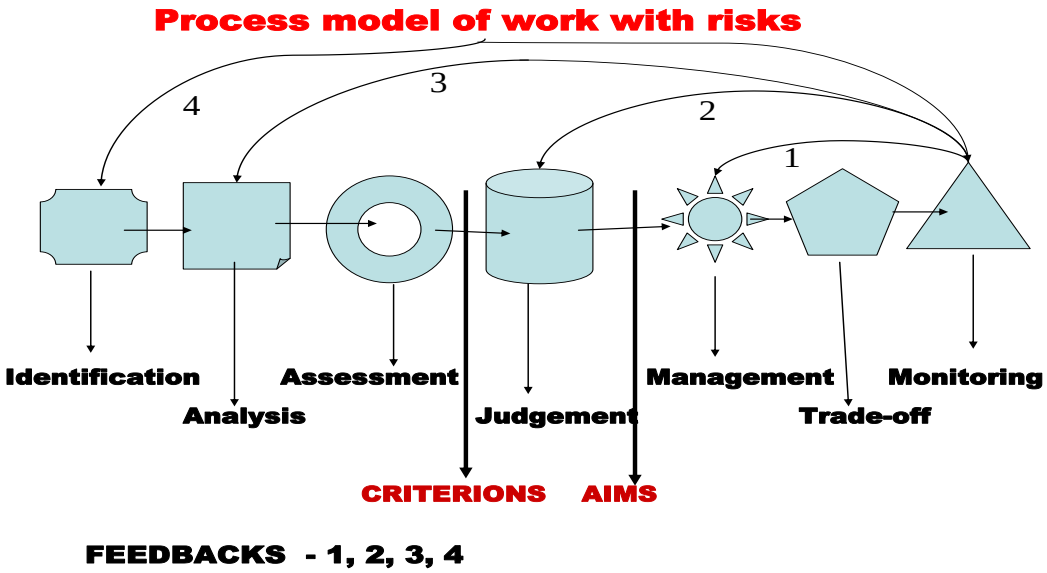

Fig.1. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks

In present practice we distinguish five different concepts for work with system risks, Figure 2, which are summarized and described in work [5].
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 critical spots with a potential to start the system cascade failures,

ISSN 2055-6578(Print), ISSN 2055-6586(online)

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.

The assessment of criticality of individual systems (sectors) of infrastructures and the whole infrastructure is not trivial matter because under different conditions the sectors and the 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 infrastructure criticality but it increases expenses etc.

The purpose of model for infrastructure safety management is to show basic steps by which it is possible to ensure infrastructure security and infrastructure vicinity security. The model building method goes out from a system concept of infrastructures; it considers them as system of systems (several overlapping systems) [4], which means that their complex behaviour, function and development depend on both, the number and properties of partial systems and the diversities of their interconnections, i.e. their linkages and flows among them and also across them. The linkages and flows going across the partial systems are the originators of internal dependences (interdependences). The presented model is created by method of analogy to existing safety management models [3-5].

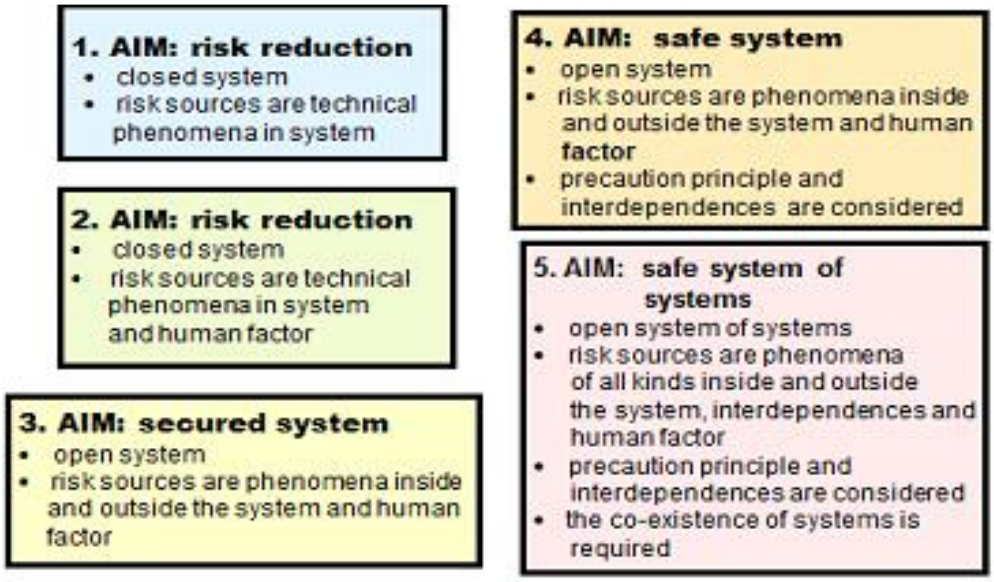

Fig.2. Concepts of risk management and engineering trade-off with risks and their objectives, arranged in chronological order according to the introduction to engineering practice

At infrastructure safety management and whole critical infrastructure safety management we need to concentrate to critical items, and therefore, it is necessary to judge the criticality of individual items. The method for judgement of criticality of individual infrastructures and of whole critical infrastructure is described in [12] and shortly below.

ISSN 2055-6578(Print), ISSN 2055-6586(online)

Model for infrastructure safety management

With regard to: data and knowledge in [3-5, 9, 11-17]; the concept promoted by the OECD [18]; the method described in works [5, 7]; and the assumption that each infrastructure is an open system (i.e. risk sources are internal and external disasters and human factor [3-5]), it is created a model for safety management having ten processes, i.e.:

1. ***Process 1*** that ensures the risk management of disasters, the sources of which are inside and outside of infrastructure plus human factor; i.e. it follows infrastructure and parameters of vicinity in which infrastructure operates. It is composed of: assessment of expected disaster size; determination of occurrence probability of important disasters; judgement of infrastructure vulnerabilities at important disasters; determination of impacts of important disasters on infrastructure. It creates a base for ensuring the safe infrastructure.
2. ***Process 2*** that ensures designing and planning the measures and activities for ensuring the infrastructure security at considering all important disasters [3,10]; i.e.: infrastructure layout (structure, function, sitting, buildings, equipment); performing the measures and activities for ensuring the infrastructure security; plan of renovation of infrastructure after disaster; plan of training the personnel performing the infrastructure; infrastructure activities´ monitoring; and correcting measures and activities for a case of important deviations in infrastructure operation.
3. ***Process 3*** that ensures designing and planning the measures and activities for ensuring the infrastructure vicinity security at considering all important disasters [3,10]; i.e.: infrastructure layout by a way that it may not threaten vicinity, i.e. all public assets; performing the measures and activities for ensuring the infrastructure vicinity security; plan of renovation of infrastructure vicinity after disaster; plan of training the personnel performing the infrastructure; infrastructure activities´ monitoring; and correcting measures and activities for a case of important deviations in infrastructure operation.
4. ***Process 4*** that ensures the harmony among the main activities connected with infrastructure commodities, i.e.: subject of supply (its manufacture, transport and distribution); following the deviations in a process of commodity management; and operating loops. It goes on ensuring the stabilities of processes, the minimisation of delays, the quality and the other critical aspects connected with the operation.
5. ***Process 5*** that ensures the safe assets of infrastructure, i.e. problems connected with: facilities, equipment or services; vehicles; shipping; products; and data systems. It also goes on averting of insiders activities.
6. ***Process 6*** that ensures the safe human sources, i.e. problems connected with: acceptation of employee; understanding the employee behaviour features important for infrastructure operation; employee training; employee self-control; implementation of procedures that ensure correct employee behaviour; and employee stimulation.
7. ***Process 7*** that ensures good business partners, i.e. problems connected with: screening the possible partners; authentication of possible partners; producing the ways of negotiation with partners regarding to their behaviour; monitoring the partners behaviours; and audits of partners.
8. ***Process 8*** that generates the capabilities for overcoming the impacts of extreme disasters that affect infrastructure, i.e. problems connected with: business continuity;

ISSN 2055-6578(Print), ISSN 2055-6586(online)

specific response training; investigation of causes of extreme impacts; assembling the evidences; reparation of harms; and court settlement.

9. ***Process 9*** that ensures the dislocation of criminal and illegal infrastructures and chains, i.e. problems connected with: formation of base for disruption (ensuring the sources, determination of means, logistics, transport of means, distribution of means); and with support of governments and customers.
10. ***Process 10*** that ensures the integral safety of infrastructure, i.e. the coordination of all pillars, i.e. processes directing to infrastructure safety (PSM – process safety management).

The infrastructure safety management model is shown in Figure 3. The base constitutes the concept at which there are determined processes that are important for all infrastructures and the critical infrastructure. On Figure 3 it is evident the principal role of concept on the basis of which the important internal and external processes and phenomena are determined. It is followed by: processes´ monitoring; judgement of impacts of all disasters (i.e. internal and external processes and phenomena) on infrastructure; and determination of optimal measures and activities directed to security of both, the infrastructure and its vicinity. Demands on determination of optimal solution for all processes and phenomena are fundamental [3, 4] because there are under way frequent conflicts among the most suitable measures for some processes [19]. Because the implementation of measures and activities needs sources, forces and means and time for realisation, it is necessary in harmony with [3]: to process program for increase of safety of infrastructure; to determine measures for judgement of safety level in the sense of effectiveness of measures and activities for ensuring the infrastructure safety (indicators); and to fill program by projects that are interconnected and contain processes realising the individual measures and activities.

ISSN 2055-6578(Print), ISSN 2055-6586(online)

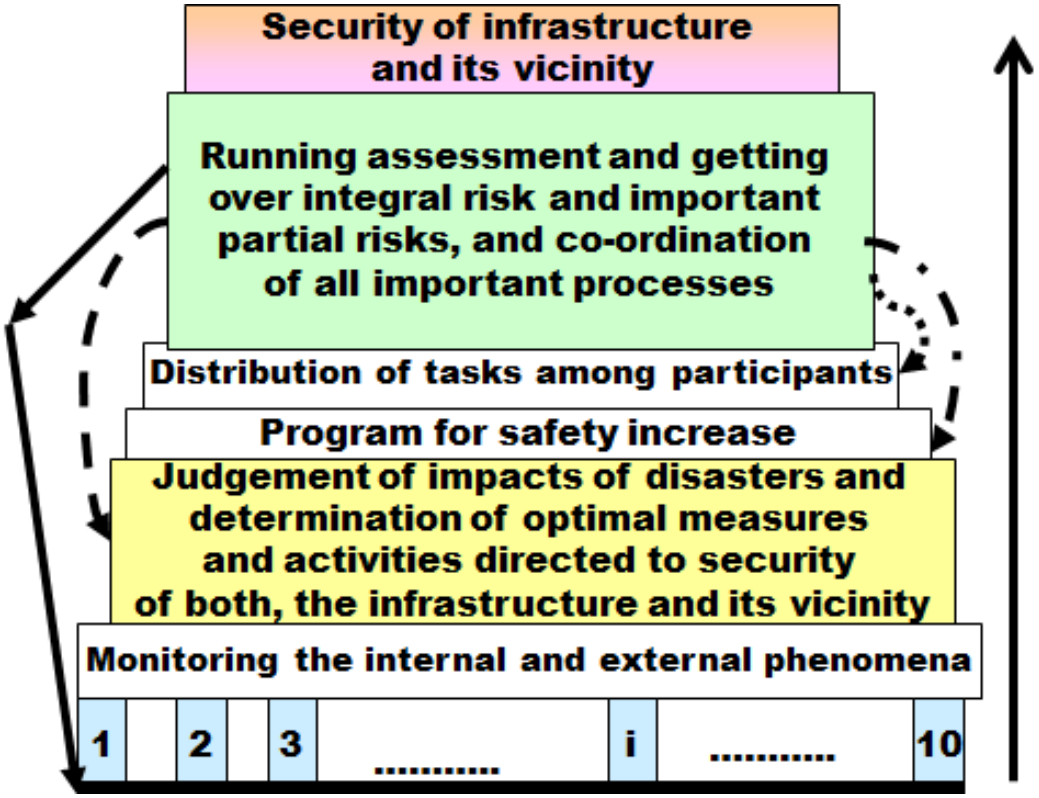

Fig.3. Model of management of infrastructure safety; black block – concept for specification of important processes of infrastructure; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4

The safety management system (SMS) of infrastructure operators includes the organisation structure, responsibilities, practices, rules, procedures and sources for determination and invoking the prevention for disasters that are results of processes inside and outside of infrastructure or at least mitigation of their unacceptable impacts. As a rule it is connected with many aspects, apart from the organisation of employees, identification and assessment of hazard size, risk size, organising system, management of changes, emergency and crisis planning, safety monitoring, audits and scrutiny processes.
With regard to data in works [3, 18] the program for increase of supply chain safety has the following steps:

1. Determination of tasks (partial targets) and strategic goals for infrastructure with regard to safety directed to security of both, the infrastructure and the infrastructure vicinity.
2. For each process that is connected with infrastructure to determine suitable target and running indicators for safety level judgement.
3. To process dictionary for needs connected with integral safety management.
4. To harmonize standards, good practice methods and local procedures.
5. To determine set of target indicators.
6. To determine set of running indicators.
7. To determine way of assessment of target indicators specific for a given supply chain.
8. To determine way of assessment of running indicators specific for a given supply chain.
9. To determine way of assessment of all indicators together and marginal limits for a given infrastructure.

ISSN 2055-6578(Print), ISSN 2055-6586(online)

In practice it means that for each sector of selected authority the target and running indicators are determined and they have form of limits and checklists [3, 18]. To them there are assigned criteria for assessment and scales by which it is determined if target is reached or is not reached. For creation of an effective safety management system the basic principle is that all participants play certain roles and at safety realization they must fulfil these roles (see stage in Figure 3 „distribution of tasks among participants“).

Because the world dynamically changes it is necessary to follow continuously the safety level, i.e. the size of integral risk that includes also the cross-sectional risks connected with interdependences and important partial risks of infrastructure. In case that limits and conditions are not kept, it is necessary to perform changes as shown feedbacks in Figure 3. Because changes requires sources, forces and needs, firstly it is realised feedback 1 and only if it does not ensure expected result the feedback 2 is realised etc. Only in the case of occurrence of extreme phenomena with catastrophic impacts, the feedback 4 is immediately realised.

Safety management system for infrastructure is lean on the concept of disaster prevention or at least of mitigation of severe disaster impacts that include the obligation to introduce and keep the safety management system [3,18] in which the following problems are taking into account:

- roles and responsibilities of persons participating in important hazards management on all organising levels and in ensuring the training,
- plans for systematic identification of important hazards and risks connected with them that are connected with normal, abnormal and critical conditions, and for assessment of their occurrence probability and severity,
- plans and procedures for ensuring the safety of all components and functions, namely including the object and facilities maintenance,
- plans for implementation of changes in territory, objects and facilities,
- plans for identification of foreseeable emergency situations by a systematic analysis including the preparation, tests and judgement of emergency plans for response to such emergency situations,
- plans for continuous evaluation of harmony with targets given in safety concept and in the SMS, and mechanisms for examination and performance of corrective activities in case of failure with aim to reach determined targets,
- plans for periodic systematic assessment of safety concept, effectiveness and convenience of the SMS and of criterions for judgement of safety level by top workers group.

Assessment of capabilities of concepts of risk management and of engineering trade-off with risks applied to critical infrastructure to ensure the territory safety

Individual infrastructures that comprise the critical infrastructure possess the comparable and quite specific items that are mutually incommensurable. From the theoretical viewpoint the model critical infrastructure safety is analogical to this given in Figure 3 but instead of processes 1 – 10 there are infrastructures 1 – 9 (1 - energy system; 2 - water supply system; 3 – sewage system; 4 - transport system; 5 - communication and information systems; 6 - bank and finance system; 7 - emergency services; 8 - basic services; 9 - state and regional administrations). For its capability to cope with abnormal and critical conditions it is

ISSN 2055-6578(Print), ISSN 2055-6586(online)

necessary to create the tool by help of which it is possible by a simple way to control the critical infrastructure safety.

At its production we go from analyses of territories summarised in work [3], i.e. which in each correctly strategically managed territory it is 5 – 7 disasters that can evoke the critical conditions, and according to method described in detail in [12] we:

- use factors that are targeted to protection of protected assets of human system: **1**-rate of capability of protection; **2**-rate of vulnerability; **3**-rate of hazard for human lives and health; **4**-rate of impact on environment; **5**-rate of expensiveness of exchange or repair; **6**-rate of time necessary for exchange or repair; **7**-rate of relevance for ensuring the rescue and emergency functions in territory; **8**-rate of relevance for ensuring the functions of government on levels local, regional and state; **9**-rate of relevance for ensuring the functions of army and police; **10**-rate of redundancy or replaceable service; **11**-rate of relevance for ensuring the communication functions; **12**-rate of impact of supply failure on economy of region (state); **13**-rate of relevance of operability and interoperability; **14**-rate of relevance in domain of symbols and culture,
- determine the scale for criticality rate 0 to 5 (0 - factor contributes to criticality little, …5 - factor contributes to criticality fundamentally); e.g. 0 – losses and damages are lower than 50 EUR, 1 - losses and damages are between 50 – 500 EUR, 2 - losses and damages are between 500 – 5000 EUR, etc. OR sum of maximum values for all 14 factors is ss = 14 x 5 = 70; if real value is more than 95% ss – criticality is extreme high, if real value is more between 70 - 95% ss – criticality is very high; if real value is more between 45 - 70% ss – criticality is high; if real value is more between 25 - 45% ss – criticality is medium; if real value is more between 5 - 25% ss – criticality is low; if real value is more lower than 5% ss – criticality is very low,
- select five or six experts so that all important aspects connected with the human protection and the human system safety are covered who appreciate the real situation with help of all 14 factors for each critical disaster in a given territory and for each concept from five concepts of work with system risks given in Figure 2 (criterions for expert selection are in [9]),
- norm the criticality rate values to values between 0 and 1,
- determine the optimum values of criticality rate for each and each disaster on the basis of assumption that ***safety rate = 1 – criticality rate*** and application of Maximum Utility Theory [20] on safety rate,
- perform the same for the whole critical infrastructure. But here it is problem with lack of knowledge at evaluation of interdependences among individual infrastructures, and therefore, we often use integrated criticality rate (sum of criticality rates of individual infrastructures normed to value between 0 and 1or weighted sum of criticality rates of individual infrastructures normed to value between 0 and 1).

By the evaluation of real values criticality rates we can determine critical spots to which we need to concentrate attention at territory safety upgrade.

Real result for the transport infrastructure in the Czech Republic

Performed detail investigation for transport infrastructure [12] revealed that its criticality is high in the Czech Republic and that the railway transport criticality is very high. From works [21, 22] it follows that at reaching the threshold value for criticality rate “high”, it is necessary from reason of protection of inhabitants and economic sphere to carry out preventive, mitigation and reactive measures and activities. Because measures against one disaster may be disserviceable

ISSN 2055-6578(Print), ISSN 2055-6586(online)

against another one [19], it is necessary to seek for optimum for all possible disasters in a given territory that belong to critical ones as the strategic management principles stipulate [3].

Real result of assessment of concepts of risk management and of engineering trade-off with risks applied to critical infrastructure to ensure the territory safety

The results of research for whole critical infrastructure [23], based on the application of the Maximum Utility Theory [20], which dealt with the evaluation of the criticality rates of concepts of risk management and trade-off with risks (Figure 2), show that none of the concepts, used today for the management and trade-off with risks, has not a negligible rate of criticality, Figure 4, taking into account the assets of the human system (i.e. human lives, health and security; property and welfare; environment; critical infrastructures and technologies), i.e. the rate of criticality in the application:

- the classical concept of risk management and engineering trade-off with risk (case 1 in Figure 2) is extremely high,
- the classical concept of risk management and engineering trade-off with risk considering the human factor (case 2 in Figure 2) is very high,
- the concept of management and engineering trade-off with risk focused on secure system (case 3 in Figure 2) is high,
- the concept of management and engineering trade-off with risk focused on safe system (case 4 in Figure 2) is the medium,
- the concept of management and engineering trade-off with risk focused on the safe system of systems (case 5 in Figure 2) is low.

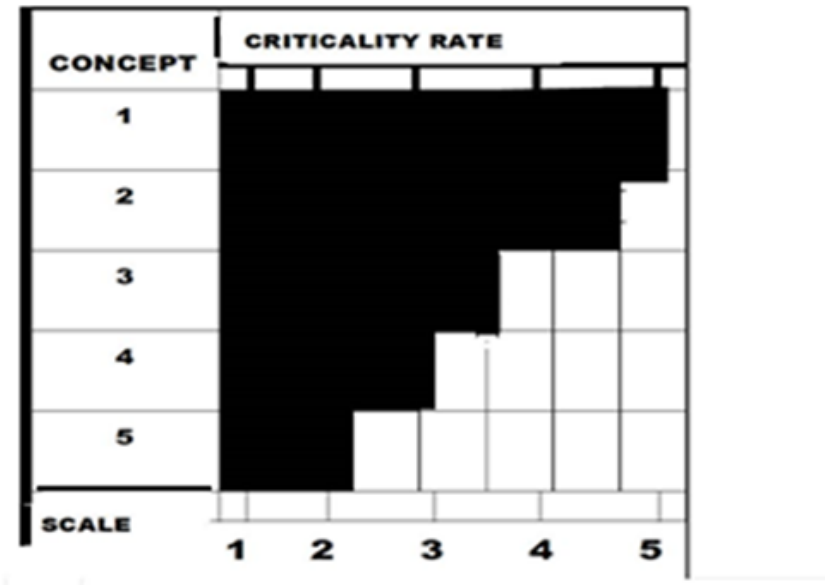

Fig. 4. The criticality rate of concepts for risk management and trade-off with risks: 1 – the classic concept of risk management and trade-off with risks; 2 – the classic concept of risk management and trade-off with risks considering the human factor; 3 – the concept of risk management and trade-off with risks focused on secure system; 4-the concept of risk management and trade-off with risks focused on the safe system; and 5 - the concept of risk management and trade-off with risks focused on the safe system of systems

ISSN 2055-6578(Print), ISSN 2055-6586(online)

CONCLUSION

Model for safety management of infrastructures compiled on the basis of present knowledge is the process model in which they are represented the both, the individual important elements of process of safety management, and the feedbacks by which it is possible to correct cases in which demands of safety are not fulfilled. For application in practice the model for critical infrastructure safety management is supplemented by mechanism for ensuring the capability to be effective at abnormal and critical conditions.
To ensure the critical infrastructure safety it is necessary to use the concept of work with system risks which is directed to system of systems safety.

REFERENCES

[1] UN. Human development report. New York 1994, www.un.org.
[2] EU. Safe Community. PASR projects, Brussels 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] PROCHÁZKOVÁ D. Safety of critical infrastructure (in Czech). ISBN: 978-80-01-05103-0. Praha: ČVUT 2012, 318p.
[6] PROCHÁZKOVÁ D. Critical infrastructure safety management. In: Reliability, Risk and Safety. []Theory and Applications. ISBN 978-0-415-55509-8, CRC Press / Balkema, Leiden 2009, pp 1875-1882, CD ROM, ISBN 978-0-203-85975-9.
[7] PROCHÁZKOVÁ D. Identification and management of risks of system of systems. In: Proceedings. ISBN: 978-1-62276-436-5. IPSAM & ESRA, Helsinki 2012, pp 6542-6551
[8] PROCHÁZKOVÁ D. Identification and management of risks of system of systems. International Journal of Computer an Information Technology, ISSN: 2279-0764, 2 (2013), No 2, 232-239. http://ijcit.com/current.php
[9] PROCHÁZKOVÁ D. Principles of management of safety of critical infrastructure (in Czech). ISBN: 978-80-01-05245-7. Praha: ČVUT 2013, 213p.
[10] FEMA. Guide for all-hazard emergency operations planning. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[11] EU. FOCUS project. Brussels: EU. www.focusproject.eu
[12] PROCHÁZKOVÁ D. Criticality of transport infrastructure (in Czech). Periodica Academica, ISSN 1802-2626, VIII (2013), No. 2, pp 112-128.
[13] STEIN W., HAMMERLI B., POHL H., POSCH R. (eds). Critical infrastructure protection – status and perspectives. Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[14] MOTEFF J., COPELAND C., FISCHER J. Critical infrastructures: What makes an infrastrucuture critical? Report for Congress, 2003, CRS Web, Order Code RL31556.
[15] CISP. Workshop on critical infrastructure protection and civil emergency planning-dependable structures, cybersecurity, commnon standard. Zurich: Centre for International Security Policy 2005, www.eda.admin.ch
[16] RINALDI S. M. Modelling and simulating critical infrastructures and their interdependencies. In: Proceedings of the 37th Hawaii International Conference on System Sciences–2004. Sandia: Sandia National Laboratories 2004 http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1265180

ISSN 2055-6578(Print), ISSN 2055-6586(online)

[17] RINALDI S. M., PEERENBOOM J. P., KELLY T. K. Critical infrastructure interdependencies (identifying, understanding, and analysing). IEEE Control Systems Magazine, Vol. 21, December 2001, pp.12-25. www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf
[18] 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.
[19] PROCHÁZKOVÁ D. Methodology for estimation of costs for renovation of property at territories affected by disaster (in Czech). SPBI SPEKTRUM XI Ostrava 2007, ISBN 978-80-86634-98-2, 251p.
[20] KEENY, R.L., RAIFFA, H. Decision analysis with multiple conflicting objectives. New York: J. Wilex 1976
[21] US. Guide for Critical Infrastructure Protection. US government, Washington 2005.
[22] EMA. Critical infrastructure emergency risk management and assurance. Handbook Emergency Management Australia, 2003, www.ema.gov.au
[23] PROCHÁZKOVÁ, D. Optimum concept of management and trade-off with risks. Safety and Reliability: Methodology and Application. ISBN 978-1-138-02681-0. CD ROM. London: Taylor & Francis Group 2015, pp 1463-1471.

Acknowledgment:
The work was supported by the Czech Technical University in Prague and by the EU – FOCUS project. Authors thank for support.

ISSN 2055-6578(Print), ISSN 2055-6586(online)