UDC 005.93:004.056

D. PROCHAZKOVA, J. PROCHAZKA

Czech Technical University in Prague, Faculty of Transportation Science, Praha, Czech Republic

MODEL OF CRITICAL INFRASTRUCTURE SAFETY MANAGEMENT

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 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.

Key words: *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 integral risk of a given system by increase of cross-section risks of system of systems [4-6]. As a consequence of growing globalisation the new sources of disasters take on force, it goes on critical infrastructure failures. 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.

1. 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 must 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.

2. Safe critical infrastructure and relevant terms

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 the following:

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.

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.

3. Infrastructures under account

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 supported by the Czech 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]. 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 [11]. 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.

4. 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. Feedbacks denoted in this Figure 1 are used if risk level is not on required level [9]. 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.

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 presented model is created by method of analogy to existing safety management models [3-5].

At infrastructure safety management and whole critical infrastructure safety management we must concentrate to critical items, and therefore, it is necessary to judge their criticality. The method for judgement of criticality of individual infrastructures and of whole critical infrastructure is described in [20].

5. Model for infrastructure safety management

With regard to data and knowledge in [3-5, 9-17], 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.

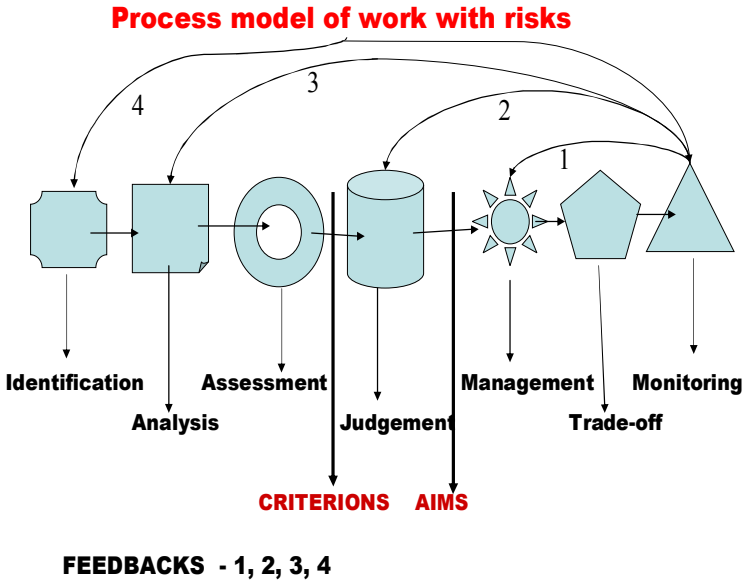

Fig. 1. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks

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; 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 2. The base constitutes the concept at which there are determined processes that are important for all infrastructures and the critical infrastructure. On Figure 2 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.

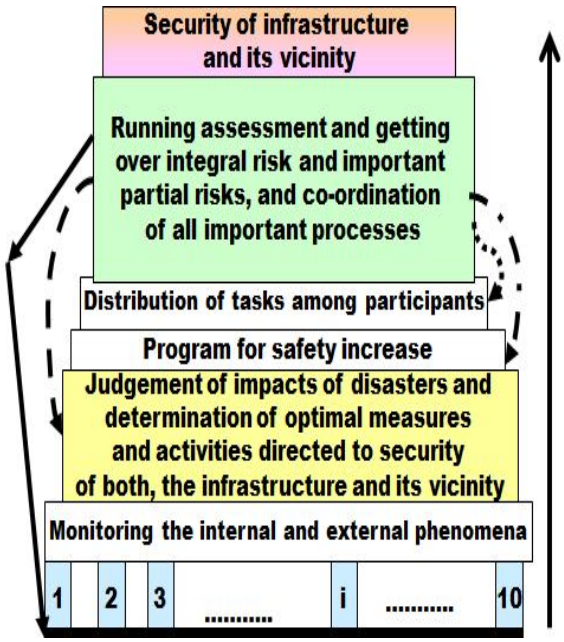

Fig. 2. Model of management of infrastructure safety; black block – concept for specification of important processes of infrastructure; dotted line – feedback 1; broken line – feedback 2; dashed line – feedback 3; full line – feedback 4

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.

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 1. 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.

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.

References

1. UN. Human development report [Elactronic resource] / New York, 1994. – Available to: http://www.un.org.

2. EU. Safe community [Text] / PASR projects, Brussels, 2004.

3.Procházková, D. Strategické řízení bezpečnosti území a organizace [Text] / D. Procházková // ISBN: 978-80-01-04844-3. – ČVUT, Praha, 2011. – 483 p.

4. Procházková, D. Analýza a řízení rizik [Text] / D. Procházková // ISBN: 978-80-01-04841-2. – ČVUT, Praha, 2011. – 405 p.

5. Procházková, D. Bezpečnost kritické infrastruktury [Text] / D. Procházková // ISBN: 978-80-01-05103-0. – ČVUT, Praha, 2012. – 318 p.

6. Procházková, D. Critical infrastructure safety management. in: reliability, risk and safety. theory and applications [Text] / D. Procházková // ISBN 978-0-415-55509-8. – Balkema, Leiden, 2009. – P. 1875-1882.

7. Procházková, D. Identification and management of risks of system of systems [Text] / D. Procházková // In: Proceedings. ISBN: 978-1-62276-436-5. – IPSAM & ESRA, Helsinki, 2012. – P. 6542-6551.

8. Procházková, D. Identification and management of risks of system of systems [Text] / D. Procházková // In: International Journal of Computer an Information Technology. – ISSN: 2279-0764. – 2013. – Vol. 2, No 2.– P. 232-239.

9. Procházková, D. Základy řízení bezpečnosti kritické infrastruktury [Text] / D. Procházková // ISBN: 978-80-01-05245-7. – ČVUT, Praha, 2013. – 213 p.

10. FEMA. Guide for all-hazard emergency operations planning. state and local guide (SLG) 101 [Text] / FEMA, Washinton, 1996.

11. EU. FOCUS project [Electronic resource]. – Available to: http://www.focusproject.eu.

12. ISO. Risk management principles and guidelines [Electronic resource]. – Available to:.www.iso.org/iso/cataloguedetail?csnumber=43170. – Nov., 2011.

13. Critical infrastructure protection – status and perspectives [Electronic resource] / W. Stein, B. Hammerli, H. Pohl, R. Posch (eds) // Workshop on CIP, Frankfurt am Main. – Available to: http://www.informatik2003.de.

14. Moteff, J. Critical infrastructures: what makes an infrastrucuture critical ? [Text] / J. Moteff, C. Copeland, J. Fischer // Report for Congress. – CRS Web, Order Code RL31556. – 2003.

15.CISP. Workshop on critical infrastructure protection and civil emergency planning-dependable structures, cybersecurity, commnon standard. – Zurich, 2005, Centre for International Security Policy [Electronic resource]. – Available to: http://www.eda.admin.ch.

16. Rinaldi, S. M. Modelling and simulating critical infrastructures and their interdependencies [Electronic resource] / S. M. Rinaldi // In: Proceedings of the 37th Hawaii Int. Conf. on System Sciences, 2004, Sandia National Lab. – Sandia, 2004. – Available to: http://explore.ieee.orgpl/freeabs_all.jsp?arnumber= 126518.

17. Rinaldi, S. M. Critical infrastructure interdependencies. (identifying, understanding, and analysing) [Electronic resorce] / S. M. Rinaldi // In: IEEE Control Systems Magazine. – 2001. – Vol. 21. – P. 12-25. – Available to. http://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, prepa-redness and response [Text] / OECD, Paris, 2002. – 191 p.

19. Procházková, D. Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou [Text] / D. Procházková // ISBN 978-80-86634-98-2SPBI. – SPEKTRUM XI, Ostrava, 2007. – 251 p.

20. Procházková, D. Kritičnost dopravní infrastruktury [Text] / D. Procházková // In:Periodica Academica. – ISSN 1802-2626. – 2013. – Vol. 8, №2. – P. 78-86 .

21. US. Guide for critical infrastructure protection [Text] / US government, Washington, 2005.

22. EMA. Critical infrastructure emergency risk management and assurance. Handbook emergency management Australia, 2003 [Electronic resource]. – Available to: http://www.ema.gov.au.

Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 25.03.2013

Рецензент: канд. техн. наук, доц. Е. В. Брежнев, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина.

МОДЕЛЬ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Д. Прохазкова, Ж. Прохазка

В эпоху глобализации безопасность общества напрямую зависит от уровня безопасности критических инфраструктур, которые территориально обеспечивают людей такими необходимыми услугами, как поставки энергии, водоснабжения, продовольствия, доступа к информации и т.д. Произошедшие недавно события, связанные с критическими инфраструктурами, указывают на их особую важность. Критические инфраструктуры представляют собой многоуровневые взаимно дублируемые системы, т.е. большие сложные системы, разнообразные вложенные системы. Данная статья представляет модель управления безопасностью критических инфраструктур, позволяющую легко определить как критичность отдельных инфраструктур, так и общей инфраструктуры.

Ключевые слова: критическая инфраструктура; обеспечение территориальных услуг; информационная безопасность; функциональная безопасность; модель управления безопасностью.

МОДЕЛЬ КЕРУВАННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУР

Д. Прохазкова, Ж. Прохазка

В епоху глобалізації безпека суспільства залежить від рівня безпеки критичних інфраструктур, що територіально забезпечують людей такими необхідними послугами, як поставленням енергії, водопостачанням, продовольчими товарами, доступом до інформації і т.п. Нещодавні події, пов'язані із критичними інфраструктурами, вказують на їх особливу важливість. Критичні інфраструктури є багаторівневими взаємно дубльованими системами, тобто великими складними системами, різноманітними вкладеними системами. Дана стаття описує модель керування безпекою критичних інфраструктур, що дозволяє легко визначити як критичність окремих інфраструктур, так і загальної інфраструктури.

Ключові слова: критична інфраструктура; забезпечення територіальних послуг; інформаційна безпека; функціональна безпека; модель керування безпекою.

Прохазкова Дана – д-р техн. наук, проф., Чешский Технический Университет, Прага, Чехия, e-mail: Dr.Prochazkova.Dana@seznam.cz.

Прохазка Жан – канд. наук, Чешский Технический Университет, Прага, Чехия, e-mail: japro2am@seznam.cz.