

Mezinárodní konference „Critical Infrastructure Safety and Security (CrISS-Dessert´11)“

Ve dnech 11. – 13.5.2011 se v Kirovogradu (Ukrajina) uskutečnila mezinárodní konference „Critical Infrastructure Safety and Security (CrISS-Dessert´11)“. Pořadatelem konference byla National Aerospace University s podporou IEEE (Institute of Electrical and Electronics Engineers), Research and Production Corporation RADIY a dalších. Účastníků konference bylo 105 z 10 zemí (UK, USA, Kanada, ČR, Řecko, Bulharsko, Ruská Federace, Irán, Ukrajina, Gruzie).

Doc. RNDr. D. Procházková, DrSc. přednesla 2 sdělení s problematikou projektu FOCUS, a to: *Principles of Mitigating and Managing the Human System Risks; Overview of Fine Exact Methods of Safety Engineering*. Z konference byl vydán dvoudílný sborník „Critical Infrastructure Safety and Security (CrISS-Dessert´11)“ pod záštitou IEEE. **Výstupy v něm spojené s projektem FOCUS jsou:**

1. D. Procházková: *Principles of Mitigating and Managing the Human System Risks*. In: Critical Infrastructure Safety and Security (CrISS-Dessert´11). ISBN 978-966-662-226-9. National Aerospace University, Kirovograd 2011,v1, 4-22.

Abstract: Security situation in the world and in each territory continuously changes with time, and therefore, there is formed new safety culture that takes into account actual knowledge and experiences with interdependences among the public assets leading to extreme social crises. With regard to the historical development of human activities related to fight with disasters there are: a lot of preventive and mitigation measures that have been applied into practice by legal rules, technical standards and norms and public instructions; response systems; and renovation ways. These ensure protection against to design basis disasters and not to severe impacts of beyond design disasters and to unexpected impacts of random combination of interdependences that are as a rule the causes of catastrophes. Problem solving the complex territory safety related to all public assets requires proactive, strategic risk management based on qualified data, methods, knowledge and good practices techniques application. The paper summarizes the set of principles that ensures the qualified decision-making for risk management in the sense of risk governance at all life stages directed to human security and sustainable development. The account is only directed to the most important domains connected with effective risk management.

2. D. Procházková: *Overview of Fine Exact Methods of Safety Engineering*. In: Critical Infrastructure Safety and Security (CrISS-Dessert´11). ISBN 978-966-662-226-9. National Aerospace University, Kirovograd 2011,v1, 65-72.

Abstract: The safety, security and risk engineering are systematic use of general findings, engineering knowledge and experiences for: ensuring safe object from internal hazards (risk engineering); from internal and external hazards (security engineering); and in present concept for optimising the protection of human lives, environment, property and economic affairs (safety engineering). From the professional view it goes on process seeking all potential conditions that could threaten favourable operation of a given system in all stages of its life cycle, and identifying the capabilities for their defeating by prevention, preparedness, response and renovation. It uses tools, methods and techniques that indicate how we could: texturize the problem; determine what we ought to solve; collect and create data sets so they might have a clear evidence to a given problem; select method for data processing so outputs might be relevant to a given problem; interpret the outputs in given conditions. Therefore, it uses a family of exact methods, tools and techniques and present work contains the survey of their fine members and it proposes their systemization.

3. D. Procházková: *Safety Management of Critical Infrastructure*. In: Critical Infrastructure Safety and Security (CrISS-Dessert´11). ISBN 978-966-662-226-9. National Aerospace University, Kirovograd 2011,v1, 102-112.

Abstract: The critical infrastructure is a set of mutually interconnected networks, i.e. the systems of various sectors of human system. An interconnection of systems means the mutual dependence. Therefore, in linkage with the safe critical infrastructure and with sustainable development potential there is necessary to solve several problems, namely safety of partial infrastructures and safety of a set of mutually dependent infrastructures. With regard to a present knowledge we know that the optimum safety of the set of infrastructures there is not the set of optimum safeties of partial infrastructures, and therefore, we must search for solution by other way. The work indicates a possible approach for solution acquisition.

4. D. Procházková: *Critical Infrastructure is Prerequisite for Region Safety*. In: *Critical Infrastructure Safety and Security (CrISS-Dessert'11)*. ISBN 978-966-662-226-9. National Aerospace University, Kirovograd 2011, v1, 153-163.

Abstract: The paper describes the specific properties of the Critical Infrastructure (CI). By help of analyses of selected cases of CI failures and by theoretical analysis of behaviour of the System of Systems (SoS) partial systems and the whole CI with the What, If method and with the All Hazard Approach use there are determined for 6 important disasters in the Czech Republic both, the direct impacts on partial infrastructures and the impacts at which the failure of one infrastructure was transferred by cascade form to another infrastructures. With regard to these data there are identified on the technical and operating / managerial levels the corresponding sources of risks. Because the CI is complex SoS, the responsibilities for critical infrastructure safety in a region have all stakeholders. On the data set used there are specified problems in 5 professional domains and in each of them there are determined critical items. From the comprehensible reasons the special attention is devoted to the public protection.

Získané poznatky:

1. Problematika kritické infrastruktury (KI) je chápána jako zásadní. Její bezpečí a bezpečnost jsou skloňovány výzkumníky, zástupci veřejného i privátního sektoru.
2. Analýza referátu zúčastněných ukázala, že legislativní zabezpečení ochrany KI mají USA, Kanada a země EU (Bulharsko, ČR, Řecko, UK). Ruská Federace připravuje legislativu. Ostatní země se věnují problematice KI jen v oblasti výzkumu.
3. USA, Kanada a země EU používají terminologii založenou na doporučení UN z r. 1994 a INSAG z r. 1986, tj. rozlišují stav (security) a soubor opatření a činností, kterými lidé stav zajišťují (safety). Země bývalého SSSR zatím neodlišují pojmy bezpečnost a bezpečí a utápějí se v opisech problémů; nepoužívají pojem SoS, ale komplexní systém.
4. Model řízení bezpečnosti používaný v Ruské Federaci a na Ukrajině má fáze: prevence; ochrana; monitoring; včasné varování + detekce; reakce; řízení důsledků; obnova. V některých referátech se použila definice, že ochrana = prevence + detekce + odezva.
5. Charakteristiky KI: velké množství aktérů; rozrůstající struktura a vnitřní vazby; nelineární zpětné vazby; složitá adaptace; propojené odpovědnosti; mnoho vlastníků; alternativy; složitě chování v proměnných podmínkách. Je třeba pečovat o integritu (celistvost), transparentnost a odpovědnosti.
6. Problémy KI byly v řadě referátů řešeny staticky a deterministicky. V některých referátech byl použit stochastický přístup s tím, že varianty byly generovány metodou Monte Carlo.
7. V referátech o modelech KI, které respektovaly dynamiku problému, byla snaha o přesné řešení (matematicky velmi dobré; problémově trochu nereálné, protože na

základě disponibilních údajů neznáme všechny parametry, které předurčují chování KI v čase a prostoru).

8. Výsledky prezentovaných referátů vycházely z aplikace Markovových procesů, shlukové analýzy, FMEA a některé z aplikace Fuzzy sets. Referáty přednesené doktorandy byly metodicky správné, ale nevycházely z reálných dat,
9. Kritičnost systémů i KI byly oceňovány pomocí sestavené hierarchie (realita – nepřihlíželo se k tomu, že ve skutečnosti jsou řešení výrazně site specific).
10. Analýza Three Mile Islands 28.3.1979 – loss of normal water supply to diesel generator. Analýza Černobyli 26.4.1986 a Forsmark 25.7.2006 – loss of normal electric energy. Do dneška se používalo jen single failure criterion, po havárii v JE Fukushima se očekává změna, tj. zpřísněné kritérium – posun k vyšší bezpečnosti.