Sborník vědeckých prací Vysoké školy báňské – Technické univerzity Ostrava
číslo 1, rok 2007, ročník LIII, řada bezpečnostní inženýrství

Dana PROCHÁZKOVÁ*

SHRNUTÍ VÝSLEDKŮ REŠERŠE ZAMĚŘENÉ NA OCHRANU KRITICKÉ INFRASTRUKTURY*)

SUMMARY OF RESULTS OF BIBLIOGRAPHIC SEARCH AIMED TO CRITICAL INFRASTRUCTURE PROTECTION

*) ***Výsledky projektu MV ČR „Procesní analýza zranitelnosti prvků kritické infrastruktury“.***

Abstrakt

Článek obsahuje výsledky rešerše literatury a dokumentů pojednávajících o ochraně kritické infrastruktury. Předmětem rešerše bylo 204 zdrojových materiálů. Na základě dokumentů EU a sdělení představitelů EU se připravují podklady pro osnovu operačních plánů na ochranu kritické infrastruktury. EU se však zajímá jen o kritickou infrastrukturu důležitou pro EU, ostatní ponechává na členských státech. Na úrovni EU a vládních úřadů členských zemí EU se především řeší definice kritické infrastruktury a právní zajištění ochrany kritické infrastruktury. Nejčastěji se v souvislosti s kritickou infrastrukturou zvažují teroristické útoky a kybernetická infrastruktura jako oblast jejich cílů.

Abstract

The paper concentrates the results of bibliographic search of literature and documents dealing with critical infrastructure and its protection. There were used 204 sources. With regard to the EU documents and the EU announcements there are prepared the data for outline of operating plans for critical infrastructure protection. The EU itself is just interested in the critical infrastructure important for the EU, the other it leaves to Member States. On the EU level and on the Member States Authorities there is above all dealt with the definition of the critical infrastructure and with the legal ensuring the critical infrastructure protection. In connection with the critical infrastructure protection much often there are considered the terrorist attacks and a cyber infrastructure as a domain of their targets.

Key words: critical infrastructure, protection, process analysis.

doc., RNDr., DrSc., Policejní akademie České republiky, Praha, prochazkovad@polac.cz

1. Úvod

Předmětem rešerše byly dva úseky, a to:

1. Procesní analýza. Zmapování a popsání metod a principů vhodných pro provedení procesní analýzy, pro hledání kritických vazeb mezi jednotlivými prvky kritické infrastruktury.
2. Zmapování přístupů používaných v zemích EU (USA) a ČR při vyhledávání kritických míst napříč kritickou infrastrukturou.

Předložená práce obsahuje vyhodnocení znalostí uvedených v literatuře domácí i zahraniční a je zpracována na základě údajů z 204 odborných prací, viz příloha a práce (Procházková 2006a). Aby bylo zřejmé k čemu se poznatky vztahují, je použit koncept ochrany kritické infrastruktury (Procházková 2006b) sestavený dle odborné literatury a zkušeností autorky z praxe.

2. Současný stav

V České republice existují dva téměř nesmiřitelné tábory, které se zabývají ochranou kritické infrastruktury, proto je při rešerši především zahraniční literatury hledána odpověď na to, který přístup je ve vyspělých zemích více obvyklý nebo za jakých podmínek se jednotlivé přístupy používají. První tábor, do kterého patří odborníci z oblasti územního plánování, navrhování, projektování, výstavby, provozování, oprav a údržby objektů, infrastruktur a technologií, tvrdí, že procesní model pro ochranu funkčnosti kritické infrastruktury je procesní model založený na řízení bezpečnosti, který obsahuje všechny lidské činnosti v oblasti řízení a opírá se v nich o dosavadní poznání. Druhý tábor, do kterého především patří odborníci zabývající se odezvou na mimořádné události, tvrdí, že procesní model pro ochranu funkčnosti kritické infrastruktury je procesní model opírající se o robustní výkonné složky, které zvládnou vše.

Na základě filosofických konceptů OSN, IAEA (Mezinárodní agentura pro atomovou energii), OECD, OTA (Office for Technology Assessment v USA 1972-1996), EU (především koncept a směrnice jak aplikovat v praxi princip předběžné opatrnosti) aj. je v závěru ukázáno, že koncept první je účinnější a zaručuje aplikaci současného poznání a zkušeností do oblasti zajišťování bezpečnosti a udržitelného rozvoje lidského systému. Je strategický, proaktivní a zajišťuje řešení problémů v nadčasovém rozměru. Druhý koncept je pouze reaktivní a jeho úkolem je zvládnout momentální problémy. To znamená, že připravuje plány odezvy včetně plánů zásahů výkonných složek, které obsahují účinnou reakci na situaci a efektivní zvládnutí nastalých problémů.

Z hlediska zásad teorie řízení druhý způsob obsahující de facto jen organizační opatření se dle OTA (Office for Technology Assessment) používá jen tehdy, když nelze aplikovat zásadní technická opatření. Proto je třeba, aby tam, kde je to možné se pro ochranu kritické infrastruktury používal procesní model založený na proaktivním a strategickém přístupu. To však neznamená, že nebudou rozpracovávány popisy nouzových situací a návrhy (scénáře) pro jejich úspěšné vyřešení, které musí v zájmu stabilizace a rozvoje lidského systému:

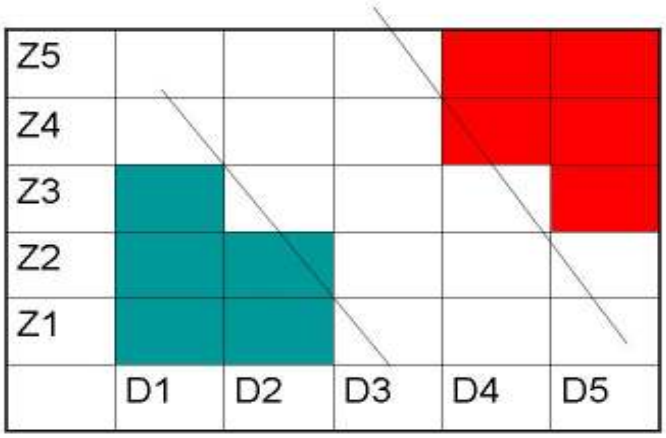
- znát výkonné složky i veřejná správa, aby byly schopné provést účinnou a cílenou odezvu,
- nacvičit výkonné složky, aby byly schopné provést kvalitní zásah, který je základem pro úspěšné zvládání nouzových i kritických situací, které z hlediska poznání patří do dynamického vývoje lidského systému, který je modelem prostoru, v němž žijí lidé.

3. Shrnutí výsledků pro rešerši 1

Publikace, které jsou uvedené v příloze (Seznam použitých zdrojů) a které popisují metody a principy vhodné pro provedení procesní analýzy a pro hledání kritických vazeb mezi jednotlivými prvky kritické infrastruktury, ***vychází z příčin, tj. z živelních a jiných pohrom a nebo z vnitřních vazeb***, které jdou napříč jednotlivými infrastrukturami nebo napříč několika infrastruktur (elektrická energie, informační technologie, antropogenní řízení, finanční toky) a ***ne ze stavů, tj. nouzových situací, mezi které patří v ČR také mimořádné události***, které výše uvedené příčiny vyvolají[**)].

Procesní analýza se provádí tak, že se:

1. *Aplikuje koncept řízení bezpečnosti s tím, že se zváží celý proces spojený s existencí kritické infrastruktury, tj. umisťování, navrhování, projektování, výstavba, provozování a změny.*
2. *Procesní model sestaví pro celý proces spojený s existencí kritické infrastruktury a teprve pro dílčí úkoly se z celého procesního modelu vybírají modely pro dílčí části nebo se vytváří vysoce podrobné modely pro části, které jsou předmětem určitého speciálního zájmu.*
3. *Používá se přístup „ALL HAZARD APPROACH". To znamená, že se zajišťuje ochrana proti všem relevantním živelním a jiným pohromám, a to dle zákonů, norem, standardů a přístupů dobré praxe pro územní plánování, výběr míst, navrhování, projektování, výstavba, provozování, opravy, údržby, změny a obnovy.*
4. *Používají se vhodné metody rizikového inženýrství, a to jak k určení velikostí rizik, tak k určení prioritních rizik, které nejvíce přispívají ke zranitelnosti dané infrastruktury.*
5. *Rizika se chápou jako ztráty, škody a újmy na chráněných zájmech v konkrétním místě, tj. ne jako čísla bez jasného vyjádření negativního potenciálu. S takto určenými riziky se vyjednává s cílem snížit ztráty, škody a újmy na chráněných zájmech v daném místě.*
6. *U existujících infrastruktur se zjistí stávající rizika, stanoví se ta rizika, která nejvíce přispívají ke zranitelnosti dané infrastruktury a vůči nim se provede zodolnění, je-li to možné a především se připravují vnitřní nouzové plány, plány kontinuity a popř. i plány krizové.*
7. *Pro vyhledávání kritických vazeb mezi jednotlivými prvky kritické infrastruktury se nejčastěji používají rozhodovací matice. Protože praxe čas od času vyžaduje také řešení specifických úkolů, pro které aplikace matice kritičnosti (tj. rozhodovací matice pro vyhledání kritické infrastruktury nebo kritických prvků, vazeb a toků dané kritické infrastruktury) je příliš hrubým nástrojem, jsou používány metody preciznější založené na teorii grafů, a to např. metoda kritické cesty (tzv. CPM), metoda optimalizace řešení problému v čase a prostoru (tzv. PERT) a metoda modelování procesů v síti (tzv. Petriho sítě)* (Procházková 2006c). Příklad matice kritičnosti je na obrázku 1.
8. *Pro zajištění funkčnosti kritické infrastruktury v prostoru a čase se používají specifické kontrolní seznamy. Tato metoda je především obvyklá u veřejné správy a u inspekčních orgánů* (Procházková et al. 2006).



Matice kritičnosti infrastruktury a technologií v území.

(zranitelnost vs. důležitost; zásadní parametr je čas)

Obr. 1. Matice kritičnosti infrastruktury a technologií v území, tj. zranitelnost vs. důležitost infrastruktury v území.

Poznámka:

***) Žádný ze zdrojů, které jsou v seznamech literatury neobsahuje v souvislosti se zajištěním funkčnosti kritické infrastruktury pojem mimořádná událost, tj. v anglicky psané literatuře pojem „Extraordinary Event" a v německy psané literatuře pojem „außerordrntlicher Vorfall". V oblasti dostupné ruské literatury nebyly nalezeny příslušné souvislosti. Všechny uvedené zdroje, které se zabývají hledáním příčin selhání kritické infrastruktury a opatřeními na zodolnění kritické infrastruktury vycházejí z toho, že pro zajištění ochrany kritické infrastruktury jsou nutné znalosti jako je fyzikální naturel živelní či jiné pohromy, fyzikální mechanismus působení živelní či jiné pohromy na chráněné zájmy, fyzikální naturel území, objektu, technologie, infrastruktury, na které působí živelní či jiná pohroma, a fyzikální příčiny synergence uvedených aspeků.*

4. Výsledky pro rešerši 2

Všechny publikace, které jsou uvedené v příloze (Seznam použitých zdrojů) popisují metody a principy vhodné pro provedení procesní analýzy a pro hledání kritických vazeb mezi jednotlivými prvky kritické infrastruktury ***vychází z příčin, tj. z živelních a jiných pohrom a nebo z vnitřních vazeb***, které jdou napříč jednotlivými infrastrukturami nebo napříč několika infrastruktur (elektrická energie, informační technologie, antropogenní řízení, finanční toky) a ***ne ze stavů, tj. nouzových situací mezi které patří v ČR také mimořádné události***, které výše uvedené příčiny vyvolají[**)].

Kritická místa napříč kritickou infrastrukturou se vyhledávají u stávající infrastruktury tak, že se používá přístup „ALL HAZARD APPROACH" (tj. sleduje se úroveň ochrany proti všem relevantním živelním a jiným pohromám možným v daném místě, a to tak, že:

1. *Používají se vhodné metody rizikového inženýrství založené na multikriteriálních metodách.*

2. *Rizika se chápou jako ztráty, škody a újmy na chráněných zájmech v konkrétním místě, tj. ne jako čísla bez jasného vyjádření negativního potenciálu. S takto určenými riziky se vyjednává s cílem snížit ztráty, škody a újmy na chráněných zájmech v daném místě.*
3. *Pro speciální cíle se definují dílčí procesní modely tak, aby byly transparentní a aby bylo možno jejich použitím získat výsledky s vysokou nebo alespoň dostatečnou vypovídací hodnotou.*
4. *Kritéria pro vyhledávání vazeb musí být jasně formulovaná, jednoznačná a musí směřovat k vytyčenému cíli. Vhodné je použití kontrolních seznamů nebo indikátorů.*
5. *Při analýzách se používají zranitelnosti položek infrastruktury (prvky, vazby, toky), které se skórují s hodnotami důležitosti položek z pohledu funkčnosti infrastruktury.*
6. *Pro vyhledávání kritických míst napříč kritickou infrastrukturou se nejčastěji používají rozhodovací matice. Protože praxe čas od času vyžaduje také řešení specifických úkolů, pro které aplikace matice kritičnosti (tj. rozhodovací matice pro kritickou infrastrukturu) je příliš hrubým nástrojem, jsou používány metody preciznější založené na teorii grafů, a to např. metoda kritické cesty (tzv. CPM), metoda optimalizace řešení problému v čase a prostoru (tzv. PERT) a metoda modelování procesů v síti (tzv. Petriho sítě)* (Procházková 2006c). Příklad matice kritičnosti je na obrázku 1.
7. *Vyhodnocení kritických míst se provede na počátku hodnocení a pak při každé změně nebo po uplynutí určitého stanoveného časového intervalu (např. 3 roky) a mezi tím se ve zvlášť důležitých případech kritických infrastruktur používá inspekce založená na specifickém kontrolním seznamu.*

5. Závěr

Jsou státy (např. Německo a Maďarsko), ve kterých všechny technologické objekty a důležité občanské objekty mají bezpečnostní zprávy. Mezi tyto objekty v důsledku své důležitosti pro území zapadají i objekty kritické infrastruktury, tj. kritická infrastruktura v mnoha případech je důkladně sledována a lze doložit její funkčnost za normálních, abnormálních i kritických podmínek. V České republice bezpečnostní dokumentace v takovém rozsahu chybí (projektová dokumentace nejde do takových podrobností), a proto je třeba stanovit koncept péče / ochrany kritické infrastruktury, který pokrývá celý úsek řízení bezpečnosti a rozvoje území republiky.

Na základě dokumentů EU a sdělení jejich představitelů EU připravuje podklady pro osnovu operačních plánů na ochranu kritické infrastruktury. Zajímá se však jen o kritickou infrastrukturu důležitou pro EU, ostatní ponechá na členských státech. Na úrovni EU a vládních úřadů členských zemí EU se především řeší definice kritické infrastruktury a právní zajištění ochrany kritické infrastruktury. Nejčastěji se v souvislosti s kritickou infrastrukturou zvažují teroristické útoky a kybernetická infrastruktura jako oblast jejich útoku. Pouze země s vyspělou technologickou tradicí jako např. SRN, Švýcarsko, Velká Británie, USA (Procházková 2006a,b,c, Procházková et al. 2006) používají stejný přístup jako je ten, který je popsán v práci (Procházková 2006b). K analýze kritických infrastruktur používají kontrolní seznamy, což je pro veřejnou správu nejpřijatelnější nástroj. Odborníci SRN zpracovali v několika jazycích (němčina, angličtina, francouzština, ruština) koncept ochrany kritické infrastruktury „Baseline Protection Concept“ (Procházková 2006a), který při navazování spolupráce v předmětné oblasti nabízejí partnerům. Tento koncept je složen ze stejných kroků jako procesní model uvedený v práci (Procházková 2006b).

Řada publikací uvedených v příloze (Seznam použitých zdrojů) se také v souvislosti s ochranou kritické infrastruktury zabývá nouzovým řízením (Emergency Management) a pro tento případ navrhuje zpracovávat pro kritickou infrastrukturu:

- vnitřní nouzové plány vysoké kvality,

- plány kontinuity,
- krizové plány.

Při zpracování uvedených plánů pro kritickou infrastrukturu se opět ***vychází z příčin, tj. z živelních a jiných pohrom a nebo z vnitřních vazeb***, které jdou napříč jednotlivými infrastrukturami nebo napříč několika infrastruktur (elektrická energie, informační technologie, antropogenní řízení, finanční toky) a ***ne ze stavů, tj. nouzových situací mezi které patří v ČR také mimořádné události***, které výše uvedené příčiny vyvolají.

Stejný koncept platí v současné době i v České republice dle nového stavebního zákona, tj. zákona č. 183/2006 Sb., který novelizoval i zákon č. 239/2000 Sb. ***Dle této novelizace havarijní plány zpracovávané pod gescí zákona č. 239/2000 Sb. nesmí obsahovat opatření, která jsou v rozporu s opatřeními územního plánu.***

Ochrana kritické infrastruktury je v rámci nouzového řízení nebo civilní ochrany sledována ve starých zemích EU i v USA již od konce 70. let, a to přesto, že pojem kritická infrastruktura je poměrně nový (cca od r. 1998). Dříve se používal pojem např. funkce podporující nouzovou odezvu (Emergency Support Functions) (Procházková 2006b). V době studené války a předtím patřilo materiálně technické zajištění státu pod oblast obrany státu, tj. ne pod civilní organizace. Pojem kritický se začal používat v souvislosti s rozvojem poznání, např. teorie grafů, mezní stavy, rozhraní stavů apod., a označoval místa, kde může nastat určitá změna a obvykle ani neměl negativní zabarvení.

Shromážděné znalosti ukazují, že problém ochrany kritické infrastruktury je problém komplexní. Základní koncept ochrany musí vycházet z územního plánování a z činností na něho navazujících. *Protože stávající kritickou infrastrukturu nelze jedním mávnutím vyřadit a nahradit ji moderní, která splňuje všechny ideální požadavky a nároky,* ***existuje řada úkolů i na úseku odezvy***. Proto dle závěrů prací (Procházková 2006a,b,c, Procházková et al. 2006) mají své nezastupitelné místo:

- speciální plány odezvy pro kritické infrastruktury, které zpracovává vlastník / provozovatel / držitel licence kritické infrastruktury,
- plány kontinuity ze strany vlastníka / provozovatele / držitele licence kritické infrastruktury, které zajišťují přežití / minimální funkčnost kritické infrastruktury pro splnění nároků území, jehož obslužnost závisí na této infrastruktuře,
- plány kontinuity ze strany správce území a ochránce veřejného blaha a veřejných zájmů, kterým je veřejná správa, která zajišťuje bezpečnost a rozvoj území,
- krizové plány ze strany vlastníka / provozovatele / držitele licence kritické infrastruktury, které zajistí přežití jeho podnikání a nevyvolají nepřijatelné dopady na základní chráněné zájmy, a to především na lidské zdraví a životy.

To znamená, že základní koncept ochrany kritické infrastruktury se musí v ČR zpracovat na základě filosofie řízení bezpečnosti (integrální / komplexní / agregované) a z něho se musí odvodit požadavky na řízení odezvy a obnovy pro případ, je-li kritická infrastruktura postižena nepřijatelnými dopady vyvolaným živelní nebo jinou pohromou. Teprve z tohoto konceptu lze odvodit způsob účasti výkonných složek a jejich úkoly. Bez prosazení logického postupu a provázání činností budou všechny procesní modely vytvořené s nejlepším úmyslem představovat řešení problému metodou ad hoc či jinak označovanou jako metodou okamžitého nápadu / vnuknutí / osvícení apod.

Literatura

Procházková, D. Procesní analýza zranitelnosti prvků kritické infrastruktury. Rešerše přístupů používaných v ČR a ve vybraných zemích EU. Výzkumná zpráva pro Fakultu bezpečnostního inženýrství. Praha 2006 a, 45s.

Procházková, D. Problém ochrany kritické infrastruktury. In: Sborník MV-GŘ HZS ČR. Praha 2006 b, 26s.

Procházková, **D.** Plány obnovy, kritická infrastruktura, plány kontinuity a podpůrný systém pro rozhodování. Odborná zpráva č. 3 k projektu WB 21-05. CITYPLAN spol. s r.o. Praha 2006 c, 204s.

Procházková, D.; Říha, J.; Mozga, J.; Šenovský, M.; Bartlová, I. Plán obnovy majetku v územích postižených živelnou nebo jinou pohromou, který zohledňuje zajištění kontinuity kritické infrastruktury. Metodická příručka pro veřejnou správu. CITYPLAN, spol. s r.o., Praha 2006, 40s. ISBN 80-239-8285-0.

Příloha - Seznam použitých zdrojů

[1] Federal Response Plan. 9230.1-PL. FEMA 1999.

[2] Emergency Management Plan. State of Texas 2000.

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

[4] The Tennessee Emergency Management Plan. State of Tennessee 1995.

[5] Interim Assessment Guide for Hazardous Facilities. FEMA 1999.

[6] PDD-63 (22. května 1998): The Clinton Administration´s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. 10p.

[7] US Critical Infrastructure Conception. Washington 2001.

[8] The State Energy Assurance Guidelines. National Association of State Energy Officials, Washington, 2004, www.nasoe.org

[9] OCHA Orientation Handbook on Complex Emergencies. OCHA 2000.

[10] Qiao Linag, Wang Xiangsui: Unrestricted Warfare (trans. Foreign Broadcast Information Service). Beijing, China, February 1999.

[11] 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.

[12] Notfallvorsorge 3/1996, S. 15-18; NACC/PfP(COEC)D(96)1. Dokumenty NATO z r. 1996.

[13] A Secure Europe in a Better World. European Security Strategy, Brussels, 12.12.2003.

[14] US (15.3.2001): A Concert for Preserving Security and Promoting Freedom. Governmental report to „The Clinton Administration´s Policy on Critical Infrastructure Protection:.“ Washington.

[15] Homeland Security Office: Presidential Decision Directive. Washington, Oct. 10, 2001.

[16] D. Procházková et al.: Podklady pro zabezpečení kritické infrastruktury v ČR. Knihovna MV-GŘ HZS, Praha 2002, 161p.

[17] Usnesení BRS č. 4/2002. Praha 30.7.2002.

[18] I. Beneš et al. (2002): Studie strategická bezpečnosti energetických zásobovacích systémů v České republice. CITYPLAN spol. s.r.o. Praha.

[19] A Guide to Highway Vulnerability Assessment. SAIC, May 2002, Vienna.

[20] Bezpečnostní strategie České republiky, Praha 2003.

[21] J. Solana: Bezpečná Evropa v lepším světě. EU, Brusel, květen 2003.

[22] J. F. Gustin: Disaster & Recovery Planning: a Guide for Facility Managers. The Fairmont Press, Inc., ISBN 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn 2002, 304p.

[23] Usnesení BRS č. 2/2004, k závěrům analýzy bezpečnostního systému České republiky.

[24] T. Cloake, L. K. Siu: Standardized Classification System to Assess the State and Condition of Infrastructure in Edmonton. In: Conference INFRA, Montreal 2002,www.ceriu.qc.ca.

[25] E. M. Stovall, S. D. Turner: Methodology for Developing a Prioritized List of Critical And Vulnerable Local Government Higway Infrastructure. University Transportation Center for Alabama 2004, Report 03114.

[26] Guideline for Assessing the Performance of Oil and Natural Gas Pipeline Systems in Natural Hazard and Human Threat Events (2005), www.americanlifelinealliance.org.

[27] Orange County Facility Vulnerability Assessment. www.orangecountyfl.net.

[28] Risk Analysis Self-Assesment: Guide for Critical Infrastructure Protection. Utah Division of Homeland Security 2005, 10p., www.des.utah.gov.

[29] Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries (2003). Američan Petroleum Institute Washington, www.api.org.

[30] Bezpečnostní předpisy a standardy IAEA (Mezinárodní agentura pro atomovou energii), EU, OECD, US NRC, ASCE, ASME.

[31] D. Procházková: Poučení z dlouhodobého výpadku elektrického proudu ve východní části USA a Kanady v 2003. In: Environmentální aspekty podnikání. ISSN 1211-8052.CEMC, Praha 2004, 9-12.

[32] Critical Information Infrastructure Protection. Project, EU CI2RCO, 2005-07.

[33] D. Procházková: Řízení pro podporu lidské bezpečnosti a udržitelného rozvoje. Zpráva pro Ministerstvo vnitra č. 1 – výzkumný projekt RN200552005003. CITYPLAN spol. s r.o., Praha 2005, 350p.

[34] D. Procházková, J. Říha: Krizové řízení. MV-GŘ HZS ČR, ISBN 80-86640-30-2, Praha 2004, 225p.

[35] J. Halouzka et al.: Příručka manažera – Bussiness Continuity Planning. Tate International s.r.o., ISBN 80-86813-02-9, Praha 2004, 210p.

[36] D. Procházková: Some Problems of Critical Information Infrastructure. In: European CIIP Newsletter. 1(2005) 12-14.

[37] D. Procházková: Dopady selhání energetické infrastruktury. In: Energetické koncepce Středočeského kraje / Jihočeského kraje. Zprávy pro Krajské úřady. CITYPLAN spol. s r.o., Praha 2004, á 48p.

[38] 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. OECD, Paris 2002, 191p.

[39] Proceedings of TRANSFIN 2006 in Nice. ICBI (UK) London 2006.

[40] Green Paper on European Programme for Critical Intrastructure Protection, Brusel 17.11.2005, COM(2005) 576.

[41] D. Procházková: Doplnění výsledků uvedených ve zprávách 1 – 5, návrh metodické příručky a publikovaná sdělení výsledků projektu. Odborná zpráva č. 6 k projektu 28/04; smlouva, č. WB 28200452, č.j.: 24512/2004-52, CES 3010. CITYPLAN spol. s r.o. Praha 2006, 125p.

[42] D. Procházková: Plány obnovy, kritická infrastruktura, plány kontinuity a podpůrný systém pro rozhodování. Odborná zpráva č. 3 k projektu WB 21-05. CITYPLAN spol. s r.o. Praha 2006, 155p.

[43] D. Procházková: Kritické položky v území a zásady pro plány obnovy. Odborná zpráva č. 2 k projektu WB 21-05. CITYPLAN spol. s r.o. Praha 2006, 205p.

[44] D. Procházková: Seismické inženýrství na prahu třetího tisíciletí. Monografie – vlastní vydání, ISBN 80-238-8661-4, Praha 2002, 28p. + CD-ROM - 20 MB.

[45] D. Procházková: Bezpečnost a krizové řízení. ISBN 80-86477-35-5. POLICE HISTORY, Praha 2006, 255p.
[46] A. Boyd, J. Caton: Critical Incident management Guidelines. Volpe National Transportation Center, Cambridge 1998, 142p.
[47] Si.PRO.CI. INTERREG III. Project EU, 2005, 202p.
[48] www.aknz.de
[49] www.civilprotection.gr
[50] www.ndgdm.hu
[51] M. Dunn, I. Wiegert: Critical Information Infrastructure Protection. International CIIP Handbook. ETH, Zuerich 2004, 405p.
[52] EMA: Australian Emergency Manual Disaster Recovery. Emergency Management Australia. Sydney 1996, 166p.
[53] V. H. Guthrie, D. A. Walker: Modeling Security Risk. ABSG Consulting, Inc.; Knoxville, Tennessee 2000. Web: (http://www.abs-jbfa.com).
[54] Ministerstvo životního prostředí: Vyhodnocení katastrofální povodně v srpnu 2002 a návrh úpravy systému prevence před povodněmi. MŽP ČR Praha. Web: http://www.env.cz /www/zamest.nsf/defc72941c223d62c564b30064fdcc/4c2fc130c4339f89 c1256e3e004b7861/$FILE/zaverecna_zprava.pdf
[55] M. Konvička et al.: Město a povodeň. Strategie rozvoje měst po povodních. ERA s.r.o., ISBN: 80-86517-38-1, Brno 2002, 220 p.
[56] Spolana: Povodeň 2002. Soubor informací k průběhu povodně ve Spolaně Neratovice a výsledky auditů SPOLANA a.s. Neratovice. Spolana, a.s. Neratovice 2003. Web: http://www.unipetrol.cz/prilohy/c3ed070e/Zprava%20o% 20povodniI. pdf
[57] Ministerstvo zemědělství: Strategie ochrany před povodněmi pro území České republiky. Praktická příručka 35/2000. MZe ČR, Praha 2000. Web: http://www.mze.cz.
[58] A European Manual for „Off-site Emergency Planning and Response to Nuclear Accidents“. The Belgian Research Centre B-2400 Mol, Belgium. ISBN 90-76971-06-4, 341p.
[59] CEP Handbook 2001. Civil Emergency Planning in the NATO/EAPC Countries. ISBN 91 7097 086 6. Svenska Tryckcentralen AB, Avesta 2001.
[60] Generic Crisis Management Handbook. NATO. Dokument NATO/NACC/PfP (COEC)D(97)2. 1997 (B.A. Goetze).
[61] US RG 1.70: Regulation Guide 1.70. Revision 3. Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. LWR Edition, November 1978. Office of Standards Development, U.S. Nuclear Regulatory Commission 1978.
[62] IAEA: Safety Guides and Technical Documents. IAEA, Vienna.
[63] COMAH Safety Report Assessment Manual: UK- HID CD2, London 2002, 570p.
[64] Office of Energy Assurance: Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities. U.S. Department of Energy, Washington 2002.
[65] G. W. Hausner, R. M. Chung (eds): Natural Disaster Reduction. Proceedings of the ASCE Conference in Washington 1996. ASCE, ISBN 0-7844-0153-5, New York 1997, 407p.
[66] Our Community Pty Ltd http://www.ourcommunity.com.au/ ABN 24 094 608 705 National Headquarters: 51 Stanley St, West Melbourne Victoria 3003 Australia(POBox 354 North Melbourne 3051 Victoria) Phone (03) 9320 6800 Fax (03) 9326 6859 Email service@ourcommunity.com.auCopyright and disclaimer.
[67] http://www.ourcommunity.com.au/insurance/insurancearticle.jsp?articleId= 1244.
[68] Disaster Preparedness for Persons with Disabilities Improving California´s Response a Report by the California Department of Rehabilitation, April 1997.

[69] Worksheets for Electric Utility Vulnerability and Risk Assessment. www.esisac.com.
[70] Průkazná dokumentace k jaderným elektrárnám ČR. Archiv. ČEZ Praha.
[71] L. Satrapa et al.: Povodňové škody. ČVTVHS, Praha 1999.
[72] L. Čamrová et al.: Povodně jako průřezový problém státní politiky. ISBN 80-86684-09-01, IEEP, Praha 2004, 174p.
[73] J. Wever: Integral Safety in Netherland. Paper presented at the Australan Institute of Criminology in 2000, www.aic.gov.au/conference.
[74] K. Kapuy: The Relevance of the Local Level for Human Security. Human Security Perspectives, 1 (2004) No 1 www.hs-perspectives.etc-graz.at/pdfiles.
[75] Defining Indicators and Metrics for Measuring improvements in Chemical Safety (2002)
[76] Comparison of Human Security Definitions. www.gdrc.org/sustdev/husec/comparison.pdf. MKOPSC Report, http://process-safety.tamu.edu
[77] Definitions and Dimension of Human Security. www.un.ltv./files/2002/chapter1.pdf
[78] Seguridad humana (2003). Investigación realizada per EyE como Nodo Latinoamericano, Projecto Millenium www.esyes.com.ar.
[79] Duality of Life. EPA 1972.
[80] Briefing on Selected Sustainable Development Tools (2003). Final Report to the English Regions Network www.cagconsultants.co.uk.
[81] J. Hardi, P. Zdan: Assessing Sustainable Development Principles in Praktice. International Institute of Sustainable Development, Winnipeg, Manitoba 1997, ISBN 1-895536—07-3, http://iisd1.iisd.ca/measure/1.htm.
[82] www.stats.govt.nz/analytical-report.
[83] www.epa.gov/solec
[84] Projekt CRISP. http://crisp.cstb.fr
[85] Projekt PASTILLE. www.lse.ac.uk/collections/PASTILLE
[86] www.regionalstewardship.org/indicators
[87] www.ima.kth.se/IM/envsite/indicat.htm
[88] J. Frankish, B. Kwan, J. Flores: Assessing the Health of Communities, Indicator Projects and their Impacts. Institute of Health Promotion Research, University of British Columbia 2002 www.uhpr.ubc.ca
[89] J. Mozga: Podklady pro základnu koncepčního modelu pro řešení projektu MMR WB-21-05. Kritéria pro integrální bezpečnost a podklady pro kritickou infrastrukturu. Zpráva, Hradec Králové 2006.
[90] Supplementary Guidance – The Sustainability Checklist. Planning Policy Team, Ealing Council www.ealing.gov.uk/planpol.
[91] H. Haberl, H. Schaudl: Indicators of Sustainable Land Use – Concepts for Analysis of Society-Nature Interrelations and Implication for Sustainable Development. Environmental Management and Health, 10 (1999), No 3.
[92] P. Maurice, M. Lavoie, A. Chapdelaine, B. H. Bonneau: Safety and Safety Promotion: Conceptual and Operational Aspects. Chronic Disease in Canada, 18 (1999) No. 4.
[93] EEA (2004): EEA Core Set of Indicators (CSI), 2004. Background document for Point Meeting 21-23 April 2004. Copenhagen, Denmark. Web: http://themes.eea.eu.int/IMS/About/CSIMainFinal.pdf.
[94] OECD (2002): Indicators to Measure Decoupling of Environmental Pressure from Economic Growth. OECD SG/SD(2002)1/FINAL, 16. 5. 2002.
[95] F. Hinterberger, R. Zacherl: Ways towards Sustainability in the European Union - beyond the European Spring Summit 2003. SERI Sustainable Europe Research Institute.

February 2003. Vienna , Austria. Web: http://www.seri.at/ Data/personendatenh/SERI%20Ways %20towards%20SD%20in%20the%20EU_Final%20Version.pdf.
[96] Bundesamt für Bevölkerungsschutz: KATARISK. http://www.bevoelkerungsschutz. admin.ch/internet/bs/de/home/themen/ gefaehrdungen/katarisk.html
[97]Bundesamt für Bevölkerungsschutz:KATAPLAN. http://www.bevoelkerungsschutz.admin.ch /internet/bs/de/ home/themen/gefaehrdungen/kataplan.html
[98] www.southampton.gov.uk
[99] http://en.wikipedia.org
[100] www.extension.edu
[101] J. Moteff, C. Copeland, J. Fischer: Critical Infrastrures: What makes an Infrastrucuture Critical Report for Congress, 2003, CRS Web, Order Code RL31556.
[102] W. Stein, B. Hammerli, H. Pohl, R. Posch (eds): Critical Infrastructure Protection – Status and Perspectives. Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[103] A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation–Transportation Policy and Analysis Center, Vinna 2002.
[104] Critical Infrastructure Emergency Risk Management and Assurance.Handbook Emergency Management Australia, 2003, www.ema.gov.au
[105] Worksheets for Electric Utility Vulnerability and Risk Assessment. www.esisac.com
[106] 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
[107] www.psepc-gppcc.gc.ca/Keeping-Canada-safe
[108] www.bizmanualzcom
[109] www.esse.ou.edu
[110] http://wordnet.prionceton.edu
[111] www.safeguardingaustralia.org.au
[112] C. S. Holling: Resilience and Stability of Ecosystem. Annual Review of Ecology and Systematics , 4 (1973) No 1.
[113] L. Gunderson, C. S. Holding: Panarchy: Understanding Transformation in Human and Natural Systems, Washington, Island Press 2002.
[114] S. Franklin, T. Downing: Resilience and Vulnerability, GECAFS Project, Stockholm Environment Institute 2004.
[115] N. W. Adger: Social and Ecological Resilience, Progress in Human Geography 24, (2000) No 3.
[116] F. Langeweg, E. E. Espeleta: Human Security and Vulnerability in a Scenario Context, 2001, HDP Update 2.
[117] Framework for Vulnerability Analysis in Sustainability Science. Proceeding of National Academy of Science 100 (14).
[118] R. Chambers: Vulnerability, Coping and Policy, IDS Bulletin. 20 (1990) No. 2.
[119] J. M. Watts, G. H. Bohle: The Space of Vulnerability, Progress in Human Geography 17 (1993) No. 1.
[120] K. Dow: Exploring Differences in Our Commnon futruje, Geoforum 23 (1991) No. 3.
[121] M. Glantz: Global Warming and Environmental Change,1992, Global Environmental Change 2.

[122] J. Smithers, B. Smit:Human Adaptation to Climatic Variability and Change, 1997, Global Environmental Change 7 (2).
[123] G. W. Hausner, R. M. Chung (eds): Natural Disaster Reduction. Proceedings of the ASCE Conference in Washington 1996. ASCE, ISBN 0-7844-0153-5, New York 1997, 407p.
[124] The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. USA 14.2.2003.
[125] www.southalabama.edu
[126] www.mywhateever.com
[127] www.iqda.org
[128] Focus on Recovery (2005). Ministry of Civil Defense and Emergency Management, Wellington. ISBN 0-488-25463-6.
[129] www.gita.state.az.us
[130] P. Ramesh: Business Continuity Planning Technology. Review 4, (2002) www.tcs.org.
[131] www.thebci.org
[132] Working together: Lifelines Utlities and Emergency Management. Ministry of Civil Defense and Emergency Management (CDEM) 2002, www.civildefense.govt.nz
[133] A. C. Boyd, J. Singleton, A. Bromley ,P. Yorks: Continuity of Operations Planning Guidelines for Transportation Agencie. Transportation Research Board, Washington 2005, ISBN 0-309-08841-0, www.trb.org
[134] Continuity of Operations Implementation Guidance. Florida Division of Emergency Management, www.ehs.ufl.edu.
[135] Continuity of Operations Plan Templáře.Virginia Department of Emergency Management, 2002 , www.vaemergency.com
[136] Guidelines for Provincial Emergency Management Programs in Ontario. Emergency Management Ontario, 2004, www.oaem.ca
[137] Preparing for an Emergency – Continuity of Operations Planning for Public Institutions. Maryland Continuity of Operations Planning Manual, 2005, www.mema.state.md.us
[138] The State Energy Assurance Guidelines. National Association of State Energy Officials, Washington, 2004, www.nasoe.org
[139] Flood Mitigation and Recovery – An Interactive Exercise for Local Governments. Manual. Spangle Associates and The Mitigation Assistance Corporation. August 1995.
[140] FEMA: Multi Hazard Identificacion and Risk Assessment, The Cornerstone of the National Mitigation Strategy, 1997.
[141] PEMA: Hazard Mitigation Planning - An On-Line Introduction. Part III: Hazard Vulnerability Analysis (HVA). Pennsylvania Emergency Management Agency, 29.05.2002. Web: http://sites.state.pa.us/PA_Exec/PEMA/programs/mitigation
[142] ARCADIS: Posílení rizikové analýzy a stanovení aktivních zón v českém vodním hospodářství. Nizozemský program "Partners for Water" - Ministerstvo zemědělství ČR. 25. května 2004. 110302/of4/1o2/000852/le. http://www.mze.cz/attachments/ posileni_rizikove_ analyzy.pdf.
[143] U. Beck: Risk society: Towards a New Modernity. London 1992.
[144] J. G. Voeller: CIPP - Critical Infrastructure Protection Priorities. In: The Construction Sciences Research Foundation, Inc. Baltimore, USA. Updated March 5, 2005. Web: http://www.csrf.org/pubs/cipp.html
[145] Zpráva Komise EU Radě, Evropskému parlamentu, Ekonomickému a sociálnímu výboru a Výboru pro regiony „Výstavba společného přístupu k přírodním a technologickým rizikům" 30.4.2003.

[146] S. Mueller et al.: Safety Culture – A Reflection of Risk Avareness. Swiss Re, Zuerich 1998, 45p.
[147] A. Mueller: Integrated Risk Management. Der Rueck fehlerhafter Produkte. Muenchener Rueck, Muenchen 2003, 36p.
[148] UNEP: Management of Industrial Accident Prevention and Preparedness. A Training Resource Package. Web: http://www.unepie.org/home.html.
[149] US Department of Agriculture: Disaster Recovery and Business Resumption Plans. Washington 2005. http://www.ocio.usda.gov/directives/files/dm/ DM3570-001.htm.
[150] M. Swanson et al.: Contingency Planning Guide for Information Technology Systems. National Institute of Standards and Technology, 2002, http://csrc.nist.gov/publications/ nistpubs/800-34/sp800-34.pdf
[151] Disaster Advisors Inc.: Bussiness Continuity Planning. 2003. http://www.disasteradvisors.com/disasterplanning.htm.
[152] M. Richburg: How to Establish a Business Continuity Plan. M-systems, Inc.2005, http://www.msystemsinc.net/images/AITP_BCP3_Presentation.ppt
[153] J. Nash: Continuity of Operations Plan. NIST 2004, http://csrc.nist.gov/fasp/FASPDocs/ contingency-plan / TreasCOOPBSP.htm
[154] Strohl Systems: Living Disaster Recovery Planning System (LDRPS). http://www.strohlsystems.com/CompanyInfo/Services/Training.asp
[155] U.S. Department of Energy: Continuity of Operations Plan. 2005. http://en.wikipedia.org/wiki/Continuity_of_Operations_Plan; http://cio.doe.gov/ITReform/ sqse/ download/ contin.doc
[156] ICF Consulting Inc.: Continuity Planning Emphasizes Comprehensive, All-Hazards Approach. 2005. http://www.icfconsulting.com/Publications /Perspectives-2005/continuity-planning.asp
[157] J. Newton: Emergency Preparedness FMJ Article. The key to survival: Planning ahead for bisiness recovery. IFMA - International Facility Management Association 2004. http://www.ifma.org/ tools/ep/fmj/keysurvival_ newton.cfm
[158] North Carolina Wesleyan College: The Safety and Security of Critical Infrastructure. 2005. http://faculty.ncwc.edu/toconnor/431/431lect06.htm
[159] G. McBean, D. Henstra: Disaster Resilient Cities - a Goal for the Future. 2004. http://www.opinion-canada.ca/en/articles/article_79.html
[160] J. Petterson: A Review of the Literature and Programs on Local Recovery from Disaster. Natural Hazards Research and Applications Information Center, Institute of Behavioral Science, University of Colorado, Natural Hazards Research Working Paper #102. Boulder 1999. http://www.colorado.edu/hazards/wp/wp102/wp102org.html
[161] American Planning Association: Post-Disaster Recovery Planning. 2005. http://www.fema.gov
[162] FEMA: Indicators, Hazard Identificacion and Risk Assessment. Wshington 1992.
[163] CH. Pusch: Preventable Losses: Saving Lives and Property Through Hazard Risk Management. A Comprehensive Risk Management Framework for Europe and Central. Working paper series No. 9. The World Bank, Washington, D. C. October 2004. http://www.worldbank.org/hazards/files/ECA_strategy.pdf.
[164] US National Research Council 1983. Risk Management.
[165] E. L. Krinitzsky, D. B. Slemmons (eds): Neotectonics in Earthquake Evaluation. Am. Geol. Soc., Boulder 1990, 125p.
[166] J. Šebek; Ochrana infrastruktury před teroristickými útoky. Internetový odkaz http://www.enviweb.cz/?secpart=havarie_archiv_ffbic_cz (stav ke dni 1. 3. 2006)

[167] Dosavadní zkušenosti v oblasti řešení problematiky ochrany kritické infrastruktury v působnosti Ministerstva průmyslu a obchodu. http://www.dsm.tate.cz/index.php?typ=DAA&showid=289&id=71021&fla=0 (stav ke dni 3. 3. 2006).
[168] D. Procházková, B. Šesták: Kontrolní seznamy a jejich aplikace v praxi. Nástroj rizikového inženýrství. Policejní akademie ČR, ISBN 80-7251-225-0, Praha 2006, v tisku.
[169] Seminář „Zkušenosti s ochranou kritické infrastruktury“. MV-GŘ HZS ČR, Lázně Bohdaneč 2006, CD-ROM.
[170] ESRAB Report: A Report from the European Security Research Advisory Board. EU, Brussels 2006, 95p.
[171] FEMA: Promoting Critical Infrastructure Protection by Emergency Managers and First Responders Nationwide. 2005. www.usfa.fema.gov
[172] Protecting the Homeland. Report of the Defense Science Board Task Force on Defensive Informations. Office of the Undersecretary of Defense, Washington 2001, 181p.
[173] GAO: Critical Infrastructure Protection. Dept. Of Homeland Security, Washington 2005, 78p.
[174] I. Beneš: CIP in the Czech Republic (Experiences with CIP). CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[175] J. Giller: Critical Infrastructure Protection (CIP) in Austria. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[176] L. Cigánik: Služby polície pri ochrane kritickej infraštruktúry. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[177] P. Danihelka, P. Poledňák: Chemical Industry as a Part of Critical Infrastructure. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[178] J. Nunes de Almeida: The EPCIP Present State. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[179] E. Luiijf: CIP Status in the Netherlands. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[180] E. Luiijf: Vital Infrastructure Threats and Assurance (VITA) Project. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[181] E. Luiijf, M. H. A. Klaver: Protection of the Dutch Critical Infrastructures. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[182] E. Luiijf: SCADA: An Inroad to Critical Infrastructure Disaster. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[183] P. Petrovič: Ochrana kritickej infrastruktury ve Slovenské republice. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[184] Dublin Declaration. European Action Plan on the PPP, Dec. 19,2003. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[185] H. Hanzlikova: Critical Infrastructure Protection in the Czech Republic. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[186] D. Procházková: Strategy of Critical Information Protection. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[187] H. Werner: German National CIP Strategy. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[188] L. Kozári, K. Cecei-Mórotz: The National Programme of Critical Infrastructure Protection. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[189] S. Kurek: Experiences with the CIP in Poland. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.

[190] R. Goodchild: EU – Level Activities to Protect Critical Energy and Transport Infrastructure. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[191] C. F. M. Mazera: European Information Exchanges Needs and Challenges. CIP International Conference Bratislava, 29-30.11.2006, EU – TAIEX, 2006.
[192] L. T, Saaty: A Scaling Method for Priorities in Hierarchical Structures. In: Journal of Mathematical Psychology 15, 1977, No.3, p. 234.
[193] L. T, Saaty : The Analytic Hierarchy Process. New York, Mc Graw-Hill 1990.
[194] L. A. Zadeh: Fuzzy Sets. Inform. Control, 8, 1965.
[195] K. J. Coppersmith, R.R. Youngs: Probabilistic Seismic - Hazard Analysis Using Expert Opinion; An Example from the Pacific Northwest. In: Krinitzsky E. L., Slemmons D. B., eds - Neotectonics in Earthquake Evaluation. Am. Geol. Soc., Boulder 1990, 29-46.
[196] J. Říha, A. Dudek: Přehled vhodných metodik analýz rizik. Zpráva pro MV – GŘ HZS ČR. Praha 2003, 194p.
[197] Relex FMEA/FMECA. Relex Software Corporation, http://www.relexsoftware.com
[198] J. Dušek: Pravděpodobnostní hodnocení rizika jaderných elektráren. In: Sborník Rozhodovací proces a riziková analýza. ECOIMPACT Praha, 1996, 52-58.
[199] C. Elbing, H. W. Alfen: Risk Management for Public Private Partnership Projects and Project Portfolios from an Investors Perspective. In: QUT Research Week 2005, Conf. Proceedings, 4-5 July, 2005, Brisbane, Australia. ISBN 1-74107-101-1. http://www.rics.org/NR/rdonlyres/71A226DA-9FAC-4413-A6C0-47C9C5B645C6/0/Risk_management_public_private_partnership20051121.pdf
[200] SIEP: The Risk Assessment Matrix. Bringing it to life. Shell International Exploration and Production B.V., Den Haag, The Netherlands, November 2002. Web: http://www.energyinst.org.uk/heartsandminds/docs/ram.pdf
[201] MSU : Risk Assessment Matrix (RAM) Process. School of Criminal Justice, Michigan State University. http://www.cip.msu.edu/RAMModel&Priorit1.pdf
[202] FEMA: Emergency Management Guide for Business and Industry. Web: http://www.fema.gov/pdf/library/bizindst.pdf
[203] R. R. Mohr: Preliminary Hazard Analysis. Jacobs Sverdrup. February 2002. Web: http://www.sverdrup.com/safety/pha.pdf
[204] US Department of Transportation: Report to Congress on Public-Private Partnerships. December 2004. http://www.fhwa.dot.gov/reports/pppdec2004 /#ftn104#ftn104

Summary

The security of the world, territory and organisation has been changing with the time, and therefore, there must be systematically built the safety culture, which taking into account actual piece of knowledge and experience.
The safety culture promotion into practice requires both, the aimed management and broad participation of all staff of public administration / organisation with emphasising that the top management has the highest responsibility. It understandably leads to the assignment of higher priority to planning and safety management as well as to higher demands to the understanding level of all participants.
The results of bibliographic search of literature and documents show the following facts. There are countries in which owners of all technological buildings and important civic buildings compile the safety report to demonstrate the bulding and equipment safety. Among

these structures there are buildings and networks of critical infrastructures. It means that the critical infrastructure function is followed under the normal, abnormal and critical conditions. In the Czech Republic there is safety documentation in such extent only for selected structures, e.g. nuclear installations and a part of chemical installations.
With regard to the EU documents and the EU announcements there are prepared the data for outline of operating plans for critical infrastructure protection. The EU itself is just interested in the critical infrastructure important for the EU, the other it leaves to the Member States. On the EU level and on the Member States Authorities there are above all dealt with the definition of the critical infrastructure and with the legal ensuring the critical infrastructure protection. In connection with the critical infrastructure protection much often there are considered the terrorist attacks and a cyber infrastructure as a domain of their targets. To analyze critical infrastructure protection there are used the checklists because for Public Administration use they are well acceptable. The German professionals prepare in several languages (German, English, French, Russian) the critical infrastructure concept „Baseline Protection Concept" which is based on technological and legal principles used e.g. by the IAEA and the OECD, and included in the Czech technical norms and standards.
Several papers given in Annex deals with the connections of critical infrastructure protection and emergency management. For this purpose they propose to generate:

- on-site emergency plan of high quality,
- continuity plan,
- crisis plan.

To process those plans there is necessary to take into account disasters of all kinds, interrealations and intedependencees going across the infrastructures (electric energy network, information network, antropogenic management, financial flows), not to start from emergencies that are consequences of disasters.
The same concept currently holds in the Czech Republic according to building law (i.e. law No. 183/2006 Sb., that amended the law No. 239/2000 Sb., on the Integrated Rescue System. According to this amendment the off-site emergency plans processed under the law No. 239/2000 Sb. mustn't include steps, which they are in contradiction with principals and trends of land- use plan.

The critical infrastructure protection has been followed under the emergency management in old EU countries and in the USA since the end of 70s under the term “Emergency Support Functions”. In historical times the material and technical facilities ensuring the state power and sovereignty belonged under the defence ministry auspice. The term “critical” corresponds to nuclear domain concept, theory of graps etc. It marks the boundary between positive and negative situation.
Assembeld knowledge shows that the critical infrastructure protection problem is global. The basic concept must go out from the land-use plan and from activities linked with it. Because existing critical infrastructures cannot be replaced by advanced ones immediately, there are a lot of tasks also in the response domain. Therefore, there are special importance the following tools:

- special response plans for critical infrastructures processed by owners / operators / licence holders,
- continuity plans for critical infrastructures processed by owners / operators / licence holders, ensuring the live through the emergency and minimal function of critical infrastructures necessary for services in land that is dependent on this critical infrastructure outputs,
- continuity plans from the side of land administrator as the public interest protector, who is responsible for services in land,

- crisis plans for critical infrastructures processed by owners / operators / licence holders, ensuring the live through the emergency and averting the unacceptable impacts on protected interests, namely to human lives and environment.

It means that the critical infrastructure protection concept for the Czech Republic must be processed on the general safety management concept and from it there must be derived demands on response management and renovation for case if critical infrastructure would be affected by disaster of a different kind possible in a given land. Only from this concept it is possible to determine the way of effective participance of executive forces and their tasks and duties. Without enforcement of this logic procedure and interconnecting the activities of all participants all process models created with best intention will onyl represent ad hoc solution of problem under account.