BEZPEČNOSTNÍ MEZERA V OCHRANĚ INFRASTRUKTURY: ZRANITELNOST SÍŤOVÝCH ODVĚTVÍ

GAP SECURITY IN THE INFRASTRUCTURE PROTECTION: VULNERABILITIES OF NETWORK INDUSTRIES

Josef ŘÍHA
riha.joe@volny.cz

Abstract

This paper addresses the gap security in the infrastructure protection relating to the vulnerabilities of network industries, as well as axioms for a deep understanding of infrastructure systems. There are major differences between object-oriented systems and network-oriented systems. The network-oriented infrastructures systems need better-supported techniques for the comparison of project alternatives, e.g. a new conceptual approach and extended analytical tools. This paper suggests a new approach, using traditional network graph theory that couples with MAUT (Multi-Atribute Utility Theory) and MCDA (Multi-Criteria Decision Analysis).

Key words

Axiomatic design, convolution, critical infrastructure, multi-atribute utility theory, network-oriented systems, network graph theory, object-oriented systems, redundancy, risk triplet, vulnerability.

Motto: „*Bezpečnost je proces, nikoliv produkt*."
1.1 *(Bruce Schneier, CRYPTO-GRAM)*

Úvod do problému

Univerzální bezpečnostní koncepce pro oblast kritické infrastruktury vychází z nereálné skutečnosti a chybných předpokladů. Autor posoudil soubor poznatků[1], které vyžadují změnit mylné elementární myšlení. Jde o závažný epistemologický problém rizikové analýzy, jehož řešení nesnese odklad.

Úsilí o velkolepou ochranu KI na nadnárodní úrovni známé jako „společný rámec EPCIP" se stal utopií a po deseti letech hledání byl zredukován na pouhé čtyři pan-evropské kritické infrastruktury. Dosud deklarovaná ochrana kritické infrastruktury nerozlišuje vlastnosti a opomíjí existenci dvou základních typů: objektově orientované systémy a síťově orientované systémy. Topologie a vlastnosti síťových odvětví trpí zvýšenou zranitelností a umožňují mimořádný vliv specifických rizikových indikátorů; fyzická bariérová ochrana není možná.

V teoretické oblasti jsou některé segmenty předpokladů na hranici „matematického nesmyslu". Je to jednak koncept a algoritmus pro metriku rizika, jednak nekorektní aplikace často používané metody analýzy projevů a důsledků poruch FMEA, způsobené nevhodnou strukturou vzorce priority rizika RPN; vzorec postrádá vnitřní konzistenci a potenciálně poskytuje nepřesné výstupy. Silně jsou podceňovány zásady operačního výzkumu (operační analýzy), možnosti teorie grafů a smíšené topologie systémů; jen výjimečně je uvažována podmíněná pravděpodobnost a efekt konvoluce.

Často deklarovaná aplikace axiomatické teorie kardinálního užitku MAUT nebývá precizní, použité veličiny nebývají důsledně normalizovány, nejsou uvažovány jednorozměrné

funkce užitku a vyhodnocovací křivky; zdaleka nebývá respektováno jádro analytického hierarchického procesu AHP. Hlubší pochopení systémů síťově orientované infrastruktury a její smysluplná ochrana postrádá zohlednění nezbytných axiomů (tabulka 2).

Fatálně slabou stránkou bezpečnostní vědy je v této oblasti neustálená terminologie. Uplatňují se aspekty teritoriální a sémantické. Termíny „nebezpečí“, „ohrožení“, „riziko“ jsou v běžné řeči zaměňovány; v médiích i v oficiálních dokumentech jsou často užívány chybně. Totéž platí o angličtině - matoucí je slovo „hazard“, které je spojováno s termínem „risk“ (některé slovníky definují „hazard“ jako "*a danger or risk*"). Jedním z důvodů je absence teorie krizového managementu. Existující „chaos“ v domácí odborné literatuře rizikového managementu vysvětluje [2], v mezinárodním měřítku toto fatálně dokládá Bílá kniha *IRGC [30] z roku 2006.* Zásadně platí axiomatický předpoklad: ohrožení, riziko a zranitelnost nelze zaměňovat, nicméně ohrožení a zranitelnost jsou součástí rizika. Riziko je v komplexním pojetí chápáno jako relace mezi očekávanou ztrátou a neurčitostí uvažované ztráty (zpravidla vyjádřenou pravděpodobností nebo frekvencí výskytu). Vyjadřuje možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Klíčová norma ISO 31000: 2009 [31] definuje riziko[2] jako „účinek nejistoty na dosažení cílů“.

Obr. 1
Paradigma jednosměrného vztahu tušeného nebezpečí k riziku; upraveno podle [78]

Autor dokumentu [48] zdůrazňuje, že pojmy nebezpečí (hazard) a ohrožení (threat) jsou často zaměňovány, přičemž jde o dvě různé věci[3]. Avšak připomíná se, že někteří teoretici se o kategorii „hazardu“ přímo opírají [1]. Pojem „nebezpečí“ se jeví jako obecný pojem pro jakýkoli negativní jev, událost, proces. V mysli člověka lze nebezpečí přirovnat předtuše, viz obr. 1.

Slabá místa v konceptu ochrany kritické infrastruktury

Kritická infrastruktura je v současnosti mezinárodní fenomén. Narušení funkce může mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Podle [16] z roku 2006 se *kritickou infrastrukturou* rozumí „zařízení fyzických a informačních technologií, sítě, služby a majetek, které v případě narušení nebo zničení by měly vážný dopad na zdraví, bezpečnost, zabezpečení nebo hospodářské blaho občanů nebo účinné fungování vlád v zemích EU“. Někdy se místo pojmu KI výstižně používá termín „život podporující sítě“ (lifeline support network). Tento pojem propaguje zejména Austrálie a Nový Zéland.

Jednotlivé infrastruktury jsou vzájemně horizontálně i vertikálně propojené ve smyslu konceptu SoS. Současně existuje jejich vzájemná závislost CII. Tato *vzájemná závislost*

(interdependency) kritických infrastruktur byla klasifikována nejméně pro čtyři oblasti, např. *fyzikální*, kde činnost jedné infrastruktury závisí na látkovém výstupu z jiné infrastrukrury, nebo *geografická*, kde závislost na místních environmentálních činitelích působí na několik infrastruktur současně apod., podrobněji [55], [58], [71]. Často bezbřehý výčet možných situací neumožňuje řídit *správu rizik*[4] bez potřebného algoritmu a zůstává na úrovni informace.

Životně důležitý význam KI vede společnost k úsilí o její ochranu ve smyslu CIP. Na nadnárodní úrovni se o to pokouší EU od roku 2003 [5], [22]. Nicméně formálně přiznané selhání velkorysého *Evropského programu na ochranu kritické infrastruktury,* připravovaného od 2003 [14], podporuje názor euroskeptiků o obtížné až nemožné integraci přeshraničních koncepcí a strategií. Deklarovaný „společný rámec EPCIP" podle EK Zelené knihy z roku 2005 s tvrzením, že „mnoho infrastruktur je součástí širší sítě" se stal utopií a po deseti letech hledání byl zredukován na pouhé čtyři pan-evropské kritické infrastruktury, tj. Eurocontrol (letecký provoz), Galileo (satelitní navigační systém), elektrickou a plynovou přenosovou síť. V roce 2013 většina členských států vyjádřila znepokojení, že primární cíl Směrnice – zvýšení bezpečnosti ECI – je vnímán jako oblast s nejnižší úrovní zlepšení, viz dokument [15]. Deklaruje se potřeba řešit „nedostatky současného přístupu", tj. *de facto* nesplnění představ administrativy podle [70]. Chaotický přístup v hledání „nového přístupu k EPCIP" dokládá „objev" z roku 2013, že napříště, cit. „…bude Komisí podporován systémový přístup".

Dosavadní společný rámec členských zemí EU není konzistentní ani pro úroveň národních kritických infrastruktur, protože zcela přirozeně se v konceptu kritické infrastruktury odrážejí zkušenosti a zvyklosti států [81]. Jednotlivé země se neshodují v definiční ani obsahové oblasti [21]. Stejně tak na rozdíl od jiných zemí v ČR není do seznamu KI uveden explicitně a samostatně např. jaderný průmysl, chemický průmysl, vesmír a výzkum, poštovní a kurýrní služby, apod. Obdobně podstatné rozdíly existují ve vnímání KI v EU a v USA [9]. Např. EU zaostává a ignoruje poštovní a kurýrní služby (postal and shipping), národní památky (national monumets and icons), přehradní nádrže (dams), aj.

Infrastruktura by měla být vnímána v širokém holistickém konceptu, tzn. z hlediska technického, organizačního a personálního. Jak ve strategických [46], tak ani v hodnotících dokumentech [25] nenacházíme zmínku o rozhodujícím významu *síťové kritické infrastruktury* NS. Namísto klíčového problému jsou do nekonečna opisovány dříve přijaté obecné uzance. Pojem síťový podnik, zařízení, služby (network utilities) přichází ze světa byznysu. Podle [19] „síťové systémy poskytují infrastrukturu a základ pro fungování ekonomiky a společnosti. Síťová odvětví hrají v současném životě rozhodující roli. Vyskytují se v mnoha formách a zahrnují nejen hmotné sítě, např. dopravní, logistické, komunikační a energetické, ale i abstraktní sítě ekonomické, finanční, společenské a znalostní". Pro síťová odvětví schází explicitní definice [24], [51]; podle [47] „síťové odvětví vyžaduje fixní síť pro doručení svých služeb". Pro síťová odvětví je charakteristický zejména vznik *přirozeného monopolu*[5] a existence *silných bariér*[6] *pro vstup* do odvětví. Uplatňuje se *síťový efekt* způsobující, že užitek spotřebitelů ze služeb dodávaných síťovým odvětvím roste s tím, jak roste množství uživatelů mající přístup k této síti. Silně se projevuje vliv *externalit*[7], protože hodnota produktu/služby pro spotřebitele se mění v závislosti na počtu spotřebitelů užívajících tohoto produktu či služby. Podrobnější charakteristiky nabízejí [4], [6], [7], [36], [52].

Standardně jsou do nich řazena především odvětví energetiky (výroba, přenos a distribuce elektrické energie, zemního plynu a tepla), vodohospodářství (veřejné vodovody a kanalizace) a telekomunikací. Firmy působící v síťových odvětvích patří mezi podniky, které se dotýkají veřejného zájmu, tj. mají sloužit potřebám veřejnosti a chránit a podporovat blahobyt společnosti. Ochrana a stabilita těchto odvětví má strategický význam pro stát a jeho environmentální, sociální a hospodářskou politiku [43]. Proto většina států světa přistupuje k jejich *regulaci*[8]. Např. státní regulace energetických firem se dotýká nejen cen výrobků (např.

elektřiny, zemního plynu, vody, tepla), ale i pravidel pro vstup a výstup z odvětví, rozsahu, kvality a především *spolehlivosti poskytovaných služeb*.

Bezpečnost infrastruktury a spolehlivost služeb v síťových odvětvích je silně oslabena rizikovými faktory, které jsou imanentně zakódovány do jejich podstaty. Předběžná analýza soustřeďuje pozornost na šest *specifických rizikových faktorů*, které oslabují bezpečnost síťové kritické infrastruktury, tj. (a) silné tendence k přirozenému monopolu, (b) nezbytnost poskytované služby (produkt je nezastupitelný), (c) kapitálová náročnost (vysoké kapitálové vstupní a udržovací investice), (d) omezená skladovatelnost (neskladovatelnost) produktu, (e) časová variabilita poptávky (v rámci dne, týdne i sezónních období), (f) geografická exkluzivita (výsostné postavení na daném území).

Ke zvýšení rizika přispívá svým dílem *liberalizace*. Proces nevyhnutelné *restrukturalizace* a *liberalizace infrastruktury* přináší vedle kladných stránek i „…hluboce zakořeněné obavy v mnoha ohledech, např. jaká je záruka pro plnění závazků v oblasti veřejných služeb, národních zájmů, bezpečného zásobování, nebo podpory rozvoje udržitelného životního prostředí“, cit. [20].

Rizikové trojče a diskrepance v teorii

Riziko je obvykle popsáno spojitou nebo přetržitou veličinou R_E, která může nabývat různých hodnot. Cílem rizikového inženýrství je jeho *odhad*, jehož předpokladem je *identifikace nebezpečí a ohrožení*, formulace *scénáře nebezpečí a ohrožení* a *kvantifikace rizika*. Jde o tři operace (tzv. rizikové trojče – risk triplet [33]), které poskytnou odpověď na tři otázky [35]:

- identifikace nebezpečí ☞ *jaké nepříznivé události mohou nastat ?*
- scénář nebezpečí ☞ *jaká je pravděpodobnost výskytu takových událostí ?*
- kvantifikace rizika ☞ *pokud některá nepříznivá událost nastane, jaké to bude mít následky ?*

Uvedené tři otázky vedou k *definici rizika* jako *n*-tice vektorů

$$R_{Ei} \equiv \left(p_i, E_i, C_i\right) \qquad \left(i = 1, ..., n\right), \tag{1}$$

kde R_{Ei} je riziko scénáře nebezpečí a ohrožení;
p_i - pravděpodobnost výskytu scénáře;
E_i - scénář nebezpečí a ohrožení (*tj. sekvence možných událostí pro dané nebezpečí vedoucí k nežádoucím důsledkům*);
C_i - důsledky vzniklé realizací scénáře (*tj. ve smyslu vzniklé újmy či škody různého druhu např. finanční nebo věcné ztráty, úmrtí, zranění, duševní újmy, aj.*);
i - index scénáře;
n - celkový počet scénářů (variant).

Za předpokladu, že pro scénář nebezpečí E_i je možné stanovit numerické hodnoty p_i a C_i, potom stupeň, míru či úroveň rizika lze standardně určit podle

$$R_{Ei} = p_i \times C_i . \tag{2}$$

Scénář nebezpečí vyplývající z úmyslně vedeného *teroristického činu* se bytostně liší od rizika vyvolaného přírodními vlivy [68]. Základní rozdíly přehledně uvedl [38]. Z důvodu značně odlišného typu nejistoty *teroristického rizika* nelze běžným způsobem aplikovat teorii pravděpodobnosti pro bezpečnostní riziko; musí být použita podmíněná pravděpodobnost

(např.: *útok způsobující škodu*|*výskyt útoku*). Známé a ověřené metody rizikového managementu pro oblast susperterorismu nepostačují, podrobněji [64]. Pokusy o matematickou interpretaci pracují s výrazem *konvoluce*[9]. Pod pojmem *hrozby* se rozumí „scénář ohrožení“, tzn. ohrožení implicitně zahrnuje *znalost, vlastnosti* a *plán útoku* teroristů. *Zranitelnost* je definována jako pravděpodobnost úspěšného ohrožení včetně uvážení použitých ochranných opatření, takže ohrožení a zranitelnost společně vyjadřují pravděpodobnost úspěšného teroristického útoku.

V inženýrské praxi se způsob hodnocení míry rizika liší jednak v oblasti kvalitativní analýzy, jednak v oblasti kvantitativní analýzy. Při kvantitativní analýze rizika se obecný tvar rovnice (1) supluje referenčním vzorcem, kde je pozornost soustředěna na strukturu vzorce a použité proměnné parametry, které riziko ovlivňují. Téměř důsledně se rozlišuje kategorie ohrožení *T* (*Threat*) od kategorie rizika *R* (*Risk*); standardně se používá zranitelnost *V* (*Vulnerability*) a hodnota aktiva *A* (*Asset*). Namísto parametru *A* je někdy ve vzorci uplatněna veličinou závažnosti dopadu či důsledku *I* (*Impact*) anebo (*Consequence*), popř. náklady *N* (*Cost*). Rozmanitost je v referenčním vzorci komplikována subjektivní volbou operátorů, tj. násobitelů nebo sčítanců, popř. dělenců a dělitelů. Neuspořádané názory na referenční vzorec dokládá několik vybraných příkladů. Veličina *T* má ve všech vzorcích rozměr pravděpodobnosti. Míra rizika *R* je definována vzorcem $R = T \times V \times A$ podle [73], $R = T \times V \times I$ podle [37], $R = T + V + A$ podle [75], $R = T \times V \times N$ podle [29], $R = (T \times V \times N)/B$ podle [32], kde symbol *B* jsou náklady na bezpečnostní protiopatření, $R = T \times V$ podle [77]; shodný vztah uvádí stěžejní dokument OSN z roku 2005 [79), kde je však činitel *T* explicitně chápán jako nebezpečí (“hazard”). Různé modifikace rovnice rizika představují z hlediska algoritmu *„matematický nesmysl“,* jak upozornil [42]. K tomu zároveň vyvolal diskuzi se širokou odezvou na stránkách www.bloginfosec.com.

Marasmus se dále projevuje v triviální aplikaci obecně uznávaného pomocného nástroje *rizikové matice*. Škála na obou osách je zpravidla lineární v intervalu (1 až 5) a posuzovatel tím sdílí absurdní rozhodnutí, že veličina s hodnotou „5“ je pětkrát horší, než veličina s hodnotou „1“. Tímto je fatálně ignorováno současné poznání vědy včetně domácího výzkumu z roku 2005, kdy byl objasněn *význam nelineární stupnice* pro proces rizikové analýzy [69].

V současnosti patří metoda FMEA k nejpoužívanějším metodám prediktivní analýzy spolehlivosti a je využívána v řadě oborů, nejen pro analýzu technických systémů, ale také pro analýzu procesů a softwarů. Metoda je u nás popsána v normě ČSN IEC 812 – *Postup analýzy způsobů a důsledků poruch*. Aktuální informace a přehled literatury je k dosažení na webové stránce FMEA *Info Centre*[10]. Předpokladem pro vyhodnocení analýzy FMEA je určení relativní významnosti poruchy prvku nebo procesu pomocí čísla priority rizika *RPN* podle vztahu (a původní symboliky)

$$RPN = S \times O \times D \quad , \tag{3}$$

kde *RPN* je číslo priority rizika;
S … závažnost dopadu (důsledky) a následné poruchy či selhání;
O … očekávaný výskyt poruchy;
D … odhalitelnost (zjistitelnost) poruchy.

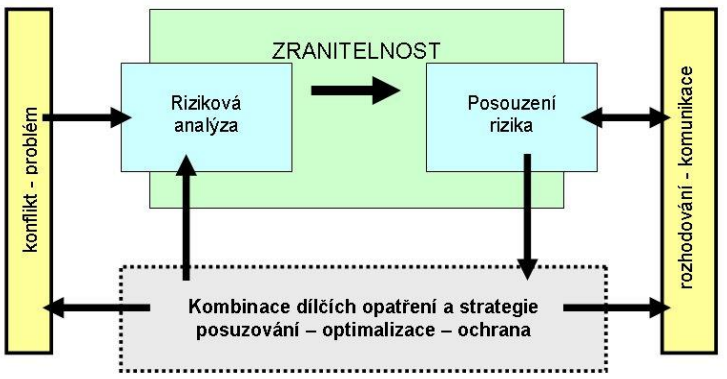
Odborná sféra od 90-tých let min. stol. upozorňuje na nevhodnou matematickou strukturu vzorce *RPN*. Podle původního konceptu vznikají problémy s interpretací numerické hodnoty tohoto ukazatele. Výhrady k *RPN* formulovala řada autorů[11]; souhrnný přehled odborné diskuze s kritickými závěry je v [61]. Ze závažných důvodů *nelze souhlasit* s používáním metody FMEA, kde je zakódován původní algoritmus pro výpočet čísla *RPN*.

Nebezpečí, ohrožení a zranitelnost

Z hlediska zranitelnosti systémů infrastruktury studie [74] zásadně rozlišuje *objektově orientované systémy* OS (object-oriented systems) a *síťově orientované systémy* NS (network-oriented systems). Nebezpečí, ohrožení a rizika pro infrastrukturu jsou zpravidla intuitivně uváděny v triviálním formátu *kontrolního seznamu* (checklistu), tj. v rámci kategorií hrozeb naturogenních (živelních), antropogenních (společenských) tj. technických a technologických, bez zdůraznění interakcí napříč jejich spektrem. Naopak sofistikovaný a obsáhlý seznam 45 kategorií potenciálních rizik (včetně vzájemných interakcí) je v dokumentu z roku 2010 [49]. Neopominutelný znalostní přehled nabízí dokument [30]. Nicméně současné metodologické znalosti o rozsahu nebezpečí či ohrožení pro infrastrukturu jsou podle [41] silně neuspořádané a nestejnorodé.

Zranitelnost (vulnerability) je bytostně komplexní entita systému, dynamická, tzn. nikoliv statická veličina (obr. 2), podrobně [59]. V měřítku času a prostoru (např. průmětu do území) určité aspekty dominují v různém časovém okamžiku a na různém místě. Vyjadřuje náchylnost ke vzniku škody (ztráty, újmy). Verbálně to je antonymum pro dva zavedené pojmy *pevnosti* (robustness) a *pružnosti* (resilience). Obecně označuje *okolnost* (condition) nebo *náchylnost* (predisposition). Aplikuje se pro jedince, skupinu, společnost, ale též např. pro stavební konstrukce a obecně pro životní prostředí. Týká se *ovlivnitelnosti* (susceptibility) a *pružnosti* v podmínkách ohrožení a nebezpečné události. Ovlivnitelnost je dána bezprostřední *blízkostí* (proximity) a *expozicí* (exposure) události mimořádného významu. Je to potenciál jednak způsobit škodu, jednak odvrátit ztrátu. Pružnost vyjadřuje přístup ke zdrojům a kapacitám, které určují schopnost obnovy po dopadu pohromy. V praxi může být systém ovlivnitelný či náchylný k napadení, ale nikoliv zranitelný. Zranitelnost lze identifikovat a upravit pomocí pro-aktivních opatření.

Úsilí *kvantifikovat zranitelnost* je soustředěno na *způsob měření* vlastností pohrom vč. připravenosti, odolnosti, společenské zranitelnosti a expozice nebezpečí. Ve všech případech se pracuje s informacemi zatíženými *neurčitostmi*. Modelový způsob řešení navrhuje [18], viz Infrastructure Vulnerability Assessment Model (I-VAM), praktické řešení pomocí softwaru nabízí [54]. V oblasti kvalitativní analýzy je kvantifikace omezena na verbálně numerickou stupnici s deskriptorem např. podle [10], viz tabulka 1.



Obr. 2
Zranitelnost představuje ústřední prvek rizikové analýzy a integrovaného rizika [59]

Tabulka 1
Verbálně numerická stupnice pro posouzení míry zranitelnosti systému metodou známkování, podle [10]

Stupeň potenciální zranitelnosti (odolnosti)	**Známka**	**Očekávaný dopad** **Důsledky selhání objektu infrastruktury**
Nejmenší možná incidence	< 0,1	Žádný, nulový. Nehrozí potenciální ztráta životů, majetku, produkce, tržby, poskytovaných služeb.
Významně nižší než průměrná incidence (velmi malá)	0,1	Umírněný, tolerovaný, zanedbatelný, krátkodobý-přerušovaný. Stupeň zranitelnosti může způsobit drobné škody na majetku, nebo drobné ztráty na produkci, tržbě a poskytovaných službách.
Trochu nižší než průměrná incidence (malá)	0,3	Slabý, tolerovaný, nezanedbatelný, krátkodobý. Stupeň zranitelnosti může způsobit zřetelné škody na majetku, na produkci, tržbě a poskytovaných službách.
Průměrná incidence	0,7	Středně silný, trvalý. Důsledky selhání jsou nepřijatelné.
Trochu vyšší než průměrná incidence (vysoká)	0,9	Vážný, kritický, dlouhodobý-trvalý. Důsledky selhání jsou nepřijatelné.
Významně vyšší než průměrná incidence (velmi vysoká)	0,95	Významný, kritický, dlouhodobý, nezvratný. Důsledky selhání jsou nepřijatelné.
Nejvyšší možná incidence	> 0,95	Katastrofální, obrovský s totální destrukcí všech poskytovaných služeb.

V oblasti kvantitativní analýzy většina prezentovaných modelů pro posuzování zranitelnosti vyjadřuje přibližně shodný algoritmus [59], [72] podle obecné rovnice

$$V = f\,(T, p\,, f, V_M)\,, \tag{4}$$

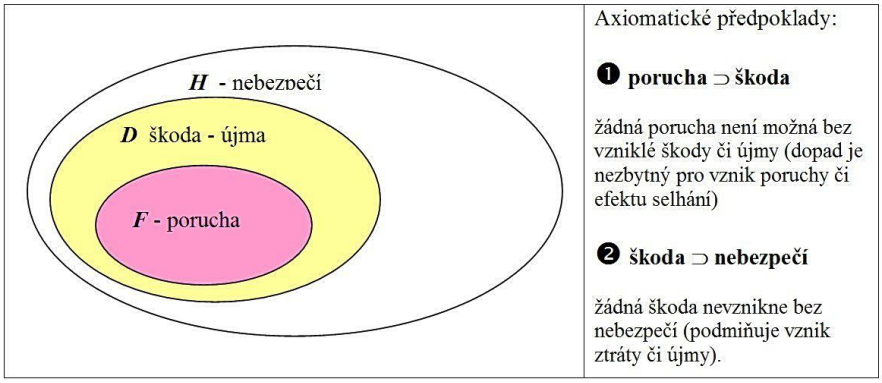
kde V je zranitelnost (vulnerability);
T … činitel ohrožení (threat);
p … pravděpodobnost výskytu scénáře ohrožení (probability);
f … četnost (frekvence) iniciující událost závažné nehody (frequences);
V_M .. zranitelnost existujících opatření (vulnerability measures).

Analytický pohled na veličinu zranitelnosti podle [1] zdůrazňuje integrovaná a nedělitelná jednota tří veličin systému, tj. škody *D*, poruchy *F* a nebezpečí *H*. Podle této studie je uvedena analýza možného dopadu a vzniku škody různého rozsahu ve struktuře systému vedoucí až k úplnému selhání systému jako následek nebezpečí[12]. Standardní matematický výraz pro *podmíněnou pravděpodobnost* výskytu analyzovaných veličin je

$$p(F \,\&\, D \,\&\, H) = p(F \,|\, D \,\&\, H) \times p(D \,|\, H) \times p(H) \quad , \tag{5}$$

kde je D … škoda, újma (damage);
F … porucha, selhání (failure);
H … nebezpečí (hazard);
p … pravděpodobnost (probability).
„|“ … označuje podmíněnou pravděpodobnost.

Jinými slovy podle [1] rovnice vyjadřuje skutečnost, že pravděpodobnost společně se vyskytujících veličin *D*, *F* a *H* se rovná pravděpodobnosti vzniku poruchy *F* pro společný výskyt *D* a *H*, násobené pravděpodobností *D* pro výskyt *H*, násobený pravděpodobností výskytu *H*.



Obr. 3
Vztah množin pro veličinu rizika R, škody D a poruchy F; podle [1]

Rovnici 5 lze zjednodušit na tvar

$$p(F \,\&\, D \,\&\, H) = p(F \mid D) \times p(D \mid H) \times p(H) \quad , \tag{6}$$

kde výraz na pravé straně rovnice

$$p(F \mid D) \times p(D \mid H) \tag{7}$$

představuje výraz pro *zranitelnost*, podrobněji [1]. Platí axiomatické předpoklady, že
(a) $F \supset D$,
(b) $D \supset H$, viz obr. 3.

Uvedená struktura obecného výrazu pro zranitelnost varuje před skutečností, že např. zranitelnost stavebních konstrukcí vykazují vysokou numerickou hodnotu členu $p(F \mid D)$ pro velmi malé hodnoty *D*; jinými slovy počáteční malá škoda v důsledku např. slabého zemětřesení nebo teroristického útoku může iniciovat postupný avšak úplný kolaps statiky konstrukce. V tomto poznatku vč. důkazu spočívá význam analytického pohledu na zranitelnost systémů ve své vnitřní podstatě. Nelze opomenout princip *celistvosti* (integrity), který vyžaduje holistické pochopení stresové analýzy, chování a únavu materiálu, mechaniky selhání a interakce jednotlivých složek systému.

Axiomy pro proces posuzování a predikci dopadu

Z hlediska operační analýzy se v posuzování infrastruktury silně projevuje *faktor nejistoty*. Přičiny nejistoty spatřuje [8] jednak v *nejasnosti* (ambiguity), jednak v *neurčitosti* (vagueness) posuzovaných jevů. Studie [28] zdůrazňuje trend nadměrně sílící nejistoty, který směřuje ke stavu *nevědomosti*. Pro *míru nejistoty* predikce dopadu studie [26] definuje čtyři různé úrovně. Typologie různých stavů nejistoty má klíčový význam pro průběh systémové

analýzy a rozhodovací proces. Při rozhodování za *jistoty* jsou známy všechny budoucí stavy (následky rozhodnutí) a tyto stavy lze jednoznačně určit. Rozhodování za *rizika* předpokládá, že jsou rovněž známy všechny následné stavy, avšak za předpokladu určité jejich pravděpodobnosti, která je známa. Při rozhodování za *nejistoty* nejsou známy následky rozhodnutí ani jejich pravděpodobnost. V tradičním pojetí je proto riziko spojeno s pravděpodobností, nejistota s neurčitostí. *Neurčitost* je svou povahou unikátní, bezprecedentní, *nelze se opřít o empirické zkušenosti*.

Axióm nenulového rizika diktuje povinnost sledovat míru nejistoty pro každý posuzovaný scénář. S určováním hodnoty rizika úzce souvisí tzv. *scénář* vzniku uvažované nepříznivé události, tedy popis typů, sledu a návazností jednotlivých fází události a jejích důsledků. Téměř vždy je možné generovat více scénářů, které umožní dosáhnout nižších hodnot rizika. Návod na sestavení úplného souboru všech relevantních scénářů nepříznivé události nelze podat, je to výlučně záležitost znalostí, zkušeností, představivosti a předvídavosti [76]. Potíže s generováním relevantních scénářů nepříznivé situace jsou znásobeny se zjišťováním výchozích (vstupních) údajů. Provozovatel tyto údaje často „utajuje", i když k havarijní situaci již dříve došlo. *Proces kritického a axiomaticky bezpečného posuzování* ASCAP charakterizuje [44]. Vždy závisí na existujících normativních axiomech a na společenských konvencích.

Současná úroveň poznání standardně nabízí *axiomatickou teorii kardinálního užitku*[13] MAUT, která umožňuje určit nejvýhodnější (pseudo-optimální) scénář pro zadaný soubor kritérií. Respektuje přijaté uzance analytického hierarchického procesu AHP [23], který v roce 1977 autorizoval L.T. SAATY [67]. Metodu párového porovnávání kritérií obohatil o subjektivní měření vzájemné „vzdálenosti" kritérií. Bez ohledu na určité výhrady se tento koncept stal zásadním přístupem pro hodnocení parametru relativní důležitosti, tj. *váhy kritéria*.

Přibližně po dobu jednoho sta let ekonomové definovali *užitek*[14] jako míru prospěchu nebo osobního štěstí jednotlivce a předpokládali možnost kvantifikace této kategorie v tzv. *utilech* (utils). Toto kardinální pojetí užitečnosti chápalo užitečnost jako psychickou realitu jednotlivců, kterou je možno kvantitativně měřit (tzv. národohospodářská škola rakouská). V třicátých letech 20. století však bylo prokázáno, že teorie užitné hodnoty nezávisí na absolutní míře, ale pouze na pořadí. Logické vyvrcholení přechodu od *kardinálního* pojetí užitečnosti k *ordinálnímu,* započaté V. PARETEM, představuje dílo J. R. HICKSE, podrobněji [65]. Z hlediska aplikace teorie užitečnosti pro rozhodovací proces v současné době je věnována pozornost poznatkům z rozvinuté teorie her, umožňující formulovat (pro konkrétní případ) *ordinální stupnici užitečnosti*. K tomuto účelu je v praxi využíván koncept komparativního posuzování rizika CRA a multikriteriální rozhodovací analýza MCDA [40]. V domácí praxi je pro významné akce dlouhodobě užívána formalizovaná metoda *Totálního ukazatele kvality prostředí*[15] TUKP [65], která umožňuje vyjádřit číselné hodnoty *souhrnné funkce užitku U*. Řešení je prováděno standardním způsobem pomocí nástrojů *operačního výzkumu (analýzy)*[16] a maticové tabulky interakcí. Podrobná informace o algoritmu metody byla uvedena v tomto časopise v roce 2013 [56].

Možnosti axiomatického posuzování doplňuje soubor dvanácti axiomů[17] pro hlubší pochopení různých systémů infrastruktury v tabulce 2.

Východiskem pro axiomatické posuzování NS je vhodná aplikace *teorie grafů* FTA. Nicméně současná úroveň poznání v problematice sítí obecně a síťové infrastruktury zvláště je na počátku rozvoje. Podle hodnocení Rady pro národní výzkum USA [50] jsou současné základní vědecké poznatky o sítích na primitivní úrovni, cit. *„…existuje obrovská mezera mezi tím, co potřebujeme vědět pro činnost společnosti a současnou primitivní úrovní našich základních znalostí"*. Základem *teorie sítí* je popis sítí, jež je hlavním předmětem topologie sítí [45]. Topologie sítí se zabývá elementy sítí – uzly a propojeními a povahou propojení mezi uzly sítě. Základními obecnými typy topologií jsou centralizované a decentralizované sítě.

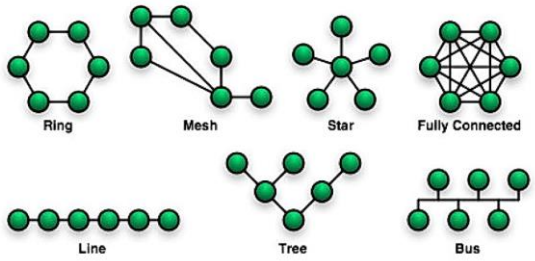
Konkrétními typy síťových topologií jsou prstencové propojení, propojení hvězdové, plně propojené, lineární propojení stromové, propojení roštové či omnibusové, viz obr. 4.

Tabulka 2
Soubor jednoho tuctu axiomů pro hlubší pochopení systémů infrastruktury se zvláštním zřetelem na topologii sítí

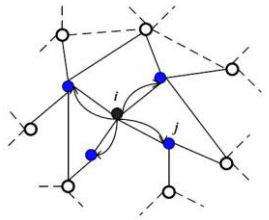
1	Systémy infrastruktury jsou komplexní sítě absolutně nezbytné pro činnost moderní společnosti.
2	Infrastruktury jsou propojené a vzájemně závislé na mnohočetné úrovni, čímž zvyšují celkovou výkonnost.
3	Existují dva odlišné typy infrastruktury: objektově orientované systémy OS a síťově orientované systémy NS.
4	Komplexní systémy infrastruktury jsou inherentní sociálně technologické systémy. Míra bezpečnosti vyplývá z jejich podstaty bez ohledu na dokonalost projektového návrhu.
5	Zcela odolná síťová infrastruktura není realizovatelná ani opodstatněná.
6	Ohrožení, riziko a zranitelnost nelze zaměňovat, nicméně ohrožení a zranitelnost jsou součástí rizika.
7	Zranitelnost infrastruktury je míra škody pro určitý ohrožený prvek vyplývající z dané hrozby a úrovně závažnosti; představuje více než technický problém. Funkční zranitelnost je zpravidla významnější než strukturální zranitelnost.
8	Fyzická ochrana[18] představuje prvek ochranného systému. Nicméně topologie NS systémů neumožňuje ochranu obvodu pomocí pasivní zábrany.
9	Posuzování zranitelnosti je proces identifikace, kvantifikace a určování pořadí zranitelnosti v systému. Zranitelnost a odolnost ovlivňují tři proměnné – škoda (újma), selhání a riziko; současně se uplatňuje podmíněná pravděpodobnost a fenomén konvoluce.
10	Spolehlivost a bezpečnost infrastruktury v síťových odvětvích je silně oslabena specifickými rizikovými faktory.
11	Existuje významný počet metodik pro posouzení rizika infrastruktur. Podrobné posouzení rizika není vhodné a je nezbytná určitá úroveň abstrakce.
12	Při rozhodování za rizika a neurčitosti je prvek subjektivity neodstranitelný (rozuměj inteligence člověka).

Pro řešení infrastruktury v síťových odvětvích má zvláštní význam tzv. *smíšená topologie* (mesh topology), ve které jsou některé uzly přímo propojeny s více než jedním dalším uzlem v síti. Pro tuto topologii neexistuje v češtině uspokojivý název. Příklad smíšené topologie sítě je uveden pod označením „mesh“. Smíšené topologii se jednoznačně přiznávají výhody, tzn. při selhání linky k uzlu, který má více připojení, lze s uzlem stále komunikovat a neexistuje centrální prvek, jehož selhání by vyřadilo celou síť. S tím souvisí koncept *redundance*, která umožňuje komunikaci i při výpadku některých linek nebo uzlů. Uzly, které jsou pro síť důležitější nebo u kterých se vyžaduje vyšší odolnost proti výpadku, se navrhují s větším počtem připojení do sítě.

Analýza systému NS se týká jednak analýzy struktury systému, jednak analýzy chování systému. Jsou to úlohy zajišťující existenci zkoumaného systému nikoliv pouhým zajištěním spolupráce mezi jeho různorodými prvky, ale dodržením zákonů systémové analýzy, které jsou analogií Kirchhoffových zákonů z elektrotechniky [11], cit.: „Systém je schopen existovat a vyvíjet se tehdy, jestliže (a) je roven nule součet všech vstupů a výstupů prvků, (b) je roven nule součet všech rozdílů mezi vstupy a výstupy pro uzavřenou zpětnou vazbu v systému.“ Na obr. 5 je znázorněno chování síťové infrastruktury při selhání uzlu [82].



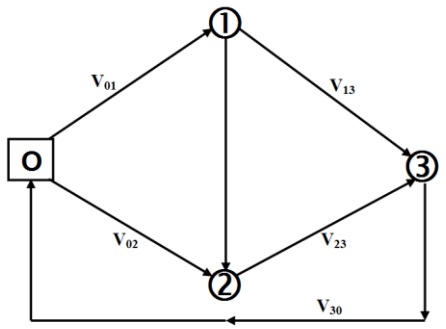
Obr. 4
Typy síťových topologií; podle [45]



Obr. 5
Vizualizace přerozdělení zátěže při selhání uzlu i; podle [82]

Např. systém na obr. 6 vyjadřuje cirkulační síť, kde prvek O značí okolí systému, jejíž vazby zobrazují toky (hmot, energie, informace) mezi prvky[19] a ohodnocení *vazeb* značí odpovídající velikosti toků. Zákony systémové analýzy vyjadřuje bilance toků:

$$v_{30} - v_{01} - v_{02} = 0$$
$$v_{01} - v_{12} - v_{13} = 0$$
$$v_{02} + v_{12} - v_{23} = 0$$
$$v_{13} + v_{23} - v_{03} = 0$$



Obr. 6
Cirkulační síť; podle [11]

V té souvislosti je diskutován pojem „preferovaného spojení“ (*preferential attachment)* v síti [13].

Modelové řešení *pravděpodobnostní odezvy* vzájemně závislých síťových infrastruktur pomocí teorie grafů nabízí [12]. Problém spočívá v analýze jednak statických topologických vlastností sítí, jednak v poznání efektů těchto vlastností v dynamické odezvě. Odezva byla modelově zjišťována pro případ ztráty různých komponentů tvořící topologii sítě pro dvě hlavní vlastnosti systému, tj. (a) odolnost sítě a (b) fragmentaci sítě. Bylo zjištěno, že odezva je silnější při odstranění uzlu v porovnání s odstraněním vazby, na kterou je síťová infrastruktura méně citlivá. Jedním z originálních výstupů této práce je koncept „*křivky křehkosti vzájemné závislosti*“ (interdependent fragility curves) síťových infrastruktur. Vhodná aplikace metamodelů (pro optimální, suboptimální a původní konfiguraci) umožňuje predikovat očekávané finanční ztráty pro různou topologii narušené sítě a parametry podmíněné pravděpodobnosti selhání (např. náklady na opravy, zmírňující opatření, nutnou redundanci).

Závěry

Kritická infrastruktura netvoří homogenní entitu, která by umožňovala triviální definici. V terminologii je třeba pěstovat jazykovou čistotu a rozlišovat obsah pojmů nebezpečí a ohrožení. Pro rizikovou analýzu jsou rozhodné dva odlišné typy infrastruktury: objektově orientované systémy OS a síťově orientované systémy NS. Zvláštní pozornost je třeba věnovat síťové infrastruktuře, na kterou působí specifická rizika a systém je bytostně silně zranitelný z hlediska odolnosti a fragmentace. Stěžejní význam síťové infrastruktury pro moderní společnost vyžaduje generovat aplikační postup (metodiku) pro navrhování a výběr preventivních opatření k odvrácení hrozeb a možných dopadů specifických rizikových faktorů; je výzvou k použití modelových přístupů. Na základě současné úrovně poznání lze doporučit semi-kvantitativní přístup. Studie představuje vytýčení směru pro další potřebné bádání. K tomu účelu byl sestaven soubor jednoho tuctu axiomatických předpokladů (tab. 2) jako doplňku pro proces DSS. Zohlednění axiomů a použití teorie grafů pomůže zlepšit dosavadní primitivní myšlení aktérů v této oblasti.

Résumé

The study addresses the gap security in the infrastructure protection relating to the vulnerabilities of network industries, as well as axioms for a deep understanding of infrastructure systems. The society of today is becoming increasingly dependent upon the service of reliable technical infrastructures. All infrastructur systems are subject, to a greater or lesser degree, to hazards. The functioning of these systems is particularly important after a major disaster and can either aid, or hinder, rescue efforts and longer term recovery plans. Multiple owners, operators, and regulators can complicate governance, preparedness, and response.

Every infrastructure-system consist of structures (individual and interconnected structures), equipment, power-supply, control systems etc. There are major differences between object-oriented systems as hospitals, police- and fire-stations, central food-storage etc. and network-oriented systems as electricity-, gas-, water-, sewer-systems. The characteristics and the individual importance of those systems vary in every country from site to site. It is easy to understand that the disfunctionality of a single element in the network-oriented systems will inevitably lead to a series of events with destructive consequences.

The complex coincidences that cause systems to fail could rarely have been foreseen by the people involved. Our understanding of the range of infrastructure risks is uneven. The very nature of terrorism creates a difficulty in predicting new and emerging threats. The special characteristics of terrorism compared with major natural hazards are in [38]. The current

protection *of network industries (civil infrastructure systems) against illegal acts through physical, mechanical and technical protection devices, is not possible as a whole. Special features of network industries reduce service reliability and security of infrastructural network-oriented systems [20].*

Vulnerability is defined as the degree of loss to a given element at risk resulting from a given hazard at a given severity level. Conventional vulnerability assessment [Fig. 2] concentrates often only on structural vulnerability (damage to the structural system), but the functional vulnerability is at least as important. Functional vulnerability usually is higher than structural vulnerability, such that functional failure precedes the structural failure.

Traditional quantitative risk analysis is considering the processes used in evaluating the probability of events and consequences, as well as studying the implementation method of estimations in the decision making process. In fact, this phase includes the identification, quantification and measurement of risks [33] and has to answer three questions – „the set of triplets": "Which are the potential negative effects?", "To what extent are they probable?" and "What are the consequences?" By answering these questions, one can evaluate, accept, avoid or manage risks.

Risk is defined in general as a relation between likelihood and consequence; conceptually, a low likelihood/high consequence event can have the same risk as a high likelihood/low consequence event. For a terrorist act, risk must consider the likelihood of a successful terrorist attack and the consequences of that attack. For a terrorist act, we will mathematically define Risk as a relation among: Threat, Vulnerability, and Consequence. In the context of (see Note 9), i denotes a specific threat scenario, j a specific facility, and k a specific type of consequence. The " ✶" operation represents convolution, since Threat, Vulnerability, and Consequence are not numbers but "likelihood" distributions. Vulnerability is defined as the likelihood of success of the threat, considering the protective measures in place; thus, Threat and Vulnerability together provide the likelihood of a successful terrorist attack. We cannot completely eliminate risk but we can increase protection and so eliminate the potential threat.

This research paper comments the drawbacks and discrepancy in the risk formula as well as in traditional FMEA method, whose theoretical framework is not still well founded. The „Risk = Threat ✕ Vulnerability ✕ Impact" formula is mathematical nonsense and should be discarded [42]. The traditional FMEA has been a well-accepted safety analysis method; however, it suffers from several drawbacks. As a result of its application, it allows "quantifying" how „dangerous" a failure mode is, and also provides a rank of risk priorities of failure modes and a list of corrective actions to remove them. In the FMEA approach, the RPN index, see Equation (7), is determined by calculating the product of the three indexes: severity (S), frequency (O) and detection (D). The most critical disadvatage of the traditional FMEA is that various set of (S), (O) and (D) may produce an identical value of RPN; however, the risk implication may be totally different.

Security risk management is a systematic and analytical process, whose role is to assess the likelihood of threat, to define measures to reduce risk, to take effective means to mitigate its potential consequences and to support key decisions in order to protect property and persons; is always contingent on existing normative axioms and social conventions.

This paper discusses the advances of axiomatic design and presents a dozen axioms for a deep understanding of infrastructure systems (see Table 2), e.g., (1) Civil infrastructure systems are complex networks that are absolutely necessary for the function of modern society, (2) Infrastructures are interconnected and interdependent at multiple levels to enhance their overall performance, (3) Object-oriented systems and network-oriented systems are two different types of infrastructures, (4) Complex infrastructure systems are inherently socio-technological systems. Therefore, they are not inherently safe, no matter how well designed, (5)

An entire resilient infrastructural network-oriented system is economically not feasible and also not reasonable, (6) Threats, vulnerabilities, and risk are not interchangeable terms although threat and vulnerability are a part of risk; Understanding the difference between threats, vulnerabilities, and risk is the first step, (7) Vulnerability is the degree of loss to a given element at risk resulting from a given hazard at a given severity level; Infrastructure vulnerability is more than an engineering issue. Functional vulnerability usually is higher than structural vulnerability, (8) The physical protection is an element of the civil defence system, Nevertheless, passive barriers for infrastructural network-oriented systems are unrealistic for topology reason (perimeter protection), (9) A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Vulnerability and resilience of the system control three variables – damage, failure and hazard as well as conditional probability and convolution phenomenon, (10) Special features of network industries reduce service reliability and security of infrastructural network-oriented systems, (11) There is a significant number of risk assessment methodologies for infrastructures. Detailed risk assessment is not applicable and a certain level of abstraction is necessary, (12) It is clearly not possible to eliminate the subjective elements from the decision-making under conditions of risk and uncertainty.

Systems are traditionally modelled using physically based models (e.g. a hydraulic model for a water distribution system), which are useful at providing scenario based information. However, due to their complexity, they can be found lacking when used to inform us of the resilience of the system and highlight structural inadequacies. To solve this problem, recent studies [13] have applied network graph theory to model the complex interactions between individual components. Infrastructure systems can be modelled using network graph theory by using nodes to represent the individual components (e.g. power stations, communities in an electrical distribution system for example) and links to model the connections between these individual components (e.g. the transmission lines), see Figures 4, 5, 6.

The network-oriented infrastructures systems need better-supported techniques for the comparison of project alternatives, e.g. a new conceptual approach and extended analytical tools. This paper suggests a new approach, using traditional network graph theory that couples with MAUT (Multi-Atribute Utility Theory) and MCDA (Multi-Criteria Decision Analysis).

POZNÁMKY:

[1] Článek vznikl na základě kritické analýzy a excerpce autorem dříve řešených grantových projektů, kontrolovaných aktuální rešerší odborné literatury. Byly využity výstupy grantu reg.č. IAA711680701 „Bezpečnostní rizika v procesu posuzování vlivu na životní prostředí“ (2007-2009), reg.č. IAA7986301 „Teoretický základ komplexních ekonomických a environmentálních problémů pro udržitelný rozvoj“ (2003-5), reg.č. GA103/98/0016 „Vliv internacionalizace EIA na metody strategického posuzování životního prostředí-SEA“ (1998-2000), reg.č. GA103/95/0070 „Metody pro posuzování vlivu na životní prostředí–EIA“ (1995-1997) a reg.č. VF20122015018 „Bezpečnost občanů – krizové řízení“ (2011-2014).

[2] RISK Index = (Negative IMPACT of risk event to objectives) × (LIKELIHOOD of occurrence)

[3] Nebezpečí a ohrožení vyjadřuje označení dvou různých stavů dynamického systému pro stejný problém. *Nebezpečí* (hazard) charakterizuje v určitých podmínkách potenciální možnost vzniku neštěstí např. v blízkosti aktivního vulkánu nebo energetického zdroje s nekvalifikovanou údržbou. Naopak *hrozba* (threat) vyjadřuje bezprostřední ohrožení např. v záplavové zóně po vzniku povodňové vlny vlivem nadměrných ovzdušných srážek nebo následkem protržení hráze nádrže.
JANOŠEC [32] upřesňuje pojem *hrozby* jako „… vždy primární, nezávisle existující, neodvozený fenomén, který chce nebo může poškodit nějakou chráněnou hodnotu. Je to vnější fenomén (činitel),

existuje nezávisle na chtění člověka. Závažnost hrozby je (přímo) úměrná povaze chráněné hodnoty a tomu, jak je tato hodnota ceněna. *Neintencionální hrozba* je jevem přírodním, kde můžeme uvést hrozbu povodní, vichřice, zemětřesení, které jsou zpravidla náhodné povahy. *Intencionální hrozba* (antropogenní) je zamýšlená. Připravuje ji, spouští a uskutečňuje jedinec jako v případě hrozby teroristické akce…".

[4] Jako vhodnější (než *management*) jsou obhajovány režimy správy založené na pluralitě rozhodování širší škály aktérů, pro něž je v anglické terminologii používán výraz „*governance*" (v překladu do češtiny „*správa*", resp. „*spravování*"), viz [30]. Případně se ke zdůraznění rozptýlené povahy rozhodování používají adjektiva jako např. „*multilevel*" governance.

[5] O přirozeném monopolu hovoříme v situaci, kdy jedna firma dokáže uspokojit poptávku s nižšími průměrnými náklady, než kdyby na trhu působilo více firem. Přirozený monopol realizuje úspory z rozsahu, což lze vyjádřit klesající křivkou průměrných nákladů.

[6] Bariéry vstupu do odvětví jsou způsobeny zejména vysokou pořizovací cenou kapitálových statků, jejich nízkou mobilitou a silou podniků, které již v odvětví působí.

[7] *Externalita je* označení pro vnější účinek nějakého ekonomického rozhodnutí, resp. činnosti, tzn. část dopadů činnosti, kterou nese někdo jiný než její původce.

[8] Veškeré metody regulace jsou založeny na tom, že regulovanému podniku musí být umožněno (nikoliv zajištěno) pokrýt své náklady a dosáhnout přiměřené návratnosti oprávněných kapitálových investic. Tento koncept se opírá o výpočet tzv. povolených výnosů (*revenue requirement* RR).
Vznikly tři základní regulační režimy [39], tj.

- regulace založená na nákladech spojených se službami (c*ost-of-service regulation*, COS),
- pobídková (stimulační) regulace (*incentive regulation; performance-based regulation*, PBR),
- regulace na základě porovnávání s konkurenčními podniky (*yardstick competition*).

Všechny tyto základní režimy regulace vycházejí ze stanovení povolených výnosů RR.

[9] Pro *riziko teroristického činu* musí být uvážena pravděpodobnost úspěšného teroristického útoku a důsledek tohoto útoku. O matematickou definici teroristického rizika se pokusil [8] pomocí vzájemného vztahu tří veličin *hrozby*, *zranitelnosti* a *důsledku*, tj.
$Teroristické\ riziko_{i,j,k} = Ohrožení_i \ \bigstar \ Zranitelnost_{i,j} \ \bigstar \ Důsledek_{i,j,k}$,
kde je i ... index scénáře ohrožení; j ... index zařízení nebo objektu; k ... index typu důsledku;
$\bigstar$ … operátor vyjadřující konvoluci .
Operátor "$\bigstar$" vyjadřuje *konvoluci*, protože ohrožení, selhání a důsledek nejsou čísla, ale pravděpodobnostní rozdělení (konvoluce je matematická operace, která kombinuje sloučením dva signály tak, aby vznikl signál třetí).
Podrobněji viz článek v tomto časopise [57].

[10] Viz <http://www.fmeainfocentre.com/>

[11] Shoda kritiky *RPN* se soustřeďuje na zjištění, že

- vzorec pro výpočet *RPN* je sporný a diskutabilní. Dva ze tří činitelů O, D mají povahu pravděpodobnosti a z formálního hlediska neexistuje důvod, aby byly vzájemně násobeny. Z tohoto důvodu model *RPN* není korektní, postrádá vnitřní konzistenci a potenciálně poskytuje nesprávné zavádějící výstupy;
- činitelé S ,O, D mají zakódovanou stejnou relativní důležitost (váhu). Při praktických aplikacích metody FMEA tento předpoklad nemá univerzální platnost;
- k deformaci přispívá shodná metrika tří odlišných činitelů, subjektivní hodnocení a nelineární charakter jednotlivých stupnic (1-10), především pro pravděpodobnost. Výsledkem mohou být scénáře s nízkou numerickou hodnotou *RPN*, avšak s vysokým stupněm rizika;
- rozdílná citlivost na malé změny jednoho činitele v závislosti na různé velikosti ostatních činitelů;
- porovnání výsledných hodnot *RPN* je zavádějící, protože použité stupnice jsou pořadové (ordinální) a nikoliv poměrové (kardinální);
- za nejslabší místo se pokládá skutečnost, že různá kombinace činitelů S ,O, D generuje stejnou numerickou hodnotu *RPN*, přičemž reálné riziko se může lišit;
- legitimnost výsledků zpochybňuje prostá úvaha pro porovnání dvou scénářů s vysokou a nízkou hodnotou činitele $S = 8$ a $S = 2$, kdy je možné obdržet shodnou číselnou hodnotu $RPN = 8$ pro případ, že $RPN(S, O, D)$ … $RPN(8, 1, 1) \leftrightarrow RPN(2, 2, 2)$.

[12] Studie [1] používá explicitně výraz „hazard", nikoliv „risk".

[13] Původní výklad *teorie užitku* poskytl *Vilfredo* PARETO (✯ 15. 7.1848, ✞ 19. 8. 1923), byl italský ekonom a sociolog, položil základy ordinalistické teorie užitku. Konstatoval, že statky nejsou na sobě navzájem nezávislé, nýbrž jsou navzájem komplementy nebo substituty. Tím není spotřebitel schopen posoudit užitečnost určitého statku jako takovou, ale pouze vždy jen v relaci s jiným statkem. Spotřebitelé pak porovnávají kombinace statků.

[14] Výraz „užitek", „užitečnost" či „míra užitku" je užíván v několika odlišných smyslech [3], tj. jako
- vlastnost objektu (statku, zdroje přírody),
- psychický stav (uspokojení),
- veličina ke stanovení preferenčního uspořádání v konkrétním rozhodovacím procesu bez věcného vymezení termínu „užitek".

[15] Reference a příklady aplikace metody TUKP: Multikriteriální posouzení scénářů Jaderné elektrárny Temelín podle protokolu z Melku [60], Státní surovinové politiky ČR [62], Rekonstrukce/modernizace dálnice D1 [63], Státní energetické koncepce ČR [66], apod.

[16] Základním východiskem systémové analýzy je *operační výzkum* (operační analýza), jehož základním charakteristickým rysem je použití konstrukce, analýzy a řešení matematických modelů při řízení operací (původně vojenských).

[17] Axiom - tvrzení, která jsou ve shodě s naší zkušeností, ovšem nelze je dokázat.

[18] Systém fyzické ochrany obsahuje čtyři stěžejní funkce: (a) detekci narušitele s využitím technických prostředků, (b) ověření poplachové informace např. pomocí kamerového systému, (c) zpomalení, (d) odezvu pomocí reakce fyzické ochrany.

[19] Existuje shoda [27] pro terminologii „systémovou“ (prvek, vazba) a terminologií „grafovou“ (uzel, hrana).

Zkratky

AD	AXIOMATIC DESIGN
AHP	ANALYTICAL HIERARCHY PROCESS
ASCAP	THE AXIOMATIC SAFETY–CRITICAL ASSESSMENT PROCESS
BIS	BUSINESS INTERRUPTION STUDY
CI	CRITICAL INFRASTRUCTURE
CII	CRITICAL INFRASTRUCTURE INTERDEPENDENCIES
CIP	CRITICAL INFRASTRUCTURE PROTECTION
COS	COST-OF-SERVICE REGULATION
CRA	COMPARATIVE RISK ASSESSMENT / POSUZOVÁNÍ SROVNÁVACÍHO RIZIKA
DHS US	US DEPARTMENT OF HOMELAND SECURITY
DoD US	US DEPARTMENTS OF DEFENSE
DSS	DECISION SUPPORT SYSTEMS
ECI	EUROPEAN CRITICAL INFRASTRUCTURE
EIA	ENVIRONMENTAL IMPACT ANALYSIS/ASSESSMENT
EK	EVROPSKÁ KOMISE
EPCIP	THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION
EU	EVROPSKÁ UNIE
FMEA	FAILURE MODE AND EFFECTS ANALYSIS
FTA	FAULT TREE ANALYSIS
GŘHZS	GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU
HSE	HEALTH AND SAFETY EXECUTIVE
IA	IMPACT ANALYSIS
IRGC	INTERNATIONAL RISK GOVERNANCE COUNCIL

KI	KRITICKÁ INFRASTRUKTURA
MAUT	MULTI-ATRIBUTE UTILITY THEORY
MCDA	MULTI-CRITERIA DECISION ANALYSIS
MU	MIMOŘÁDNÁ UDÁLOST
MVČR	MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
NI	NETWORK INFRASTRUCTURE
NRC	NATIONAL RESEARCH COUNCIL
NS	NETWORK-ORIENTED SYSTEMS
OS	OBJECT-ORIENTED SYSTEMS
PBR	PERFORMANCE-BASED REGULATION
RAM	RISK ASSESSMENT METHODOLOGY
RPN	RIKS PRIORITY NUMBER
RR	REVENUE REQUIREMENT
SEA	STRATEGIC ENVIRONMENTAL ASSESSMENT
SoS	SYSTEM OF SYSTEMS
TUC	TRADES UNION CONGRESS
TUKP	TOTÁLNÍ UKAZATEL KVALITY PROSTŘEDÍ

Literatura

[1] AGARWAL, J. and D.I. BLOCKLEY. Structural Integrity: Hazard, Vulnerability and Risk. In: *Int. J. Materials and Structural Integrity*. 2007, Vol. 1, Nos. 1/2/3, pp.117–127. Dostupné z http://www.inderscience.com/storage/f127618521043119.pdf

[2] BABINEC, F. *Management rizika*. Brno: Slezská Universita v Opavě, Ústav matematiky, 2005, 95 s. Dostupné z http://www.slu.cz/math/cz/knihovna/ucebni-texty/Analyza-rizik/Analyza-rizik-1.pdf

[3] BAŠTA, A. *Plánové rozhodovací procesy a jejich systém*. Praha: ACADEMIA, 1977, 225 s.

[4] BONBRIGHT, James C., A.L. DANIELSEN, R. D. KAMERSCHEN. *Principles of public utility rates*. Arlington: Public Utilities Reports, 1988. 700 p. ISBN 0-910325-23-5.

[5] CEC. *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels: Commission of the European Communities. 17.11.2005. COM(2005) 576 final.

[6] CLIFTON, Judith and Daniel DÍAZ-FUENTES. Evaluating EU Policies on Public Services: A Citizens´ Perspective. In: *Annals of Public and Cooperative Economics* (July 1, 2010). Vol. 81, No. 2, pp. 281–311. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597770

[7] CREW, Michael A. and David PARKER. *International handbook on economic regulation*. Cheltenham: Edward Elgar, 2006, XIV, 405 p. ISBN 18-437-6671-X.

[8] DARBY, J.L. *Estimating Terrorist Risk with Possibility Theory*. Los Alamos: Los Alamos National Laboratory, University of California. 2004. Dostupné z www.osti.gov/energycitations/servlets/purl/836683-GMGm8L/native/836683.pdf

[9] DHS. *Critical Infrastructure Sectors*. Washington D.C.: The Department of Homeland Security US, 2014. Dostupné z http://www.dhs.gov/critical-infrastructure-sectors

[10] DoD US. *Unified Facilities Criteria (UFC). DoD Security Engineering Facilities Planning Manual*. UFC 4-020-01. Washington D.C.: Departments of Defense US, 11 September 2008, 321 p. Dostupné z http://www.wbdg.org/ccb/DOD/UFC/ufc_4_020_01.pdf

[11] DUDORKIN, Jiří. *Systémové inženýrství a rozhodování*. Praha: Vydavatelství ČVUT, fakulta elektrotechnická, 164 s. ISBN 80-01-02737-6.

[12] DUEÑAS-OSORIO, Leonardo et al. *Probabilistic Response of Interdependent Infrastructure Network*. Dostupné z http://mceer.buffalo.edu/research/international_research/ancer/activities/2004/osorio_l_maec.pdf

[13] DUNN, Sarah et al. Modelling Infrastructure Systems for Resilience and Sustainability. In: *Proc. Of the International Symposium for Next Generation Infrastructure*. October 1-4, 2013, Wollongong: Newcastle University, 7 pp. Dostupné z https://blogs.ncl.ac.uk/.../Sarah-Dunn-ISNGI-Presentation-1sthalf.pptx

[14] EC. *The European Programme for Critical Infrastructure Protection* (EPCIP). MEMO/06/477. European Commission, Brussels, 12 December 2006.

[15] EK. *Pracovní dokument komise o novém přístupu k Evropskému programu na ochranu kritické infrastruktury. Budování bezpečnější Evropské kritické infrastruktury* [online]. 28. 8. 2013, SWD(2013) 318 v konečném znění. Brusel: Evropská komise, 2013. Dostupné z http://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrastruktury-european-programme-for-critical-infrastructure-protection.aspx

[16] EK. Sdělení Komise ze dne 12. prosince 2006 o *Evropském programu na ochranu kritické infrastruktury* (KOM(2006) 786 v konečném znění – Úřední věstník C 126 ze dne 7.6.2007) [online]. Brusel: Evropská komise, 2006. Dostupné z http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_cs.htm

[17] EK. *Zelená kniha o Evropském programu na ochranu kritické infrastruktury* (předložený Komisí). V Bruselu dne 17.11.2005, KOM(2005) 576 v konečném znění. Brusel: Evropská komise, 2005. Dostupné z http://krizport.firebrno.cz/

[18] EZELL, B.Ch. *Infrastructure Vulnerability Assessment Model (I-VAM)*. Fort Monroe (Virginia): The Army School System Directorate, 2005, 42 pp. Dostupné z http://create.usc.edu/assets/pdf/51834.pdf

[19] FIALA, Petr. Síťová ekonomika. In: *FCC Public*. 2014. Dostupné z http://www.odbornecasopisy.cz/index.php?id_document=30577

[20] FINGER, M. and R. KÜNNEKE. Introduction. In: *International Handbook of Network Industries. Liberalization of Infrastructures*. Edited by FINGER, M. and KÜNNEKE, R. Elgaronline, 2011. ISBN 9781847206428. Dostupné z http://www.elgaronline.com/view/9781847206428.xml

[21] GAVENDOVÁ, Hana. *Komparace ochrany kritické infrastruktury v ČR a EU*. Dipl. práce. Brno: Masarykova univerzita, Ekonomicko správní fakulta, 2009, 100 s.

[22] GIANNOPOULOS, G., R. FILIPPINI, M. SCHIMMER. *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, EUR 25286 EN. Luxembourg: Publications Office of the European Union, 2012, 70 pp. ISBN 978-92-79-23839-0. Dostupné z http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

[23] GMU. *Analytical Hierarchy Process (AHP)*. George Mason University Classweb Directories, 2008. 13 s. Dostupné z http://classweb.gmu.edu/aloerch/573-AHP.pdf

[24] HÁBA, Stanislav. *Síťová odvětví v EU: Hodnocení regulace elektroenergetiky v ČR*. Dipl. práce. Praha: Vysoká škola ekonomická v Praze, Fakulta mezinárodních vztahů, 2010, 107 s. Dostupné z http://www.vse.cz/vskp/24775_sitova_odvetvi_v%C2%A0eu

[25] HABADOVÁ, Ludmila. *Stav kritické infrastruktury v ČR*. 27. duben 2012. Dostupné z http://www.cicar.cz/article/show-article/stav-kriticke-infrastruktury-v-cr

[26] HABEGGER, B., ed. *International handbook on risk analysis and managemen*. Zurich: Center for Security Studies, ETH Zurich, 2008. Dostupné z www.crn.ethz.ch

[27] HLINĚNÝ, Petr. *Základy teorie grafů*. BRNO: Masarykova universita, Fakulta informatiky, 2010, 135 s. Dostupné z http://is.muni.cz/el/1433/podzim2010/MA010/um/Grafy-text10.pdf

[28] HSE. *Reducing Risks, Protecting People*. (Health and Safety Executive´s decision-making process.) Norwich: Health and Safety Commission UK, 2001. Dostupné z www.hse.gov.uk/risk/theory/r2p2.pdf

[29] ICHARTER. *The Risk Equation*. London: International Charter. © 1997-2012. Dostupné z http://www.icharter.org/articles/risk_equation.htmlhttp://www.icharter.org/articles/risk_equation.html

[30] IRGC. *Risk governance: Towards an integrative approach*, White paper n. 1. Ženeva: International Risk Governance Council, 2006, pp 156. Dostupné z http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf

[31] ISO 31000:2009. Risk management – Principles and Guidelines. Geneva (Switzerland), 2009, 24 p. Dostupné z http://www.iso.org/iso/catalogue_detail?csnumber=43170

[32] JANOŠEC, Josef. *Hrozba a riziko v bezpečnostní terminologii* [online]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2010. Dostupné z https://dspace.upce.cz/bitstream/10195/37995/1/Jano%C5%A1ecJ_HrozbaARiziko_2010.pdf

[33] JOHANSSON, J. *Risk and Vulnerability Analysis of Large-Scale Technical Infrastructures. Electrical Distribution Systems*. Lund: Lund University, Department of Industrial Electrical Engineering and Automation, Faculty of Engineering, 2007. Dostupné z http://www.iea.lth.se/publications/Theses/LTH-IEA-1053_rev2.pdf

[34] JONKMAN, S.N. and A. LENTZ. *Propositions for loss-of-life modelling in risk assessment*. Draft. Delft: Delft University of Technology/Technical University Munich. 2006. Dostupné z www.ifed.ethz.ch/events/Forum04/Jonkman_paper.pdf

[35] KAPLAN, Stanley and B. John GARRICK. On The Quantitative Definition of Risk. In: *Risk Analysis.* 1981, vol. 1, pp.11–27.

[36] KATZ, Michael L. and Carl SHAPIRO. Network Externalities, Competition, and Kompatibility. In: *The American Economic Review*. 1985. Vol. 75, No. 3, pp. 424-440. Dostupné z http://links.jstor.org/sici?sici=0002-8282%28198506%2975%3A3%3C424%3ANECAC%3E2.0.CO%3B2-M

[37] KOLESÁR, Ján and Martin PETRUF. Safety Management System Protection against Acts of Unlawfull Interference of Civil Airport. In: *Journal of Logistics Management*. 2012, 1(2): 6-12. Dostupné z http://article.sapub.org/10.5923.j.logistics.20120102.01.html

[38] KUNREUTHER, Howard et al. *Assessing, Managing and Financing Extreme Events: Dealing with Terrorism*. November 20, 2003. 35 pp. Dostupné z http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.6564&rep=rep1&type=pdf

[39] LESSER, Jonathan. *Fundamentals of Energy Regulation*. Vienna: Public Utilities Reports, 2007.

[40] LINKOV, I. et al. From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications [online]. In: *Environment International* 32, 2006, 1072–1093. Dostupné z http://www.sciencedirect.com/science/article/pii/S0160412006000833

[41] LITTLE, R.G. *Managing the Risk of Aging Infrastructure*. Los Angeles: The Price School of Public Policy, University of Southern Kalifornia, 2012, pp 37. Dostupné z http://irgc.org/wp-content/uploads/2012/09/R.-G.-Little_Public-Sector_-IRGC_sep12.pdf

[42] LOWDER, Jeff. *Why the "Risk = Threats x Vulnerabilities x Impact" Formula is Mathematical Nonsense*. 2010. Dostupné z http://www.bloginfosec.com/2010/08/18/decision-theory-is-the-foundation-for-information-security-risk-management/

[43] MACHEK, Ondřej a Jiří HNILICA. *Metody regulace síťových odvětví*. 2013, 9 s. Dostupné z www.ekonomikaamanagement.cz/getFile.php?fileKey...lang=cz

[44] MONFALCONE, M. E., L. M. KAUFMAN and T. C. GIRAS. Safety Assessment of a Direct Traffic Control (DTC) Train Control System using the Axiomatic Safety-Critical

Assessment Process (ASCAP). In: *Proceedings of the Reliability and Maintainability Symposium*. 2001, 352–357. New Jersey: Institute of Electri-cal and Electronics Engineers.

[45] MV ČR. *Networkingová studie*. Praha: Ministerstvo vnitra ČR, 2010, 23 s. Dostupné z http://www.eifzvip.cz/dokumenty/EIF_Networkingova%20studie_01.pdf

[46] MV GŘ HZS. *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030*. Praha: Ministerstvo vnitra – Generální ředitelství Hasičského záchranného sboru České republiky, 2013, 61 s. Dostupné z http://www.vlada.cz/assets/ppov/brs/dokumenty/Koncepce-ochrany-obyvatelstva-2020-2030_1_.pdf

[47] NEWBERY, David M. *Privatization, restructuring, and regulation of network utilities*. 3rd print. Cambridge: MIT Press, 1999. ISBN 978-026-2640-480.

[48] NEWSOME, Bruce. *Practical skills and applied knowledge in Security, defense, and risk management*. Coronado: 2015. Dostupné z http://www.brucenewsome.com/contact.html

[49] NFPA 1600. *Standard on Disaster/Emergency Management and Business Kontinuity Programs*. Quincy, Massachusetts, USA: National Fire Protection Association, 2010, 52 pp. ISBN 978-161665005-6 (PDF). Dostupné z http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf

[50] NRC. *Network Science*. Washington, DC: National Research Council, National Academy Press, 2005. Dostupné z http://www.nap.edu/catalog/11516/network-science

[51] OLŠÁKOVÁ, Alice. *Soutěžní politika a sektorová regulace*. Diplomová práce. Brno: Masarykova univerzita, Ekonomicko-správní fakulta, 2014, 77 s. Dostupné z https://is.muni.cz/th/366160/esf_m/

[52] PHILLIPS, Charles Franklin. *The regulation of public utilities: theory and practice*. Arlington: Public Utilities Reports, 1993. 1025 s. ISBN 0-910325-45-6.

[53] Rada EU. Směrnice Rady EU 2008/114/ES, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

[54] RENFROE, N.A. and J.L. SMITH. *Threat/Vulnerability Assessments and Risk Analysis*. Washington, DC: National Institute of Building Science, 2015. Dostupné z http://www.wbdg.org/resources/riskanalysis.php

[55] RINALDI, S.M., J.P. PEERENBOOM, T.K. KELLY. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. In: *IEEE Control Systems Magazine*. 2001, Vol. 21, pp. 11-25. Dostupné z http://user.it.uu.se/~bc/Art.pdf

[56] ROSA, Jaroslav a Josef ŘÍHA. Model pro zmírňování rizik a zvyšování spolehlivosti vodárenských soustav. In: *The Science for Population Protection*. 2013, Vol. 5, No. 2, p. 45–64. ISSN 1803-568X. Dostupné z www.population-protection.eu/attachments/046_vol5n2_rosa_riha.pdf

[57] ŘÍHA, Josef. Scénáře pro prevenci a zmírnění vnějšího ohrožení infrastruktury zásobování vodou. In: *The Science for Population Protection*. 2012, Vol. 4, No. 1, p. 65–81. ISSN 1803-568X. Dostupné z http://www.population-protection.eu/attachments/040_vol4n1_riha.pdf

[58] ŘÍHA, Josef. Typologické znaky kritické infrastruktury. In: *The Science for Population Protection*. 2009, Vol. 1, No. 1, p. 99–118. ISSN 1803-635X. Dostupné z http://www.population-protection.eu/

[59] ŘÍHA, Josef. Zranitelnost infrastruktury a systémů životního prostředí. In: *SPEKTRUM*. 2008, roč. 8, č. 1, s. 22–27. ISSN 1211-6920.

[60] ŘÍHA, Josef. Jaderná elektrárna Temelín a proces EIA podle Protokolu z Melku. In: *Stavební obzor*. 2001, č. 10, s. 304–310.

[61] ŘÍHA, Josef. Diskrepance spojené s číslem priority rizika RPN [online]. In: *SPEKTRUM*. 2013, roč. 13, č. 2, s. 57. ISSN 1211-6920 (print), 1804-1639 (on-line). Dostupné z file:///C:/Users/x/Downloads/Spektrum%202013-2-abstrakty%20(31).pdf

[62] ŘÍHA, Josef. Multikriteriální analýza scénářů státní surovinové politiky jako součást procesu SEA. In: *Sborník konference se zahraniční účastí „Komplexní řešení ochrany a tvorby ŽP ve městech a v průmyslových oblastech"*. Praha: ČSVTS-Společnost pro životní prostředí, Most 21.–22. 9. 1999, s. 66–71. ISBN 80-02-99859-6.
[63] ŘÍHA, Josef. Multikriteriální rozhodovací analýza scénářů rekonstrukce/modernizace D1. In: *Analýza rizik variantních řešení zvýšení kvality dopravy na dálnici D1*. Praha: Fakulta dopravní ČVUT, 2013, s. 43–46; příloha s.1–42.
[64] ŘÍHA, Josef. Odhad rizika teroristického činu. In: *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva*. 2008, roč. VII, č. 3, s. 22–26. ISSN 1213-7057.
[65] ŘÍHA, Josef. *Posuzování vlivů na životní prostředí. Metody pro předběžnou rozhodovací analýzu*. Praha: Vydavatelství ČVUT Praha (2001), 477 s. ISBN 80-01-02353-2.
[66] ŘÍHA, Josef. a kol. *Posouzení vlivu na životní prostředí ke koncepčnímu materiálu „Scénář MŽP pro aktualizaci Státní energetické koncepce ČR"*. Praha: CITYPLAN spol. s r.o. a ViP spol. s r.o. Praha, 2003. Dostupné z http://www.env.cz/AIS/web-pub.nsf/$pid/MZPLSF4246UY
[67] SAATY, L. T. Decision making with the analytic hierarchy process. In: *Int. J. Services Sciences.* 2008, Vol. 1, No. 1, pp. 83–98. Dostupné z http://colorado.edu/geography/leyk/geog_5113/readings/saaty_2008.pdf
[68] SANDIA. *Risk Assessment Methodologies* [online]. Livermore: Sandia National Laboratories Security Livermore, California. 2007. Dostupné z http://www.sandia.gov/ram/
[69] SKALICKÝ, J. a Y. ŠLECHTOVÁ. *Projektový management*. Projekt AKADEMIK 05 – Rozvojový projekt MŠMT ČR. Plzeň: FEK, Katedra managementu, inovací a projektů. 2005. Prezentace. 27 s. Dostupné z www.kip.zcu.cz/AKADEMIK06/Aka_SkaPM06.ppt
[70] Směrnice Rady 2008/114/EK z 8. prosince 2008 o určování a označování EKI a o posouzení potřeby zvýšit jejich ochranu. Úřední věstník EU, L345/75.
[71] SMITH, Patrick et al. *Network-Based Risk Assessment of the U.S. Crude Pipeline Infrastructure*. 2012. Dostupné z www.tisp.org/index.cfm?pk=download&pid=10261&id=12558
[72] SOLANO, E. *Methods for Assessing Vulnerability of Critical Infrastructure*. DURHAM, Research Triangle Park, NC: Institut for Homeland Security Solution, 2010.
[73] STEINER, František. *Případová studie analýzy rizik informační bezpečnosti*. Business Process Management. 2007. Dostupné z http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html
[74] STUDER, J.A. *Vulnerability of Infrastructure*. Zürich: STUDER ENGINEERING, 2010. Dostupné z http://www.zlg.ethz.ch/downloads/publ/publ_Bl15/Studer.pdf
[75] TAG. *Threat, vulnerability, risk – commonly mixed up terms*. Threat Analysis Group, LLC. Independent Security Consulting, 2010. Dostupné z www.threatanalysis.com/blog/?p=43
[76] TEPLÝ, Břetislav. Je analýza rizik ve stavebnictví užitečná? In: *Stavebnictví.* 2010. Dostupné z http://www.casopisstavebnictvi.cz/analyzy-trendy-bezpecnost-a-rizika-ve-vystavbe_R220
[77] TERVOOREN, Tyler. *What is Risk? This Formula Will Explain Everything*. 2013. Dostupné z http://riskology.co/everyday-risk-formula/
[78] Trades Union Congress (TUC). What is the diference between a „hazard" and a „risk"? In: *TUC Worksmart*. 2015. Dostupné z https://worksmart.org.uk/health-advice/health-and-safety/hazards-and-risks/what-difference-between-hazard-and-risk
[79] UN. *Living with Risk: A global review of disaster reduction initiatives* [online]. 2004 Version - Volume II Annexes., Geneva: UN, 2004, pp. 133. Dostupné z http://www.unisdr.org/files/657_lwr21.pdf

[80] VALÁŠEK, Jarmil. Chápání rizik. In: *The Science for Population Protection*. 2008, č. 0, s. 113–123. ISSN 1803-568X.
[81] VERNEROVÁ, Zdenka. *Pojetí kritické infrastruktury v mezinárodním srovnání*. Bakalářská práce [online]. Pardubice: Univerzita Pardubice, Fakulta ekonomicko-správní. 2011, 79 s. Dostupné z https://dspace.upce.cz/bitstream/10195/39136/1/VernerovaZ_PojetiKriticke_OS_2011.pdf
[82] WANG, Shaolin. Cascading Model of Infrastructure Networks based on Complex Network. In: *Journal of Networks.* Vol. 8, No. 6, June 2013. p. 1448–1454.